Regeringens proposition 2017/18:232

Brottsdatalag

Prop. 2017/18:232

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 19 april 2018

Stefan Löfven

Morgan Johansson
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

Regeringen föreslår att EU:s nya dataskyddsdirektiv i huvudsak genomförs genom en ny ramlag, brottsdatalagen. Syftet med den föreslagna lagen är både att skydda fysiska personers grundläggande rättigheter och friheter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Lagen ska vara generellt tillämplig inom det område som direktivet reglerar. Lagen ska även vara subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar.

Regeringen föreslår också vissa ändringar i offentlighets- och sekretesslagen, lagen om belastningsregister, lagen om misstankeregister, domstolsdatalagen och lagen om internationellt polisiärt samarbete.

Lagändringarna föreslås träda i kraft den 1 augusti 2018.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringen föreslår att riksdagen antar regeringens förslag till

1. brottsdatalag,
2. lag om ändring i lagen (1998:620) om belastningsregister,
3. lag om ändring i lagen (1998:621) om misstankeregister,
4. lag om ändring i offentlighets- och sekretesslagen (2009:400),
5. lag om ändring i domstolsdatalagen (2015:728),
6. lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete.
7. lag om ändring i lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning,
8. lag om ändring i brottsdatalagen (2018:000).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till brottsdatalag

Härigenom föreskrivs[1] följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, här benämnt dataskyddsdirektivet.

Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

4 § Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, i den ursprungliga lydelsen.

Lagen gäller inte heller i sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Avvikande bestämmelser i annan författning

5 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Definitioner

6 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Behörig myndighet	1. En myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller 2. en annan aktör som har anförtrotts myndighetsutövning för ett syfte som anges i 1, när den behandlar personuppgifter för ett sådant syfte.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen.
Dataskyddsombud	Den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter

	behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen.
Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.
Medlemsstat	En stat som är medlem i Europeiska unionen samt Island, Liechtenstein, Norge och Schweiz.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.
Registrerad	Den fysiska person som personuppgiften gäller.
Tillsynsmyndigheten	Myndighet som regeringen utser enligt dataskyddsdirektivet för att utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.
Tredjeland	En stat som inte är en medlemsstat.

Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgift som rör hälsa	Personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Rättsliga grunder

1 § Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Med en behörig myndighets uppgift avses en uppgift som framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

2 § Utöver vad som sägs i 1 § får personuppgifter behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Ändamål

3 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.

Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

4 § Innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att

1. det finns en rättslig grund enligt 1 § för den nya behandlingen, och
2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

5 § En behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Författningsenlig och korrekt behandling

6 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifternas kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Åtskillnad mellan olika slag av personuppgifter

9 § Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

10 § Så långt det är möjligt ska personuppgifter som grundar sig på fakta särskiljas från personuppgifter som grundar sig på personliga bedömningar. Om det inte framgår av sammanhanget eller på annat sätt vad uppgiften grundas på ska det tydliggöras genom en särskild upplysning.

Känsliga personuppgifter

11 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket när det är absolut nödvändigt för ändamålet med behandlingen.

12 § Biometriska uppgifter och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

13 § Personuppgifter som avses i 11 och 12 §§ (känsliga personuppgifter) får alltid behandlas med stöd av 2 §.

14 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

15 § Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

När personuppgifter lämnas ut till en behörig myndighet ska mottagaren så långt det är möjligt ges information som gör att det går att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga.

16 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

Längsta tid som personuppgifter får behandlas

17 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

18 § Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för ändamål inom denna lags tillämpningsområde, ska den personuppgiftsansvarige årligen se över behovet av att fortsätta behandla personuppgifterna.

Automatiserade beslut

19 § Om ett beslut har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne och beslutet enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet prövat på nytt av någon person.

Automatiserade beslut får inte enbart grundas på känsliga personuppgifter.

Överföring av personuppgifter till en annan medlemsstat

20 § Om det inte är särskilt föreskrivet får villkor för behandling av personuppgifter inte ställas upp i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om det inte i motsvarande fall får ställas upp samma typ av villkor i förhållande till en svensk mottagare.

Uppgiftslämnande för rättsstatistik

21 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Behandling för ändamål utanför denna lags tillämpningsområde

22 § Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

3 kap. Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

1 § Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

2 § Den personuppgiftsansvarige ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

3 § Den personuppgiftsansvarige ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

4 § Den personuppgiftsansvarige ska se till att det i automatiserade behandlingssystem som regel inte är möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

5 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

6 § Den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

7 § Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska den personuppgiftsansvarige innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Säkerheten för personuppgifter

Säkerhetsåtgärder

8 § Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Personuppgiftsincidenter

9 § Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

10 § Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten.

Underrättelseskyldigheten gäller inte om den personuppgiftsansvarige

1. har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av incidenten,
2. har säkerställt att det inte längre finns särskild risk för otillbörligt intrång i registrerades personliga integritet, eller
3. skulle behöva göra oproportionerliga ansträngningar för att underrätta alla berörda.

I fall som avses i andra stycket 3 ska allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade får nödvändig information.

11 § Den personuppgiftsansvarige får avstå från att lämna information enligt 10 § i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans rättigheter och friheter skyddas.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

Samarbete med tillsynsmyndigheten

12 § Den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.

Dataskyddsombud

13 § Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

14 § Dataskyddsombud ska
1. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge den personuppgiftsansvarige råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

15 § Den som fullgör uppgift som dataskyddsombud får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

Personuppgiftsbiträden

16 § Den personuppgiftsansvarige får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på den personuppgiftsansvariges vägnar. Innan ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behand-

lingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

17 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från den personuppgiftsansvarige.

18 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

19 § Det som sägs om den personuppgiftsansvariges skyldigheter i 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden.

Gemensamt personuppgiftsansvar

20 § Två eller flera behöriga myndigheter är gemensamt personuppgiftsansvariga om de gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen.

Den registrerade får utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Bemyndigande

21 § Regeringen får meddela föreskrifter om skyldighet att föra register över kategorier av behandling av personuppgifter och skyldighet att införa interna rutiner för anmälan av överträdelser.

4 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Den personuppgiftsansvarige ska göra följande allmänna information tillgänglig för den registrerade:

1. den personuppgiftsansvariges identitet och kontaktuppgifter,
2. dataskyddsombudets kontaktuppgifter,
3. kategorier av ändamål för behandlingen,
4. rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av uppgifterna,
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
6. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

2 § Den personuppgiftsansvarige ska i ett enskilt fall lämna följande information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter:

1. den rättsliga grunden för behandlingen,
2. kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
3. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
4. övrig nödvändig information.

Vid bedömningen av om information enligt första stycket 4 ska lämnas ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap.

3 § Den personuppgiftsansvarige ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden för behandlingen,
4. ändamålen med behandlingen,
5. mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
6. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det,
7. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
8. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

Utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

4 § Den som har varit föremål för ett sådant beslut som avses i 2 kap. 19 § har rätt att på begäran få närmare information om beslutet av den personuppgiftsansvarige.

Begränsning av rätten till information

5 § Informationsskyldigheten i 2 och 3 §§ gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans rättigheter och friheter skyddas.

Om förutsättningarna i första stycket är uppfyllda, är den personuppgiftsansvarige inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 9 eller 10 §.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantagen i första och andra styckena även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

6 § Informationsskyldigheten i 3 § gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för vetenskapliga, statistiska eller historiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

7 § Om en begäran enligt 3 § är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Av 12 § andra stycket framgår att den personuppgiftsansvarige i vissa fall får ta ut avgift i stället för att avslå begäran.

Möjligheten att begära kontroll genom tillsynsmyndigheten

8 § I 5 kap. 3 § finns bestämmelser om att en fysisk person får begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt.

Rätten till rättelse, radering och begränsning av behandlingen

9 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

10 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne, om de behandlas i strid med 2 kap. 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket. Detsamma gäller om det krävs radering för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar av bevisskäl, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

11 § Den personuppgiftsansvarige avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

12 § Information enligt 1, 2 och 4 §§ ska lämnas utan avgift. Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 3 § oftare än en gång per år, får den personuppgiftsansvarige ta ut en rimlig avgift eller avslå begäran enligt 7 § första stycket.

5 kap. Tillsyn

Tillsynsmyndighetens uppdrag

1 § Tillsynsmyndigheten ska verka både för att fysiska personers grundläggande rättigheter och friheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom denna lags tillämpningsområde.

Tillsynsmyndighetens uppgifter

2 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling,
2. handlägga klagomål från registrerade,
3. utföra kontroll enligt 3 §, och
4. på begäran bistå en tillsynsmyndighet i en annan medlemsstat.

Tillsynen ska inte omfatta behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet.

3 § Tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär en sådan kontroll ska visa att han eller hon har begärt information enligt 4 kap. 3 § eller en åtgärd enligt 4 kap. 9 eller 10 §.

Myndigheten får vägra att utföra kontrollen om begäran är orimlig eller uppenbart ogrundad.

4 § Tillsynsmyndigheten ska vid förhandssamråd enligt 3 kap. 7 § och när det i övrigt är påkallat ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

5 § Tillsynsmyndigheten har rätt att av personuppgiftsansvariga och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,

3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och

4. den hjälp och den information som behövs för tillsynen.

Förebyggande befogenheter

6 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

7 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 6 § första stycket försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,

2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,

3. förbjuda fortsatt behandling om bristen är allvarlig, eller

4. besluta om en sanktionsavgift enligt 6 kap.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Verkställighet av beslut

8 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

Samarbete med tillsynsmyndigheter i andra medlemsstater

9 § Tillsynsmyndigheten får vägra en begäran om bistånd från en tillsynsmyndighet i en annan medlemsstat endast om det skulle strida mot en lag eller en förordning att tillmötesgå den.

10 § När tillsynsmyndigheten på begäran bistår en tillsynsmyndighet i en annan medlemsstat har den de befogenheter som anges i 5–7 §§.

11 § Tillsynsmyndigheten får, om det är förenligt med svenska intressen, lämna ut en uppgift till en tillsynsmyndighet i en annan medlemsstat, även om uppgiften är sekretessbelagd enligt offentlighets- och sekretesslagen (2009:400).

12 § Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat får inte användas för något annat ändamål än det för vilket informationen begärdes.

6 kap. Administrativa sanktionsavgifter

Överträdelser som kan leda till en sanktionsavgift

1 § En sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av någon av

1. 2 kap. 1–5, 7–12 eller 14–18 §§, 19 § andra stycket eller 22 §,
2. 3 kap. 2–8 §§, eller
3. 8 kap. 1–6 §§ eller 8 §.

En sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar en sådan incident, låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

2 § En sanktionsavgift får tas ut av ett personuppgiftsbiträde vid överträdelse av 3 kap. 5, 6 eller 8 §.

En sanktionsavgift får också tas ut om ett personuppgiftsbiträde låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Hur sanktionsavgiften ska bestämmas

3 § Sanktionsavgiften ska vid överträdelser av 3 kap. 6 eller 7 § eller av bestämmelser om dokumentation av personuppgiftsincidenter bestämmas till högst 5 000 000 kronor.

Vid överträdelser av övriga bestämmelser som anges i 1 och 2 §§ ska avgiften bestämmas till högst 10 000 000 kronor.

Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlingar, ska sanktionsavgiften bestämmas efter överträdelsernas allvar. Sanktionsavgiften får aldrig överstiga maximibeloppet för den allvarligaste överträdelsen.

4 § Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas ska särskild hänsyn tas till

1. om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen, och
5. om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift.

Beslut om sanktionsavgift

6 § Tillsynsmyndigheten beslutar om sanktionsavgift.

Sanktionsavgiften tillfaller staten.

7 § En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Betalning av sanktionsavgift

8 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Bemyndigande

9 § Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt denna lag.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Överklagande

Överklagande av personuppgiftsansvariga myndigheters beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 4 kap. 9 § första stycket, radering enligt 4 kap. 10 § första stycket, eller begränsning av behandlingen enligt 4 kap. 9 § andra stycket eller 10 § andra stycket, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 4 kap. 3 §, att ta ut avgift enligt 4 kap. 12 § andra stycket eller att inte medge prövning av ett automatiserat beslut enligt 2 kap. 19 § första stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Första stycket gäller inte beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som avses i 2 och 3 §§ får inte överklagas.

8 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för överföring

1 § En behörig myndighet får överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet, och
3. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 3 §,

b) tillräckliga skyddsåtgärder enligt 4 §, eller

c) ett undantag för särskilda situationer enligt 5 §.

En behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation, ska särskilt beakta risken för att enskilda får ett försämrat skydd för sina personuppgifter.

2 § Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

Om medgivandet på grund av tidsbrist inte kan inhämtas i förväg, får personuppgifter ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller någon annan medlemsstat.

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit under de förutsättningar som anges i 1 och 2 §§. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

4 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter, under de förutsättningar som anges i 1 och 2 §§, ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade, eller
2. den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får en överföring, eller en samling av överföringar, av personuppgifter, under de förutsättningar som anges i 1 och 2 §§, göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. värna den registrerades eller någon annan fysisk persons vitala intressen, eller andra berättigade intressen som den registrerade har,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Vidareöverföring

6 § En svensk behörig myndighet får inte tillåta att sådana personuppgifter som anges i 2 § första stycket, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation, om inte någon behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras.

7 § När en svensk behörig myndighet ska ta ställning till om personuppgifter som har överförts från Sverige till en annan medlemsstat, som har överfört dem till ett tredjeland eller en internationell organisation, får vidareöverföras till ett tredjeland eller en internationell organisation, ska alla kända omständigheter som har samband med vidareöverföringen beaktas. Särskild vikt ska läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten och nivån på skyddet av personuppgifter i tredjelandet eller hos den internationella organisationen som uppgifterna ska vidareöverföras till.

Överföring till andra än behöriga myndigheter

8 § En svensk behörig myndighet får i ett enskilt fall överföra personuppgifter till någon som inte är en behörig myndighet i ett tredjeland. Personuppgifterna får överföras endast om de övriga förutsättningarna i 1 och 2 §§ är uppfyllda och om

1. det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en uppgift enligt 1 kap. 2 § som den har ansvar för,
2. den svenska myndigheten informerar den som ska ta emot personuppgifterna om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas, och
3. det skulle vara ineffektivt eller olämpligt att överföra dem till en behörig myndighet i tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs.

Första och andra styckena gäller inte en sådan annan aktör som är behörig myndighet enligt definitionen i 1 kap. 6 §.

Villkor om användningsbegränsning

9 § Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och gäller på grund av en överenskommelse med tredjelandet eller den internationella organisationen villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

10 § En svensk behörig myndighet får vid överföring av personuppgifter till ett tredjeland eller en internationell organisation i ett enskilt fall ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till den enskildes rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.

---

1. Denna lag träder i kraft den 1 augusti 2018.
2. Genom lagen upphävs lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.
3. Bestämmelsen i 3 kap. 5 § om loggning tillämpas från och med den 6 maj 2023 i fråga om automatiserade behandlingssystem som inrättats före den 6 maj 2016.
4. En sanktionsavgift enligt 6 kap. får beslutas endast för överträdelser som har skett efter ikraftträdandet.
5. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.
6. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

2.2 Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs att 1 b § lagen (1998:620) om belastningsregister[1] ska upphöra att gälla vid utgången av juli 2018.

[1] Senaste lydelse av 1 b § 2013:331.

2.3 Förslag till lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs att 1 b § lagen (1998:621) om misstankeregister[1] ska upphöra att gälla vid utgången av juli 2018.

[1] Senaste lydelse av 1 b § 2013:332.

2.4 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 9 kap. 2 § ska ha följande lydelse,

dels att det i lagen ska införas en ny paragraf, 17 kap. 7 c §, och närmast före 17 kap. 7 c § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
2 §[1]	
Bestämmelser som begränsar möjligheten att använda vissa uppgifter som en svensk myndighet har fått från en myndighet i en annan stat finns i	
1. lagen (1990:314) om ömsesidig handräckning i skatteärenden,	
2. lagen (2017:496) om internationellt polisiärt samarbete,	
3. lagen (2000:344) om Schengens informationssystem,	
4. lagen (2000:562) om internationell rättslig hjälp i brottmål,	
5. lagen (2000:1219) om internationellt tullsamarbete,	
6. lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar,	
7. lagen (2011:1537) om bistånd med indrivning av skatter och avgifter inom Europeiska unionen,	
8. lagen (1998:620) om belastningsregister,	
9. lagen (2012:843) om administrativt samarbete inom Europeiska unionen i fråga om beskattning,	
10. lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen,	
11. lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet,	*10*. lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet,
12. lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton,	*11*. lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton,
13. lagen (2017:182) om automatiskt utbyte av land-för-land-rapporter på skatteområdet, *och*	*12*. lagen (2017:182) om automatiskt utbyte av land-för-land-rapporter på skatteområdet,
14. lagen (2017:1000) om en europeisk utredningsorder.	*13*. lagen (2017:1000) om en europeisk utredningsorder, *och*
	14. brottsdatalagen (2018:000).

[1] Senaste lydelse 2017:1012.

Internationellt samarbete avseende behandling av personuppgifter

7 c §

Sekretess gäller i tillsynsmyndighetens verksamhet enligt 5 kap. brottsdatalagen (2018:000) för uppgift som, utan samband med en svensk begäran, har lämnats av en tillsynsmyndighet i en stat inom Europeiska ekonomiska samarbetsområdet (EES) eller i Schweiz, om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Denna lag träder i kraft den 1 augusti 2018.

2.5 Förslag till lag om ändring i domstolsdatalagen (2015:728)

Härigenom föreskrivs att 5 § domstolsdatalagen (2015:728) ska ha följande lydelse.

Lydelse enligt prop. 2017/18:113	*Föreslagen lydelse*
5 §	
De avvikande bestämmelser som finns i *lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen, ska tillämpas i stället för bestämmelserna i denna lag. Detsamma gäller i fråga om* Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur.	De avvikande bestämmelser som finns i Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur, *ska tillämpas i stället för bestämmelserna i denna lag*.

Denna lag träder i kraft den 1 augusti 2018.

2.6 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

Härigenom föreskrivs att 6 kap. 2 § lagen (2017:496) om internationellt polisiärt samarbete ska upphöra att gälla vid utgången av juli 2018.

2.7 Förslag till lag om ändring i lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs i fråga om lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning

dels att punkt 4 i ikraftträdande- och övergångsbestämmelserna ska upphöra att gälla,

dels att 1 kap. 4 § ska ha följande lydelse.

Lydelse enligt prop. 2017/18:105	*Föreslagen lydelse*
1 kap.	
4 §	
Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen *(1996:627)* eller föreskrifter som har meddelats i anslutning till den lagen.	Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen *(2018:000)* eller föreskrifter som har meddelats i anslutning till den lagen.

Denna lag träder i kraft den 1 april 2019 i fråga om 1 kap. 4 § och i övrigt den 1 augusti 2018.

2.8 Förslag till lag om ändring i brottsdatalagen (2018:000)

Härigenom föreskrivs att 3 kap. 9 § brottsdatalagen (2018:000) ska ha följande lydelse.

Lydelse enligt lagförslag 2.1	*Föreslagen lydelse*
3 kap.	
9 §	
Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen *(1996:627)* eller föreskrifter som har meddelats i anslutning till den lagen.	Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen *(2018:000)* eller föreskrifter som har meddelats i anslutning till den lagen.
Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet.	Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet.

Denna lag träder i kraft den 1 april 2019.

3 Ärendet och dess beredning

Europeiska unionen har enats om en genomgripande dataskyddsreform som ska vara genomförd under våren 2018. Reformen omfattar dels Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här kallad dataskyddsförordningen, dels Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, här kallat dataskyddsdirektivet. Dataskyddsdirektivet bifogas som *bilaga 1*.

Regeringen beslutade den 17 mars 2016 kommittédirektiv om genomförande av dataskyddsdirektivet (dir. 2016:21). Utredningen om 2016 års dataskyddsdirektiv redovisade den 5 april 2017 delbetänkandet Brottsdatalag (SOU 2017:29), i vilket utredningen föreslår att direktivet i huvudsak ska genomföras genom en ny ramlag, brottsdatalagen. Lagen ska gälla för myndigheters behandling av personuppgifter vid bl.a. brottsbekämpning, lagföring och straffverkställighet. Delbetänkandets lagförslag behandlas i denna proposition. En sammanfattning av delbetänkandet och dess lagförslag finns i *bilaga 2* och *3*. Delbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2017/03283/L4).

Utredningens slutbetänkande redovisades den 4 oktober 2017 (SOU 2017:74). I detta föreslås de anpassningar som krävs i rättsväsendets centrala registerförfattningar. Det föreslås också vissa ändringar i den föreslagna brottsdatalagen och följdändringar med anledning av det i delbetänkandet lämnade förslaget att lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) ska upphävas. Lagförslagen som rör brottsdatalagen och 2013 års lag behandlas i denna proposition. Slutbetänkandets övriga lagförslag kommer att tas om hand i två kommande propositioner. En sammanfattning av slutbetänkandet och dess lagförslag som behandlas i denna proposition finns i *bilaga 5* och *6*. Slutbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 7*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2017/07698/L4). Utredningens uppdrag innefattar inte vilken myndighet som ska utses till tillsynsmyndighet eller hur tillsynsverksamheten ska organiseras.

Regeringen beslutade den 22 december 2014 att tillkalla en särskild utredare med uppdrag att överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet (dir. 2014:164). Genom tilläggsdirektiv den 17 december 2015 beslutade regeringen om förlängd utredningstid (dir. 2015:139). Utredningen (Ju 2015:02) redovisade sitt uppdrag i betänkandet Ett samlat ansvar för

tillsyn över den personliga integriteten (SOU 2016:65). Betänkandet innehåller bl.a. en kartläggning över vilken tillsyn över behandling av personuppgifter som bedrivs i dag och överväganden om den i större utsträckning kan samlas hos en myndighet. Det behandlar också frågor om vilken eller vilka myndigheter som bör vara tillsynsmyndighet enligt dataskyddsförordningen respektive dataskyddsdirektivet och som ska representera Sverige i Europeiska dataskyddsstyrelsen. Även frågor om hur företrädare för tillsynsmyndigheten ska utses och hur verksamheten ska organiseras behandlas i betänkandet. I denna proposition behandlas de delar av betänkandet som är nödvändiga för genomförandet av dataskyddsdirektivet. En sammanfattning av betänkandet och dess lagförslag finns i *bilaga 8* och *9*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 10*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2016/06793/Å).

Lagrådet

Regeringen beslutade den 1 mars 2018 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 11*. Lagrådets yttrande finns i *bilaga 12*. Lagrådets synpunkter och förslag behandlas i avsnitt 6.1.3, 6.4.4, 6.6, 7.6.4, 8.1.3, 8.1.4, 10.2.7, 11.3.1, 12.6.2, 12.7.2 och 15.2.3 samt i författningskommentaren. I förhållande till lagrådsremissens lagförslag har vissa språkliga och redaktionella ändringar gjorts. Vidare har, efter förslag från Lagrådet, de bestämmelser som upplyser om regeringens föreskriftsrätt tagits bort.

4 Dagens reglering och reformer på dataskyddsområdet

4.1 Huvuddragen i dagens personuppgiftsreglering

4.1.1 Regeringsformen och Europakonventionen

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en – utöver vad som anges i första stycket i paragrafen – skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Grundlagsskyddet omfattar enbart betydande intrång. I förarbetena till ändringen framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses det allmännas hantering av uppgifterna normalt vara. Även hantering av ett litet fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor

vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget (prop. 2009/10:80, s. 183). Konstitutionsutskottet har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållit att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll ska regleras särskilt i lag (se bl.a. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 43).

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som svensk lag (SFS 1994:1219). Enligt artikel 8 har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i dessa rättigheter får endast göras med stöd av lag och för vissa i artikeln uppräknade ändamål, bl.a. hänsyn till den allmänna säkerheten och förebyggande av oordning och brott. Artikel 8 skyddar bl.a. mot felaktig behandling av personuppgifter (se Segerstedt-Wiberg m.fl. mot Sverige, Ansökan 62332/00).

Även Europeiska unionens (EU) stadga om de grundläggande rättigheterna (rättighetsstadgan) innehåller bestämmelser om behandling av personuppgifter (se avsnitt 4.7.1).

4.1.2 Personuppgiftslagen

Grundläggande begrepp

Genom datalagen (1973:289) introducerades termen personregister som ett centralt begrepp i svensk lagstiftning om behandling av personuppgifter. Med personregister avsågs register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. Genom datalagen blev termen register den allmänt använda termen för datoriserade uppgiftssamlingar. Termen register används fortfarande i vissa författningar.

Det traditionella registerbegreppet kom med tiden att kritiseras bl.a. därför att det har en teknisk anknytning och för tankarna till på visst sätt organiserade eller systematiserade samlingar av uppgifter. I personuppgiftslagen (1998:204) nämns inte register utan det talas i stället om behandling av personuppgifter, vilket numera är det gängse begreppet. Den vars personuppgifter behandlas benämns dock alltjämt den registrerade.

Lagens tillämpningsområde

Genom personuppgiftslagen genomfördes Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, här kallat 1995 års dataskyddsdirektiv. Lagen innehåller generella regler för all behandling av personuppgifter. Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Begreppet behandling av

personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, t.ex. att samla in, söka, bevara eller sprida uppgifter.

Lagen ska enligt 5 § tillämpas på helt eller delvis automatiserad behandling av personuppgifter. Dessutom är den tillämplig på manuell behandling av personuppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen reglerar även sådan verksamhet som faller utanför unionsrätten. Enligt 2 § gäller särreglering i lag eller förordning framför bestämmelserna i personuppgiftslagen. Sådan särreglering finns framför allt i olika registerförfattningar.

Behandling av uppgifter om juridiska personer (som definitionsmässigt inte utgör personuppgifter) omfattas inte av personuppgiftslagen.

Grundläggande krav för behandlingen

I 9 § personuppgiftslagen slås fast vissa grundläggande krav för behandling av personuppgifter. Sådana uppgifter ska alltid behandlas lagligt, på ett korrekt sätt och i enlighet med god sed. Personuppgifter ska samlas in och behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Efter insamlingen får uppgifterna inte behandlas för något annat ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in (den s.k. finalitetsprincipen). De personuppgifter som behandlas ska vidare vara adekvata och relevanta i förhållande till ändamålen med behandlingen och får inte heller vara fler än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Om det är nödvändigt ska uppgifterna vara aktuella. Om personuppgifterna är felaktiga eller ofullständiga, ska den personuppgiftsansvarige vidta alla rimliga åtgärder för att utplåna, blockera eller rätta uppgifterna.

Personuppgifter får inte sparas längre än nödvändigt med hänsyn till de ändamål för vilka de behandlas.

Tillåten och otillåten behandling

I 10–12 §§ finns en uttömmande uppräkning av de fall där behandling av personuppgifter är tillåten. Personuppgifter får alltid behandlas om den registrerade har gett sitt samtycke. Återkallar personen sitt samtycke får ytterligare personuppgifter om honom eller henne inte behandlas.

I vissa fall får personuppgifter behandlas även om den registrerade inte har gett sitt samtycke. En förutsättning i dessa fall är att behandlingen är nödvändig för ändamålen.

Personuppgifter får behandlas i samband med ett avtal med den registrerade, när det behövs för att fullgöra avtalet eller när det behövs för att på den registrerades begäran vidta åtgärder innan avtalet träffas. Vidare får behandling utföras om den är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet. Dessutom får personuppgifter behandlas för att skydda vitala intressen för den registrerade. Likaså får personuppgifter behandlas om det är nödvändigt för att den personuppgiftsansvarige, eller en tredje man till vilken personuppgifter lämnas ut, ska kunna utföra en arbetsuppgift i samband med myndighetsutövning. Slutligen får personuppgifter behandlas om en avvägning ger

vid handen att den personuppgiftsansvariges berättigade intresse av behandling väger tyngre än den registrerades intresse av skydd.

Behandling av känsliga personuppgifter

I 13 § personuppgiftslagen förbjuds behandling av känsliga personuppgifter. Med det avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och uppgifter som rör hälsa eller sexualliv.

Förbudet mot behandling av känsliga personuppgifter är inte undantagslöst. I 14–19 §§ anges under vilka förutsättningar sådana uppgifter får behandlas. Om den registrerade har gett sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort de känsliga uppgifterna får de enligt 15 § behandlas. Vidare görs i 16 § undantag för nödvändig behandling, bl.a. för att den personuppgiftsansvarige ska kunna fullgöra skyldigheter eller utöva rättigheter inom arbetsrätten, för att den registrerades eller annans vitala intressen ska kunna skyddas i fall där den registrerade inte kan lämna samtycke till behandlingen eller för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras.

Undantag görs också i 17 § för ideella organisationer med politiskt, filosofiskt, religiöst eller fackligt syfte, som får behandla uppgifter om bl.a. sina medlemmar.

Likaså finns det undantag i 18 § för behandlingen av känsliga personuppgifter för hälso- och sjukvårdsändamål och i 19 § för forskning och statistik. Regeringen, eller den myndighet regeringen bestämmer, får enligt 20 § föreskriva ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse.

Uppgifter om brott och behandling av personnummer

Det är enligt 21 § personuppgiftslagen förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Sådana uppgifter får dock behandlas för forskningsändamål om behandlingen godkänts vid etikprövning. Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare undantag från förbudet. Likaså kan i enskilda fall undantag medges.

Uppgifter om personnummer och samordningsnummer får enligt 22 § behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Automatiserade beslut

Enligt 29 § personuppgiftslagen ska, om ett beslut som har rättsliga följder för en fysisk person eller annars har märkbara verkningar för honom eller henne och beslutet grundas enbart på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma egenskaper hos personen, den som berörs av beslutet ha möjlighet att på begäran få beslutet omprövat av någon person.

Information till den registrerade

Personuppgiftslagen innehåller ett flertal bestämmelser som syftar till att genom information trygga den enskildes rätt att kontrollera om hans eller hennes personuppgifter behandlas. Den personuppgiftsansvariges skyldighet att självmant lämna information till registrerade gäller enligt 23 § i första hand uppgifter som den registrerade själv har lämnat. Har uppgifterna samlats in från annan källa, föreskrivs i 24 § att den personuppgiftsansvarige självmant ska informera den registrerade när uppgifterna registreras, eller om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången. Information behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet av uppgifterna i lag eller annan författning. Information behöver heller inte lämnas om det skulle vara omöjligt eller kräva en oproportionerligt stor arbetsinsats.

Informationen ska enligt 25 § omfatta uppgift om vem som är personuppgiftsansvarig, ändamålen med behandlingen och all övrig information som den registrerade behöver för att kunna ta till vara sina rättigheter i samband med behandlingen. Informationsskyldigheten omfattar bara sådana uppgifter som den registrerade inte redan känner till.

Den personuppgiftsansvarige är vidare enligt 26 § skyldig att på ansökan, en gång per år, gratis informera om uppgifter om sökanden behandlas, ändamålen med behandlingen, vilka uppgifter som behandlas, varifrån dessa kommer och till vem de lämnas ut. Någon information behöver dock inte lämnas om personuppgifter som endast behandlas i löpande text som ännu inte fått sin slutliga utformning eller utgör minnesanteckning, utom i de fall där uppgifterna har lämnats ut till tredje man eller – i fråga om behandling i löpande text – har behandlats längre än ett år.

Informationsskyldigheten gäller enligt 27 § inte heller om uppgifterna omfattas av sekretess eller tystnadsplikt.

Rättelse

Personuppgifter som har behandlats i strid med personuppgiftslagen eller föreskrifter som har meddelats med stöd av den, ska enligt 28 § på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgiftsansvarige. Om felaktiga personuppgifter har lämnats ut till tredje man, ska denne i vissa fall informeras om korrigeringen.

Säkerheten vid behandling

I 30 och 31 §§ personuppgiftslagen finns allmänna bestämmelser om säkerheten vid behandling av personuppgifter. Bestämmelserna avser att trygga både den tekniska säkerheten och att de personer som behandlar personuppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige ansvarar för säkerheten.

Överföring av personuppgifter till tredjeland

Enligt 33 § personuppgiftslagen är det förbjudet att till tredjeland föra över personuppgifter under behandling om landet i fråga inte har en adekvat nivå för skyddet av personuppgifter. Förbudet gäller också överfö-

ring av personuppgifter för behandling i tredjeland. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. I paragrafen anges vilka omständigheter som ska tillmätas särskild vikt.

I 34 § anges vissa undantag från förbudet i 33 §. Ett viktigt undantag är att det är tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk behandling av personuppgifter (i fortsättningen dataskyddskonventionen). Enligt 35 § personuppgiftslagen har regeringen möjlighet att besluta om ytterligare undantag från förbudet i 33 §. I bilagor till personuppgiftsförordningen (1998:1191) anges vilka stater som enligt beslut av Europeiska kommissionen (i fortsättningen kommissionen) anses ha en adekvat skyddsnivå för behandlingen av personuppgifter vid överföring till vissa i besluten specificerade mottagare.

Tillsyn

Datainspektionen är enligt 2 § personuppgiftsförordningen tillsynsmyndighet enligt personuppgiftslagen. Datainspektionen är som regel också tillsynsmyndighet för sådan behandling av personuppgifter som regleras i särskilda registerförfattningar. Inspektionen har bl.a. till uppgift att verka för att människor skyddas mot att den personliga integriteten kränks genom behandling av personuppgifter. Datainspektionen informerar bl.a. om gällande regler, utövar tillsyn över att reglerna efterlevs och ger råd och hjälp åt personuppgiftsombud. I 43–47 §§ personuppgiftslagen regleras tillsynsmyndighetens befogenheter, t.ex. rätten att meddela vite och möjligheten att förbjuda viss behandling.

Sanktioner

Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada och kränkning av den personliga integriteten för den registrerade, har han eller hon enligt 48 § personuppgiftslagen rätt till skadestånd från den personuppgiftsansvarige. Ersättningsrätten omfattar både personskada, sakskada och ren förmögenhetsskada som kränkningen av den personliga integriteten kan ha medfört. Skadeståndsansvaret är i princip strikt. Den registrerade behöver bara visa att det förekommit en felaktig behandling och att den skadat eller kränkt honom eller henne.

En straffbestämmelse finns i 49 §. Till böter eller fängelse i högst sex månader döms bl.a. den som behandlar personuppgifter i strid med bestämmelserna om behandling av känsliga personuppgifter eller för över personuppgifter till tredjeland i strid med bestämmelserna i 33–35 §§. I ringa fall döms inte till ansvar. Vidare får ansvar inte utkrävas för en gärning som omfattas av ett vitesföreläggande enligt lagen.

4.1.3 Personuppgiftslagens förhållande till annan lagstiftning

I 2 § personuppgiftslagen föreskrivs, som nyss nämnts, att om det i en annan lag eller en förordning finns bestämmelser som avviker från lagen ska de bestämmelserna gälla. Sådan särreglering finns för de flesta av de

verksamhetsområden som berörs av det nya dataskyddsdirektivet, vilket redovisas närmare i det följande. Regleringen har, av de skäl som anges i avsnitt 4.1.1, normalt lagform.

Författningar som reglerar personuppgiftsbehandling är ofta konstruerade så att de gäller utöver personuppgiftslagen. Det innebär att författningarna i fråga bara innehåller de bestämmelser som avviker från olika bestämmelser i personuppgiftslagen. Inom det nya direktivets tillämpningsområde är lagen (2001:617) om behandling av personuppgifter inom kriminalvården ett exempel på det.

Det finns emellertid även författningar som gäller i stället för personuppgiftslagen. Det innebär att de i sin helhet ersätter personuppgiftslagen inom sitt tillämpningsområde. I vissa av dessa anges genom hänvisningar vilka bestämmelser i personuppgiftslagen som ändå ska tillämpas. Den lagstiftningstekniken används inom det nya direktivets tillämpningsområde för flertalet av de centrala författningarna. Det gäller t.ex. polisdatalagen (2010:361), kustbevakningsdatalagen (2012:145) och åklagardatalagen (2015:433).

4.2 Särregler för brottsbekämpande verksamhet

4.2.1 Polisen

Allmänt om polisdatalagen

Polisdatalagen är generellt utformad och gäller i polisens brottsbekämpande verksamhet. Det finns dock även andra författningar som reglerar personuppgiftsbehandling i polisens brottsbekämpande verksamhet, framför allt lagstiftning som reglerar behandling i särskilda register. I 1 kap. 3 § polisdatalagen undantas från lagens tillämpningsområde behandling av personuppgifter enligt vapenlagen (1996:67), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister och lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. Eftersom det, med undantag för den sistnämnda lagen, inte har ingått i utredningens uppdrag att se över de författningar som undantas från polisdatalagens tillämpningsområde berörs de inte vidare här.

Lagens tillämpningsområde

Polisdatalagen gäller vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen och i Ekobrottsmyndighetens polisiära verksamhet, med undantag för behandling i de register som anges i 1 kap. 3 §. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Lagen tillämpas enligt 1 kap. 6 § även i viss utsträckning på behandling av uppgifter om juridiska personer.

I annan verksamhet än den brottsbekämpande tillämpar Polismyndigheten personuppgiftslagen, om det inte finns en specialreglering. Myndigheten tillämpar t.ex. utlänningsdatalagen (2016:27) i verksamhet som

den bedriver enligt utlännings- och medborgarskapslagstiftningen, om det inte är fråga om brottsbekämpning.

Förhållandet till personuppgiftslagen

Polisdatalagen gäller enligt 2 kap. 1 § i stället för personuppgiftslagen. I 2 kap. 2 § hänvisas dock till ett betydande antal bestämmelser i personuppgiftslagen som ska tillämpas vid behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd.

Ändamål för behandling och utlämnande av uppgifter

I 2 kap. polisdatalagen anges för vilka ändamål personuppgifter får behandlas. Ändamålen delas in i primära och sekundära ändamål. De primära ändamålen avser behandling av personuppgifter för att tillgodose de behov som finns i polisens brottsbekämpande verksamhet. Dessa ändamål är uttömmande angivna i 2 kap. 7 § polisdatalagen. Personuppgifter får enligt denna paragraf behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden.

De sekundära ändamålen aktualiseras när personuppgifter som behandlas i polisens brottsbekämpande verksamhet lämnas ut till andra myndigheter eller organisationer för deras behov eller till andra delar av polisverksamheten. Enligt de sekundära ändamålen, som anges i 2 kap. 8 § polisdatalagen, får personuppgifter behandlas genom sådant utlämnande när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket eller hos utländsk myndighet eller mellanfolklig organisation. Personuppgiftsbehandling genom utlämnande är också tillåtet om den är nödvändig för att tillhandahålla information som behövs i Polismyndighetens handräckningsverksamhet eller, om det finns särskilda skäl, att tillhandahålla informationen i annan verksamhet som myndigheten ansvarar för. Likaså får personuppgifter i ett enskilt fall behandlas för att lämnas ut för vissa andra i paragrafen specificerade ändamål eller för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Personuppgifter får enligt 2 kap. 9 § också behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Polismyndigheten eller Ekobrottsmyndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 15 § finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol och Europol, utländsk underrättelse- eller säkerhetstjänst och annan utländsk myndighet eller mellanfolklig organisation. Sekretessbrytande bestämmelser som gäller i förhållande till Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket finns i 2 kap. 16–18 §§ polisdatalagen.

Behandling av känsliga personuppgifter

Behandling av känsliga personuppgifter regleras i 2 kap. 10 § polisdatalagen. Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter om det är absolut nödvändigt för syftet med behandlingen.

Register som regleras särskilt i polisdatalagen

Några register regleras särskilt i 4 kap. polisdatalagen. Dessa är register över dna-profiler, dvs. dna-registret, utredningsregistret och spårregistret, fingeravtrycks- och signalementsregister, penningtvättsregister och det internationella registret. För dessa register finns särskilda bestämmelser om ändamål, gallring och direktåtkomst.

Behandling av personuppgifter för forensiska ändamål

I 5 kap. polisdatalagen finns bestämmelser om personuppgiftsbehandling vid Polismyndigheten för forensiska ändamål. Där regleras framför allt ändamålen med sådan personuppgiftsbehandling som avviker från regleringen i övrigt i lagen, på grund av att avdelningen Nationellt forensiskt centrum har en särskild roll som expertmyndighet åt hela rättsväsendet. Kapitlet innehåller även särskilda bestämmelser om bevarande och gallring. När det gäller behandling av känsliga personuppgifter, utlämnande av personuppgifter och uppgiftsskyldighet gäller i huvudsak samma bestämmelser som för Polismyndigheten.

Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet

I 6 kap. polisdatalagen finns bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Där regleras framför allt ändamålen för Säkerhetspolisens personuppgiftsbehandling, som delvis avviker från regleringen för Polismyndigheten. Det finns även särskilda bestämmelser om bevarande och gallring. När det gäller utlämnande av personuppgifter och uppgiftsskyldighet gäller i huvudsak samma bestämmelser som för Polismyndigheten.

4.2.2 Tullverket

Lagens tillämpningsområde

Tullbrottsdatalagen (2017:447), som har utformats i nära anslutning till polisdatalagen, kustbevakningsdatalagen och åklagardatalagen, reglerar all behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Lagen gäller enligt 1 kap. 2 § endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Lagen tillämpas enligt 1 kap. 4 § i viss utsträckning även på behandling av uppgifter om juridiska personer.

Förhållandet till personuppgiftslagen

Lagen gäller i stället för personuppgiftslagen, men hänvisningar görs i 2 kap. 2 § till vissa bestämmelser i personuppgiftslagen som ändå ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd.

Ändamål för behandling och utlämnande av uppgifter

De ändamål för vilka personuppgifter får behandlas i Tullverkets brottsbekämpande verksamhet är uppdelade i primära och sekundära ändamål. Personuppgifter får enligt 2 kap. 5 § behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, för att utreda eller beivra brott eller för att fullgöra förpliktelser som följer av internationella åtaganden. Personuppgifter som behandlas enligt den paragrafen får enligt 2 kap. 6 § också behandlas för vissa sekundära ändamål. Sådan behandling får ske när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket eller en utländsk myndighet eller mellanfolklig organisation. Personuppgiftsbehandling genom utlämnande är enligt samma paragraf också tillåten om den är nödvändig för att tillhandahålla information som behövs i verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten och i annan verksamhet som Tullverket ansvarar för, om det finns särskilda skäl för att tillhandahålla informationen. Likaså får personuppgifter i ett enskilt fall behandlas för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen). Särskilda regler finns för behandling av vissa personuppgifter från transportföretag.

Personuppgifter får enligt 2 kap. 7 § också behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Tullverket i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 12 § finns en sekretessbrytande bestämmelse som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol och Europol, polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol och tullmyndighet eller kustbevakning inom Europeiska ekonomiska samarbetsområdet (EES). En sekretessbrytande bestämmelse som gäller i förhållande till Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket finns i 2 kap. 13 §.

Behandling av känsliga personuppgifter

Känsliga personuppgifter, dvs. uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv, får enligt 2 kap. 10 § inte behandlas enbart på grund av vad som är känt om en persons sådana förhållanden. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med känsliga personuppgifter när det är absolut nödvändigt för syftet med behandlingen.

4.2.3 Kustbevakningen

Allmänt om kustbevakningsdatalagen

För Kustbevakningens behandling av personuppgifter gäller kustbevakningsdatalagen. Lagen reglerar i princip all behandling av personuppgifter i Kustbevakningens operativa verksamhet. I 3 och 4 kap. regleras behandling av personuppgifter i Kustbevakningens brottsbekämpande verksamhet och i 5 kap. behandling av personuppgifter i annan operativ verksamhet som Kustbevakningen bedriver. Behandling för de ändamål som anges i 5 kap. ligger i allt väsentligt utanför direktivets tillämpningsområde och berörs därför inte vidare här. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Förhållandet till personuppgiftslagen

Kustbevakningsdatalagen gäller enligt 2 kap. 1 § i stället för personuppgiftslagen, men i 2 kap. 2 § finns hänvisningar till vissa bestämmelser i personuppgiftslagen som ändå ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd.

Ändamålen för behandling och utlämnande av uppgifter

Kustbevakningsdatalagen är uppbyggd på i princip samma sätt som polisdatalagen. De ändamål för vilka personuppgifter får behandlas är indelade i primära och sekundära ändamål. De primära ändamålen avser behandling av personuppgifter för att tillgodose de behov som finns inom Kustbevakningen.

De primära ändamålen för den brottsbekämpande verksamheten anges uttömmande i 3 kap. 2 § lagen. Enligt den paragrafen får personuppgifter behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra förpliktelser som följer av internationella åtaganden.

Personuppgifter som behandlas i Kustbevakningens brottsbekämpande verksamhet får enligt 3 kap. 3 § också behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Skatteverket eller utländsk myndighet eller mellanfolklig organisation. Personuppgifter får även behandlas om det är behövs för att tillhandahålla information som behövs i annan verksamhet hos Kustbevakningen för utredning och beslut i ärenden som rör vattenföroreningsavgift eller tillsyn och kontroll enligt lag eller förordning. Personuppgifter får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i en annan myndighets verksamhet, om Kustbevakningen enligt lag eller förordning är skyldig att bistå myndigheten med viss uppgift eller om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott. Likaså får personuppgifter i ett enskilt fall behandlas för att lämnas ut för vissa andra i paragrafen specificerade ändamål eller för något annat ända-

mål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Personuppgifter får enligt 2 kap. 6 § också behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Kustbevakningen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 3 kap. 6 § regleras i vilka fall personuppgifter får lämnas till Interpol och Europol, polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol eller utländsk kustbevaknings- eller tullmyndighet inom EES. Personuppgifter får lämnas ut till dem om det är förenligt med svenska intressen och det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott. Uppgifter får vidare lämnas ut till utländsk myndighet eller mellanfolklig organisation om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande. I 3 kap. 7 § anges under vilka förutsättningar personuppgifter som omfattas av sekretess får lämnas ut till Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Skatteverket.

Behandling av känsliga personuppgifter

I 2 kap. 7 § kustbevakningsdatalagen regleras behandling av känsliga personuppgifter. Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter om det är absolut nödvändigt för syftet med behandlingen.

4.2.4 Skatteverket

Lagens tillämpningsområde

Skattebrottsdatalagen (2017:452), som har utformats i nära anslutning till polisdatalagen, kustbevakningsdatalagen och åklagardatalagen, reglerar all behandling av personuppgifter i Skatteverkets brottsbekämpande verksamhet. Skatteverkets brottsbekämpande verksamhet avser i första hand sådana brott som anges i 1 § lagen (1997:1024) om Skatteverkets brottsbekämpande verksamhet, bl.a. brott mot skattebrottslagen (1971:69) och lagen (2014:836) om näringsförbud. Skatteverket får enligt den paragrafen medverka vid förundersökning i fråga om andra brott, om åklagaren finner särskilda skäl för det. Tillämpningsområdet omfattar även sådana brott.

Skattebrottsdatalagen gäller enligt 1 kap. 2 § endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Lagen tillämpas enligt 1 kap. 4 § i viss utsträckning även på behandling av uppgifter om juridiska personer.

Förhållandet till personuppgiftslagen

Lagen gäller i stället för personuppgiftslagen, men hänvisningar görs i 2 kap. 2 § till vissa bestämmelser i personuppgiftslagen som ändå ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter, information till den registrerade, tillsyn och skadestånd.

Ändamålen för behandling och utlämnande av uppgifter

De ändamål för vilka personuppgifter får behandlas i Skatteverkets brottsbekämpande verksamhet är uppdelade i primära och sekundära ändamål. Personuppgifter får enligt 2 kap. 5 § behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, för att utreda brott eller för att fullgöra förpliktelser som följer av internationella åtaganden. Personuppgifter som behandlas enligt den paragrafen får enligt 2 kap. 6 § också behandlas för vissa sekundära ändamål. Sådan behandling får ske när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen eller en utländsk myndighet eller mellanfolklig organisation. Personuppgiftsbehandling genom utlämnande är enligt samma paragraf också tillåten bl.a. när det är nödvändigt för att tillhandahålla information som behövs i annan verksamhet som Skatteverket ansvarar för, om det kan antas att informationen behövs i ett ärende i den verksamheten. Personuppgifter får i ett enskilt fall behandlas även för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Personuppgifter får enligt 2 kap. 7 § också behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Skatteverket i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 11 och 12 §§ finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till svenska brottsbekämpande myndigheter och till en utländsk myndighet eller mellanfolklig organisation.

Behandling av känsliga personuppgifter

Känsliga personuppgifter, dvs. uppgifter som avslöjar en persons ras, etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv, får enligt 2 kap. 8 § inte behandlas enbart på grund av vad som är känt om en persons sådana förhållanden. Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen.

4.2.5 Åklagarväsendet

Åklagare har till uppgift både att bekämpa och lagföra brott, men eftersom åklagares brottsbekämpning huvudsakligen syftar till att lagföra redovisas regleringen av åklagarväsendets personuppgiftsbehandling i avsnitt 4.3.1.

4.2.6 Lagen om internationellt polisiärt samarbete

Lagen (2017:496) om internationellt polisiärt samarbete tillämpas på polisiärt samarbete mellan Sverige och andra stater i den utsträckning som följer av internationella överenskommelser. Om inte annat följer av lagen om internationellt polisiärt samarbete eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller polisdatalagen för polisens behandling av personuppgifter vid sådant samarbete.

I 7 kap. lagen om internationellt polisiärt samarbete finns bestämmelser om uppgiftsutbyte enligt Prümrådsbeslutet och den behandling av personuppgifter som är tillåten vid sådant uppgiftsutbyte. I 8 kap. regleras på motsvarande sätt uppgiftsutbyte enligt CBE-direktivet. I 9 kap. finns bestämmelser om uppgiftsutbyte i informationssystemet för viseringar (VIS) enligt VIS-rådsbeslutet för utredning av vissa grova brott och för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar sådana brott. Detta kapitel i lagen reglerar den behandling av personuppgifter som är tillåten för dessa syften.

4.2.7 Lagen om internationellt tullsamarbete

Lagen (2000:1219) om internationellt tullsamarbete tillämpas på internationellt tullsamarbete som följer av vissa internationella åtaganden och som har till syfte att förhindra, upptäcka, utreda eller beivra överträdelser av tullbestämmelser. Den gäller inte bara för straffrättsliga överträdelser av tullbestämmelser utan även överträdelser som hanteras i Tullverkets verksamhet under Effektiv handel.

I 2 kap. 6–8 §§ finns bestämmelser om utbyte av uppgifter. Regleringen gäller för både spontant uppgiftsutbyte och utlämnande av uppgifter på begäran av en behörig utländsk myndighet eller mellanfolklig organisation. Enligt 8 § ska den myndighet som översänt uppgifter till en utländsk mottagare på begäran av den person som uppgiften rör underrätta honom eller henne om vilken mottagare uppgiften översänts till och för vilket ändamål. Personen behöver dock inte underrättas i vissa i paragrafen angivna situationer.

4.2.8 Lagen om register över tillträdesförbud vid idrottsarrangemang

Lagen om register över tillträdesförbud vid idrottsarrangemang ger Polismyndigheten och idrottsorganisationer möjlighet att behandla personuppgifter för att på ett ändamålsenligt sätt kunna upprätthålla gällande beslut om tillträdesförbud vid idrottsarrangemang. Polismyndigheten får enligt

2 § med hjälp av automatiserad behandling föra ett tillträdesförbudsregister, som innehåller uppgifter om personer som har meddelats tillträdesförbud enligt lagen (2005:321) om tillträdesförbud. I förarbetena framhålls att Polismyndighetens personuppgiftsbehandling enligt lagen åtminstone delvis är brottsbekämpande (se Register över tillträdesförbud vid idrottsarrangemang, prop. 2013/14:254, s. 43).

4.3 Särregler för lagföring

4.3.1 Åklagarväsendet

Allmänt om åklagardatalagen

Åklagardatalagen är uppbyggd på samma sätt som polisdatalagen och kustbevakningsdatalagen. Lagen gäller för behandling av personuppgifter i åklagarväsendets operativa verksamhet. Personuppgifter får behandlas både i åklagares brottsbekämpande verksamhet och om det behövs för att åklagare ska kunna fullgöra andra operativa uppgifter enligt bestämmelser i lag eller förordning. Behandling för sistnämnda ändamål ligger utanför direktivets tillämpningsområde och berörs därför inte vidare här. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Lagens tillämpningsområde

Åklagardatalagen gäller i åklagarväsendets operativa verksamhet, dvs. åklagarverksamhet vid Åklagarmyndigheten och Ekobrottsmyndigheten. Lagen gäller däremot inte för behandling av personuppgifter i den polisiära verksamheten vid Ekobrottsmyndigheten där polisdatalagen gäller i stället.

Åklagardatalagen gäller enligt 1 kap. 4 § till viss del även för behandling av uppgifter om juridiska personer.

Förhållandet till personuppgiftslagen

Åklagardatalagen gäller i stället för personuppgiftslagen men i 2 kap. 2 § finns hänvisningar som innebär att ett flertal bestämmelser i personuppgiftslagen ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter och bestämmelser om information till den registrerade, tillsyn och skadestånd.

Ändamålen för behandling och utlämnande av uppgifter

De ändamål för vilka personuppgifter får behandlas är indelade i primära och sekundära ändamål. De primära ändamålen avser behandling av personuppgifter för att tillgodose de behov som finns inom åklagarväsendet. De primära ändamålen för behandling anges uttömmande i 2 kap. 5 § åklagardatalagen. Personuppgifter får behandlas i åklagarväsendets brottsbekämpande verksamhet om det behövs för att förebygga eller förhindra brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Personuppgifter får

även behandlas i åklagarväsendets operativa verksamhet om det behövs för att åklagare ska kunna fullgöra andra författningsreglerade uppgifter.

De sekundära ändamålen är aktuella när personuppgifter som får behandlas i åklagarväsendets brottsbekämpande verksamhet lämnas ut till andra myndigheter eller organisationer för deras behov. Enligt de sekundära ändamålen, som anges i 2 kap. 6 §, får personuppgifter behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen och Skatteverket, eller hos utländsk myndighet, ett EU-organ eller en mellanfolklig organisation. Likaså får personuppgifter i ett enskilt fall behandlas för att lämnas ut för vissa andra i paragrafen specificerade ändamål eller för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Personuppgifter får enligt 2 kap. 7 § också behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till åklagarväsendet i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I 2 kap. 13 § regleras i vilka fall personuppgifter får lämnas till Interpol och Europol eller en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol. Personuppgifter får lämnas ut till dem om det är förenligt med svenska intressen och det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott. Uppgifter får vidare lämnas ut till utländsk myndighet eller mellanfolklig organisation om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. I 2 kap. 14 § anges under vilka förutsättningar personuppgifter som omfattas av sekretess får lämnas ut till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen och Skatteverket.

Behandling av känsliga personuppgifter

Känsliga personuppgifter, dvs. uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv, får enligt 2 kap. 8 § inte behandlas enbart på grund av vad som är känt om en persons sådana förhållanden. Om uppgifter om en person behandlas på någon annan grund får de dock kompletteras med sådana uppgifter när det är absolut nödvändigt för syftet med behandlingen.

4.3.2 Domstolsväsendet

Allmänt om domstolsdatalagen

Domstolsdatalagen (2015:728) gäller vid behandling av personuppgifter i de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Lagens tillämpningsområde

Domstolsdatalagen är enligt 2 § – i motsats till polisdatalagen och Tullverkets och Skatteverkets motsvarande lagar – tillämplig i all rättskipande och rättsvårdande verksamhet vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

I de allmänna domstolarna är det framför allt hanteringen av brottmål och vissa anknytande ärenden (t.ex. ärenden om hemliga tvångsmedel, om ändring och undanröjande av påföljd och om internationell rättslig hjälp i brottmål) som omfattas av direktivets tillämpningsområde. För de allmänna förvaltningsdomstolarna är det i huvudsak hanteringen av mål som rör verkställighet av straffrättsliga påföljder som är av intresse.

Förhållandet till personuppgiftslagen

Domstolsdatalagen gäller enligt 4 § i stället för personuppgiftslagen men i 5 § domstolsdatalagen finns hänvisningar som anger att vissa bestämmelser i personuppgiftslagen ska tillämpas. Det gäller bl.a. personuppgiftslagens definitioner, vissa grundläggande bestämmelser om behandlingen av personuppgifter och bestämmelser om information till den registrerade, tillsyn och skadestånd.

Ändamålen för behandling och utlämnande av uppgifter

Enligt 6 § domstolsdatalagen får personuppgifter behandlas om det behövs för handläggning av mål och ärenden. Personuppgifter som behandlas enligt den paragrafen får enligt 7 § även behandlas om det behövs för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning.

Behandling av känsliga personuppgifter

I 13 § domstolsdatalagen föreskrivs att uppgifter om en person inte får behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

4.3.3 Register över ordningsbot och strafföreläggande

Föreläggande av ordningsbot och strafföreläggande

Föreläggande av ordningsbot och strafföreläggande är förenklade former av lagföring som innebär att den misstänkte föreläggs att inom viss tid godkänna och betala ett i föreläggandet angivet bötesstraff och eventuellt vissa kostnader. Gör den misstänkte det gäller föreläggandet enligt 48 kap. 3 § rättegångsbalken som en lagakraftvunnen dom.

Åklagare får även enligt 48 kap. 4 § rättegångsbalken genom strafföreläggande förelägga den misstänkte villkorlig dom eller sådan påföljd i förening med böter, om det är uppenbart att rätten skulle döma till sådan påföljd.

Förordningen om register över strafföreläggande

I förordningen (1997:902) om register över strafföreläggande regleras i 2 § Tullverkets rätt att föra register över utfärdade strafföreläggande och i 4 § Polismyndighetens skyldighet att föra ett register över uppbörd i ärenden om strafföreläggande (se avsnitt 4.4.3 beträffande sistnämnda register).

Ett strafföreläggande register får enligt 6 § användas för handläggning av ärenden om strafföreläggande, för visst uppgiftslämnande och för framställning av statistik. I 9 § anges uttömmande vilka uppgifter ett strafföreläggande register får innehålla.

Numera gäller reglerna om register över strafföreläggande bara för Tullverket, vars tullåklagare får utfärda strafföreläggande. Åklagardatalagen är generellt tillämplig och när den infördes konstaterades det att särreglerna i nu aktuell förordning inte längre behövs i åklagarväsendet (prop. 2014/15:63, s. 66). De särregler som avsåg åklagarväsendet upphävdes därför.

Förordningen om register över ordningsbot

I förordningen (1997:903) om register över ordningsbot ges Polismyndigheten rätt att behandla personuppgifter i ett register över föreläggande av ordningsbot.

Registret används inte bara av Polismyndigheten utan även av Säkerhetspolisen, Tullverket och Kustbevakningen. All registrering av föreläggande av ordningsbot utfärdade vid Polismyndigheten, Tullverket och Kustbevakningen hanteras i registret. Enligt 4 § får Säkerhetspolisen ha direktåtkomst till registret och Tullverket och Kustbevakningen får ha direktåtkomst till uppgifter i de ärenden i registret som handläggs hos respektive myndighet.

Registret får enligt 2 § användas i ärenden om föreläggande av ordningsbot för handläggning, uppbörd och underrättelser till myndigheter samt för tillsyn, planering, uppföljning och framställning av statistik. I 5 § anges uttömmande vilka uppgifter registret får innehålla.

4.4 Särregler för verkställighet av straff

4.4.1 Särreglering bara för vissa former av verkställighet

Fängelse, skyddstillsyn, villkorlig dom med samhällstjänst och böter

Kriminalvården ansvarar för verkställighet av flertalet straffrättsliga påföljder. Det gäller fängelsestraff och frivårdspåföljder i form av skyddstillsyn och villkorlig dom med samhällstjänst.

Både Polismyndigheten och Kronofogdemyndigheten har uppgifter när det gäller betalning av böter. Polismyndigheten ansvarar för uppbörd, dvs. frivillig betalning, och Kronofogdemyndigheten för indrivning.

Om rätten beslutar om överlämnande till särskild vård enligt 31 kap. brottsbalken eller överlämnande till särskild vård för unga enligt 32 kap. brottsbalken är det andra myndigheter som ansvarar för verkställigheten. Vid vård enligt lagen (1988:870) om vård av missbrukare i vissa fall är det socialnämnden eller ett hem där sådan vård meddelas som ansvarar för verkställigheten.

Om påföljden är rättspsykiatrisk vård ansvarar enligt 6 § lagen (1991:1129) om rättspsykiatrisk vård en sjukvårdsinrättning som drivs av ett landsting för verkställigheten.

Är påföljden ungdomsvård eller ungdomstjänst ansvarar socialnämnden för verkställigheten. I de fall där påföljden bestäms till sluten ungdomsvård ansvarar enligt 3 § lagen (1998:603) om verkställighet av sluten ungdomsvård Statens institutionsstyrelse för verkställigheten.

De regler om behandling av personuppgifter som gäller i dessa verksamheter och som ligger inom direktivets tillämpningsområde redovisas i det följande.

4.4.2 Verkställighet av fängelse, skyddstillsyn och villkorlig dom med samhällstjänst

Allmänt om lagen om behandling av personuppgifter inom kriminalvården

Lagen om behandling av personuppgifter inom kriminalvården innehåller endast övergripande bestämmelser om behandlingen av personuppgifter. Bestämmelser om de register som ska föras (centrala kriminalvårdsregistret och säkerhetsregistret) och detaljerade regler om vilka typer av uppgifter som får behandlas om olika personkategorier finns i stället i förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

Lagens tillämpningsområde

Lagen gäller enligt 1 § vid behandling av personuppgifter i fråga om personer som

- är föremål för personutredning,
- är häktade,
- är dömda till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, eller är ålagda fängelse som förvandlingsstraff för böter eller vite, eller som på grund av en utländsk dom ska verkställa någon av dessa påföljder i Sverige,
- på någon annan grund är intagna i häkte eller kriminalvårdsanstalt, eller
- annars transporteras av Kriminalvårdens transporttjänst.

Förhållandet till personuppgiftslagen

Lagen om behandling av personuppgifter inom kriminalvården gäller utöver personuppgiftslagen och innehåller bara vissa särbestämmelser i förhållande till personuppgiftslagen, som i övrigt gäller inom Kriminalvården.

Ändamålen med behandlingen

Personuppgifter får enligt 3 § lagen behandlas bara om det behövs för att

- Kriminalvården ska kunna fullgöra sina uppgifter i enlighet med lag eller förordning,
- underlätta tillgången till sådana uppgifter om verkställighet av påföljd eller häktning som rättsväsendets myndigheter behöver, eller
- upprätthålla säkerheten och förebygga brott under den tid som häktning, verkställighet av påföljd, intagning av annat skäl eller transport utförd av Kriminalvården pågår.

Behandling av känsliga personuppgifter

Uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv får enligt 5 § lagen inte behandlas enbart på grund av vad som är känt om personens sådana förhållanden. Om känsliga personuppgifter behandlas på annan grund, får uppgifterna kompletteras med sådana personuppgifter om det är absolut nödvändigt för syftet med behandlingen.

Förordningen om behandling av personuppgifter inom kriminalvården

I förordningen om behandling av personuppgifter inom kriminalvården finns dels generella regler om vilka uppgifter som får behandlas, dels bestämmelser om särskilda register. Vilka uppgifter som får behandlas varierar med grunden för att en person förekommer inom kriminalvården. Reglerna är t.ex. olika beroende på vilken påföljd som verkställs.

Det centrala kriminalvårdsregistret regleras i 34–36 §§. Ändamålet med registret är dels att möjliggöra för myndigheten att fullgöra sina författningsenliga uppgifter, dels att underlätta tillgången till sådana uppgifter om verkställighet av påföljd som rättsväsendets myndigheter behöver. Endast personer som har dömts till fängelse, skyddstillsyn, villkorlig dom med samhällstjänst eller har ålagts förvandlingsstraff för böter eller vite eller personer som ska verkställa en utländsk sådan påföljd i Sverige får finnas i registret.

Säkerhetsregistret regleras i 39–41 och 43–45 §§. Ändamålet med registret är att upprätthålla säkerheten och att förebygga brott. Endast personer som är häktade eller intagna i vissa fängelser för att avtjäna fängelsestraff eller som ska verkställa en utländsk sådan påföljd får finnas i registret. Registrering förutsätter dessutom att vissa särskilda omständigheter föreligger, t.ex. att den registrerade tidigare har rymt eller gjort sig skyldig till allvarligt hot eller våld mot personal eller mot andra intagna eller att det finns särskild anledning att anta att han eller hon kan komma att göra det.

Förordningen innehåller också regler om de journaler som ska föras över verkställigheten. Vid överflyttning av verkställighet av påföljd till en annan stat får enligt 48 § bl.a. sådana journaler lämnas ut till den myndighet i den andra staten som är ansvarig för verkställigheten.

4.4.3 Verkställighet av bötesstraff

Regler om verkställighet av böter

Enligt 1 § bötesverkställighetslagen (1979:189) verkställs bötesstraff antingen genom uppbörd eller indrivning. Uppbörd innebär att den bötfällde frivilligt betalar bötesbeloppet. Uppbörd kan också bestå i att belopp som har betalats som förskott på böter tas i anspråk. Bötesstraff som ålagts genom strafföreläggande eller föreläggande av ordningsbot ska enligt 2 § i första hand verkställas genom uppbörd. Detsamma gäller böter som ålagts genom dom eller slutligt beslut av allmän domstol. Om uppbörd inte ska ske eller om uppbörd inte leder till full betalning ska böterna enligt 6 § lämnas vidare för indrivning.

Uppbörd av böter

Polismyndigheten är enligt 3 § bötesverkställighetsförordningen (1979:197) central uppbördsmyndighet. Polismyndigheten ansvarar för uppbörd av böter oavsett vilken myndighet som utfärdat ett föreläggande av ordningsbot eller ett strafföreläggande. Polismyndigheten ansvarar även för uppbörd av böter som utdömts av allmän domstol.

I Polismyndighetens verksamhet med uppbörd av böter tillämpas personuppgiftslagen om det inte finns någon särreglering. Som tidigare nämnts får Polismyndigheten föra register över förelägganden av ordningsbot och strafförelägganden (se avsnitt 4.3.3). Registren är bl.a. avsedda att utgöra hjälpmedel i Polismyndighetens roll som central uppbördsmyndighet.

I departementspromemorian Uppbörd av böter (Ds 2015:5) föreslås en ny lag och förordning om uppbörd av böter. De är avsedda att ersätta de nuvarande bestämmelserna om uppbörd av bötesstraff. Promemorian har remitterats. En utredare har haft i uppdrag att anpassa förslagen till EU:s dataskyddsreform. Uppdraget redovisas i departementspromemorian Uppbörd av böter efter EU:s dataskyddsreform (Ds 2018:3). Promemorian har remitterats.

Verkställighet av böter som inte betalas frivilligt

Indrivning innebär att betalning för böter tas ut tvångsvis genom åtgärder som Kronofogdemyndigheten vidtar. Om gäldenären inte betalar kan under vissa förutsättningar bötesstraffet komma att förvandlas till fängelse. På initiativ av Kronofogdemyndigheten prövar åklagare om det finns skäl att väcka talan vid allmän domstol om omvandling av straffet. Förfarandet regleras dels i 15–23 §§ bötesverkställighetslagen, dels i 17–23 §§ bötesverkställighetsförordningen.

4.4.4 Verkställighet av rättspsykiatrisk vård, vård enligt socialtjänstlagen, ungdomsvård och ungdomstjänst

Rättspsykiatrisk vård

När det gäller rättspsykiatrisk vård finns det ingen särskild reglering av personuppgiftsbehandling i sådan verksamhet, utan patientdatalagen (2008:355) gäller för vårdgivares behandling av personuppgifter liksom inom annan hälso- och sjukvård (1 kap. 1 och 3 §§ patientdatalagen). I övrigt tillämpas personuppgiftslagen.

I 2 kap. 2 § patientdatalagen, som gäller utöver personuppgiftslagen, anges i vilken utsträckning behandling av personuppgifter är tillåten med eller utan den registrerades samtycke. Personuppgifter får enligt 2 kap. 4 § behandlas bl.a. för att uppfylla kraven på journalföring i 3 kap. och att upprätta annan dokumentation som följer av lag, förordning eller annan författning. Vårdgivaren är enligt 2 kap. 6 § personuppgiftsansvarig. Uppgifter om lagöverträdelser får behandlas endast om det är absolut nödvändigt. Det gäller även en vårdgivare som inte är en statlig myndighet, landsting eller kommun. Behandling av känsliga personuppgifter och behandling av uppgifter om lagöverträdelser regleras i 2 kap. 8 §. I 3 kap. regleras skyldigheten att föra patientjournal och där finns också vissa bestämmelser om behandling av personuppgifter i sådana journaler. Lagen innehåller också bestämmelser om skadestånd och överklagande.

Ungdomsvård, vård enligt socialtjänstlagen och vård av missbrukare

Statens institutionsstyrelse, som ansvarar för verkställighet av sluten ungdomsvård, tillämpar lagen (2001:454) om behandling av personuppgifter inom socialtjänsten i sin verksamhet. Lagen gäller utöver personuppgiftslagen. Personuppgifter får enligt 6 § bara behandlas om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska utföras och för uppgiftslämnande som föreskrivs i lag eller förordning. Lagen reglerar i 7 § bl.a. behandling av känsliga personuppgifter och uppgifter om lagöverträdelser, domar i brottmål och straffprocessuella tvångsmedel.

Kommunala myndigheter tillämpar också lagen om behandling av personuppgifter inom socialtjänsten i verksamhet enligt lagstiftningen om socialtjänst och lagstiftningen om vård utan samtycke av unga eller missbrukare. Det innebär att lagen är tillämplig när kommunala myndigheter behandlar personuppgifter beträffande någon som har dömts till överlämnande till särskild vård enligt lagen om vård av missbrukare eller till ungdomstjänst eller ungdomsvård.

4.4.5 Internationellt samarbete rörande verkställighet av straffrättsliga påföljder

Ett flertal lagar och förordningar reglerar internationellt samarbete beträffande verkställighet av påföljd. Det gäller exempelvis lagen (1963:193) om samarbete med Danmark, Finland, Island och Norge angående verkställighet av straff, lagen (1972:260) om internationellt samarbete rörande verkställighet av brottmålsdom, lagen (2015:96) om

erkännande och verkställighet av frihetsberövande påföljder inom Europeiska unionen, lagen (2009:1427) om erkännande och verkställighet av bötesstraff inom Europeiska unionen och lagen (2011:423) om erkännande och verkställighet av beslut om förverkande inom Europeiska unionen. Flera av de myndigheter vars registerförfattningar har redovisats i detta kapitel fullgör olika uppgifter enligt dessa lagstiftningar som kräver behandling av personuppgifter.

4.5 Regler om personuppgiftsbehandling hos andra aktörer än myndigheter

4.5.1 Uppgifter om brottsbekämpning, lagföring eller straffverkställighet

Det är inte bara myndigheter som behandlar uppgifter som rör brottsbekämpning, lagföring och straffverkställighet. Åtskilliga andra aktörer får i sin verksamhet i större eller mindre utsträckning tillgång till uppgifter om t.ex. domar i brottmål. I vilken utsträckning sådana uppgifter får behandlas regleras dels i personuppgiftslagen, dels i andra författningar som ligger utanför direktivets tillämpningsområde.

Som framgår i avsnitt 4.1.2 förbjuds andra än myndigheter i personuppgiftslagen att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från förbudet. Datainspektionen har meddelat sådana föreskrifter (DIFS 1998:3). Föreskrifterna innebär att personuppgifter om lagöverträdelser får behandlas bl.a. om behandlingen

- är nödvändig för att fullgöra en föreskrift på socialtjänstområdet,
- avser uppgift i fristående skolors elevvårdsverksamhet eller motsvarande verksamhet hos enskilda anordnare av högskoleutbildning,
- är nödvändig för att kontrollera att en jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet, eller
- bara avser enstaka uppgift som är nödvändig för att anmälningsskyldighet enligt lag ska kunna fullgöras.

4.5.2 Offentliga försvarare och annat juridiskt biträde

I förundersökningar och brottmålsrättegångar biträds både den misstänkte och i vissa fall målsäganden av ett juridiskt biträde. Endast den som är advokat får enligt huvudregeln i 21 kap. 5 § rättegångsbalken utses till offentlig försvarare. Till målsägandebiträde får enligt 4 § lagen (1988:609) om målsägandebiträde jämförd med 26 § rättshjälpslagen (1996:1619) förordnas en advokat, en biträdande jurist eller någon annan som är lämplig för uppdraget. Motsvarande krav ställs på den som enligt 5 § lagen (1999:997) om särskild företrädare för barn får utses till särskild företrädare. Den som fullgör uppgifter som offentlig försvarare,

målsägandebiträde eller särskild företrädare för barn behandlar i stor utsträckning personuppgifter som härrör från förundersökningar, brottmålsrättegångar och straffverkställighet.

I 8 kap. rättegångsbalken finns bestämmelser om advokatväsendet. En advokat ska vara ledamot av Sveriges advokatsamfund, vars verksamhet delvis är av offentligrättslig natur genom den tillsyn som samfundets styrelse och disciplinnämnd enligt 8 kap. 6 och 7 §§ rättegångsbalken utövar över advokaterna.

Enligt 8 kap. 4 § rättegångsbalken ska en advokat i sin verksamhet redbart och nitiskt utföra de uppdrag som anförtrotts honom och iaktta god advokatsed.

Det finns inte några särregler för behandling av personuppgifter som utförs av någon av de kategorier som nämns i detta avsnitt. De tillämpar således personuppgiftslagen.

4.5.3 Idrottsorganisationer

En idrottsorganisation får enligt 7 § lagen om register över tillträdesförbud vid idrottsarrangemang behandla personuppgifter från det tillträdesförbudsregister som Polismyndigheten för, om det behövs för att förebygga, förhindra eller upptäcka överträdelse av ett tillträdesförbud vid ett idrottsarrangemang som organisationen anordnar. En sådan organisation har också enligt 9 § rätt att ta del av uppgifter i tillträdesförbudsregistret trots att det gäller sekretess för uppgifterna. Uppgifter ur tillträdesförbudsregistret får enligt 10 § lämnas ut till en idrottsorganisation på medium för automatiserad behandling.

4.6 Lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen

Allmänt om lagen

Lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (i fortsättningen 2013 års lag) genomför rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (i fortsättningen dataskyddsrambeslutet). Lagen gäller när personuppgifter överförs eller har överförts eller görs eller har gjorts tillgängliga inom ramen för polissamarbete eller straffrättsligt samarbete. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Lagen gäller för behandling av personuppgifter i verksamhet som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder, om uppgifterna inom ramen för polissamarbete eller straffrättsligt samarbete görs eller har gjorts tillgängliga eller överförs eller har överförts mellan en svensk myndighet och en medlemsstat i EU eller mellan en svensk myndighet och Island, Norge, Schweiz eller Liechtenstein eller mellan en svensk myndighet och ett EU-organ eller EU-informationssystem.

Från lagens tillämpningsområde undantas i 4 § dels behandling av personuppgifter som rör nationell säkerhet, dels personuppgifter som görs eller har gjorts tillgängliga eller överförs eller har överförts genom visst informationsutbyte som specificeras i paragrafen.

Personuppgifter som en svensk myndighet har tagit emot får enligt 5 § endast behandlas för andra ändamål än det som uppgifterna först överfördes eller gjordes tillgängliga för om syftet med behandlingen är att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott, verkställa straffrättsliga påföljder eller att vidta rättsliga eller administrativa åtgärder med direkt anknytning till något av dessa ändamål eller att avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får även behandlas för andra ändamål om den som överfört eller gjort uppgifterna tillgängliga har lämnat sitt medgivande eller den som uppgifterna avser har samtyckt till det.

Särskilda begränsningar gäller för överföring av personuppgifter som en svensk myndighet har erhållit enligt 6 § för överföring till enskilda och enligt 7 § för överföring till tredjeland eller internationella organ.

I lagen finns också bestämmelser om villkor för användningen av personuppgifter.

4.7 Gällande unionsrättsakter

4.7.1 Rättighetsstadgan

I artikel 8 i rättighetsstadgan slås fast att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

I artikel 52 i stadgan anges i vilken utsträckning inskränkningar får göras i de rättigheter som erkänns i stadgan. Utgångspunkten är att sådana inskränkningar endast får göras i lag och ska vara förenliga med det väsentliga innehållet i rättigheterna. Begränsningar får endast göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

4.7.2 Dataskyddsdirektivet från 1995

Den allmänna regleringen av behandling av personuppgifter inom Europeiska unionen finns i dag i 1995 års dataskyddsdirektiv. Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Direktivet, som har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204) med tillhörande förordning (se avsnitt 4.1.2), gäller inte för behandling av personuppgifter utanför gemenskapsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område.

4.7.3 Dataskyddsrambeslutet

Dataskyddsrambeslutet är tillämpligt på uppgifter som överförs eller görs tillgängliga mellan medlemsstaterna och mellan medlemsstater och EU-organ och mellan medlemsstater och vissa utpekade informationssystem. Dataskyddsrambeslutet gäller däremot inte för nationell personuppgiftsbehandling. Från tillämpningsområdet undantas också personuppgiftsbehandling inom området nationell säkerhet.

Dataskyddsrambeslutet har genomförts i svensk rätt främst genom 2013 års lag med tillhörande förordning (se avsnitt 4.6).

4.8 Europeiska unionens dataskyddsreform

4.8.1 Två nya rättsliga instrument

Diskussionerna om det behövdes ett nytt rättsligt instrument som skulle ersätta 1995 års dataskyddsdirektiv pågick länge. Kommissionen presenterade den 25 januari 2012 förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Paketet omfattade inte bara en förordning med en generell reglering som skulle ersätta 1995 års dataskyddsdirektiv utan även ett nytt direktiv med särregler för främst den brottsbekämpande sektorn som skulle ersätta dataskyddsrambeslutet men ha ett bredare tillämpningsområde.

Det huvudsakliga syftet med kommissionens förslag var att ytterligare harmonisera och effektivisera skyddet av personuppgifter inom EU i syfte att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Förslaget till förordning baserades till stor del på den struktur och reglering som finns i 1995 års dataskyddsdirektiv. Generellt innebar förslaget stärkt skydd för enskilda vid behandling av personuppgifter. Förordningen innehöll även en rad nyheter jämfört med dataskyddsdirektivet. Dit hörde nya regler om de nationella tillsynsmyndigheternas ställning, villkor och uppgifter och om obligatoriskt ömsesidigt bistånd och samarbete dem emellan. En annan nyhet var skyldigheten för den personuppgiftsansvarige att utan dröjsmål underrätta tillsynsmyndigheten om en personuppgiftsincident ägt rum.

Förslaget till direktiv anslöt i stor utsträckning till den reglering som gäller enligt dataskyddsrambeslutet. Nya inslag var bl.a. kravet på att, så långt det är möjligt, vid behandlingen skilja mellan personuppgifter som avser olika kategorier av personer och likaså mellan uppgifter med olika grad av riktighet och tillförlitlighet. En annan nyhet var skyldigheten för den personuppgiftsansvarige att utan dröjsmål underrätta tillsynsmyndigheten om en personuppgiftsincident ägt rum. Vidare föreslogs nya regler om de nationella tillsynsmyndigheternas ställning, villkor och uppgifter och om obligatoriskt ömsesidigt bistånd och samarbete dem emellan. Till skillnad från dataskyddsrambeslutet föreslogs det nya dataskyddsdirektivet vara tillämpligt inte bara på utbyte av information över gränserna utan även på nationell personuppgiftsbehandling för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Efter flera års förhandlingar enades Europaparlamentet och rådet den 27 april 2016 om en ny reglering av skyddet för enskilda vid behandling av personuppgifter. Den består av två rättsliga instrument, en förordning och ett direktiv.

4.8.2 En dataskyddsförordning

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, här kallat dataskyddsförordningen, börjar tillämpas den 25 maj 2018.

Förordningen utgör en ny generell reglering för behandling av personuppgifter inom EU som ska ersätta dataskyddsdirektivet från år 1995 och som är direkt tillämplig. När förordningen träder i kraft måste personuppgiftslagen upphävas. Andra författningar som omfattas av den nya förordningens tillämpningsområde måste upphävas i de delar förordningen innehåller motsvarande föreskrifter och i övrigt anpassas till den.

Förordningen reglerar bl.a. grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, tillsyn över personuppgiftsbehandling och rätten för enskilda att få tillgång till rättsmedel och sanktioner mot ansvariga som inte lever upp till förordningens krav.

Från förordningens tillämpningsområde undantas personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Personuppgiftsbehandling för dessa syften ligger i stället under det nya dataskyddsdirektivets tillämpningsområde (se avsnitt 4.8.3).

En särskild utredare har haft i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Utredningen fick namnet Dataskyddsutredningen. Dataskyddsutredningen har samrått med Utredningen om 2016 års dataskyddsdirektiv. Betänkandet Dataskyddslag redovisades den 12 maj 2017 (SOU 2017:39 Ny dataskyddslag). Lagrådsremissen Ny dataskyddslag beslutades av regeringen den

21 december 2017. Propositionen Ny dataskyddslag (prop. 2017/18:105) beslutades av regeringen den 15 februari 2018. I propositionen lämnas förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning, här kallad dataskyddslagen.

4.8.3 Ett nytt dataskyddsdirektiv

Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, här kallat direktivet, ska vara genomfört i nationell rätt senast den 6 maj 2018.

Direktivet ska dels skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt. Direktivet ersätter dataskyddsrambeslutet. En närmare beskrivning av innehållet i direktivet finns i avsnitt 5.2.

4.8.4 Viss personuppgiftsbehandling ligger utanför båda instrumenten

Viss behandling av personuppgifter undantas från både dataskyddsförordningens och dataskyddsdirektivets tillämpningsområden. Det gäller personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

Vidare undantas den personuppgiftsbehandling som förekommer vid EU:s myndigheter och andra organ. Den regleras i stället i Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter. Inom EU pågår förhandlingar om regleringen av behandlingen av personuppgifter vid unionens myndigheter och andra organ.

4.9 Dataskyddskonventionen

Europarådets ministerkommitté antog år 1981 en konvention till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen (nr 108). Konventionen trädde i kraft den 1 oktober 1985. Dess syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter. Utgångspunkten är att vissa av den enskildes rättigheter kan behöva skyddas i förhållande till den princip om fritt flöde av information, oberoende av gränser, som finns inskriven i internationella överenskommelser om mänskliga rättigheter. Konventionens tillämpningsområde är enligt

huvudregeln automatiserade personregister och automatisk databehandling av personuppgifter i allmän och enskild verksamhet.

I konventionen anges krav på de personuppgifter som undergår automatisk databehandling, bl.a. krav på att uppgifterna ska hämtas in och behandlas på ett korrekt sätt och vara relevanta med hänsyn till ändamålet, att vissa typer av uppgifter inte får behandlas automatiserat om inte nationell lagstiftning ger ett ändamålsenligt skydd, och att lämpliga säkerhetsåtgärder ska vidtas för att skydda personuppgifter gentemot oavsiktlig eller otillåten förstörelse.

Konventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. En sådan rekommendation rör polisen.

Sverige har, i likhet med övriga medlemsstater i EU, anslutit sig till dataskyddskonventionen.

Europarådet inledde år 2010 en översyn av konventionen och rekommendationerna. Arbetet med översynen kan förväntas vara slutfört inom en nära framtid.

5 Det nya dataskyddsdirektivet

5.1 Allmänt om direktivet

Det nya dataskyddsdirektivet riktar sig till medlemsstaterna och kräver att de genomför viss lagstiftning inom två år efter ikraftträdandet. Det innebär att direktivet ska vara genomfört senast den 6 maj 2018. Direktivet är indelat i tio kapitel och innehåller totalt 65 artiklar.

I detta avsnitt beskrivs kortfattat innehållet i samtliga artiklar, för att skapa en översiktlig bild av vilka krav på lagstiftning som direktivet ställer. Det närmare innehållet i artiklarna redovisas i de kapitel som behandlar sakfrågorna.

Av skäl 99 framgår att Storbritannien och Irland inte är bundna av bestämmelserna i direktivet i vissa delar.

Danmark ska enligt skäl 100 inom sex månader efter antagandet av direktivet besluta om man ska genomföra direktivet i sin nationella lagstiftning eller inte.

Av skäl 101–103 framgår att Norge, Island, Schweiz och Liechtenstein är bundna av direktivet genom att de har anslutit sig till Schengenregelverket.

5.2 Innehållet i direktivet

Artiklarna 1–3: Allmänna bestämmelser

Enligt *artikel 1* innehåller direktivet bestämmelser om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot och förebygga och förhindra hot mot den allmänna säkerheten. Syftet

med direktivet är att dels skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels säkerställa att, när det krävs utbyte av personuppgifter inom unionen mellan behöriga myndigheter, detta utbyte varken begränsas eller förbjuds av hänsyn till skyddet för fysiska personer mot behandling av personuppgifter. Det slås också fast att direktivet inte hindrar att medlemsstaterna föreskriver strängare skyddsåtgärder när det gäller registrerades rättigheter och friheter.

Artikel 2 anger direktivets tillämpningsområde. Direktivet ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1. Direktivet ska tillämpas dels på helt eller delvis automatiserad behandling av personuppgifter, dels på annan behandling av personuppgifter som ingår i eller kommer att ingå i register. Däremot ska direktivet inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller på personuppgiftsbehandling som utförs av unionens institutioner eller andra organ.

Artikel 3 innehåller definitioner. Där anges bl.a. vad som avses med personuppgift, behandling, register, behörig myndighet, personuppgiftsansvarig, personuppgiftsbiträde och personuppgiftsincident. Vidare definieras genetiska och biometriska uppgifter.

Artiklarna 4–11: Principer

I *artikel 4* anges grundläggande principer för behandling av personuppgifter. Personuppgifter ska

- behandlas på ett lagligt och korrekt sätt,
- samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,
- vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,
- vara korrekta och, om nödvändigt, uppdaterade,
- inte möjliggöra identifiering av den registrerade under längre tid än nödvändigt, och
- behandlas på ett sätt som säkerställer säkerheten för uppgifterna.

Behandling för något annat ändamål som anges i artikel 1.1 än det för vilket uppgifterna samlades in är tillåten om den personuppgiftsansvarige har rätt att behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till det nya ändamålet. Behandlingen kan inkludera arkivändamål som är av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1, om det finns lämpliga skyddsåtgärder.

Enligt *artikel 5* ska lämpliga tidsgränser föreskrivas för när personuppgifter ska raderas eller för regelbunden översyn av behovet av att lagra sådana uppgifter. Det ska finnas regler för att säkerställa att tidsgränserna hålls.

Enligt *artikel 6* ska den personuppgiftsansvarige så långt möjligt göra åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, som misstänkta, dömda, brottsoffer och andra som berörs av brott, exempelvis personer som kan komma att kallas som vittnen.

I *artikel 7* föreskrivs att åtskillnad så långt möjligt ska göras mellan personuppgifter som grundar sig på fakta och uppgifter som grundar sig på personliga bedömningar. Behöriga myndigheter ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Om felaktiga personuppgifter har överförts eller personuppgifter överförts olagligen ska mottagaren omedelbart underrättas om det. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen av dem begränsas.

Enligt *artikel 8* är behandling laglig endast om och i den utsträckning behandlingen är nödvändig för att behöriga myndigheter ska kunna utföra sådana uppgifter som anges i artikel 1.1 och som grundas på unionsrätt eller nationell rätt. Den nationella rätten ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och ändamålet med behandlingen.

I *artikel 9* föreskrivs att personuppgifter som samlats in för något av de i direktivet angivna ändamålen inte får behandlas för något annat ändamål om inte sådan behandling är tillåten enligt unionsrätten eller nationell rätt. När personuppgifter behandlas för andra ändamål än dem som anges i artikel 1.1 ska dataskyddsförordningen tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. Om de behöriga myndigheterna har andra uppgifter än dem som anges i artikel 1.1, ska dataskyddsförordningen tillämpas på behandling för sådana ändamål. Det gäller även behandling för arkivändamål som är av allmänt intresse eller för statistiska, historiska eller vetenskapliga ändamål. I artikeln anges också vad som gäller för överföring av uppgifter för behandling för andra ändamål.

Artikel 10 reglerar behandling av det som brukar kallas känsliga personuppgifter. Med det avses uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Regleringen omfattar även behandling av genetiska uppgifter, biometriska uppgifter i identifieringssyfte eller uppgifter om hälsa, sexualliv eller sexuell läggning. Behandling av sådana uppgifter är bara tillåten om den är absolut nödvändig, det finns tillräckliga skyddsåtgärder och behandlingen är tillåten enligt unionsrätt eller nationell rätt för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person eller om det är fråga om uppgifter som den registrerade själv har offentliggjort.

I *artikel 11* förbjuds att beslut, som har negativa rättsverkningar eller i betydande grad påverkar den registrerade, fattas om de enbart grundas på automatiserad behandling, såvida inte de är tillåtna enligt unionsrätten eller nationell rätt och det finns lämpliga skyddsåtgärder. Profilering som leder till diskriminering på grundval av känsliga personuppgifter ska förbjudas.

Enligt *artikel 12* ska den personuppgiftsansvarige utan kostnad lämna den registrerade information om hans eller hennes rättigheter. Informationen ska vara koncis, lättillgänglig och språkligt lättfattlig. Den personuppgiftsansvarige ska utan onödigt dröjsmål skriftligen besvara en begäran från den registrerade om information om hur hans eller hennes personuppgifter behandlas. Om en registrerads begäran är uppenbart ogrundad eller orimlig får den personuppgiftsansvarige antingen ta ut en avgift eller vägra tillmötesgå begäran.

I *artikel 13* anges vilken information som alltid måste göras tillgänglig för den registrerade. Det är den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter, ändamålen med den avsedda behandlingen, rätten att klaga till en tillsynsmyndighet och dess kontaktuppgifter och rätten att begära att få del av personuppgifter, rättelse, radering eller begränsning av behandlingen. Därutöver ska den personuppgiftsansvarige i specifika fall lämna viss annan information för att göra det möjligt för den registrerade att utöva sina rättigheter.

Artikel 14 behandlar den registrerades rätt till tillgång till personuppgifter. Om inte annat sägs i artikel 15 ska den registrerade ha rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör honom eller henne behandlas och, om så är fallet, få tillgång till personuppgifterna och följande information:

– ändamålen med behandlingen och den rättsliga grunden,
– vilka kategorier av personuppgifter som behandlas,
– vilka mottagare eller kategorier av mottagare som har fått personuppgifterna,
– hur länge uppgifterna kommer att lagras eller, om det inte är möjligt, kriterierna för att fastställa lagringstiden,
– rätten att begära rättelse, radering eller begränsning av behandlingen, och
– rätten att klaga hos en tillsynsmyndighet och dess kontaktuppgifter.

Enligt *artikel 15* får medlemsstaterna genom lagstiftning, så länge åtgärden är nödvändig och proportionell, helt eller delvis begränsa den registrerades rätt till tillgång till personuppgifter och information i syfte att undvika att förundersökningar och andra utredningar eller förfaranden, brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder försvåras eller i syfte att skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter.

Artikel 16 behandlar rätten till rättelse eller radering av personuppgifter eller begränsning av behandlingen och vilka skyldigheter den personuppgiftsansvarige har i sådana frågor. Den registrerade ska ha rätt att utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen ska den registrerade även kunna få ofullständiga personuppgifter kompletterade. I vissa fall ska den registrerade även ha rätt att få personuppgifter raderade.

I stället för att radera personuppgifterna ska den personuppgiftsansvarige i vissa fall begränsa behandlingen av uppgifterna.

Enligt *artikel 17* ska den registrerades rättigheter även kunna utövas genom den behöriga tillsynsmyndigheten om tillgången till information har begränsats.

I *artikel 18* öppnas möjlighet att föreskriva att rätten till information, tillgång till uppgifter, rättelse, radering och begränsning av behandling ska utövas enligt nationell rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredning och straffrättsliga förfaranden.

Av skäl 107 framgår att direktivet inte hindrar att det i nationell straffprocesslagstiftning finns bestämmelser om den registrerades rätt till information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden och begränsningar i dessa rättigheter.

Artiklarna 19–28: Personuppgiftsansvarig och personuppgiftsbiträde

Den personuppgiftsansvarige ska enligt *artikel 19* vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med direktivet.

Artikel 20 behandlar inbyggt dataskydd och dataskydd som standard.

Artikel 21 öppnar en möjlighet att låta två eller flera personuppgiftsansvariga ha gemensamt personuppgiftsansvar för ett register.

I *artikel 22* regleras vilka krav som ställs när en personuppgiftsansvarig anlitar ett personuppgiftsbiträde. Som huvudregel får ett personuppgiftsbiträde enligt *artikel 23* bara behandla uppgifter enligt instruktioner från den personuppgiftsansvarige.

Artikel 24 innehåller detaljerade regler om personuppgiftsansvarigas skyldighet att föra register över olika typer av behandlingar. I *artikel 25* ställs krav på att det ska finnas loggar över olika typer av behandling i automatiserade behandlingssystem. Registren och loggarna ska på begäran göras tillgängliga för tillsynsmyndigheten.

Enligt *artikel 26* ska personuppgiftsansvariga och personuppgiftsbiträden på begäran samarbeta med tillsynsmyndigheten.

I *artikel 27* ställs krav på att den personuppgiftsansvarige gör en förhandsbedömning av behandlingens konsekvenser för skyddet av personuppgifter när det gäller en ny typ av behandling som sannolikt leder till hög risk för fysiska personers rättigheter och friheter.

Artikel 28 ställer krav på att den personuppgiftsansvarige under vissa förutsättningar ska samråda med tillsynsmyndigheten innan nya register inrättas.

Artiklarna 29–31: Säkerhet för personuppgifter

Artikel 29 innehåller krav på säkerhet i samband med behandlingen av personuppgifter. Den personuppgiftsansvarige och personuppgiftsbiträdet ska – med beaktande av bl.a. kostnaderna och behandlingens art, omfattning och ändamål – vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa lämplig säkerhetsnivå. Säkerheten ska omfatta åtkomstskydd för utrustning, kontroll av datamedier, lagringskontroll, användar-

kontroll, åtkomstkontroll, kommunikationskontroll, indatakontroll, transportkontroll, återställande, driftsäkerhet och dataintegritet.

I *artikel 30* regleras den personuppgiftsansvariges skyldigheter om det inträffar en personuppgiftsincident. En sådan ska anmälas till tillsynsmyndigheten utan dröjsmål och enligt huvudregeln senast 72 timmar efter att den personuppgiftsansvarige har fått kännedom om incidenten. I artikeln anges också vad en sådan anmälan ska innehålla och vilken dokumentation om incidenten som krävs.

Artikel 31 innehåller regler om information till den registrerade om en personuppgiftsincident och i vilka fall det inte krävs någon sådan information.

Artiklarna 32–34: Dataskyddsombud

Enligt *artikel 32* ska den personuppgiftsansvarige utnämna ett dataskyddsombud. Undantag får göras för domstolars och andra oberoende rättsliga myndigheters dömande verksamhet. Flera myndigheter får ha samma dataskyddsombud. Ombudets kontaktuppgifter ska dels offentliggöras, dels meddelas till tillsynsmyndigheten.

Enligt *artikel 33* ska den personuppgiftsansvarige säkerställa att dataskyddsombudet kan delta i frågor som rör skyddet av personuppgifter och stödja dataskyddsombudet i hans eller hennes uppgifter.

Dataskyddsombudets uppgifter anges i *artikel 34*. I uppgifterna ingår bl.a. att informera och ge råd till den personuppgiftsansvarige och de anställda som behandlar personuppgifter, att övervaka att direktivet efterlevs och att samarbeta med och vara en kontaktpunkt för tillsynsmyndigheten.

Artiklarna 35–40: Överföring av personuppgifter till tredjeländer eller internationella organisationer

I *artikel 35* anges allmänna principer för överföring av personuppgifter till tredjeland och internationella organisationer. Där föreskrivs bl.a. att överföringen ska vara nödvändig för något av de ändamål som anges i artikel 1.1 och att den ska riktas till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är behörig för sådana ändamål. Om uppgifterna kommer från en annan medlemsstat ska den enligt huvudregeln ge förhandstillstånd till överföringen.

Artikel 36 reglerar överföring till mottagare i tredjeland eller internationella organisationer som enligt kommissionens beslut har en adekvat skyddsnivå. Sådana överföringar kräver inte särskilt tillstånd.

Även om det inte finns något beslut om en adekvat skyddsnivå får, enligt *artikel 37*, uppgifter överföras till mottagare i ett tredjeland eller en internationell organisation om lämpliga skyddsåtgärder kan säkerställas i ett enskilt fall.

I *artikel 38* görs också undantag för överföring i särskilda situationer, bl.a. för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland.

Artikel 39 reglerar överföring direkt till vissa mottagare som inte är behöriga myndigheter.

Kommissionen och medlemsstaterna åläggs i *artikel 40* att bl.a. utveckla rutiner för det internationella samarbetet för att underlätta en effektiv

tillämpning av lagstiftningen om skydd för personuppgifter och att också erbjuda bistånd till tredjeland och internationella organisationer i det syftet.

Artiklarna 41–51: Oberoende tillsynsmyndigheter

Enligt *artikel 41* ska varje medlemsstat utse en eller flera myndigheter som ska vara ansvariga för att övervaka tillämpningen av direktivet. Samma myndighet som har utsetts till tillsynsmyndighet enligt dataskyddsförordningen får utses att vara tillsynsmyndighet enligt direktivet.

Tillsynsmyndigheten ska enligt *artikel 42* vara fullständigt oberoende när den utför sina uppgifter och utövar sina befogenheter enligt direktivet. I artikeln utvecklas vilka krav som ska vara uppfyllda för att myndigheten ska anses vara oberoende.

De som ska leda tillsynsmyndigheten ska enligt *artikel 43* utses genom ett öppet förfarande av parlamentet, regeringen, statschefen eller ett oberoende organ. I artikeln anges också i vilka situationer de som ska leda myndigheten ska lämna sina uppdrag eller avsättas.

Enligt *artikel 44* ska inrättandet av myndigheten och regler och förfaranden för bl.a. tillsättning av dem som ska leda myndigheten föreskrivas i författning. Tillsynsmyndigheten och dess personal, inkluderande de som ska leda myndigheten, ska ha tystnadsplikt.

Tillsynsmyndighetens behörighet regleras i *artikel 45*. Tillsynsmyndigheten ska utföra de uppgifter och ha de behörigheter som framgår av direktivet. Tillsynen ska dock inte omfatta tillsyn över domstolarna i deras dömande verksamhet. Medlemsstaterna får undanta även andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet från tillsyn.

Tillsynsmyndighetens uppgifter räknas upp i *artikel 46*. Till uppgifterna hör bl.a. att övervaka tillämpningen av de bestämmelser som antas i enlighet med direktivet, att ge råd till lagstiftande organ i frågor som rör personuppgiftsbehandling, att på begäran ge registrerade information om hur de ska kunna utöva sina rättigheter enligt direktivet och att avgiftsfritt behandla klagomål från registrerade. Om en begäran är uppenbart ogrundad eller orimlig får dock tillsynsmyndigheten ta ut avgift eller vägra att tillmötesgå begäran.

Tillsynsmyndighetens befogenheter anges i *artikel 47*. Tillsynsmyndigheten ska ha rätt att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och få all information som myndigheten behöver för att kunna fullgöra sina uppgifter. Tillsynsmyndigheten ska vidare ha effektiva korrigerande befogenheter t.ex. att kunna varna den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar kan stå i strid med de bestämmelser som genomför direktivet och kunna beordra rättelse, radering eller begränsning av behandlingen eller förbjuda den. Tillsynsmyndigheten ska också ha rätt att anmäla överträdelser till rättsliga myndigheter.

De behöriga myndigheterna ska enligt *artikel 48* ha effektiva mekanismer för att rapportera överträdelser av direktivet.

Tillsynsmyndigheten ska enligt *artikel 49* upprätta en årlig rapport om sin verksamhet. Rapporten ska överlämnas till parlamentet, regeringen

och andra myndigheter som anges i nationell rätt. Den ska också göras tillgänglig för bl.a. allmänheten och kommissionen.

Tillsynsmyndigheterna ska enligt *artikel 50* utbyta information med och ge varandra ömsesidigt bistånd. Varje tillsynsmyndighet ska kunna besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och senast inom en månad och får bara vägra att tillmötesgå en begäran om myndigheten inte är behörig eller det skulle stå i strid med direktivet, unionsrätt eller nationell rätt. Kommissionen får genom genomförandeakter ange formerna för ömsesidigt bistånd.

I *artikel 51* anges vilka uppgifter den styrelse som inrättats genom dataskyddsförordningen ska ha när det gäller behandling av personuppgifter enligt direktivet.

Artiklarna 52–57: Rättsmedel, ansvar och sanktioner

Artikel 52 reglerar rätten för registrerade att lämna in klagomål över personuppgiftsbehandling till en tillsynsmyndighet. Har klagomålet lämnats till fel myndighet ska den utan dröjsmål överlämna klagomålet till rätt myndighet. Den registrerade ska underrättas om handläggningen av klagomålet och vad det resulterar i.

I *artikel 53* föreskrivs att en fysisk eller juridisk person har rätt till effektivt rättsmedel mot en tillsynsmyndighets beslut som är rättsligt bindande och avser dem. Detsamma gäller om tillsynsmyndigheten inte behandlat ett klagomål inom tre månader eller inte informerat den registrerade enligt artikel 52.

Rätten till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde regleras i *artikel 54*.

Enligt *artikel 55* ska den registrerade ha rätt att ge ett organ, en organisation eller en sammanslutning i uppdrag att ge in klagomål och att låta den utöva de rättigheter som anges i artiklarna 52–54 för hans eller hennes räkning.

Den som lidit skada till följd av olaglig behandling av personuppgifter eller någon annan åtgärd som står i strid med de bestämmelser som genomför direktivet ska enligt *artikel 56* ha rätt till ersättning från den personuppgiftsansvarige eller annan myndighet som är behörig enligt nationell rätt.

Artikel 57 ställer krav på att det finns sanktioner för överträdelser av de bestämmelser som genomför direktivet. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Artikel 58: Genomförandeakter

Artikel 58 reglerar kommissionens kommittéförfarande.

Artiklarna 59–65: Slutbestämmelser

Enligt *artikel 59* upphävs dataskyddsrambeslutet.

I *artikel 60* slås fast att direktivet inte påverkar särskilda bestämmelser om skydd av personuppgifter i gällande unionsrättsakter på området för straffrättsligt samarbete och polissamarbete och i *artikel 61* regleras förhållandet till tidigare ingångna avtal på området för straffrättsligt samarbete och polissamarbete.

Artikel 62 reglerar kommissionens skyldighet att senast sex år efter ikraftträdandet och därefter vart fjärde år utvärdera direktivet.

I *artikel 63* föreskrivs att medlemsstaterna ska ha införlivat direktivet senast den 6 maj 2018. Medlemsstaterna får dock i undantagsfall föreskriva att datasystem som inrättats före ikraftträdandet ska stå i överensstämmelse med bestämmelsen om loggning i direktivet senast den 6 maj 2023. Under exceptionella omständigheter kan tiden förlängas ytterligare i högst tre år.

Av *artikel 64* framgår att direktivet träder i kraft dagen efter att det har offentliggjorts i EU:s officiella tidning och enligt *artikel 65* riktar sig direktivet till medlemsstaterna.

6 En ny ramlag och dess tillämpningsområde

6.1 En ramlag för personuppgiftsbehandling vid brottsbekämpning, lagföring och straffverkställighet bör införas

6.1.1 En ny reglering behövs

Regeringens bedömning: Det behövs en ny reglering för att genomföra dataskyddsdirektivet i svensk rätt. Regleringen ska ha lagform.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna delar utredningens bedömning eller har inget att invända mot den.

Skälen för regeringens bedömning: 1995 års dataskyddsdirektiv – som upphör att gälla när dataskyddsförordningen börjar tillämpas – har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204). Personuppgiftslagen har gjorts generellt tillämplig, vilket innebär att den gäller även utanför EU-rättens tillämpningsområde och reglerar behandling av personuppgifter oavsett ändamålet med behandlingen. Lagen gäller således även för verksamheter som omfattas av det nya dataskyddsdirektivet.

Personuppgiftslagen är subsidiär i förhållande till andra lagar och förordningar. Inom flera områden finns det särregler i registerförfattningar som helt eller delvis ersätter personuppgiftslagen. Som framgår av avsnitt 4.2–4.4 utgår registerförfattningarna när det gäller brottsbekämpning, lagföring och straffverkställighet från bestämmelserna i personuppgiftslagen. Antingen gäller registerförfattningarna utöver personuppgiftslagen, och innehåller bara de bestämmelser som avviker från bestämmelserna i den lagen, eller så gäller de i stället för personuppgiftslagen men hänvisar till de bestämmelser i den lagen som ska tillämpas.

Det nya dataskyddsdirektivet ska vara genomfört i svensk rätt senast den 6 maj 2018. Personuppgiftslagen innehåller, tillsammans med myndigheternas registerförfattningar, bestämmelser som i stor utsträckning

motsvarar de krav på reglering som direktivet ställer. När dataskyddsförordningen börjar tillämpas den 25 maj 2018 kommer personuppgiftslagen och föreskrifter som har meddelats med stöd av den lagen att behöva upphävas. Det regelverk som ersätter personuppgiftslagen – dataskyddsförordningen och kompletterande nationella bestämmelser – kommer inte att vara anpassat till de särskilda förutsättningar som gäller för personuppgiftsbehandling inom brottsbekämpning, lagföring och straffverkställighet, eftersom sådan verksamhet är undantagen från förordningens tillämpningsområde. Det krävs därför en ny reglering för att genomföra direktivet. Direktivets bestämmelser är av den arten att regleringen lämpligen bör ha lagform (jfr Dataskydd vid europeiskt polissamarbete och straffrättsligt samarbete, prop. 2012/13:73, s. 58). Dessutom finns redan i dag de författningsbestämmelser som styr myndigheternas behandling av personuppgifter inom direktivets tillämpningsområde huvudsakligen i lag. Regeringen delar därför utredningens bedömning att den nya regleringen för att genomföra direktivet ska ha lagform.

6.1.2 En generellt tillämplig men subsidiär lag

Regeringens förslag: Dataskyddsdirektivet ska i huvudsak genomföras genom en ny lag som ska vara generellt tillämplig. Särregler i annan lag eller förordning ska dock gälla framför den nya lagen. Lagen ska benämnas brottsdatalagen.

Utredningens förslag överensstämmer med i sak med regeringens.

Remissinstanserna: De flesta remissinstanserna är positiva till utredningens förslag eller har inget att invända mot det. *Dataskydd.net* ifrågasätter dock nyttan med speciallagstiftningar om dataskyddsdirektivet genomförs med en generell reglering. *Förvaltningsrätten i Stockholm* framhåller att det är önskvärt att direktivet genomförs i registerförfattningar. *Domstolsverket* påpekar att det är önskvärt att subsidiaritetsbestämmelser i ramlagen och dataskyddslagen utformas på liknande sätt. *Sveriges advokatsamfund* efterfrågar en spärr för att förtydliga att möjligheten till subsidiaritet inte gäller i den mån avvikelsen åsidosätter direktivet.

Skälen för regeringens förslag

En generell reglering

I föregående avsnitt gör regeringen bedömningen att dataskyddsdirektivet ska genomföras genom en ny reglering i lag. Frågan är om det bör göras genom ändringar i befintlig lagstiftning, framför allt i berörda myndigheters registerförfattningar, eller genom att det införs en helt ny lag.

Den nuvarande regleringen av personuppgiftsbehandling på direktivets tillämpningsområde är komplex. Myndigheterna måste förhålla sig till flera olika författningar beroende på för vilket ändamål personuppgifterna behandlas. Som ett exempel kan nämnas att Polismyndigheten vid uppgiftsutbyte med en annan EU-medlemsstat kan behöva tillämpa inte bara personuppgiftslagen och polisdatalagen, utan också lagen om internationellt polisiärt samarbete eller 2013 års lag. Alternativet att genom-

föra direktivet genom ändringar i myndigheternas registerförfattningar skulle ha den fördelen att det skulle ge myndigheterna en mer sammanhållen reglering.

Det finns dock flera nackdelar med att placera den nya regleringen i de olika registerförfattningarna. En sådan är att registerförfattningarna skulle tyngas i onödan av bestämmelser som är desamma för flera av dem. En annan är att det skulle behöva införas nya registerförfattningar för de myndigheter som i dag inte har någon sådan utan enbart tillämpar personuppgiftslagen. Eftersom myndigheterna i dag inom direktivets tillämpningsområde antingen tillämpar personuppgiftslagen vid sidan av sin registerförfattning eller genom hänvisningar i registerförfattningen ändå tillämpar vissa bestämmelser i personuppgiftslagen, är det inget nytt för dem att förhålla sig till en ramlagstiftning som innehåller den generella regleringen. Regeringen instämmer därför till skillnad från *Dataskydd.net* och *Förvaltningsrätten i Stockholm* i utredningens förslag att så långt som möjligt skapa ett gemensamt regelverk för behandling av personuppgifter inom direktivets tillämpningsområde som kompletteras av registerförfattningar. Det bör därför införas en ny ramlagstiftning för brottsbekämpning, lagföring och straffverkställighet. Att den även bör gälla för upprätthållande av allmän ordning och säkerhet behandlas i avsnitt 6.4.3.

Lagen bör vara subsidiär

Ramlagen kommer att vara anpassad till skyldigheterna och kraven i direktivet. I utredningens uppdrag har ingått att anpassa myndigheternas registerförfattningar till ramlagen. Även andra författningar som innehåller bestämmelser om personuppgiftsbehandling på ramlagens tillämpningsområde måste ses över så att de, i den mån de innehåller bestämmelser som avviker från ramlagen, inte står i strid med direktivet.

Av artikel 18 framgår att det är tillåtet att i nationell rätt ha regler som avviker från direktivets bestämmelser om enskildas rätt till information och korrigeringsåtgärder om personuppgifterna ingår i domstolsbeslut, rättsliga protokoll eller ärenden som behandlas i samband med brottsutredningar och straffrättsliga förfaranden. Som utvecklas i avsnitt 10.2.2 finns det således inget som hindrar att reglerna om rätt till information vid förundersökning och andra straffrättsliga förfaranden har företräde framför ramlagens bestämmelser om information.

Mot den bakgrunden instämmer regeringen i utredningens förslag att ramlagen, på samma sätt som personuppgiftslagen, bör vara subsidiär i förhållande till bestämmelser i lag eller annan författning.

När det gäller subsidiaritetsbestämmelsens utformning ifrågasätter *Domstolsverket* om den föreslagna subsidiaritetsbestämmelsen är tillräcklig för att uppfylla kravet i artikel 18. Domstolsverket anser också att bestämmelsen i ramlagen ska utformas på liknande sätt som den utformas i dataskyddslagen på dataskyddsförordningens område. Regeringen anser att en allmän subsidiaritetsbestämmelse liknande den som i nuläget gäller i 2 § personuppgiftslagen är tillräcklig och konstaterar att övervägandena om utformningen gör sig gällande även på förordningens område. Mot denna bakgrund anser regeringen att utredningens förslag ska vara utgångspunkt för utformningen av subsidiaritetsbestämmelsen.

Ordalydelsen bör dock vara i enlighet med den som föreslås i den kommande dataskyddslagen (prop. 2017/18:105 s. 8).

I det lagstiftningsärendet efterfrågade Lagrådet ytterligare överväganden angående skälen för en ordning som innebär att föreskrifter i förordning ska gälla framför dataskyddslagens bestämmelser. Lagrådet påpekade vidare att detta innebär att räckvidden av den formella lagkraftens princip enligt 8 kap. 18 § regeringsformen begränsas (Ny dataskyddslag, prop. 2017/18:105 s. 331 f.).

I den propositionen anför regeringen att det på dataskyddsområdet är en väl etablerad ordning att även föreskrifter på förordningsnivå kan ges företräde framför den generella regleringen om skydd för personuppgifter. En förutsättning för detta är givetvis att föreskrifterna har beslutats med stöd av regeringens restkompetens eller med stöd av ett bemyndigande i lag.

Enligt regeringens bedömning kommer det även i fortsättningen finnas ett stort behov av både lagar och förordningar som innehåller bestämmelser som rör behandling av personuppgifter även på dataskyddsdirektivets tillämpningsområde. Mot denna bakgrund gör regeringen bedömningen att såväl lagar som förordningar som avviker från ramlagen bör ha företräde framför ramlagen, på motsvarande sätt som hittills har gällt i förhållande till personuppgiftslagen.

När personuppgiftslagen infördes övervägdes om det skulle införas en spärr som tydliggjorde att särregler i annan författning bara skulle gälla i den utsträckning de inte stred mot 1995 års dataskyddsdirektiv (Integritet, Offentlighet, Informationsteknik, SOU 1997:39, s. 210 f.). Datalagskommittén stannade dock för att inte föreslå någon sådan regel, eftersom man menade att det bara skulle skapa oro utan att medföra någon motsvarande nytta. *Sveriges advokatsamfund* har påtalat att en sådan spärr borde införas i ramlagen.

Befintlig lagstiftning har setts över genom utredningen och andra översyner på området. Utredningen har i likhet med Datalagskommittén bedömt att det inte finns behov av att föreslå någon generell spärr av det slag som diskuterades men förkastades i förarbetena till personuppgiftslagen. Regeringen delar denna uppfattning. När ny eller ändrad lagstiftning övervägs i framtiden måste det också säkerställas att det inte införs bestämmelser som står i strid med direktivet.

En delvis ändrad struktur

Som framgår av avsnitt 4.2 och 4.3 gäller bl.a. polisdatalagen, kustbevakningsdatalagen, åklagardatalagen och domstolsdatalagen i stället för personuppgiftslagen. Dessa författningar innehåller hänvisningar till de bestämmelser i personuppgiftslagen som är tillämpliga i myndigheternas verksamhet. När personuppgiftslagen ersätts av en ny ramlag som enbart ska gälla inom direktivets tillämpningsområde går det inte att ha en systematik där registerförfattningarna gäller i stället för ramlagen, eftersom utgångspunkten är att i princip alla bestämmelser i ramlagen kommer att vara tillämpliga i myndigheternas verksamhet. De uppräknade registerförfattningarna kommer därför att behöva anpassas till ramlagen på så sätt att de ska gälla utöver ramlagen och bara innehålla de bestämmelser som innebär undantag eller avvikelser från bestämmelserna i ramlagen.

De registerförfattningar som i dag gäller utöver personuppgiftslagen måste också anpassas så att de i stället ska gälla utöver ramlagen.

En konsekvens av den ändrade strukturen är att vissa bestämmelser som nu finns i registerförfattningarna bör flyttas till ramlagen, om de är av den arten att de bör gälla för all verksamhet inom direktivets tillämpningsområde. Som exempel kan nämnas regler om hur känsliga personuppgifter får behandlas (se avsnitt 8.1.4). Om det finns behov av särregler för de olika myndigheterna när det gäller hur känsliga personuppgifter får behandlas bör de finnas kvar i myndigheternas registerförfattningar. Förslag till de förändringar som behöver göras i myndigheternas registerförfattningar som en följd av ramlagen kommer att lämnas i en kommande proposition.

Lagens benämning

Ramlagen kommer som framgår av avsnitt 6.4 att tillämpas när behöriga myndigheter behandlar personuppgifter inom ramen för brottsbekämpning, lagföring och straffverkställighet och för att upprätthålla allmän ordning och säkerhet. Den kommer att tillämpas ofta och det kommer i stor utsträckning att hänvisas till den. Lagen bör därför ha ett så enkelt och tydligt namn som möjligt.

Ett namn som skulle kunna återspegla lagens huvudsakliga innehåll men ändå är förhållandevis kort är lagen om behandling av personuppgifter vid brottsbekämpning, lagföring och straffverkställighet. Namnet har dock ingen naturlig kortform eller förkortning som kan användas vid hänvisningar till den. Lagrådet kritiserade dessutom ett liknande förslag (lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet) när den nu gällande polisdatalagen granskades. Lagrådet ansåg att rubriken var alltför intetsägande (prop. 2009/10:85 s. 66 och 519). I förslaget till skattebrottsdatalag motiveras lagens namn med hänvisning till nyss nämnda lagrådsyttrande (prop. 2016/17:89 s. 48).

De registerförfattningar som har införts på direktivets tillämpningsområde de senaste åren har alla ordet datalag i namnet, t.ex. polisdatalagen, åklagardatalagen, domstolsdatalagen och tullbrottsdatalagen. Ett alternativ är därför, som utredningen föreslår, att benämna ramlagen brottsdatalagen. Det är ett kort namn som det är lätt att hänvisa till och som skulle kunna förkortas BDL.

Nackdelen med benämningen brottsdatalag är att det inte framgår att lagen gäller för behandling av personuppgifter vid straffverkställighet. Straffverkställighet handlar dock om att verkställa en påföljd för brott eller särskild rättsverkan av brott. Den tydliga kopplingen mellan straffverkställighet och brott gör att namnet inte är missvisande. I avsnitt 6.4.3 föreslår regeringen att lagen även ska omfatta behandling av personuppgifter i syfte att upprätthålla allmän ordning och säkerhet. Det täcks inte av benämningen brottsdatalag. Fördelarna med ett kort namn som det är lätt att hänvisa till uppväger dock nackdelen att det inte uttömmande anger lagens tillämpningsområde. Lagen bör därför benämnas brottsdatalagen.

Direktivet innehåller i vissa artiklar mycket detaljerade regler i fråga om exempelvis dokumentations- och underrättelseskyldighet. Sådana detaljregler bör inte tas in i lagen utan regleras i förordning. Regeringen delar utredningens bedömning att det är nödvändigt att komplettera brottsdatalagen med en förordning för att genomföra direktivet i dess helhet.

6.1.3 Ramlagens syfte

Regeringens förslag: Syftet med ramlagen ska vara dels att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter, dels att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* anser att det inte med tillräcklig tydlighet framgår att den nya ramlagen även ska syfta till att värna en effektiv och rättssäker informationshantering för brottsbekämpningen. *Datainspektionen* anser att det bör tydliggöras att ett syfte särskilt ska vara att skydda fysiska personers personliga integritet vid behandling av personuppgifter.

Skälen för regeringens förslag: Av artikel 1.2 framgår att det nya dataskyddsdirektivet har dubbla syften. Regleringen ska skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Samtidigt ska den säkerställa att behöriga myndigheters utbyte av personuppgifter inom unionen, när sådant utbyte krävs enligt unionsrätten eller nationell rätt, varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

I registerförfattningar förekommer ibland bestämmelser som anger lagens övergripande syfte. I exempelvis 1 kap. 1 § polisdatalagen anges det övergripande syftet med lagen vara att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Bestämmelser om syftet med en reglering saknar normalt egentligt materiellt innehåll. Man kan därför fråga sig om det behövs en sådan bestämmelse i ramlagen. Det har emellertid inte enbart en symbolisk eller informativ betydelse att uttryckligen slå fast lagens syfte. Att en lags syfte uttryckligen anges kan få relevans i rättstillämpningen genom att det ger vägledning för tolkningen av de materiella bestämmelserna i lagen (Myndighetsdatalag, SOU 2015:39, s. 220).

Det finns därför skäl att införa en bestämmelse om lagens syfte så att det tydligt framgår att regleringen har dubbla syften. Att fysiska personers grundläggande rättigheter och friheter ska skyddas vid behandling av personuppgifter är en central målsättning för regleringen. Samtidigt är vissa intrång i den personliga integriteten nödvändiga för att myndigheterna ska kunna utföra sina uppgifter och för att brottsoffer ska kunna få sin rätt tillgodosedd. Olika intressen ställs alltså mot varandra. En brottsutredning eller brottmålsrättegång innehåller ofta personuppgifter om

såväl brottsoffer, misstänkta och vittnen som tjänstemän som deltar i verksamheten. Regleringen bör därför ge uttryck för en väl avvägd balans mellan, å ena sidan, skyddet för den personliga integriteten, och, å andra sidan, samhällets behov av att myndigheter kan behandla personuppgifter i den verksamhet som omfattas av direktivets tillämpningsområde. Regeringen delar till skillnad från *Polismyndigheten* och *Datainspektionen* utredningens bedömning att den dubbla målsättningen och balansen mellan de olika intressena bäst tillgodoses och uttrycks genom en bestämmelse som föreskriver att lagens syfte är att skydda fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att samtidigt säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra.

I lagrådsremissens förslag till reglering angavs ”att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter” som ett syfte. Mot bakgrund av hur direktivet är utformat och för att tydliggöra att det är fråga om rättigheter och friheter i direktivets mening förordar *Lagrådet* att uttrycket ”fri- och rättigheter” där det förekommer i lagtexten ersätts med ”rättigheter och friheter”. Regeringen håller med Lagrådet om att en sådan formulering förtydligar att det rör sig om rättigheter och friheter i direktivets mening och ändrar därför till den lydelsen även på övriga ställen där uttrycket förekommer.

6.1.4 2013 års lag bör upphävas

Regeringens förslag: Lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen och vissa hänvisningar till den lagen ska upphävas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller har inga synpunkter på det.

Skälen för regeringens förslag: Enligt artikel 59 ska dataskyddsrambeslutet upphöra att gälla samma dag som medlemsstaterna ska ha införlivat direktivet i nationell rätt.

Rambeslutet bygger i huvudsak på 1995 års dataskyddsdirektiv. Eftersom Sverige i princip genomförde det direktivet även inom de sektorer som rambeslutet reglerar fanns det redan i stor utsträckning bestämmelser som motsvarade artiklarna i rambeslutet i personuppgiftslagen och i myndigheternas registerförfattningar när rambeslutet skulle genomföras. De återstående delarna av rambeslutet genomfördes i 2013 års lag. Lagen tillämpas framför allt när uppgifter överförs från eller till en annan EU-medlemsstat, Island, Norge, Schweiz eller Liechtenstein i verksamheter som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder. I den mån motsvarande bestämmelser behövs för att genomföra direktivet bör dessa tas in i ramlagen så att regleringen blir så sammanhållen som möjligt. Regeringen delar därför utredningens bedömning att 2013 års lag ska upphävas. Därmed bör också alla de bestämmelser som hänvisar till den lagen upphävas. Sådana hänvisningar finns dels i myndigheternas

registerförfattningar, dels i vissa författningar som reglerar enskilda register eller annan personuppgiftsbehandling inom rambeslutets tillämpningsområde. Hänvisningarna i de lagar som inte är registerförfattningar och i domstolsdatalagen behandlas i denna proposition. Hänvisningarna i övriga registerförfattningar kommer att ses över i samband med anpassningen av dem.

6.2 Definitioner

Regeringens förslag: Vissa uttryck som används i ramlagen ska definieras.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser är positiva till eller har inte några invändningar mot förslaget. *Förvaltningsrätten i Stockholm* anser att uttrycket register bör definieras. *Dataskydd.net* anser att uttrycken profilering och pseudonymisering bör definieras samt att utredningens definition av biometriska uppgifter bör ändras. *Rättsmedicinalverket* belyser vikten av att det blir en tydlig och ändamålsenlig reglering av hanteringen av uppgifter om avlidna.

Skälen för regeringens förslag

Definitionerna bör ligga så nära direktivets definitioner som möjligt

I artikel 3 definieras vissa uttryck som är av grundläggande betydelse för förståelsen av bestämmelserna i direktivet. Definitionerna överensstämmer i allt väsentligt med definitionerna i artikel 4 i dataskyddsförordningen. Som framgår av avsnitt 6.4.4 kommer de myndigheter som är behöriga i ramlagens mening att också tillämpa förordningen i delar av sin verksamhet. För att underlätta tillämpningen finns det därför, som utredningen föreslår, skäl att i så stor utsträckning som möjligt använda direktivets terminologi så att definitionerna i ramlagen och förordningen blir så lika som möjligt. Det innebär att motsvarande definitioner i personuppgiftslagen inte bör användas i den mån de avviker från direktivets terminologi, trots att de har tillämpats under lång tid och stämmer bättre överens med terminologin i svensk lagstiftning.

I artikel 3.3 finns en definition av uttrycket ”begränsning av behandling”. Som framgår av avsnitt 10.4.3 stämmer direktivets definition inte överens med vad som får antas vara avsikten med åtgärden. En definition i enlighet med direktivets lydelse blir därför missvisande och en definition i enlighet med syftet blir innehållslös. Regeringen delar därför utredningens bedömning att begränsning av behandling inte bör definieras i ramlagen.

Både 1995 års dataskyddsdirektiv och det nya dataskyddsdirektivet innehåller en definition av uttrycket register. När 1995 års dataskyddsdirektiv genomfördes ville man komma bort från registerbegreppet som redan då ansågs otidsenligt (prop. 1997/98:44 s. 39). Någon definition av register infördes därför inte i personuppgiftslagen. Definitionen i direktivet användes i stället för att avgränsa lagens tillämpningsområde genom att det i 5 § anges att lagen även gäller för manuell behandling av person-

uppgifter om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Som framgår av avsnitt 6.4.5 instämmer regeringen i utredningens bedömning att tillämpningsområdet för ramlagen nu ska anges på samma sätt. Ordet register förekommer inte i den föreslagna lagen. Därför anser regeringen till skillnad från *Förvaltningsrätten i Stockholm* att det inte finns anledning att definiera uttrycket register.

I direktivet definieras vidare profilering och pseudonymisering, uttryck som enligt *Dataskydd.net* bör definieras även i ramlagen. Profilering nämns i artikel 11 som ett exempel på beslut som grundas enbart på automatiserad behandling. I artikel 24.1 e anges att det register som den personuppgiftsansvarige ska föra över personuppgiftsbehandling i tillämpliga fall ska innehålla uppgifter om användningen av profilering. Pseudonymisering nämns i artikel 20 som ett exempel på säkerhetsåtgärder som bör vidtas. I likhet med utredningen anser regeringen inte att termerna bör användas i ramlagen och några definitioner av dem behövs därför inte.

Nedan följer en redogörelse för ett antal centrala definitioner som bör finnas i ramlagen. Ytterligare uttryck som föreslås definieras i ramlagen kommer att behandlas i anslutning till de delar av direktivet de hänför sig till.

Behandling av personuppgifter

Behandling definieras i artikel 3.2. Direktivets definition skiljer sig något i fråga om uppräkningen av exempel på behandling jämfört med 1995 års dataskyddsdirektiv och 3 § personuppgiftslagen. Definitionen i ramlagen bör, som utredningen föreslår, nära ansluta till direktivets text. Behandling av personuppgifter bör därför definieras som en åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.

Biometriska uppgifter

Varken 1995 års dataskyddsdirektiv eller personuppgiftslagen innehåller någon definition av biometriska uppgifter. Inte heller i andra författningar finns det någon sådan definition, men uttrycket biometriska data används i bl.a. passlagen (1978:302) och utlänningslagen (2005:716). Enligt artikel 3.13 avses med biometriska uppgifter personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av personen, som ansiktsbilder eller fingeravtrycksuppgifter. Biometriska uppgifter räknas upp i artikel 10 som en särskild kategori av personuppgifter som bara får behandlas under vissa förutsättningar (se avsnitt 8.1.4). Definitionen av vad som avses med biometriska uppgifter får därmed betydelse för i vilken utsträckning sådana uppgifter får behandlas.

Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras (jfr prop. 2008/09:132 s. 6 f.). När det gäller pass är det framför allt mönster av fingeravtryck, ansiktsgeometri och ögats iris som används, men även regnbågshinna, näthinna, röst, hand, blodkärl, dna eller gång går att använda. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Dessa uppgifter kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet.

I direktivets definition av biometriska uppgifter anges ansiktsbilder som ett exempel på sådana uppgifter. Det kan leda tanken till att vanliga fotografier och filmer skulle omfattas av definitionen. Om de inte bearbetas tekniskt genom en särskild metod som syftar till identifiering faller de utanför definitionen. Om de däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen. Här kan även anmärkas att de personuppgifter, t.ex. fingeravtryck, som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska uppgifter inte i sig utgör biometriska uppgifter.

Ramlagen bör innehålla en definition av uttrycket biometriska uppgifter. *Dataskydd.net* anser till skillnad från utredningen att en definition inte ska begränsas till uppgifter som tagits fram genom särskild teknisk behandling. Regeringen delar dock utredningens uppfattning att direktivets definition ska vara utgångspunkt för definitionen i ramlagen. Till skillnad från direktivets definition bör den dock inte innehålla några exempel på sådana uppgifter, eftersom det kan leda till felaktiga slutsatser om vad som omfattas. Biometriska uppgifter ska därför definieras som personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.

Genetiska uppgifter

Genetiska uppgifter definieras inte i 1995 års dataskyddsdirektiv eller i personuppgiftslagen. Med genetiska uppgifter avses enligt artikel 3.12 alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om personens fysiologi eller hälsa och som framför allt härrör från en analys av ett biologiskt prov från personen i fråga. I skäl 23 anges att det är kromosom-, dna- och rna-analyser eller andra analyser som gör det möjligt att inhämta sådan information som avses.

Genetiska uppgifter räknas upp i artikel 10 som en särskild kategori av personuppgifter som bara får behandlas under vissa förutsättningar (se avsnitt 8.1.4). Definitionen av vad som avses med genetiska uppgifter får därmed betydelse för i vilken utsträckning uppgifter som tas fram vid analys av prover från människokroppen får behandlas.

I direktivets definition nämns information om fysiologi eller hälsa. Det går dock även att få fram annan information genom analys av ett sådant

biologiskt prov, exempelvis information om en persons biogeografiska ursprung. I framtiden kommer man troligen att kunna ta fram ytterligare uppgifter ur sådana prover.

Mot den bakgrunden har utredningen ansett att all information som rör nedärvda eller förvärvade genetiska kännetecken för en person och som kan tas fram ur ett prov från människokroppen bör anses vara genetiska uppgifter. Det bör också gälla information som på motsvarande sätt kan tas fram ur spår som påträffas på en brottsplats, exempelvis blodspår. Regeringen delar denna bedömning och att det bör framgå av definitionen i lagen. Det innebär att definitionen av genetiska uppgifter i ramlagen blir något vidare än den i dataskyddsförordningen, men i likhet med utredningen anser regeringen inte att detta bör orsaka några problem i praktiken. Detta har heller inte ifrågasatts av någon remissinstans.

Genetiska uppgifter bör således definieras som personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen.

Mottagare

Enligt artikel 3.10 omfattar uttrycket mottagare i princip samtliga personer, myndigheter eller andra organ till vilka personuppgifter lämnas ut. Myndigheter som får del av personuppgifter för att kunna utföra ett särskilt uppdrag ska dock inte anses som mottagare. I skäl 22 anges som exempel på myndigheter som får del av personuppgifter för att utföra särskilda uppdrag, skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering av värdepappersmarknader.

I 3 § personuppgiftslagen, som genomför artikel 2 g i 1995 års dataskyddsdirektiv, anges att en myndighet inte ska anses som mottagare när personuppgifter lämnas ut till myndigheten för att den ska kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta. Vilka myndighetsuppdrag som åsyftas kommenteras inte i förarbetena, utan där anges endast att definitionen av mottagare är avsedd att ha samma innebörd som motsvarande uttryck i direktivet (prop. 1997/98:44 s. 116). En motsvarande definition behövs i ramlagen.

Mottagare bör, i likhet med vad utredningen föreslår, definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.

Personuppgift

Med personuppgift avses enligt både 1995 års dataskyddsdirektiv och det nya direktivet varje upplysning som avser en fysisk person som är identifierad eller som direkt eller indirekt kan identifieras. I definitionen i artikel 3.1 exemplifieras personuppgifter som upplysningar om namn, identifikationsnummer, lokaliseringsuppgift eller onlineidentifikatorer eller faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Det framgår inte uttryckligen av direktivet om det gäller för uppgifter om avlidna personer eller inte. Definitionen av personuppgift omfattar enligt sin ordalydelse även uppgifter om avlidna personer. Definitionen är densamma som i artikel 4.1 i dataskyddsförordningen. I skäl 27 i för-

ordningen anges emellertid att den inte gäller för behandling av personuppgifter om avlidna personer, men att medlemsstaterna får fastställa bestämmelser för behandlingen av sådana personuppgifter. Det kan inte ha varit avsikten att behandling av uppgifter om avlidna skulle omfattas av direktivet men inte av förordningen när definitionerna av personuppgift i princip är identiska. Regeringen betraktar det i likhet med utredningen som ett rent förbiseende att inte motsvarande skäl finns i direktivet. För att tydliggöra att personuppgift har samma betydelse som i förordningen bör det framgå av definitionen att den inte omfattar uppgifter om avlidna personer. *Rättsmedicinalverket* påtalar särskilt vikten av att det blir en tydlig och ändamålsenlig reglering av hanteringen av uppgifter om avlidna. Denna synpunkt kommer att tas om hand i samband med att speciallagstiftningen som verket tillämpar ses över.

Personuppgifter bör alltså definieras som varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.

Registrerad

I direktivets definition av personuppgift i artikel 3.1 anges att en identifierad eller identifierbar fysisk person benämns registrerad. Definitionen av personuppgift är utformad på samma sätt i 1995 års dataskyddsdirektiv. I 3 § personuppgiftslagen definieras däremot den registrerade som den som en personuppgift avser.

Utredningen har bedömt att det blir tydligare att definiera vad som avses med en registrerad än att låta det ingå som en del av definitionen av personuppgift. Regeringen delar den bedömningen och anser att registrerad därför bör definieras som den fysiska person som personuppgiften rör. Det blir då en skillnad i förhållande till dataskyddsförordningen men det saknar praktisk betydelse.

Uppgift som rör hälsa

Varken 1995 års dataskyddsdirektiv eller personuppgiftslagen definierar vad som avses med uppgift som rör hälsa. Enligt artikel 3.14 avses personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus. I skäl 24 anges att det gäller information om en persons tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Där ges också exempel på vilka uppgifter som kan anses avse hälsa. Som utredningen föreslår bör ramlagen innehålla en definition av vad som avses med uppgift som rör hälsa som motsvarar definitionen i direktivet. Uppgift som rör hälsa bör definieras som personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

Uppgifter om hälsa räknas upp i artikel 10 som en särskild kategori av personuppgifter som bara får behandlas under vissa förutsättningar (se avsnitt 8.1.4).

6.3 Dataskyddsbestämmelser i tidigare rättsakter och avtal

Regeringens bedömning: Det behövs inte någon särskild reglering för att genomföra artiklarna 60 och 61 i direktivet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* efterfrågar ett klargörande om hur unionsrättsakter som trätt i kraft efter den 6 maj 2016 förhåller sig till direktivet och ramlagen.

Skälen för regeringens bedömning

Innehållet i direktivet och nuvarande reglering

Enligt artikel 60 ska direktivet inte påverka tillämpningen av särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som trädde i kraft den 6 maj 2016 eller tidigare. En förutsättning är dock att rättsakterna reglerar behandlingen av personuppgifter mellan medlemsstaterna eller medlemsstaternas tillgång till informationssystem som är relevanta för direktivets tillämpningsområde. Kommissionen ska enligt artikel 62.6 se över om tidigare rättsakter behöver anpassas till direktivet och, om så behövs, lägga fram förslag till ändring av dessa rättsakter. De tidigare rättsakterna på området ska alltså fortsätta att gälla tills de ändras eller upphävs.

Som exempel på tidigare rättsakter som ska kvarstå oförändrade nämns i skäl 94 rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet) och konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (rådets akt av den 29 maj 2000).

Enligt artikel 61 ska internationella avtal som rör överföring av personuppgifter till tredjeland eller internationella organisationer och som ingicks av medlemsstaterna före den 6 maj 2016 fortsätta att gälla tills de ändras, ersätts eller återkallas. En förutsättning är dock att avtalen är förenliga med unionsrätten så som den tillämpades före angivet datum.

En liknande bestämmelse finns i artikel 26 i dataskyddsrambeslutet. Enligt den ska rambeslutet inte påverka medlemsstaternas eller unionens skyldigheter och åtaganden enligt de bilaterala och/eller multilaterala avtalen med tredjeland som redan gällde när rambeslutet antogs. Artikel 26 ansågs inte kräva någon lagstiftningsåtgärd (prop. 2012/13:73 s. 108).

Bestämmelser om skydd för personuppgifter i tidigare rättsakter

Det finns en rad unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som innehåller bestämmelser om skydd av personuppgifter. Sådana bestämmelser ska alltså gälla i stället för direktivet om de är äldre än det. På motsvarande sätt bör sådana svenska lagar och förordningar som genomför de tidigare antagna unionsrättsakterna ges företräde framför ramlagen. En genomgång av äldre rättsakter som trätt i kraft före direktivet och som därmed gäller i stället för direktivet redovisas i delbetänkandet Brottsdatalag (SOU 2017:29, s. 155 f.).

En unionsrättsakt av intresse i sammanhanget är Europolförordningen (Europaparlamentets och rådets förordning [EU] 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning [Europol] och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF). Förordningen ska, med något undantag, tillämpas från och med den 1 maj 2017. Den antogs den 11 maj 2016 och trädde i kraft 20 dagar efter att den hade offentliggjorts i Europeiska unionens officiella tidning, vilket gjordes den 24 maj 2016. Förordningen har alltså trätt i kraft efter den 6 maj 2016 och omfattas därför inte av artikel 60. Förordningen innehåller bestämmelser om behandling av personuppgifter, men som *Datainspektionen* påpekar är det oklart hur den förhåller sig till direktivet. Hur olika EU-rättsakter förhåller sig till varandra är inte en fråga för medlemsstaterna utan något som får avgöras av allmänna EU-rättsliga principer.

Avtal om överföring till tredjeland och internationella organisationer

Som framgått ovan ska internationella avtal som rör överföring av personuppgifter till tredjeland och internationella organisationer och som ingåtts före den 6 maj 2016 fortsätta att gälla. Med internationella avtal bör i detta sammanhang förstås varje gällande bilateralt eller multilateralt avtal mellan medlemsstater och tredjeland eller med internationella organisationer inom området för straffrättsligt samarbete och polissamarbete som rör överföring av personuppgifter.

Som exempel på bilateralt avtal om informationsutbyte som Sverige ingått med tredjeland kan nämnas avtalet med Thailand om samarbete mellan brottsbekämpande myndigheter för att bekämpa organiserad brottslighet (SÖ 2013:3). Avtalet innehåller till viss del bestämmelser om dataskydd, som hänvisar till internationella överenskommelser. Avtalet med Bosnien och Hercegovinas ministerråd om samarbete mellan brottsbekämpande myndigheter (SÖ 2013:4) innehåller liknande bestämmelser.

Sverige har även ingått ett flertal bilaterala avtal när det gäller informationsutbyte på tullområdet, t.ex. med USA och Ryssland. Avtalet med USA är genomfört i förordningen (1988:146) om tillämpning av en överenskommelse mellan Sverige och Amerikas Förenta Stater om ömsesidigt bistånd i tullfrågor. Avtalet med Ryssland regleras i förordningen (1994:8) om tillämpning av en överenskommelse mellan Sverige och Ryska federationen om ömsesidigt bistånd i tullfrågor och förordningen (1998:318) om tillämpning av ett avtal mellan Sverige och Ryssland om ömsesidigt bistånd vid bekämpning av vissa fiskala brott.

Det behövs inte någon särskild reglering för att genomföra artiklarna 60 och 61 i direktivet

Av artiklarna 60 och 61 följer att särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området och internationella avtal som rör överföring av personuppgifter till tredjeland och internationella organisationer som medlemsstaterna ingått innan direktivet antogs ska tillämpas framför direktivet och gälla tills de ändras eller upphävs. Det är alltså inte fråga om någon tillfällig eller övergående reglering, utan en

inskränkning i direktivets tillämpningsområde. De tidigare unionsrättsakter och avtal som Sverige ingått med tredjeland har i allt väsentligt genomförts i svensk rätt. I den mån sådana lagar och förordningar reglerar dataskydd på ramlagens tillämpningsområde bör de, i likhet med vad utredningen föreslår, gälla framför ramlagen.

I avsnitt 6.1.2 föreslås att ramlagen ska vara subsidiär. Där diskuteras framför allt förhållandet mellan ramlagen och myndigheternas registerförfattningar, men resonemanget gör sig gällande även här. Mot den bakgrunden delar regeringen utredningens bedömning att några särskilda bestämmelser som genomför artiklarna 60 och 61 inte behövs.

6.4 Utformningen av tillämpningsområdet

6.4.1 Personuppgiftsbehandling som behöriga myndigheter utför för vissa syften

Regeringens förslag: Ramlagens tillämpningsområde ska knytas till behandling av personuppgifter som behöriga myndigheter utför för vissa syften.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna är positiva till utredningens förslag eller har inget att invända mot det. Flera remissinstanser påtalar emellertid svårigheterna med gränsdragning i förhållande till dataskyddsförordningens tillämpningsområde (se närmare avsnitt 6.7).

Skälen för regeringens förslag: Direktivet ska enligt artikel 2.1 tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Personuppgiftsbehandling inom direktivets tillämpningsområde är enligt artikel 2.2 d i dataskyddsförordningen undantagen från förordningens tillämpningsområde. Eftersom förordningen är direkt tillämplig i svensk rätt och gäller för all personuppgiftsbehandling som regleras av unionsrätt och inte omfattas av direktivet är avgränsningen av ramlagens tillämpningsområde en central fråga.

Direktivet gäller för all personuppgiftsbehandling inom sitt tillämpningsområde, även om den är helt nationell. Det är en betydande skillnad i förhållande till dataskyddsrambeslutet, som bara gäller för behandling av personuppgifter inom ramen för polisiärt och straffrättsligt samarbete när personuppgifter överförs eller görs tillgängliga mellan EU-medlemsstater, Island, Liechtenstein, Norge och Schweiz och EU-organ och EU:s informationssystem. I övrigt är tillämpningsområdet för direktivet och rambeslutet angivet på i stort sett samma sätt – båda omfattar behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Direktivets tillämpningsområde omfattar också personuppgiftsbehandling i syfte att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Det väcker frågan om regleringen i ramlagen kan utgå från hur tillämpningsområdet är utformat i 2013 års lag.

Tillämpningsområdet för 2013 års lag bygger på i vilken verksamhet personuppgifter behandlas. En sådan lösning är enkel och tydlig för tillämparen. Som nyss nämnts bygger direktivets tillämpningsområde på dels syftet med behandlingen, dels om det är en behörig myndighet som utför den. Att enbart knyta ramlagens tillämpningsområde till i vilken verksamhet personuppgiftsbehandling utförs skulle därför, som utredningen anför, göra det för vidsträckt. Som exempel kan nämnas att man i Kriminalvårdens häktesverksamhet behandlar personuppgifter både om personer som är frihetsberövade på grund av brottsutredning, lagföring och straffverkställighet och personer som är föremål för olika administrativa frihetsberövanden, t.ex. tvångsvård eller häktning enligt konkurslagen (1987:672). Om syftet med förvaringen i häkte är brottsbekämpning, lagföring, straffverkställighet eller ordningshållning ligger det under direktivets tillämpningsområde. Är det däremot fråga om ett frihetsberövande av något annat slag gäller som regel dataskyddsförordningen.

Tillämpningsområdet kan dock inte heller knytas enbart till syftet med personuppgiftsbehandlingen. Kameraövervakning kan tas som exempel för att illustrera det. Fast monterade kameror får sättas upp i exempelvis banklokaler och butikslokaler, om syftet med övervakningen ska vara att förebygga, avslöja eller utreda brott. Bankens eller butikens personuppgiftsbehandling i samband med sådan övervakning skulle därmed omfattas av ramlagens tillämpningsområde om enbart syftet med behandlingen var avgörande. I och med att banker och butiker inte träffas av direktivets definition av behörig myndighet ligger deras personuppgiftsbehandling dock utanför tillämpningsområdet. En annan sak är att Polismyndighetens behandling av de personuppgifter som har samlats in av en bank vid exempelvis ett rån omfattas av tillämpningsområdet, eftersom myndigheten omfattas av definitionen av behörig myndighet och syftet med behandlingen är att utreda brott.

Regeringen instämmer därför i utredningens slutsats att ramlagens tillämpningsområde måste knytas både till vilket syfte behandlingen av personuppgifter har och till att det är en behörig myndighet som utför behandlingen. Om en behörig myndighet behandlar personuppgifter för något av de syften som anges i ramlagen är lagen tillämplig, oavsett om behandlingen endast utförs i ringa omfattning eller under kort tid. Innan frågan om vad som är en behörig myndighet (se avsnitt 6.4.4) behandlas är det nödvändigt att först redovisa för vilka syften personuppgifter får behandlas. I avsnitt 6.7 diskuteras sedan olika gränsdragningsfrågor knutna till uttrycket behörig myndighet och syftena med behandlingen.

6.4.2 Personuppgiftsbehandling som rör brottsbekämpning, lagföring och straffverkställighet

Regeringens förslag: Ramlagen ska gälla vid behandling av personuppgifter som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens förslag: Direktivets tillämpningsområde omfattar personuppgiftsbehandling som utförs i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

I svensk rätt brukar man skilja mellan å ena sidan verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet och å andra sidan verksamhet som syftar till att utreda och beivra konkreta brott (se t.ex. 2 § polislagen [1984:387] och 2 kap. 7 § polisdatalagen). Vid genomförandet av unionsrättsakter där det talas om att förebygga och utreda brott har ordet brott därför tolkats så att det omfattar såväl konkreta brott som sådan icke-preciserad brottslig verksamhet som exempelvis underrättelseverksamhet tar sikte på (prop. 2010/11:129 s. 110 och prop. 2012/13:73 s. 63). Samma tolkning bör göras nu.

Uttrycket förebygga, förhindra och upptäcka brottslig verksamhet – som används i flera av de berörda myndigheternas registerförfattningar – bör ges samma tolkning som hittills. I förarbetena till polisdatalagen diskuteras underrättelseverksamheten ingående (prop. 2009/10:85 s. 104 f.). Där vidgas också användningen av begreppet till att avse vad som där betecknas som underrättelsestyrd verksamhet. All sådan verksamhet, såväl på lokal nivå som regional och central nivå, och även annan planlagd verksamhet som betecknas som underrättelsestyrd bör således omfattas av ramlagens tillämpningsområde.

Spaningsverksamhet som inte är hänförlig till brottsutredande verksamhet är normalt underrättelsestyrd, exempelvis när spaning bedrivs lokalt för att kartlägga droghandel, prostitution eller någon annan typ av lokal brottslighet. Spaningsverksamhet av nu aktuellt slag bedrivs framför allt av Polismyndigheten och bör omfattas av tillämpningsområdet.

Polismyndigheten bedriver emellertid även annan verksamhet som brukar räknas till brottsförebyggande arbete, t.ex. förebyggande insatser som riktar sig till brottsoffer eller personer som riskerar att utsättas för brott. I sådant arbete torde behovet av att behandla personuppgifter vara begränsat. Det kan diskuteras om sådan brottsofferverksamhet som har anknytning till pågående eller avslutade brottsutredningar, t.ex. uppföljning av meddelade kontaktförbud eller personskydd som beviljats med anledning av begångna brott, bör hänföras till uppgiften att utreda brott eller ses som brottsförebyggande arbete. Det saknar dock betydelse i detta sammanhang eftersom det i båda fallen är en uppgift som omfattas av ramlagens tillämpningsområde. Även behandlingen av personuppgifter vid Polismyndighetens kommunikationscentraler har i viss utsträckning ansetts falla under polisdatalagens tillämpningsområde och bör därmed omfattas av ramlagens tillämpningsområde (prop. 2009/10:85 s. 140 f.).

Tullverket bedriver brottsförebyggande arbete som rör framför allt otillåten införsel av varor. Även den verksamheten, som innefattar bl.a. underrättelseverksamhet och sådan kartläggning och spaning som nyss nämnts, ligger inom ramlagens tillämpningsområde.

I förarbetena till 2013 års lag anses uttrycken upptäcka och beivra brott stämma bättre överens med språkbruket i svensk rätt än uttrycken avslöja och lagföra brott (prop. 2012/13:73 s. 63). Utredningen har ansett att den bedömningen bör gälla avseende uttrycket upptäcka brott men att ut-

trycket lagföra brott bör användas i ramlagen i stället för beivra brott av följande skäl.

Uttrycket utreda och beivra brott används i 2 kap. 7 § polisdatalagen, 3 kap. 2 § kustbevakningsdatalagen och 2 kap. 5 § åklagardatalagen. Samma uttryck används också i 2 kap. 5 § tullbrottsdatalagen. Utreda brott omfattar framför allt arbete som utförs inom ramen för en förundersökning enligt 23 kap. rättegångsbalken, medan förenklade förfaranden som mynnar ut i att strafföreläggande eller föreläggande av ordningsbot utfärdas i stället för att åtal väcks hänförs till beivra brott. Uttrycket beivra brott passar därför väl för Polismyndighetens, Tullverkets, Kustbevakningens och åklagares verksamhet, men mindre väl för handläggningen vid de allmänna domstolarna när de dömer någon till ansvar för brott och bestämmer påföljd. Däremot täcker uttrycket lagföra brott, som används i direktivet, såväl de förenklade förfaranden som Polismyndigheten, Tullverket, Kustbevakningen och åklagare tillämpar som handläggningen i domstol. Ordet lagföra framstår också som mer modernt än beivra. Regeringen instämmer i utredningens bedömning och anser därför att det mer vittomfattande uttrycket lagföra brott bör väljas i ramlagen. Frågan om även myndigheternas registerförfattningar bör ändras på motsvarande sätt kommer att behandlas när anpassningar av dessa görs.

Uttrycket verkställa påföljd används i dag inte i någon av de berörda myndigheternas registerförfattningar. Däremot används det i 2013 års lag. I förarbetena till den lagen anges att regleringen omfattar bl.a. Kriminalvården och Statens institutionsstyrelse (prop. 2012/13:73 s. 61 f.). Regeringen delar utredningens uppfattning även i denna del och anser att terminologin i 2013 års lag framstår som lämplig och bör användas även i ramlagen.

Ramlagen bör således gälla vid personuppgiftsbehandling som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Det innebär att lagen kan bli tillämplig vid underrättelseverksamhet och annan brottsförebyggande verksamhet, förundersökning och liknande utredningar som hänvisar till reglerna om förundersökning, åtalsprövning, strafföreläggande och föreläggande av ordningsbot, domstols handläggning av brottmål och verkställighet av påföljder. Det är dock inte tillräckligt att personuppgiftsbehandlingen utförs i något av dessa syften. Det krävs också att det är en behörig myndighet som utför den, vilket utvecklas i avsnitt 6.4.4.

6.4.3 Personuppgiftsbehandling som rör allmän ordning och säkerhet

Regeringens förslag: Ramlagen ska gälla vid behandling av personuppgifter som utförs i syfte att upprätthålla allmän ordning och säkerhet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* förespråkar att uttrycket ”övervaka allmän ordning och säkerhet” bör användas i stället för ”upprätt-

hålla allmän ordning och säkerhet". *Kriminalvården* anser att upprätthålla allmän ordning och säkerhet innebär en onödig begränsning som kan medföra att exempelvis vissa transporter faller utanför tillämpningsområdet. Kriminalvården förordar vidare att förebygga och förhindra hot mot den allmänna ordningen och säkerheten används i stället. *Umeå universitet* och *Dataskydd.net* ifrågasätter om inte informationssäkerhetsområdet bör omfattas av ramlagen.

Skälen för regeringens förslag

Tillämpningsområdet ska omfatta skydd av allmän säkerhet

Direktivets tillämpningsområde inkluderar personuppgiftsbehandling i syfte att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. I skäl 12 anges att polisens och andra brottsbekämpande myndigheters verksamhet främst är inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, men att sådan verksamhet också kan innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Det anges också att verksamheten även omfattar upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott.

Det är framför allt Polismyndigheten som har i uppdrag att skydda allmänheten mot hot mot den allmänna säkerheten. En av Polismyndighetens huvuduppgifter enligt 2 § polislagen är att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten och att övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat. Befogenheterna att ingripa finns bl.a. i 13–13 c §§ polislagen.

Även Kustbevakningen har vissa ordningshållande arbetsuppgifter. De rör främst sådant uppträdande i trafiken till sjöss som stör ordningen eller utgör en omedelbar fara för ordningsstörning. En kustbevakningstjänsteman har också rätt att ingripa för att avvärja brott som avser trafikregler och säkerhetsanordningar för sjötrafiken, vattenförorening från fartyg och dumpning av avfall i vatten. Vid ett ingripande i någon av dessa situationer har en kustbevakningstjänsteman enligt 3 § lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning rätt att avvisa, avlägsna eller omhänderta den som stör ordningen eller utgör en omedelbar fara för den enligt reglerna i 13 § polislagen. Kustbevakningen har också särskilda ordningshållande uppgifter enligt lagstiftningen om sjöfartsskydd respektive hamnskydd.

I förarbetena till polisdatalagen framhålls att det är svårt att dra en tydlig gräns mellan polisens ordningshållning och brottsbekämpning. Det beror på att övervakning och ordningshållande verksamhet även kan syfta till att förebygga och ingripa mot brott. Sådan verksamhet kan ofta också övergå i brottsbekämpning. Det ansågs dock föra för långt att betrakta mer renodlad övervakning och ordningshållande verksamhet som brottsbekämpande. Den verksamheten skulle därmed inte omfattas av polisdatalagens tillämpningsområde (prop. 2009/10:85 s. 75).

I artikel 1.1 anges att direktivet omfattar personuppgiftsbehandling i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Det väcker frågan om det bara är ordningshållande verksamhet som är en del av brottsbekämpningen som omfattas av direktivets tillämpningsområde. Om bara ordningshållande verksamhet som utgör en del av brottsbekämpningen skulle omfattas av direktivet, skulle det dock inte ha funnits något skäl att nämna den verksamheten särskilt. Personuppgiftsbehandling i syfte att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten räknas upp i artikeln och i skäl 12 tydliggörs att det handlar om ingripanden mot sådant som inte i sig är brott som exempelvis tvångsåtgärder vid demonstrationer. Mot den bakgrunden är det enligt utredningen tydligt att direktivet omfattar mer än det som kan sägas höra till den traditionella brottsbekämpande verksamheten. Ramlagen bör ha ett tillämpningsområde som motsvarar direktivets. Regeringen delar utredningens uppfattning och lagen bör därför gälla även för personuppgiftsbehandling som utförs för ordningshållande syften.

Åtgärder för att skydda allmän säkerhet är som framgått något annat än att skydda den nationella säkerheten. Det sistnämnda är Säkerhetspolisens arbetsuppgift och behandlas i avsnitt 6.5.1.

Vilket uttryckssätt bör användas?

I svensk rätt har uttrycket allmän ordning och säkerhet använts under lång tid i olika polisrättsliga författningar. Uttrycket, som inte har någon legaldefinition, är vittomfattande och svårdefinierat. Det används bl.a. i ordningslagen (1993:1617) och polislagen.

I polislagen används uttrycket i 1 § som anger polisverksamhetens ändamål. Där sägs att polisens arbete syftar till att upprätthålla allmän ordning och säkerhet och att i övrigt tillförsäkra allmänheten skydd och hjälp. I kommentaren till polislagen framhålls att det i polisens uppgift att upprätthålla allmän ordning och säkerhet inte bara ligger att motverka och beivra straffsanktionerade handlingar. Även i övrigt har polisen viss skyldighet att söka säkerställa förutsättningarna för en i möjligaste mån trygg och friktionsfri samlevnad medborgarna emellan (se Nils-Olof Berggren och Johan Munck, Polislagen, En kommentar, 11 uppl. 2015, i fortsättningen Berggren m.fl., s. 35).

I 1 § polislagen används alltså uttrycket allmän ordning och säkerhet som ett överordnat begrepp som både omfattar brottsutredning och annan brottsbekämpande verksamhet och olika former av övervakning. Det återspeglar den helhetssyn på polisens alla olika funktioner som eftersträvas. I de enskilda bestämmelserna i lagen, särskilt när det gäller polismans befogenheter, används uttrycket i en snävare mening som ligger mera i linje med regleringen i ordningslagen. Den lagen tar sikte på regler som riktar sig till allmänheten och som rör användningen av allmänna utrymmen och samfärdseln samt sammankomster och tillställningar av olika slag.

Uttrycket allmän ordning och säkerhet används inte helt konsekvent ens i polislagen. I vissa av bestämmelserna används uttrycket ”den allmänna ordningen” medan ”ordningen och säkerheten” används i någon

bestämmelse. Av förarbetena till 13–13 c §§ kan inte utläsas att lagstiftaren har avsett någon egentlig skillnad mellan uttryckssätten eller att de skulle avse olika situationer. Både 13 a och 13 c §§ polislagen infördes för att komma till rätta med de problem som polisen ställs inför i samband med större evenemang (prop. 1996/97:175 s. 23 f.). Det är också sådana situationer som skäl 12 i direktivet förefaller ta sikte på, eftersom myndighetsutövning vid demonstrationer, större idrottsevenemang och upplopp nämns uttryckligen. Regeringen anser, i likhet med utredningen, att uttrycket allmän ordning och säkerhet bör användas i ramlagen för att säkerställa att lagens tillämpningsområde täcker den verksamhet som är avsedd. Det stämmer också överens med hur Polismyndighetens uppgifter anges i bl.a. polislagen.

Ibland anges att polisen ska upprätthålla allmän ordning och säkerhet och ibland att polisen ska övervaka allmän ordning och säkerhet. I 2 § polislagen anges att en av polisens huvuduppgifter är att övervaka den allmänna ordningen och säkerheten. Detta uttryckssätt menar *Polismyndigheten* bör användas i ramlagen. Övervakning kan ha många olika former, t.ex. att någon i en ledningscentral följer trafikflödet eller allmänhetens rörelser på en viss plats via övervakningskameror. Det kan även vara fråga om automatisk hastighetsövervakning med övervakningskameror och allmän trafikövervakning på vägar eller fasta kontrollplatser. Övervakning kan också innebära att polisen rutinmässigt med bil passerar vissa lokaler eller områden eller att polismän eller bevakningspersonal tillfälligt eller stadigvarande bevakar en viss plats eller byggnad. För att upprätthålla allmän ordning och säkerhet krävs normalt fysisk närvaro på platsen där oordning förekommer eller riskerar att göra det. Uttrycket övervaka den allmänna ordningen och säkerheten är således mera vittomfattande än uttrycket upprätthålla allmän ordning och säkerhet. Det kan därför ifrågasättas om uttrycket övervaka skulle ge en avgränsning som går utöver vad direktivet avser. Regeringen delar mot denna bakgrund utredningens bedömning att uttrycket upprätthålla allmän ordning och säkerhet bäst återspeglar vad som enligt skäl 12 avses med direktivets uttryck skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Det bör därför användas för att avgränsa tillämpningsområdet för ramlagen. När det gäller *Kriminalvårdens* synpunkt finns det anledning att återkomma till frågan om transport i avsnitt 6.7.

I begreppet allmän ordning och säkerhet har ansetts ligga att det ska vara något som berör allmänheten, dvs. samhällsmedlemmarna i gemen, vem som helst eller en obestämd krets av enskilda (Berggren m.fl. s. 35 f. och där anmärkt litteratur).

Anpassningar av registerförfattningar

Genom att ramlagen föreslås omfatta personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet kommer den att ha ett vidare tillämpningsområde än polisdatalagen. Frågan om det bör föranleda att polisdatalagens tillämpningsområde anpassas till ramlagens kommer att behandlas i samband med att myndigheternas registerförfattningar anpassas.

Kustbevakningsdatalagen gäller enligt 1 kap. 2 § behandling av personuppgifter i Kustbevakningens operativa verksamhet som rör både brottsbekämpning och annan operativ verksamhet som sjöövervakning och räddningstjänst. I 5 kap. regleras personuppgiftsbehandling i den verksamhet som inte är brottsbekämpande. Där regleras personuppgiftsbehandling i verksamhet som gäller både upprätthållande och övervakning av allmän ordning och säkerhet. Även denna lag kommer att ses över i samband med anpassningarna av registerförfattningarna.

Omfattas informationssäkerhet?

Samhällets beroende av informationsteknik har enligt regeringen utvecklats till att bli en fråga om nationell och internationell säkerhet (Förebygga, förhindra och försvåra – den svenska strategin mot terrorism, skr. 2014/15:146 s. 26). I bl.a. 31 § personuppgiftslagen och 7 och 9 §§ säkerhetsskyddslagen (1996:627) finns bestämmelser om informationssäkerhet. Den som är ansvarig för en verksamhet ska se till att informationssäkerheten håller tillräckligt hög nivå. Alla myndigheter och organ som hanterar känslig information förutsätts arbeta aktivt med att skydda sin information.

I likhet med 1995 års dataskyddsdirektiv innehåller direktivet bestämmelser om informationssäkerhet. Direktivet innebär skärpningar i olika avseenden, bl.a. ställs det krav på att personuppgiftsincidenter ska rapporteras till tillsynsmyndigheten. Både *Umeå universitet* och *Dataskydd.net* anser att informationssäkerhet bör omfattas av ramlagens tillämpningsområde. Direktivets bestämmelser om informationssäkerhet tar – på samma sätt som 1995 års dataskyddsdirektiv – enbart sikte på att personuppgiftsansvariga bär ett särskilt ansvar för informationssäkerheten när det gäller de personuppgifter de behandlar. Det finns däremot inget som tyder på att det nya direktivet är avsett att omfatta förebyggande arbete som rör informationssäkerhet i allmänhet eller verksamhet för att förebygga och förhindra de hot som samhället kan ställas inför på informationssäkerhetens område. Tvärtom tyder skrivningarna i skäl 12 på att det som åsyftas är hot mot fysisk säkerhet. Regeringen anser därför i likhet med utredningen att när begreppet allmän ordning och säkerhet används i ramlagen för att ange tillämpningsområdet bör det inte omfatta informationssäkerhet.

6.4.4 Vad är en behörig myndighet?

Regeringens förslag: Behörig myndighet ska definieras som en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller en annan aktör som har anförtrotts myndighetsutövning för något av dessa syften, när den behandlar personuppgifter för ett sådant syfte.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Kammarrätten i Stockholm* anser att orden ”anförtrotts myndighetsutövning” ska användas i stället för uttrycket ”utövar

myndighet” som utredningen föreslår. Flera remissinstanser, däribland *Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län* och *Malmö kommun*, anser att definitionen av en behörig myndighet kan leda till felbedömningar av när ramlagen är tillämplig och att den skulle behöva förtydligas. *Sjöfartsverket* efterfrågar ett förtydligande av vilka myndigheter som är behöriga. *Datainspektionen* påpekar att det skulle kunna uppstå konkurrenssituationer när samma behandling har olika syften.

Skälen för regeringens förslag: Ramlagen ska gälla för personuppgiftsbehandling som behöriga myndigheter utför för vissa syften. Det bör därför definieras vad som avses med behörig myndighet i ramlagen. Utredningens förslag utgår från den bedömning som gjordes i förarbetena till 2013 års lag att det är en bättre lagteknisk lösning att knyta an till uppräkningen av verksamhetsuppgifter i direktivet än att i lag räkna upp de myndigheter som ska tillämpa lagen (prop. 2012/13:73 s. 62). Genom att direktivet har ett så brett tillämpningsområde är det inte lämpligt att i författningstext peka ut alla myndigheter som har sådana uppgifter att de ska betraktas som behöriga myndigheter i ramlagens mening. Det är också svårt att i lagtext ange de kategorier som enligt viss lagstiftning har behörighet att utöva myndighet inom ramlagens tillämpningsområde. En uppräkning av myndigheter och andra aktörer skulle visserligen – som flera remissinstanser, däribland *Sjöfartsverket*, påpekar – förenkla för tillämpande aktörer och framstå som tydligare, men den riskerar att bli ofullständig. Dessutom skulle en sådan uppräkning behöva förses med åtskilliga undantag, eftersom inte all deras personuppgiftsbehandling regleras i ramlagen. Definitionen bör därför enligt regeringens mening utgå från myndigheternas uppgifter och de andra aktörernas rätt att utöva myndighet.

I artikel 3.7 definieras behörig myndighet som en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten eller ett annat organ eller annan enhet som har anförtrotts myndighetsutövning för något av detta. Som framgår av avsnitt 6.4.2 och 6.4.3 bör en delvis annan formulering väljas för avgränsningen av ramlagens tillämpningsområde. Samma formulering bör användas i definitionen av behörig myndighet. Behörig myndighet bör således vara en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller en annan aktör som har anförtrotts myndighetsutövning för något av dessa syften. Både *Lagrådet* och *Kammarrätten i Stockholm* förordar formuleringen ”anförtrotts myndighetsutövning” framför begreppet ”utöva myndighet”. Regeringen håller med om att orden ”anförtrotts myndighetsutövning” gör definitionen tydligare och därför bör användas i ramlagen.

För aktörer som inte är myndigheter har det betydelse om personuppgifter behandlas som ett led i myndighetsutövning eller inte. Personuppgifter som andra aktörer behandlar när de inte utövar myndighet ligger utanför ramlagens tillämpningsområde. När det gäller myndigheter omfattas däremot all personuppgiftsbehandling inom ramlagens tillämpningsområde, oavsett om den har samband med myndighetsutövning eller inte.

Arbetsuppgifterna och syftet med behandlingen är avgörande för när en myndighet är behörig

Som utredningen beskriver är det självklart att vissa myndigheter på grund av sina uppgifter ska betraktas som behöriga myndigheter enligt ramlagen. Det är Polismyndigheten, Kustbevakningen, Skatteverket, Tullverket, Åklagarmyndigheten, Ekobrottsmyndigheten, de allmänna domstolarna och Kriminalvården som främst kommer att behandla personuppgifter som omfattas av ramlagens tillämpningsområde.

Dessa myndigheter har emellertid även uppgifter som ligger utanför ramlagens tillämpningsområde. Det gäller i hög grad Polismyndigheten och de allmänna domstolarna men också Tullverket, Kustbevakningen och Skatteverket, där den brottsbekämpande verksamheten bara utgör en del av den totala verksamheten. Även åklagare har vissa operativa uppgifter som inte omfattas av ramlagens tillämpningsområde. Den omständigheten att en myndighet har vissa uppgifter inom ramlagens tillämpningsområde gör inte att myndigheten i all sin verksamhet är behörig myndighet i ramlagens mening. Som exempel kan nämnas Skatteverket, där myndighetens brottsbekämpande enhet omfattas av definitionen av behörig myndighet, medan de enheter som arbetar med folkbokföring eller fastställande av skatt inte gör det. En myndighet kan således vara både behörig och icke behörig i ramlagens mening beroende på vilka arbetsuppgifter som utförs (se skäl 11).

Lagrådet förordar att definitionen av behörig myndighet förtydligas så att det framgår att myndigheten respektive aktören är behörig endast när den behandlar personuppgifter för sådana syften som omfattas av ramlagen. Att ramlagen endast gäller vid personuppgiftsbehandling för syftena brottsbekämpning, lagföring, straffverkställighet, och upprätthållande av allmän ordning och säkerhet framgår av avsnitt 6.4.2 och 6.4.3. Regeringen håller med Lagrådet om att det framgår tydligare att en myndighet kan vara både behörig och icke behörig beroende på omständigheterna, om det läggs in i definitionen att en myndighet är behörig endast när den behandlar personuppgifter för ett syfte som omfattas av ramlagen. Genom att regleringen i direktivet är utformad som ett undantag från dataskyddsförordningens tillämpningsområde kommer det att krävas av de behöriga myndigheterna och de enskilda tjänstemännen att de i större utsträckning än i dag överväger syftet med behandlingen av personuppgifter och om behandlingen ligger inom ramlagens tillämpningsområde. Om personuppgifter behandlas för något annat syfte än brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän och säkerhet ska ramlagen inte tillämpas.

Dubbla regelverk

Det är framför allt de myndigheter som arbetar med brottsbekämpning som kommer att möta gränsdragningsproblem. Detta har också påtalats av flera remissinstanser. Det beror bl.a. på att deras verksamhet är sådan att det inte alltid från början är tydligt om syftet med behandlingen är brottsbekämpande eller inte. Även på andra områden kan gränsdragningen ibland vara svår.

I avsnitt 6.7 redovisas vissa principer som regeringen anser bör vara vägledande i gränsdragningen. I det enskilda fallet blir det dock den

behöriga myndigheten och den handläggande tjänstemannen som får avgöra vilken lagstiftning som är tillämplig. Detta är ett resultat av den nya EU-regleringen på området som är svårt att undvika. Svårigheterna med att avgöra vilket regelverk som ska tillämpas bör dock inte överdrivas. Redan i dag tillämpar myndigheterna olika regelverk – personuppgiftslagen och myndighetsanknutna registerförfattningar – beroende på i vilken verksamhet personuppgifterna behandlas. Problematiken med dubbla regleringar när det gäller personuppgiftsbehandling är således inte ny.

Så som tillämpningsområdet för direktivet är utformat kommer fler myndigheter och andra aktörer än enbart myndigheterna i rättskedjan att i viss del av sin verksamhet behöva tillämpa ramlagen. Det gäller exempelvis den som bedriver sluten ungdomsvård eller rättspsykiatrisk vård. Vidare kommer andra aktörer som utövar myndighet inom ramlagens tillämpningsområde att behöva tillämpa den när de behandlar personuppgifter för sådana syften som lagen reglerar. De ska då betraktas som behöriga myndigheter i ramlagens mening och tillämpa den. En del av aktörerna har hittills enbart tillämpat personuppgiftslagen och kommer att i fortsättningen tillämpa dataskyddsförordningen i huvuddelen av sin verksamhet. Det ställs alltså krav på att de, när personuppgiftslagen upphör att gälla, noga överväger för vilka syften personuppgifter behandlas och vilket regelverk som ska tillämpas på behandlingen.

Datainspektionen lyfter i sammanhanget fram att det i praktiken borde uppstå situationer där samma behandling har olika syften, vilket skulle kunna leda till en konkurrenssituation. Regeringen delar utredningens uppfattning att behandling av personuppgifter i verksamhet som omfattas av unionsrätten omfattas antingen av ramlagens eller dataskyddsförordningens tillämpningsområde. Ramlagen och förordningen kan inte vara tillämpliga på samma behandling för samma syfte. Har samma behandling däremot flera olika syften kan regelverken vara tillämpliga parallellt. Det bör då betraktas som olika behandlingar av personuppgifter som var och en måste ha stöd i och följa gällande regelverk.

6.4.5 Helt eller delvis automatiserad behandling

Regeringens förslag: Ramlagen ska gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad. Lagen ska även gälla för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Förvaltningsrätten i Stockholm* efterfrågar bredare resonemang kring vilka behandlingar som omfattas av ramlagen och efterfrågar särskilt vad som gäller för behandlingar i ostrukturerat material. *Dataskydd.net* anser att ramlagen även ska omfatta behandlingar som inte är helt eller delvis automatiserade.

Skälen för regeringens förslag: En fråga är vilka slags behandlingar som ska omfattas av tillämpningsområdet. Enligt artikel 2.2 är direktivet tillämpligt på sådan behandling av personuppgifter som helt eller delvis

företas på automatiserad väg och på annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Med register avses enligt artikel 3.6 en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden. Tillämpningsområdet är detsamma enligt 1995 års dataskyddsdirektiv och dataskyddsförordningen. Det finns däremot ingen möjlighet att göra undantag för behandlingar i ostrukturerat material som *Förvaltningsrätten i Stockholm* har lyft i sitt remissvar (jfr. 5 a § personuppgiftslagen). Regeringen återkommer till frågor om informationsskyldighet när det gäller ostrukturerat material i avsnitt 10.2.8.

Som anges i avsnitt 6.2 ville man komma bort från registerbegreppet redan när personuppgiftslagen infördes. Personuppgiftslagen gäller därför för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Regleringen i personuppgiftslagen har varit utgångspunkt vid utformningen av tillämpningsområdet för myndigheternas registerförfattningar. Mot den bakgrunden instämmer regeringen – till skillnad från *Dataskydd.net* – i utredningens bedömning att tillämpningsområdet för ramlagen bör anges på samma sätt. Det innebär ingen skillnad i sak i förhållande till direktivet. Att formuleringen skiljer sig något från hur tillämpningsområdet uttrycks i dataskyddsförordningen saknar enligt regeringens bedömning någon praktisk betydelse.

6.5 Undantag från tillämpningsområdet

6.5.1 Personuppgiftsbehandling som rör nationell säkerhet

Regeringens förslag: Ramlagen ska inte gälla vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Undantaget ska också gälla i de fall där Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Lagen ska inte heller gälla när Försvarsmakten har att tillämpa lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inget undantag gällande verksamhet som omfattas av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Remissinstanserna: *Polismyndigheten* och *Uppsala universitet* efterfrågar en definition av begreppet nationell säkerhet. *Försvarsmakten* föreslår att begreppet Sveriges säkerhet ska användas i stället för begreppet nationell säkerhet. *Säkerhetspolisen* anser att det finns skäl att överväga om inte hela myndighetens brottsbekämpande verksamhet borde undantas från ramlagen. *Dataskydd.net* anser att Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet inte bör undantas

från tillämpningsområdet. Försvarsmakten anser vidare att undantaget bör gälla även Försvarsmaktens personuppgiftsbehandling som rör nationell säkerhet.

Skälen för regeringens förslag

Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet undantas

Enligt artikel 2.3 a ska direktivet inte tillämpas på personuppgiftsbehandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Av skäl 14 framgår att verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter inom verksamhet som avser den gemensamma utrikes- och säkerhetspolitiken inte omfattas av direktivets tillämpningsområde.

1995 års dataskyddsdirektiv gäller inte för sådan personuppgiftsbehandling som inte omfattades av EG-rätten när direktivet antogs, t.ex. statens verksamhet på straffrättens område eller verksamhet som rör statens säkerhet eller försvar. I förarbetena till personuppgiftslagen framhöll regeringen att om viss offentlig verksamhet generellt skulle undantas från lagen fanns det risk för att viss behandling inom den sektorn inte skulle omfattas av någon lagstiftning med motsvarande syfte som den nya lagen. Personuppgiftslagen gjordes därför generellt tillämplig och omfattar även sådan verksamhet som då föll utanför EG-rätten. Genom att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger, garanteras att behovet av särregler alltid övervägs noga i den ordning som gäller för författningsgivning (prop. 1997/98:44 s. 41).

Säkerhetspolisen anför med hänvisning till artikel 2.3 a och skäl 14 i direktivet att det finns utrymme att göra undantag för myndighetens brottsbekämpande verksamhet i sin helhet eftersom de hanterar nationella säkerhetsfrågor. *Dataskydd.net* anser i stället att Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet inte bör undantas från tillämpningsområde. Undantaget i det nya dataskyddsdirektivet är utformat så att det utesluter viss verksamhet, inte vissa typer av myndigheter eller organisationer. Säkerhetspolisens verksamhet ligger i allt väsentligt utanför direktivets tillämpningsområde. Till Säkerhetspolisens huvuduppgifter hör att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott och att utreda och beivra sådana brott. Säkerhetspolisen ansvarar vidare för personskyddet av den centrala statsledningen. Nu nämnda uppgifter hör till nationell säkerhet. Säkerhetspolisen har även andra uppgifter som hör till nationell säkerhet eller har ett mycket nära samband med sådan verksamhet. Av samma skäl som det inte bör anges i ramlagen vilka myndigheter som ska tillämpa den bör inte Säkerhetspolisens personuppgiftsbehandling generellt undantas från ramlagens tillämpningsområde. Redan i dag har myndigheten vissa uppgifter som omfattas av direktivets tillämpningsområde och det kan inte uteslutas att myndigheten i framtiden får nya sådana uppgifter. Regeringen anser därför i likhet med utredningen att undantaget bör utformas så att det endast träffar de delar av Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet.

I förarbetena till 2013 års lag diskuterades ingående hur motsvarande undantag i dataskyddsrambeslutet skulle formuleras och där stannade regeringen för att begreppet nationell säkerhet borde användas (prop. 2012/13:73 s. 69 f.). I 19 kap. brottsbalken används numera begreppet Sveriges säkerhet i stället för det äldre rikets säkerhet. När begreppet byttes ut konstaterade regeringen att innebörden av vad som betraktas som rikets säkerhet förändrats och fått ett vidare tillämpningsområde (prop. 2013/14:51 s. 20). I propositionen Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag (prop. 2017/18:89) används också begreppet Sveriges säkerhet.

Utredningen föreslår att begreppet nationell säkerhet bör användas i ramlagen. *Polismyndigheten* och *Uppsala universitet* efterfrågar en definition av begreppet nationell säkerhet. *Försvarsmakten* anser att begreppet Sveriges säkerhet ska användas i stället för nationell säkerhet.

Undantagen från tillämpningsområdet både i direktivet och dataskyddsförordningen utgår emellertid från begreppet ”nationell säkerhet” – det är ett centralt begrepp för EU:s dataskyddsreform – och regeringen anser därför i likhet med utredningen att det uttrycket bör användas i ramlagen för att avgränsa dess tillämpningsområde. Eftersom det här handlar om att förhålla sig till unionsrättens gränser ser regeringen ingen motsättning i att använda det EU-rättsliga begreppet, samtidigt som ”Sveriges säkerhet” används för att ur ett nationellt perspektiv beskriva tillämpningsområdet för annan lagstiftning. En definition av begreppet ”nationell säkerhet” skulle visserligen kunna underlätta för att avgöra om ramlagen är tillämplig eller inte. Samtidigt rör det sig om ett EU-rättsligt begrepp, som avgränsar EU:s kompetens gentemot medlemsstaterna. I förlängningen är det upp till EU-domstolen att avgöra begreppets närmare innebörd. Mot den bakgrunden anser regeringen att det inte är lämpligt att definiera begreppet ”nationell säkerhet” inom ramen för detta lagstiftningsärende.

Säkerhetspolisens personuppgiftsbehandling kommer dock inte att lämnas oreglerad inom området nationell säkerhet. I slutbetänkandet Brottsdatalag – kompletterande lagstiftning (SOU 2017:74 s. 597 f.) föreslås en ny lag om Säkerhetspolisens behandling av personuppgifter. Förslaget kommer att behandlas i en senare proposition.

Det finns även andra myndigheter som i viss omfattning hanterar personuppgifter rörande nationell säkerhet. Det gäller bl.a. Polismyndigheten, åklagare och allmänna domstolar när de behandlar personuppgifter i mål och ärenden som rör brott mot Sveriges säkerhet. Det kan inte uteslutas att även andra myndigheter i viss utsträckning hanterar sådana personuppgifter.

De överväganden som gjordes när personuppgiftslagen infördes gör sig fortfarande gällande. Nationell säkerhet bör därför inte undantas generellt från den nya lagens tillämpningsområde. Det är en mycket liten del av Polismyndighetens, åklagares och de allmänna domstolarnas verksamhet som rör nationell säkerhet. Det saknas enligt regeringens mening skäl att undanta den mycket begränsade personuppgiftsbehandling som utförs av dessa myndigheter på det området från ramlagens tillämpningsområde. De bör därför på samma sätt som i dag tillämpa samma regler som gäller för behandling av personuppgifter i verksamheten i övrigt vid utredning eller handläggning av brottmål och därtill anknutna ärenden enligt rätte-

gångsbalken som rör Sveriges säkerhet. Detsamma bör gälla om någon annan myndighet undantagsvis skulle hantera sådana personuppgifter, exempelvis om Kriminalvården skulle ha tillgång till någon personuppgift som rör nationell säkerhet vid verkställighet av påföljd.

Säkerhetspolisen ska tillämpa ramlagen i vissa fall

Även om merparten av Säkerhetspolisens personuppgiftsbehandling undantas från ramlagens tillämpningsområde, finns det viss behandling i myndighetens operativa verksamhet som bör omfattas av ramlagen eftersom den inte rör nationell säkerhet.

Säkerhetspolisen ska enligt 13 § förordningen (2014:1103) med instruktion för Säkerhetspolisen bistå vid polisverksamhet som leds av Polismyndigheten om myndigheten i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Säkerhetspolisen ska också lämna tekniskt biträde och annan hjälp till Polismyndigheten i den utsträckning som myndigheterna kommer överens om. När Säkerhetspolisen lämnar sådan hjälp omfattas personuppgiftsbehandlingen av ramlagens tillämpningsområde om den avser brottsbekämpning, lagföring eller verksamhet för att upprätthålla allmän ordning och säkerhet.

Enligt 30 § förordningen (2014:1102) med instruktion för Polismyndigheten får chefen för Nationella operativa avdelningen i samråd med biträdande säkerhetspolischefen i ett enskilt fall bestämma att en förundersökning eller annan liknande uppgift i den brottsbekämpande verksamheten ska lämnas över till Säkerhetspolisen för fortsatt handläggning. Syftet med bestämmelsen är bl.a. att jävssituationer ska kunna undvikas (prop. 2013/14:110 s. 400). När Säkerhetspolisen med stöd av ett beslut enligt den paragrafen genomför en förundersökning eller utför någon annan uppgift som normalt skulle utföras av Polismyndigheten och som omfattas av ramlagens tillämpningsområde bör Säkerhetspolisen tillämpa den lagen.

Polismyndighetens biträde till Säkerhetspolisen

En särskild fråga är vad som ska gälla för Polismyndigheten när den övertar uppgifter från Säkerhetspolisen eller biträder den på något annat sätt.

Enligt 28 § instruktionen för Polismyndigheten ska myndigheten bistå vid polisverksamhet som leds av Säkerhetspolisen om Säkerhetspolisen i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Polismyndigheten ska vidare, i den utsträckning som myndigheterna kommer överens om, lämna tekniskt biträde och annan hjälp till Säkerhetspolisen. Bestämmelsen är en spegling av 13 § instruktionen för Säkerhetspolisen.

Enligt 15 § instruktionen för Säkerhetspolisen får biträdande säkerhetspolischefen i samråd med chefen för Nationella operativa avdelningen, trots den ansvarsfördelning som annars gäller mellan myndigheterna, i ett enskilt fall bestämma att en förundersökning eller annan uppgift i den brottsbekämpande verksamheten ska lämnas över till Polismyndigheten för fortsatt handläggning. Bestämmelsen motsvarar 30 § instruktionen för Polismyndigheten.

Eftersom det när Säkerhetspolisen begär biträde av Polismyndigheten eller överlämnar en arbetsuppgift till myndigheten med stöd av 15 § in-

struktionen för Säkerhetspolisen i de flesta fall är fråga om en arbetsuppgift som ligger utanför direktivets tillämpningsområde, bör Polismyndigheten inte tillämpa ramlagen i vidare mån än vad Säkerhetspolisen skulle ha gjort om uppgiften legat kvar där.

Försvarsmaktens tillämpning av ramlagen

Försvarsmakten bedriver viss verksamhet som kan sägas falla inom ramlagens tillämpningsområde. Det rör t.ex. militärpolisen och militära skyddsvakter när de utför uppgifter med polismans befogenhet. Motsvarande kan gälla i samband med att Försvarsmakten lämnar stöd till polisen vid terrorismbekämpning.

Enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst får Försvarsmakten bl.a. behandla personuppgifter i myndighetens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen om det är nödvändigt för att klarlägga verksamhet som innefattar hot mot rikets säkerhet, eller vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet. Lagen kan därför bli tillämplig när Försvarsmakten lämnar stöd till polisen enligt lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning, men också när militärpolisen och militära skyddsvakter utför sina uppgifter. Mot denna bakgrund finns det, som *Försvarsmakten* påpekar, skäl att undanta även Försvarsmaktens behandling av personuppgifter som sker enligt lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst från ramlagens tillämpningsområde.

Det kan i detta sammanhang även nämnas att Utredningen Behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (Fö2017:03) bl.a. ska bedöma om den reglering som gäller vid behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst är ändamålsenligt utformad samt analysera om den personuppgifts-behandling i Försvarsmakten som i dag regleras i personuppgiftslagen helt eller delvis bör regleras särskilt. Utredningsuppdraget ska redovisas senast den 31 juli 2018.

6.5.2 Den gemensamma utrikes- och säkerhetspolitiken

Enligt skäl 14 undantas medlemsstaternas behandling av personuppgifter i verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken från direktivets tillämpningsområde. Regeringen kan i likhet med utredningen inte se att någon av de som är behöriga myndigheter i ramlagens mening bedriver verksamhet inom detta område. Det finns därför inget behov av att från ramlagens tillämpningsområde undanta någon myndighet eller verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Detta har inte heller ifrågasatts av någon remissinstans.

6.6 Förhållandet till offentlighetsprincipen och till tryck- och yttrandefriheten

Regeringens bedömning: Behandling av personuppgifter på tryck- och yttrandefrihetens område och allmänhetens tillgång till allmänna handlingar behöver inte regleras.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Justitiekanslern* och *Domstolsverket* anser att en upplysningsbestämmelse om ramlagens förhållande till offentlighetsprincipen och till tryck- och yttrandefriheten bör övervägas. Ingen annan remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens bedömning: I skäl 16 framhålls att direktivet inte påverkar tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar.

I dataskyddsförordningen finns bestämmelser som ger utrymme för nationell reglering om förhållandet mellan, å ena sidan, skyddet för personuppgifter och, å andra sidan, yttrande- och informationsfriheten och offentlighetsprincipen. Enligt artikel 85.1 i förordningen ska medlemsstaternas nationella lagstiftning förena rätten till integritet i enlighet med förordningen med rätten till yttrande- och informationsfrihet. Den ska omfatta personuppgiftsbehandling för journalistiska ändamål och för akademiskt, konstnärligt eller litterärt skapande. När det gäller behandling för sådana ändamål ska medlemsstaterna enligt artikel 85.2 i förordningen föreskriva om undantag eller avvikelser från stora delar av förordningens bestämmelser om det behövs för att förena rätten till integritet med yttrande- eller informationsfriheten.

Enligt artikel 86 i förordningen får personuppgifter i allmänna handlingar hos en myndighet eller vissa typer av organ lämnas ut i enlighet med unionsrätten eller nationell rätt i syfte att förena allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med förordningen. Enligt regeringens förslag i propositionen Ny dataskyddslag har tryckfrihetsförordningen och yttrandefrihetsgrundlagen företräde framför dataskyddsförordningen och den föreslagna dataskyddslagens bestämmelser (prop. 2017/18:105 s. 187).

I avsnitt 6.1.2 har den föreslagna brottsdatalagens förhållande till annan lagstiftning behandlats. Regeringen föreslår under rubriken Avvikande bestämmelser i annan författning en bestämmelse som innebär att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från lagen, så tillämpas den bestämmelsen. Paragrafen motsvarar 2 § personuppgiftslagen. Även den paragrafen har rubriken Avvikande bestämmelser i annan författning.

I 7 § första stycket personuppgiftslagen finns dessutom – under rubriken Förhållandet till tryck- och yttrandefriheten – en bestämmelse som anger att lagen inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I 8 § samma lag finns en motsvarande bestämmelse när det gäller offentlighetsprincipen. Enligt 1 kap. 7 § i förslaget till dataskyddslag ska förordningen och lagen inte tillämpas i den

utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Mot bakgrund av att remissförslaget inte innehåller någon bestämmelse som på liknande sätt behandlar relationen till grundlagarna anser *Lagrådet* att det finns behov av att ytterligare överväga detta förhållande i den fortsatta beredningen. Lagrådet framhåller även när det gäller förhållandet till mediegrundlagarna att det finns skäl att särskilt framhålla att Justitiekanslern torde vara en behörig myndighet vid fullgörandet av uppgifter som åklagare avseende tryck- och yttrandefrihetsbrott.

Behandling av personuppgifter i samband med utlämnande av allmänna handlingar ligger utanför direktivets tillämpningsområde. Av förslaget till reglering av ramlagens tillämpningsområde framgår att den gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder och vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet (se avsnitt 6.4).

När det gäller förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen i övrigt kan regeringen konstatera följande. I förarbetena till personuppgiftslagen framhålls att bestämmelser i vanlig lag inte kan ta över bestämmelser i grundlag. Regeringen ansåg att lagtexten i syfte att klargöra och underlätta tillämpningen ändå borde innehålla en uttrycklig erinran om att bestämmelserna i personuppgiftslagen inte ska tillämpas om en sådan tillämpning skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. En sådan erinran ansågs viktig för att inskärpa att tillämpningen vid fall av möjliga konflikter ska präglas av försiktighet och respekt för det grundlagsskyddade området (prop. 1997/98:44 s. 51 f. och s. 119).

I propositionen Ny dataskyddslag (2017/18:105 s. 42) konstateras att det är angeläget att dataskyddsförordningens och dataskyddslagens bestämmelser inte ger upphov till osäkerhet kring möjligheterna till personuppgiftsbehandling på det grundlagsskyddade området och att en sådan osäkerhet skulle kunna påverka vitala delar av opinionsskapande verksamhet som är av grundläggande betydelse för demokratin och som skyddas genom bl.a. censurförbudet och meddelarfriheten. Regeringen anser vidare i den propositionen att det förhållandet att den unionsrättsliga dataskyddsregleringen är en direkt tillämplig förordning, som dessutom kan leda till kännbara sanktionsavgifter, innebär ett än större behov av ett förtydligande av förhållandet till tryck- och yttrandefrihetsregleringen.

Den föreslagna brottsdatalagen ska gälla vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder och i syfte att upprätthålla allmän ordning och säkerhet. De skäl som anges för en upplysningsbestämmelse i förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 49 f.) och dataskyddslagen (prop. 2017/18:105 s. 41 f.) gör sig därför inte gällande på ramlagens tillämpningsområde.

Regeringen delar därför – till skillnad från *Justitiekanslern* och *Domstolsverket* – utredningens bedömning att den föreslagna subsidiaritetsbe-

stämmelsen inte behöver kompletteras med en särskild reglering som tydliggör att ramlagen inte ska tillämpas vid en konflikt med regleringen i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Enligt 23 kap. 14 § andra stycket rättegångsbalken får en undersökningsledare hos rätten begära ett förordnande om att en allmän handling som kan antas ha betydelse som bevis ska tillhandahållas. I 38 kap. 8 § rättegångsbalken finns en motsvarande bestämmelse som är generell och som kan åberopas exempelvis av en målsägande. En myndighet, eller någon annan aktör som omfattas av reglerna om allmänna handlingar, kan alltså med stöd av någon av dessa regler åläggas att lämna ut en allmän handling till en förundersökning eller brottmålsrättegång. Det gäller dock inte en handling för vilken sekretess gäller enligt 15 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400), som reglerar utrikessekretess respektive försvarssekretess, eller 16 kap. 1 § samma lag som reglerar statsfinanssekretess. Det gäller inte heller en handling vars innehåll är sådant att någon som haft befattning med handlingen inte får höras som vittne om dess innehåll. Likaså undantas handlingar som kan avslöja yrkeshemligheter, om det inte finns synnerlig anledning. Enligt regeringens bedömning kommer tillämpningen av 23 kap. 14 § och 38 kap. 8 § rättegångsbalken inte att påverkas i samband med att de nya EU-rättsakterna ska börja tillämpas.

6.7 Gränsdragningsfrågor som rör tillämpningsområdet

6.7.1 Bedömningen av gränsdragningsfrågor

Regeringens bedömning: Vid bedömningen av om viss personuppgiftsbehandling faller under ramlagens eller dataskyddsförordningens tillämpningsområde har det avgörande betydelse om den som behandlar personuppgiften är en behörig myndighet och i vilket syfte uppgiften behandlas.

Det är en fråga för rättstillämpningen att slutligt avgöra vilket regelverk för dataskydd som gäller i ett enskilt fall.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser påtalar problematiken med dubbla regelverk. Många remissinstanser efterfrågar mer ledning om en viss verksamhet faller inom eller utanför ramlagens tillämpningsområde, däribland *Justitiekanslern, Finansinspektionen* och *Havs- och vattenmyndigheten*. Vissa remissinstanser anser att utredningen i sin redovisning har gjort felaktiga eller olämpliga bedömningar av om en viss verksamhet ska falla under ramlagens tillämpningsområde eller inte, däribland *Polismyndigheten, Kustbevakningen* och *Kriminalvården*.

Skälen för regeringens bedömning: Som tidigare konstaterats är det, vid bedömningen av om ramlagen är tillämplig på viss behandling av personuppgifter, av avgörande betydelse om den som behandlar personuppgiften är en behörig myndighet och i vilket syfte den behandlas. Flera remissinstanser, däribland *Svea hovrätt* och *Datainspektionen*, påtalar särskilt att utredningen på ett förtjänstfullt sätt redogjort för gränsdrag-

ningsfrågor som kan uppkomma beträffande ramlagens tillämpningsområde. Regeringen delar också utredningens syn på hur gränsdragningsproblemen ska behandlas, dvs. med utgångspunkt i frågorna om den som behandlar uppgiften är en behörig myndighet och i vilket syfte en personuppgift behandlas.

Många remissinstanser påtalar svårigheterna med dubbla regelverk i form av ramlagen med tillhörande förordning inom direktivets område och dataskyddsförordningen med den föreslagna kompletterande lagen samt därutöver myndighetsspecifika registerförfattningar. Flera remissinstanser efterfrågar också mer ledning om en viss verksamhet faller inom eller utanför ramlagens tillämpningsområde, däribland *Justitiekanslern* när myndigheten tar emot och eller överklagar beslut gällande ersättning till målsägandebiträden och offentliga försvarare enligt lagen (2005:73) om rätt för Justitiekanslern att överklaga vissa beslut, *Finansinspektionen* gällande myndighetens roll i ärenden enligt lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden och underrättelse till Polismyndigheten vid misstanke om penningtvätt eller finansiering av terrorism enligt lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (sedan den 1 augusti 2017 ersatt av lagen [2017:630] om åtgärder mot penningtvätt och finansiering av terrorism) och *Havs- och vattenmyndigheten* rörande vissa frågor om fiskelagen (1993:787), däribland beslag. Som utredningen och även flera remissinstanser konstaterar är det emellertid inte möjligt att inom ramen för detta lagstiftningsärende ge klara svar på om vissa enskilda verksamheter eller arbetsuppgifter kommer att omfattas av ramlagens tillämpningsområde eller inte. Det kommer att uppstå många frågor som kommer att få lösas i den praktiska tillämpningen och i slutändan av domstol när det gäller de exakta gränserna. Det kommer även, som *Datainspektionen* påpekar, vara av stor vikt att de behöriga myndigheterna genom olika insatser, t.ex. interna arbetsdokument och utbildningar, styr handläggarna vid tveksamhet om vilket regelverk som är tillämpligt.

Vissa remissinstanser anser dock att utredningen i sin redovisning gjort felaktiga bedömningar av om en viss verksamhet ska falla under ramlagens tillämpningsområde, exempelvis påpekar både *Polismyndigheten* och *Kustbevakningen* att det är olyckligt om olika delar av behöriga myndigheters kontrollverksamheter kommer att falla under olika regelverk och *Kriminalvården* anser att transport av personer har så stark anknytning till ramlagens tillämpningsområde att den verksamheten bör omfattas oavsett bakomliggande ändamål.

Som nämnts ovan bör gränsdragningsfrågorna behandlas med utgångspunkt i frågorna om den som behandlar uppgiften är en behörig myndighet och i vilket syfte en personuppgift behandlas. Utifrån dessa förutsättningar har utredningen hållit en rak och konsekvent linje i sina bedömningar av de olika verksamheterna och om de faller inom eller utanför ramlagens tillämpningsområde. Mot bakgrund av den gränsdragning som EU valt att göra mellan dataskyddsdirektivets och dataskyddsförordningens tillämpningsområden, där syftet med en behandling av personuppgifter är avgörande, är det ofrånkomligt att båda regelverken kommer att kunna bli tillämpliga i samma arbetsmoment för olika syften.

Sammantaget delar regeringen de bedömningar som utredningen gjort när det gäller tillvägagångssättet i gränsdragningsfrågor. Ytterligare väg-

ledning kring enskilda verksamheter inom myndigheterna kan fås genom de bedömningar som utredningen redovisar i delbetänkandet. Regeringen konstaterar att det är en fråga för rättstillämpningen att slutligt avgöra vilket regelverk för dataskydd som gäller i ett enskilt fall. I avsnitt 6.7.2 nedan redogörs för ett antal allmänna principer som presenterats i delbetänkandet Brottsdatalag (SOU 2017:29) i vägledande syfte.

6.7.2 Utgångspunkter

Det är enligt regeringens mening nödvändigt att ge tillämparna information om hur man kan resonera i fråga om när ramlagen ska tillämpas och när den inte är tillämplig. Det är också viktigt att ge de behöriga myndigheterna förutsättningar att kunna utveckla en gemensam syn på olika tillämpningsfrågor. Det gäller särskilt myndigheterna i rättskedjan.

Mot denna bakgrund anser regeringen att det finns anledning att i det följande redogöra för ett antal allmänna principer som presenterats i delbetänkandet Brottsdatalag (SOU 2017:29) i vägledande syfte. Utredningen utvecklar dessa principer ytterligare genom exempel från olika verksamheter inom ramlagens tillämpningsområde (se SOU 2017:29 s. 185–234). Det kan tilläggas att utredningens redovisning inte är någon uttömmande genomgång av vad som kan göra ramlagen tillämplig.

För att ge ytterligare vägledning behandlas ett flertal gränsdragningsfrågor med exempel i författningskommentaren.

Om någon annan än en behörig myndighet behandlar personuppgifter är ramlagen inte tillämplig

Ett grundläggande krav för att ramlagen ska vara tillämplig är att den som behandlar personuppgifterna är en behörig myndighet i lagens mening och att behandlingen görs för något av de syften som anges där. Som framgår av avsnitt 6.4.4 pekas det inte ut vilka myndigheter som är behöriga. Det är enligt den föreslagna definitionen de myndigheter som fullgör uppgifter inom ramlagens tillämpningsområde och andra aktörer som utövar myndighet i samma syften som är behöriga. Är den som behandlar personuppgifterna inte en behörig myndighet gäller inte ramlagen för personuppgiftsbehandlingen.

Många myndigheter och andra aktörer är skyldiga att anmäla om det uppstått misstanke om brott. En sådan skyldighet medför inte att anmälaren ska betraktas som behörig myndighet i ramlagens mening, om anmälaren varken har ett brottsbekämpande uppdrag eller utövar myndighet för de syften som ramlagen omfattar.

Det förhållandet att en privat aktör har satt upp en övervakningskamera t.ex. i en bank eller butikslokal i syfte att förebygga, avslöja eller utreda brott innebär inte heller att behandlingen av de personuppgifter som erhålls genom övervakningen görs av en behörig myndighet i ramlagens mening. Företaget eller personen i fråga ägnar sig nämligen inte åt myndighetsutövning.

Varken typen av personuppgiftsbehandling eller personuppgiftens karaktär är avgörande för om ramlagen ska tillämpas

Det är, som tidigare nämnts, syftet med behandlingen av personuppgifter i det enskilda fallet som avgör om behandlingen över huvud taget omfattas av ramlagens tillämpningsområde. Genom att syftet avgör när det gäller personuppgiftsbehandling som omfattas av unionsrätten, kan en behörig myndighets behandling av samma personuppgift antingen styras av ramlagens eller dataskyddsförordningens regler. Typen av personuppgiftsbehandling, vilken verksamhet den behandlas i eller personuppgiftens karaktär är alltså inte avgörande för vilket regelverk som ska tillämpas.

Myndighetsutövning som har överlåtits till andra än myndigheter

I viss lagstiftning överlåts myndighetsutövning inom ramlagens tillämpningsområde till andra aktörer. Är det fråga om myndighetsutövning för ett sådant syfte som anges i ramlagen ska ramlagen tillämpas på behandlingen av personuppgifter, t.ex. när föremål tas i beslag för att säkra utredningen av ett brott eller framtida förverkande. Den som har rätt att vidta sådana åtgärder anses nämligen vara en behörig myndighet i ramlagens mening. Det gäller t.ex. om en tjänsteman i Havs- och vattenmyndigheten tar egendom i beslag för ett misstänkt fiskebrott eller om en annan aktör handhar verkställighet av en straffrättslig påföljd.

Ramlagen ska tillämpas i viss verksamhet för att stödja en behörig myndighet

Myndigheterna i rättskedjan behöver ibland stöd från myndigheter med annan kompetens. Sådan stödverksamhet kan avse t.ex. forensisk, medicinsk eller psykiatrisk kompetens. Stödet kan också avse särskilda resurser. Den som har en författningsreglerad skyldighet att biträda behöriga myndigheter med särskild kompetens eller särskilda resurser bör vid utförandet av sådana uppgifter anses som behörig myndighet och tillämpa ramlagen.

Annat stöd som inte är författningsreglerat och som lämnas till en behörig myndighet av en myndighet eller annan aktör som inte själv är behörig myndighet i ramlagens mening ligger däremot utanför ramlagens tillämpningsområde, t.ex. stöd från myndigheter som deltar i olika insatser för att förebygga brott eller att samverka mot brott och oordning. Ett exempel är när en statlig myndighet som t.ex. Pensionsmyndigheten bistår åklagare i förundersökningar om ekonomisk brottslighet.

När de processuella reglerna om ansvar för brott gäller för talan som kumuleras med ansvarstalan ska ramlagen tillämpas

I brottmål får i viss utsträckning talan föras om annat än ansvar för brott. När de processuella reglerna om talan om ansvar för brott tillämpas på en talan som rör något annat, som t.ex. enskilda anspråk, rör det sig om frågor som är så intimt förknippade med varandra att vikten av en gemensam process enligt brottmålsreglerna ansetts väga över andra intressen. Då bör sidofrågan anses vara så oupplösligt förenad med ansvarsfrågan att ramlagen bör tillämpas vid personuppgiftsbehandlingen. Ramlagen bör också tillämpas vid bevistalan mot någon under 15 år.

Om sambandet med ansvarsfrågan upphör, bör ramlagen inte tillämpas på den fortsatta handläggningen. Enskilda anspråk som överklagas enbart av enskild part är exempel på det.

Ramlagen ska inte tillämpas av den som får tillgång till ett visst register eller en viss typ av uppgifter

Den omständigheten att någon som inte har brottsbekämpande, lagförande, straffverkställande eller ordningshållande uppdrag ges tillgång till ett register som förs av en myndighet med ett sådant uppdrag innebär inte att den förra ska betraktas som behörig myndighet. Det gäller även den som på annat sätt får del av uppgifter om lagöverträdelser. Den som får tillgång till domar eller till vissa uppgifter ur t.ex. belastningsregistret eller registret över tillträdesförbud blir alltså inte en behörig myndighet av det skälet. För att ramlagen ska vara tillämplig krävs att uppgifterna i fråga behandlas av en behörig myndighet för något av de syften som ramlagen anger.

Kontrollverksamhet och allmän övervakning

Flera av de myndigheter som har till uppgift att bekämpa brott bedriver också i större eller mindre utsträckning kontrollverksamhet. Det gäller framför allt Polismyndigheten, Tullverket, Kustbevakningen och Skatteverket. Det kan gälla exempelvis gränskontroll, tullkontroll, utlänningskontroll eller skattekontroll. Personuppgiftsbehandling inom ramen för sådan kontrollverksamhet ligger utanför ramlagens tillämpningsområde i den mån den inte utförs i brottsbekämpande syfte. Det gäller även i de fall där kontrollen utförs av tjänstemän som också har brottsbekämpande uppgifter.

Förutom författningsreglerad kontrollverksamhet bedriver vissa brottsbekämpande myndigheter också allmän övervakning. Den allmänna övervakningen är oreglerad och har inte så konkret utformning eller tydligt brottsbekämpande syfte att behandlingen av personuppgifter kan hänföras under ramlagen.

Ramlagen ska inte tillämpas när syftet med behandlingen inte längre är brottsbekämpning eller något annat som regleras i lagen

Personuppgifter som från början behandlas för något av de syften som är en förutsättning för att ramlagen ska vara tillämplig kan med tiden visa sig sakna betydelse för dessa syften. Som exempel kan nämnas att Tullverket tar en viss mängd vitt pulver i beslag i tron att det är fråga om narkotika men att det senare visar sig vara något som inte är straffbart att inneha. Utöver den behandling av personuppgifter som är nödvändig för att avsluta ärendet och arkivera det får uppgifterna inte längre behandlas i den brottsbekämpande verksamheten. Ramlagen är då inte längre tillämplig. Att ett enskilt anspråk som ursprungligen har behandlats tillsammans med frågan om ansvar för brottet avskiljs för handläggning i den för tvistemål föreskrivna ordningen är ett annat exempel på när ramlagen inte längre ska tillämpas.

7 Rättslig grund och ändamål för behandling av personuppgifter

7.1 Skillnad mellan bestämmelser om rättslig grund för behandling och ändamålsbestämmelser

Regeringens bedömning: Det bör göras tydligare skillnad mellan bestämmelser om rättslig grund för behandling och ändamålsbestämmelser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten, Malmö kommun* och *Uppsala universitet* ser positivt på att det görs tydligare skillnad mellan bestämmelser om rättslig grund och bestämmelser om ändamål. Övriga remissinstanser yttrar sig inte i denna del.

Skälen för regeringens bedömning

Dagens ändamålsbestämmelser

En grundläggande princip för all personuppgiftsbehandling är att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. De får inte heller behandlas för något ändamål som är oförenligt med det ändamål för vilket de samlades in. I registerförfattningar finns det därför normalt bestämmelser om för vilka ändamål personuppgifter får behandlas. Syftet är att ange ramen för vilken behandling som är tillåten. På så sätt kan användning och spridning av personuppgifter begränsas.

I de brottsbekämpande myndigheternas registerförfattningar delas ändamålen upp i primära och sekundära, se bl.a. 2 kap. 7 och 8 §§ polisdatalagen, 2 kap. 5 och 6 §§ åklagardatalagen och 2 kap. 5 och 6 §§ tullbrottsdatalagen. Bestämmelserna har samma utformning och liknande innehåll. De primära ändamålen reglerar behandlingen av de personuppgifter som behövs i den berörda myndighetens egen brottsbekämpande verksamhet. Polismyndigheten får t.ex. enligt 2 kap. 7 § polisdatalagen behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra förpliktelser som följer av internationella åtaganden. De sekundära ändamålen reglerar i vilken utsträckning personuppgifter som behandlas för något av de primära ändamålen får behandlas för att lämnas ut till andra myndigheter eller till enskilda för att tillgodose deras behov. Tullverket får t.ex. enligt 2 kap. 6 § tullbrottsdatalagen behandla redan insamlade uppgifter när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos vissa andra myndigheter. Det kan också vara fråga om att personuppgifter i den brottsbekämpande verksamheten behöver lämnas till verksamhet i samma myndighet som inte är brottsbekämpande för den verksamhetens behov.

Syftet med uppdelningen i primära och sekundära ändamål är att göra det tydligt både hur personuppgifter får användas i den brottsbekäm-

pande verksamheten och för vilka ändamål uppgifterna får behandlas för att lämnas ut till andra.

Informationshanteringsutredningens slutsatser

Informationshanteringsutredningen (Ju 2011:11) anser att det har skett en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilda bestämda ändamål respektive tillåtna rättsliga grunder för behandling. Det finns enligt den utredningen risk att tillämparen blandar samman ändamål med rättslig grund och godtar ett i författning bestämt allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål och drar den felaktiga slutsatsen att kravet på att det ska finnas särskilda, uttryckligt angivna och berättigade ändamål för behandlingen därmed är uppfyllt. Informationshanteringsutredningen anser att det skulle ge ett bättre integritetsskydd om personuppgiftsansvariga enbart vore hänvisade till att, utifrån de grundläggande kraven i 9 § första stycket c personuppgiftslagen, på eget ansvar formulera ändamål som är tillräckligt specifika för att ge ledning för vilka personuppgifter som är adekvata och inte för många för den aktuella behandlingen. Därför innehåller förslaget till myndighetsdatalag inga ändamålsbestämmelser och förutsätter inte heller att sådana ska finnas. I förslaget anges endast att personuppgifter får behandlas om det är nödvändigt för att en myndighet ska kunna utföra sin verksamhet (SOU 2015:39 s. 277 f.).

Förslaget har fått ett blandat mottagande. Vissa remissinstanser anser att ändamålsbestämmelser har betydelse för att göra det tydligt för enskilda inom vilka ramar myndigheter får samla in och behandla personuppgifter och menar att den föreslagna bestämmelsen är alltför vag. Andra är positiva till förslaget och framhåller att det förenklar bedömningen av vilken personuppgiftsbehandling som är tillåten.

Bestämmelser om rättslig grund

Både dataskyddsdirektivet och dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund för att vara laglig. Det är alltså endast om det finns en rättslig grund som personuppgifter överhuvudtaget får behandlas.

Kravet på att det alltid ska finnas en rättslig grund för behandlingen av personuppgifter är inte nytt. Det framgår av artikel 7 i 1995 års dataskyddsdirektiv och kommer till uttryck i bl.a. 10 § personuppgiftslagen. Det förs dock inga resonemang kring kravet på rättslig grund i förarbetena till de brottsbekämpande myndigheternas registerförfattningar. Regeringen håller därför med utredningen om att det finns skäl att nu lyfta fram den frågan och diskutera hur kravet på rättslig grund förhåller sig till de primära och sekundära ändamålen i registerförfattningarna.

I likhet med utredningen anser regeringen att det finns fog för Informationshanteringsutredningens uppfattning att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. Det är därför lämpligt att det görs tydligare skillnad mellan bestämmelser om rättslig grund och ändamålsbestämmelser. Hur man bör se på ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar behandlas i avsnitt 7.5.

7.2 Rättslig grund för behandling – huvudregeln

Regeringens förslag: Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Med en behörig myndighets uppgift avses en uppgift som framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Polismyndigheten* anser att begreppet behövs bör användas i lagtexten i stället för begreppet nödvändigt. Myndigheten uttrycker även oro för att kravet på att uppgiften ska vara reglerad motverkar myndigheternas arbete med att utveckla arbetsmetoder och samverkan med andra aktörer. *Datainspektionen* väcker frågan om det förhållandet att underrättelseverksamheten i viss utsträckning är oreglerad kan leda till problem när det gäller att fastställa rättslig grund för behandling av personuppgifter i sådan verksamhet. Övriga remissinstanser yttrar sig inte särskilt om förslaget.

Skälen för regeringens förslag

När finns det rättslig grund för behandlingen?

Som anges i avsnitt 7.1 utgår dataskyddsregleringen från att varje behandling av personuppgifter måste ha en rättslig grund för att vara laglig.

Enligt artikel 8.1 i direktivet är behandling av personuppgifter laglig endast om behandlingen är nödvändig för att en behörig myndighet ska kunna utföra en uppgift på grundval av unionsrätt eller nationell rätt i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder eller skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten. För att uppfylla direktivets krav måste nationell rätt ange ramarna för när behandling av personuppgifter är tillåten. Den rättsliga grunden bör enligt skäl 33 vara tydlig och precis och dess tillämpning förutsägbar för dem som omfattas av den. I ramlagen bör det därför tas in bestämmelser som anger vad som är tillåtna rättsliga grunder för behandling av personuppgifter.

Tillämpningsområdet och den rättsliga grunden uttrycks på ett korresponderande sätt i direktivet. Samma uttryckssätt som används för att avgränsa ramlagens tillämpningsområde bör därför användas i bestämmelsen om rättslig grund (se avsnitt 6.4.2 och 6.4.3). Det innebär att den uppgift som ska ligga till grund för personuppgiftsbehandlingen ska utföras av en behörig myndighet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Personuppgiftsbehandlingen ska vara nödvändig för uppgiften och ha stöd i unionsrätt eller nationell rätt.

Nödvändighetsrekvisitet

Personuppgiftsbehandlingen ska vara nödvändig för att den behöriga myndigheten ska kunna utföra sina uppgifter. Enligt Svenska Akademiens Ordbok betyder ordet ”nödvändig” att någonting absolut fordras eller inte kan underlåtas. I unionsrätten har kravet på nödvändighet inte samma strikta innebörd. Artikel 7 i 1995 års dataskyddsdirektiv har inte ansetts utgöra ett krav på att det ska vara omöjligt att fullgöra förpliktelsen eller utföra uppgiften utan att personuppgifter behandlas (Integritet – Offentlighet – Informationsteknik, SOU 1997:39, s. 359). Den slutsatsen får stöd av ett avgörande av EU-domstolen i vilket domstolen uttalar att en myndighets förande av ett centralt register över uppgifter som redan fanns i regionala register är nödvändigt om det bidrar till att effektivisera tillämpningen av relevanta bestämmelser (dom av den 16 december 2008, Huber, C-524/06). Domen bör kunna utgöra stöd även för tolkningen av det nya direktivet. Ordet ”nödvändig” bör därför tolkas som att det är fråga om något som behövs för att på ett effektivt sätt kunna utföra arbetsuppgiften.

Polismyndigheten förespråkar att begreppet ”behövs” används i lagtexten för att undvika bokstavstolkningar med icke avsedda begränsningar som följd. I bestämmelsen om rättslig grund i artikel 6.1 i dataskyddsförordningen anges att behandling är laglig om den är nödvändig i vissa angivna fall. Regeringen anser därför, i likhet med utredningen, att ordet ”nödvändigt” bör användas även i ramlagen. En enhetlig terminologi bör, som flertalet remissinstanser påpekar, underlätta tillämpningen av dataskyddsregelverket. Personuppgifter ska alltså få behandlas bara om det är nödvändigt för att utföra vissa uppgifter.

I kravet på nödvändighet ligger att personuppgifter inte får behandlas om syftet med behandlingen kan uppnås med andra medel, t.ex. genom att anonymisera uppgifterna.

Stöd för behandlingen i unionsrätt eller nationell rätt

Den uppgift som den behöriga myndigheten ska utföra ska ha stöd i unionsrätt eller nationell rätt. Frågan är vad som avses med det. Regeringen håller med utredningen om att det inte kan vara personuppgiftsbehandlingen i sig som avses. Om så skulle vara fallet skulle de behöriga myndigheterna endast kunna behandla personuppgifter för att utföra sina uppgifter i den utsträckning det, utöver den reglering som fastställer uppgiften, också finns uttryckliga bestämmelser om att personuppgifter får behandlas för att utföra den uppgiften. Artikeln bör i stället tolkas så att personuppgiftsbehandlingen alltid ska gå att härleda till den behöriga myndighetens uppgifter så som de kommer till uttryck i unionsrätten eller i nationell lagstiftning och andra för verksamheten bindande beslut om arbetsuppgifter. Det bör framgå av ramlagen. I bestämmelsen bör därför anges att uppgiften ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt den behöriga myndigheten att utföra en sådan uppgift. Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU-rättsakter här i landet med den verkan som följer av EU-fördragen. Unionsrätten är därmed en del av den svenska rättsordningen. EU-förordningar är att jämställa med svensk lag.

Grunden för att behandla personuppgifter finns alltså i regleringen av den behöriga myndighetens uppgifter. Som exempel kan nämnas att det i 2 § polislagen (1984:387) anges att en av Polismyndighetens huvuduppgifter är att utreda och beivra brott. Den arbetsuppgiften preciseras av bestämmelser i framför allt rättegångsbalken som reglerar hur förundersökning ska bedrivas och i vilka fall en polisman får utfärda föreläggande om ordningsbot. Ytterligare bestämmelser finns i bl.a. lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare och olika lagar om användningen av straffprocessuella tvångsmedel. På motsvarande sätt anges det i 3 § förordningen (2007:853) med instruktion för Kustbevakningen att myndigheten bl.a. ska bedriva övervakning för att förebygga och ingripa mot störningar i sjötrafiken, förhindra och upptäcka brottslig verksamhet, ingripa vid misstanke om brott och utreda och beivra eller bistå med utredningen av brott. Vilka brott Kustbevakningen har till uppgift att ingripa mot framgår bl.a. av lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning och lagen (2000:1225) om straff för smuggling. Hur det ska göras regleras framför allt i rättegångsbalken och nyss nämnda lagar. Regleringar av motsvarande slag finns för övriga behöriga myndigheter.

Grunden för att behandla personuppgifter kan även finnas i regler som primärt gäller för andra myndigheter. Skyldigheten enligt 23 kap. 3 § andra stycket rättegångsbalken att biträda åklagare vid brottsutredning utgör rättslig grund för att polisen ska kunna överlämna personuppgifter till åklagare i det brottsbekämpande arbetet. Motsvarande bestämmelser finns för Tullverket, Skatteverket och Kustbevakningen.

Genom de författningar och regeringsbeslut som reglerar den verksamhet i vilken personuppgifterna behandlas, tillsammans med ramlagen och registerförfattningarna, är enligt regeringens mening kravet i direktivet på att behandlingen ska ha stöd i unionsrätt eller nationell rätt uppfyllt.

Polismyndigheten anför att arbetet med att utveckla nya arbetsmetoder och samverkansformer inte bör motverkas genom otillräckliga förutsättningar. För Polismyndighetens del anser regeringen att 2 § polislagen många gånger bör kunna ge rättsligt stöd för personuppgiftsbehandling i sådana situationer. Eftersom stödet för arbetsuppgiften inte behöver finnas i lag utan även kan framgå av förordning eller annat beslut av regeringen bör det, som *Uppsala universitet* påpekar, finnas tillräckliga verktyg för att i övrigt möjliggöra flexibilitet. Här kan även påpekas att myndigheters verksamhet enligt den svenska legalitetsprincipen måste vara fastställd i enlighet med svensk rätt. *Datainspektionen* lyfter frågan om rättslig grund för behandling av personuppgifter i underrättelseverksamhet. Även om underrättelseverksamheten i vissa avseenden inte är lika reglerad som t.ex. brottsutredande verksamhet så har de myndigheter som bedriver underrättelseverksamhet ålagts den uppgiften i författning, t.ex. framgår det av 3 § förordningen (2007:853) med instruktion för Kustbevakningen att Kustbevakningen ska förhindra och upptäcka brottslig verksamhet. Författningsstödet för uppgiften tillsammans med ramlagen och registerförfattningarna, ger enligt regeringens mening rättslig grund för personuppgiftsbehandlingen.

Lagrådet har uttalat att planering, uppföljning och utvärdering av verksamhet är en integrerad del av själva verksamheten och inte någon fristående aktivitet som behöver regleras särskilt i registerförfattningar. Det

har därför ansetts att det inte behövs någon särskild bestämmelse som ger stöd för behandling av personuppgifter för bl.a. planering och uppföljning av verksamheten (se t.ex. Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling, prop. 2004/05:164, s. 179 och Åklagardatalag, prop. 2014/15:63, s. 63). Någon särskild bestämmelse om att sådan behandling är tillåten behövs därför inte i ramlagen. Enligt utredningen bör motsvarande bedömning göras när det gäller registervård. Personuppgiftsansvariga måste kunna behandla personuppgifter om det behövs för att se till att bestämmelserna om personuppgiftsbehandling efterlevs. Regeringen håller med utredningen om att registervård måste anses vara en integrerad del av den personuppgiftsansvariges skyldigheter enligt ramlagen och registerförfattningarna och att det följaktligen inte behöver regleras särskilt att personuppgiftsbehandling för registervård är tillåten. Datainspektionen delar den bedömningen.

7.3 Rättslig grund i undantagsfall för diarieföring och handläggning

Regeringens förslag: Personuppgifter får alltid behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* tillstyrker förslaget. *Dataskydd.net* anser att den bestämmelse som föreslås bör ändras på sådant sätt att den kräver användning av pseudonymiserade uppgifter i så hög utsträckning som möjligt. Övriga remissinstanser yttrar sig inte särskilt om förslaget.

Skälen för regeringens förslag: De myndigheter som ska tillämpa ramlagen tar dagligen emot stora mängder information av vitt skilda slag, ofta i elektronisk form. De inkommande uppgifterna kan utgöra en del av en allmän handling i tryckfrihetsförordningens mening. Enligt 5 kap. 1 § offentlighets- och sekretesslagen ska som huvudregel allmänna handlingar som kommit in till en myndighet registreras, dvs. diarieföras, så snart som möjligt. Syftet är bl.a. att garantera allmänhetens tillgång till allmänna handlingar. En myndighet måste därför alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande anmälningar, ansökningar och liknande. Det gäller även i de fall där den behöriga myndigheten inte behöver behandla personuppgifterna för att utföra sina uppgifter (prop. 2009/10:85 s. 112 f.). Det bör i ramlagen tydliggöras att det är en tillåten rättslig grund för behandling.

I skäl 16 finns det stöd för att ha en sådan bestämmelse om rättslig grund. Där uttalas nämligen att direktivet inte påverkar principen om allmänhetens rätt att få tillgång till allmänna handlingar.

Dataskydd.net förespråkar ett krav på pseudonymisering vid diarieföring och handläggning i syfte att öka dataskyddet. Som utvecklas i avsnitt 8.1.5 följer det av de grundläggande kraven på behandling av personuppgifter att avidentifiering bör användas i så stor utsträckning som

möjligt. Kan en uppgift utföras tillfredsställande även om personuppgifterna utelämnas är de grundläggande kraven på adekvans och personuppgifternas omfattning inte uppfyllda (jfr SOU 2015:39 s. 285). Som sagts ovan förutsätter emellertid myndigheternas skyldighet att bl.a. garantera allmänhetens tillgång till allmänna handlingar att de handlingar som inkommit diarieförs och behandlas i oförändrat skick. Mot denna bakgrund finns det enligt regeringen inte skäl att införa ett krav på pseudonymisering i den bestämmelse som nu föreslås.

7.4 Behandling bara för särskilda, uttryckligt angivna och berättigade ändamål

Regeringens förslag: Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte särskilt om förslaget. *Justitiekanslern* anser att bestämmelsen är mycket allmänt hållen och har svårt att förstå innebörden av den och hur den kommer att förhålla sig till registerförfattningarna. Även *Domstolsverket* tycker att det bör klargöras vad som avses med ändamål i bestämmelsens mening. Enligt Domstolsverket ställer direktivet krav på att det i författning regleras för vilka specifika ändamål en behörig myndighet får behandla personuppgifter. *Uppsala universitet* anser att utredningens tolkning av direktivets krav på reglering av ändamål förefaller rimlig, liksom förslaget att ändamålet ska dokumenteras särskilt om det inte framgår av sammanhanget.

Skälen för regeringens förslag

Behandling för särskilda, uttryckligt angivna och berättigade ändamål

Den omständigheten att viss behandling är rättsligt grundad innebär inte att vilka personuppgifter som helst får behandlas eller att det får göras på valfritt sätt. Den personuppgiftsansvarige måste också iaktta övriga krav som gäller för behandling av personuppgifter.

I artikel 4.1 b i direktivet anges bl.a. att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Liknande reglering finns i artikel 6.1 b i 1995 års dataskyddsdirektiv, som har genomförts genom 9 § första stycket c personuppgiftslagen. En liknande bestämmelse bör tas in i ramlagen.

Att ändamålen ska vara särskilda innebär att de måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska kunna avgöras att inte för många uppgifter behandlas (se avsnitt 8.1.2). Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Ändamålen ska anges uttryckligen redan när personuppgifterna samlas in.

Att ändamålen ska vara berättigade innebär enligt regeringens mening en koppling till den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden. Kravet på att ändamålet för behandlingen ska vara berättigat kan också sägas innebära ett krav på att behandlingen ska vara förenlig med konstitutionella och andra rättsliga principer. Genom att det i stor utsträckning är reglerat vilken personuppgiftsbehandling som kan aktualiseras på området för brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet har lagstiftaren redan tagit ställning till att personuppgiftsbehandlingen är berättigad i de fallen.

Det är dock inte bara när personuppgifter samlas in som det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen. Varje åtgärd som vidtas med insamlade uppgifter ska naturligtvis också uppfylla de kraven (jfr prop. 2009/10:85 s. 98). I ramlagen bör det därför tydliggöras att all behandling ska utföras för särskilda, uttryckligt angivna och berättigade ändamål.

Bestämmelsen tar sikte på ändamålen i det enskilda fallet som t.ex. en förundersökning om ett visst brott eller ett ärende om förordnande av målsägandebiträde i ett visst fall. I avsnitt 9.2.7 föreslås att ändamålen med behandlingen ska förtecknas i det register som myndigheten ska föra och i avsnitt 10.2.6 att den personuppgiftsansvarige ska tillhandahålla allmän information om ändamålen med behandlingen. Det innebär inte att den personuppgiftsansvarige måste förteckna respektive lämna information om alla de enskilda fall där myndigheten behandlar personuppgifter. Det som avses är de typer av ändamål som myndigheten behandlar personuppgifter för. Som exempel kan nämnas att Polismyndigheten behandlar personuppgifter bl.a. för att ta emot anmälningar om brott, genomföra förundersökningar, verkställa uppbörd av bötesstraff och dokumentera ingripanden vid ordningsstörningar och att Kriminalvården behandlar personuppgifter för att verkställa olika straffrättsliga påföljder och hantera vissa andra frihetsberövanden.

I artikel 8.2 anges att nationell rätt åtminstone ska specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål. Uttrycken ”syftet med behandlingen” och ”behandlingens ändamål” används ofta synonymt när man diskuterar personuppgiftsbehandling. Frågan är om det finns någon saklig skillnad mellan uttrycken. I den engelska språkversionen av direktivet används uttrycken ”objectives of processing” och ”purposes of the processing”. Orden objectives och purposes är också synonymer. Användningen av obestämd form i det första uttrycket men bestämd form i det senare kan tolkas som att det första uttrycket avser bestämmelser om rättslig grund (brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet), medan det andra avser ändamålen för behandlingen i det enskilda fallet. Om någon skillnad är avsedd är det enligt regeringens mening den enda rimliga tolkningen.

Regeringen anser därmed, i likhet med *Uppsala universitet* men till skillnad mot *Domstolsverket*, att den föreslagna generella bestämmelsen om rättslig grund i ramlagen tillsammans med bestämmelsen om att personuppgifter ska behandlas för särskilda, uttryckligt angivna och berättigade ändamål, uppfyller kraven i direktivet på hur regleringen ska vara

utformad. Innebörden av den nu föreslagna bestämmelsen och hur den förhåller sig till registerförfattningarna, frågor som *Justitiekanslern* och *Domstolsverket* väcker, utvecklas vidare i avsnitt 7.5. Frågan om det bör regleras vilka personuppgifter som får behandlas diskuteras i avsnitt 8.1.5.

Ändamålen ska framgå

En särskild fråga är vad som avses med att ändamålen ska vara uttryckligt angivna. Det finns i dag inget generellt krav på att ändamålsbestämningen ska dokumenteras. Enligt 3 kap. 3 § polisdatalagen och 4 kap. 2 § kustbevakningsdatalagen ska det dock genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifter som har gjorts gemensamt tillgängliga behandlas. Bestämmelserna tillkom i samband med att möjligheten att göra uppgifter gemensamt tillgängliga reglerades. Syftet är att ge den som söker information motsvarande upplysningar som han eller hon skulle ha fått om uppgifterna hade behandlats i traditionella register. Motsvarande gäller för Tullverkets och Skatteverkets brottsbekämpande verksamhet.

Oftast framgår det av sammanhanget för vilket ändamål personuppgifter behandlas (t.ex. för förundersökningen om ett visst brott, handläggningen av ett visst mål eller ärende eller verkställigheten av ett visst straff). Behovet av att upplysa om för vilka ändamål personuppgifter behandlas gör sig framför allt gällande i den del av den brottsbekämpande verksamheten där det långtifrån alltid framgår av omständigheterna för vilket ändamål uppgifter behandlas, t.ex. i underrättelseverksamheten. Det bör finnas möjlighet att kunna kontrollera för vilket eller vilka ändamål personuppgifter behandlas oavsett i vilken verksamhet det görs. Det underlättar både för den enskilde och för tillsynsmyndigheten om ändamålet är tydligt. Om det ändamål för vilket personuppgifter behandlas inte framgår av sammanhanget eller på annat sätt bör det därför tydliggöras genom en särskild upplysning. En bestämmelse om det bör tas in i ramlagen.

Det krav på att ändamålet för behandlingen ska framgå som gäller för några av de behöriga myndigheterna omfattar bara uppgifter som har gjorts gemensamt tillgängliga. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga (se t.ex. 3 kap. 1 § polisdatalagen). Om uppgifter behandlas av en liten, klart avgränsad grupp vet de inblandade personerna som regel varifrån uppgifterna kommer och varför de behandlas. Mot den bakgrunden kan det finnas skäl att göra undantag från kravet på särskild upplysning för uppgifter som inte har gjorts gemensamt tillgängliga. Regeringen återkommer till den frågan i samband med att de brottsbekämpande myndigheterna registerförfattningar anpassas till den nya ramlagen.

7.5 Är dagens primära och sekundära ändamålsbestämmelser snarare bestämmelser om rättslig grund?

Regeringens bedömning: Bestämmelserna i de brottsbekämpande myndigheternas registerförfattningar som kallas primära och sekundära ändamålsbestämmelser bör snarare ses som en del av den rättsliga grunden för behandling av personuppgifter.

Utredningens bedömning stämmer överens med regeringens.
Remissinstanserna: Ingen remissinstans invänder mot bedömningen.

Skälen för regeringens bedömning

De primära ändamålsbestämmelserna

Som framgår av avsnitt 7.1 anser regeringen att det finns fog för Informationshanteringsutredningens uppfattning att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. Det kan leda till att tillämparen förväxlar ändamål med rättslig grund och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål i det enskilda fallet. Ett exempel som utredningen tar upp är uppgiftssamlingen benämnd ”Kringresande” som fördes av Polismyndigheten i Skåne. Säkerhets- och integritetsskyddsnämnden kritiserade vid sin granskning bl.a. att ändamålet med personuppgiftsbehandlingen var alldeles för vitt. Personuppgifterna hade samlats in för specifika ändamål men lagrades och behandlades sedan i uppgiftssamlingen för ändamålet länsövergripande brottslighet. Ändamålet låg visserligen inom ramen för sådan underrättelseverksamhet som avses i 2 kap. 7 § 1 polisdatalagen. Det uppfyllde dock enligt Säkerhets- och integritetsnämnden inte det grundläggande kravet på att behandling bara ska utföras för särskilda, uttryckligt angivna och berättigade ändamål (uttalande den 15 november 2013, dnr 173–2013).

Enligt förslaget i avsnitt 7.4 ska all behandling av personuppgifter utföras för särskilda, uttryckligt angivna och berättigade ändamål. Som anges i det avsnittet är det i förhållande till ändamålen som det ska prövas vilka personuppgifter som är adekvata och relevanta för behandlingen och att inte för många personuppgifter behandlas. Prövningen av att personuppgifter inte behandlas under längre tid än nödvändigt ska också ske i förhållande till ändamålen (avsnitt 8.2.2). Ändamålen måste därmed vara tillräckligt specifika för att ge ledning för dessa bedömningar.

Som utredningen påpekar måste författningsbestämmelser som anger för vilket eller vilka ändamål personuppgifter får behandlas i en viss verksamhet vara generellt utformade, eftersom de ska kunna tåla utvecklingen av ny teknik och vissa förändringar i myndighetens sätt att arbeta. En ändamålsbestämmelse bör dock samtidigt ge ledning för prövningen av vilka personuppgifter som är adekvata och relevanta för behandlingen.

Regeringen delar mot denna bakgrund utredningens bedömning att de primära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar snarare bör ses som bestämmelser om rättslig

grund. Bestämmelserna tydliggör att personuppgiftsbehandling är tillåten när arbetsuppgifterna fullgörs. När de brottsbekämpande myndigheternas registerförfattningar anpassas till den nya ramlagen kommer regeringen att ta ställning till om innehållet i de primära ändamålsbestämmelserna bör behållas.

De sekundära ändamålsbestämmelserna

Av avsnitt 7.1 framgår att de sekundära ändamålsbestämmelserna reglerar i vilken utsträckning personuppgifter som behandlas för något primärt ändamål även får behandlas för att lämnas till andra för att tillgodose deras behov. Enligt bestämmelserna får personuppgifter behandlas framför allt för att ge andra myndigheter information som behövs i viss typ av verksamhet där, eller för att lämna information till andra verksamheter inom den egna myndigheten för att de ska kunna utföra en viss arbetsuppgift.

På samma sätt som de primära ändamålsbestämmelserna är de sekundära i stor utsträckning allmänt hållna. I 2 kap. 8 § polisdatalagen anges t.ex. i punkten 1 att personuppgifter får lämnas ut om de behövs i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket. Det motsvarar de primära ändamålsbestämmelserna i de mottagande myndigheternas registerförfattningar. Även de sekundära ändamålsbestämmelserna bör därför enligt regeringens mening snarare ses som bestämmelser om rättslig grund. I samband med att de brottsbekämpande myndigheternas registerförfattningar anpassas till ramlagen, kommer regeringen att även ta ställning till om innehållet i de sekundära ändamålsbestämmelserna bör behållas.

7.6 Behandling för nya ändamål

7.6.1 Nuvarande reglering av behandling för nya ändamål

I 9 § första stycket d personuppgiftslagen finns en generell bestämmelse om vidarebehandling. Där regleras finalitetsprincipen, enligt vilken personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Bestämmelsen gäller för alla myndigheter i rättskedjan.

De sekundära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar innehåller särskilda regler om vidarebehandling. De reglerar, som framgår av avsnitt 7.5, när det är tillåtet att behandla personuppgifter som behandlas för något av de primära ändamålen för att tillhandahålla information till andra myndigheter eller till andra verksamheter inom den egna myndigheten för deras behov. Det handlar alltså alltid om behandling av redan insamlade uppgifter för nya ändamål. Av t.ex. 2 kap. 6 § skattebrottsdatalagen följer att personuppgifter som behandlas i Skatteverkets brottsbekämpande verksamhet även får behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos andra brottsbekämpande

myndigheter. Syftet med de sekundära ändamålsbestämmelserna är att underlätta för tillämparen. Han eller hon behöver endast avgöra om det är nödvändigt att lämna information som behövs i en annan brottsbekämpande myndighets verksamhet men tvingas inte att i de situationer som anges i den sekundära ändamålsbestämmelsen avgöra om utlämnandet är förenligt med det ursprungliga ändamålet med personuppgiftsbehandlingen. De sekundära ändamålen är inte uttömmande. För att personuppgifter som behandlas för ett primärt ändamål ska få vidarebehandlas för något annat ändamål än de sekundära, måste det emellertid göras en bedömning att vidarebehandlingen är förenlig med finalitetsprincipen. De sekundära ändamålen omfattar behandling för ändamål som ligger både inom och utanför den föreslagna ramlagens tillämpningsområde. I avsnitt 7.6.2 behandlas vad som föreslås gälla i fråga om behandling för nya ändamål inom ramlagens tillämpningsområde. Behandling för nya ändamål utanför ramlagens tillämpningsområde behandlas i avsnitt 7.6.3 och 7.6.4.

7.6.2 Nya ändamål inom ramlagens tillämpningsområde

Regeringens förslag: Innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att
1. det finns en rättslig grund för den nya behandlingen, och
2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Polismyndigheten* anser att den föreslagna prövningen stoppar upp processen med tröghet och ökad administration som följd, särskilt som utredningen anger att bedömningen inte bara ska göras för viss typsituation, utan även i det enskilda fallet. Enligt Polismyndigheten är det tillräckligt från integritetssynpunkt att de övriga kraven på behandling av personuppgifter följs även vid behandling för nya ändamål inom ramlagens tillämpningsområde. Myndigheten undrar vidare vad som avses med begreppet nödvändig i det här förslaget och tycker att det framstår som märkligt att ställa ett krav på proportionalitet just för behandling för nya ändamål, eftersom det kan tolkas som att annan behandling inte behöver vara proportionerlig. *Datainspektionen* anser att förslaget är en viktig begränsning av behöriga myndigheters möjligheter att behandla personuppgifter för nya ändamål, mot bakgrund av att finalitetsprincipen inte längre kommer att sätta gränsen för när behandling för nya ändamål får ske. *Sveriges advokatsamfund* anser, med hänvisning till regeringsformen, att förslaget bör kompletteras på så sätt att det i lagtexten även anges att det nya ändamålet ska vara godtagbart i ett demokratiskt samhälle. Övriga remissinstanser yttrar sig inte i denna del.

Behandling för nya ändamål inom ramlagens tillämpningsområde är förenlig med det ursprungliga ändamålet

Som framgår av avsnitt 6.4.1 gäller dataskyddsförordningen för all personuppgiftsbehandling som omfattas av unionsrätt men som inte ligger inom ramlagens tillämpningsområde. En behörig myndighet måste därför alltid avgöra om ändamålen med behandlingen av personuppgifter omfattas av ramlagens tillämpningsområde, oavsett om det är första gången en uppgift behandlas eller om den ska behandlas för nya ändamål. I detta avsnitt diskuteras behandling för nya ändamål inom ramlagens tillämpningsområde.

I artikel 4.1 b i direktivet regleras finalitetsprincipen, enligt vilken personuppgifter inte får behandlas på ett sätt som står i strid med insamlingsändamålet. Samtidigt framgår det av artikel 4.2 att behandling för andra ändamål inom direktivets tillämpningsområde än det för vilket personuppgifterna samlades in ska tillåtas, om den personuppgiftsansvarige enligt unionsrätten eller nationell rätt är bemyndigad att behandla personuppgifter för ett sådant ändamål och behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller nationell rätt. Regeringen håller med utredningen om att det måste innebära att all behandling för ändamål som ligger inom direktivets tillämpningsområde ska anses vara förenlig med insamlingsändamålen, under förutsättning att behandlingen är nödvändig och står i proportion till det nya ändamålet. Det saknar alltså betydelse om det är den personuppgiftsansvarige som ursprungligen samlat in personuppgifterna som utför behandlingen för det nya ändamålet eller om det är en annan personuppgiftsansvarig, så länge de båda är behöriga myndigheter och behandlingen ligger inom direktivets tillämpningsområde. Även behandling för att lämna ut personuppgifter till någon som inte är en behörig myndighet kan omfattas av direktivet, om ändamålet för den behandlingen ligger inom direktivets tillämpningsområde. Så kan vara fallet exempelvis om Polismyndigheten vid utredningen av ett bidragsbrott behöver skicka personuppgifter till Centrala studiestödsnämnden för att få information för utredningen av brottet. Om utlämnandet däremot enbart görs för att Centrala studiestödsnämnden ska kunna återkräva felaktigt utbetalda lån eller bidrag ligger ändamålet utanför ramlagens tillämpningsområde.

Mot denna bakgrund anser regeringen av samma skäl som utredningen redovisar, att det inte bör finnas någon bestämmelse om finalitetsprincipen i ramlagen.

Det ska vara nödvändigt och proportionerligt att personuppgifter behandlas för nya ändamål

Som framgår av avsnitt 7.2 och 7.4 ska det alltid finnas en rättslig grund och särskilda, uttryckligt angivna och berättigade ändamål för den personuppgiftsbehandling som utförs. Ändamålen har framför allt betydelse för att kunna kontrollera att de personuppgifter som behandlas är relevanta och adekvata för behandlingen och att inte för många personuppgifter behandlas (se avsnitt 8.1.2). Det är dock inte tillräckligt att kontrollera om personuppgifterna är adekvata och relevanta enbart när behand-

lingen påbörjas, utan det måste göras kontinuerligt. Finns det inte längre behov av att behandla personuppgifterna ska behandlingen av dem upphöra (se avsnitt 8.2.2).

Om personuppgifter behandlas för nya ändamål kan det leda till ökad spridning av uppgifterna genom att fler får tillgång till dem. Det kan också leda till att uppgifterna behandlas under längre tid än vad som var avsett från början. Behandling för nya ändamål kan därmed medföra ökat intrång i enskildas personliga integritet. Regeringen håller därför med *Datainspektionen* om att det är viktigt att en noggrann prövning görs innan personuppgifter behandlas för ett nytt ändamål. Mot detta behöver emellertid även ställas vikten av att myndigheterna ges möjlighet att använda insamlad information på ett effektivt sätt, i linje med vad *Polismyndigheten* anför. Att myndigheter kan använda information på ett effektivt sätt och även samverka och utbyta information med varandra är viktiga målsättningar i kampen mot bl.a. grov organiserad brottslighet och terrorism.

Enligt artikel 4.2 får personuppgifter behandlas för ett nytt ändamål om behandlingen är nödvändig och står i proportion till det nya ändamålet. Det innebär att det behöver prövas om det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet innan behandlingen påbörjas. Regeringen håller med utredningen om att det är fråga om en annan prövning än den som ska göras fortlöpande vid all personuppgiftsbehandling. Prövningen tar sikte på om det är nödvändigt och proportionerligt att de redan insamlade uppgifterna behandlas för ett nytt ändamål. För att tydliggöra att en särskild prövning krävs när personuppgifter ska behandlas för nya ändamål bör det, i motsats till vad *Polismyndigheten* tycker, tas in en bestämmelse i ramlagen som anger under vilka förutsättningar behandling för nya ändamål inom lagens tillämpningsområde är tillåten. Nedan beskrivs närmare vilken prövning som regeringen menar bör göras.

Det ska finnas en rättslig grund för den nya behandlingen

Artikel 4.2 är inte utformad på samma sätt som artikel 8.1, där den tillåtna rättsliga grunden för behandling regleras. Artiklarna innehåller dock enligt regeringens mening i grunden samma krav. Eftersom det alltid måste finnas en tillåten rättslig grund för behandling av personuppgifter gäller det naturligtvis även vid behandling för nya ändamål. En första förutsättning för att behandling för ett nytt ändamål ska vara tillåten bör därför vara att det finns en rättslig grund för den nya behandlingen. Det krävs alltså att den nya behandlingen är nödvändig för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Ett vanligt exempel är att det vid utredningen av ett brott upptäcks att brottet i fråga har betydelse för underrättelseverksamhet om annan brottslighet, t.ex. att vapen påträffas som skulle kunna ha samband med andra händelser. Ett annat exempel är att ett rutinmässigt dna-prov leder till att det blir träff på ett annat brott med tidigare okänd gärningsman.

Kravet på nödvändighet

För att behandling för ett nytt ändamål ska vara tillåten ska det också vara nödvändigt att personuppgifterna behandlas för det nya ändamålet. I bedömningen av om det finns en tillåten rättslig grund för behandling ingår överväganden om behandlingen är nödvändig för att en behörig myndighet ska kunna utföra vissa angivna uppgifter (se avsnitt 7.2). Det är inte klart om kravet på nödvändighet i artikel 4.2 avser något annat än det krav som ingår i bedömningen av om det finns rättslig grund för behandlingen. För en åklagare kan det t.ex. vara nödvändigt att behandla personuppgifter både i en förundersökning om ett visst brott och för att ta ställning till om ett nyupptäckt brott behöver utredas. Enligt regeringens bedömning bör utgångspunkten vara att om det finns en rättslig grund för att behandla personuppgifter för att t.ex. avgöra frågan om förundersökning ska påbörjas om det nyupptäckta brottet, så är personuppgiftsbehandlingen också nödvändig för det nya ändamålet. Med den utgångspunkten är det bara i rena undantagsfall som kravet på nödvändighet enligt artikel 4.2, utöver kravet på rättslig grund, begränsar möjligheten att behandla personuppgifter för nya ändamål.

Eftersom direktivet ställer upp ett krav på nödvändighet både när det gäller rättslig grund och när det gäller behandling för nya ändamål anser regeringen dock, i likhet med utredningen, att bestämmelsen om behandling för nya ändamål bör innehålla ett krav på nödvändighet.

Polismyndigheten väcker frågan om begreppet nödvändig har en annan innebörd i den nu föreslagna bestämmelsen än i den föreslagna bestämmelsen om rättslig grund. Enligt regeringen bör, av samma skäl som anges i avsnitt 7.2, begreppet även i den nu aktuella bestämmelsen tolkas som att det är fråga om något som behövs, snarare än något som absolut fordras eller inte kan underlåtas. Om en viss behandling för ett nytt ändamål kan anses tillåten enligt bestämmelsen blir ytterst en fråga som får avgöras i rättstillämpningen.

Kravet på proportionalitet

Direktivet ställer även krav på att behandling för ett nytt ändamål ska stå i proportion till det nya ändamålet. Att det tydligt uttrycks att det ska göras en proportionalitetsbedömning är en nyhet i förhållande till 1995 års dataskyddsdirektiv. Att åtgärder som myndigheter vidtar ska vara proportionerliga är emellertid en viktig grundprincip såväl inom EU-rätten som i nationell rätt och gäller, som *Polismyndigheten* påpekar, för all personuppgiftsbehandling.

Utredningen menar att kravet på proportionalitet innebär att skälen för att personuppgifterna behandlas för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för den enskilde. Regeringen instämmer i den bedömningen. Vad som står att vinna med behandlingen ska alltså vägas mot intrånget i enskildas integritet. Om det har inträffat ett allvarligt brott behöver Polismyndigheten t.ex. göra sökningar i olika register där det förekommer uppgifter om personer som kan ha begått likartade brott tidigare. En sådan sökning innebär naturligtvis att en bredare krets av registrerade kan drabbas av intrång än om man redan har en utpekad misstänkt. Proportionalitetsbedömningen ska inte göras i förhål-

lande till varje enskild uppgift i registren, utan behovet av sökningen ska vägas mot det samlade intrånget av att sökningen görs.

För proportionalitetsbedömningen har det också betydelse vilka personuppgifter det är fråga om och i vilken verksamhet de används. Att behandla en adressuppgift för nya ändamål är t.ex. generellt sett mer harmlöst än att behandla en uppgift som rör hälsa eller sexualliv.

En fråga är om det är proportionerligt att använda information från exempelvis förundersökningar för underrättelseverksamhet eller brottsförebyggande arbete, eftersom sådan verksamhet till sin natur inte är lika konkret. Det kan då vara svårare att avgöra vad som står att vinna med behandlingen. Samtidigt är det många gånger av avgörande betydelse för möjligheten att avslöja och utreda pågående eller framtida brottslighet att uppgifter om vissa personers brottsliga aktivitet eller kontakter får föras över från t.ex. den brottsutredande verksamheten till underrättelseverksamheten.

Tillämparen måste ställa sig frågan om intresset av att behandla personuppgifterna för det nya ändamålet väger tyngre än intresset av att något integritetsintrång inte sker. Om t.ex. en person redan är misstänkt för brott och misstanke uppkommer om att han eller hon begått ytterligare brott som kan ha betydelse för påföljden, utgår lagstiftningen från att brotten ska utredas tillsammans och att en gemensam påföljd för brotten ska kunna dömas ut. Den misstänktes intresse av att uppgifterna inte behandlas vid utredningen om det senare brottet väger då normalt inte lika tungt som intresset av att brotten utreds och behandlas i domstol samtidigt.

Syftet med ett krav på proportionalitet är alltså att det ska göras en bedömning av behovet av att behandla personuppgifter för nya ändamål ställt i relation till intrånget. Som *Polismyndigheten* påpekar synes utredningen mena att bedömningen ska göras i varje enskilt fall. Enligt regeringen utesluter dock inte kravet på proportionalitet att vissa typer av nya ändamål generellt sett anses vara av så stort värde att de alltid väger upp integritetsintrånget. Regeringen anser alltså att det kan bli aktuellt med proportionalitetsbedömningar som avser typsituationer. Polismyndigheten anmärker även att ett krav på proportionalitet vid behandling för nya ändamål kan tolkas som att annan behandling inte behöver vara proportionerlig. Här finns därför skäl att klargöra att det nu aktuella proportionalitetskravet inte ska uppfattas på det sättet. Den proportionalitetsprövning det nu är fråga om tar sikte på om det är proportionerligt att redan insamlade uppgifter behandlas för nya ändamål. De krav som i övrigt gäller för behandling av personuppgifter framgår av andra bestämmelser.

Sammanfattningsvis bör ramlagen alltså innehålla en bestämmelse om att personuppgifter får behandlas för ett nytt ändamål inom lagens tillämpningsområde under förutsättning att det finns en rättslig grund för den nya behandlingen och det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. *Sveriges advokatsamfund* anser att lagtexten även bör uppställa ett krav på att det nya ändamålet ska vara godtagbart i ett demokratiskt samhälle. Enligt regeringen är det dock tillräckligt att kraven på rättslig grund samt nödvändighet och proportionalitet är uppfyllda, eftersom behandlingen för det nya ändamålet därmed får anses vara godtagbar i ett demokratiskt samhälle.

En behörig myndighet kan ha behov av att behandla personuppgifter för nya ändamål både för att använda uppgifterna i den egna verksamheten och för att lämna ut dem till någon annan. Som framgår av avsnitt 7.1 skiljer de ändamålsbestämmelser som i dag finns i de brottsbekämpande myndigheternas registerförfattningar mellan behandling för den egna brottsbekämpande verksamhetens behov och behandling för att tillhandahålla information för andras behov. När personuppgifter som samlats in av en myndighet för att utreda ett visst brott senare används av samma myndighet för att utreda ett annat brott anses behandlingen i den senare utredningen omfattas av de primära ändamålen. När personuppgifter lämnas ut som ett led i myndighetens egen brottsbekämpande verksamhet, inte i syfte att tillgodose någon annans behov, anses utlämnandet också omfattas av de primära ändamålen. När personuppgifter däremot lämnas ut för att de behövs i brottsbekämpande verksamhet hos en annan myndighet anses utlämnandet falla under de sekundära ändamålen. Med den bestämmelse som nu föreslås kommer det att sakna betydelse om behandlingen för det nya ändamålet utförs för behov i myndighetens egen brottsbekämpande verksamhet eller för att tillgodose en annan myndighets behov av information, så länge ändamålet med behandlingen ligger inom ramlagens tillämpningsområde. Det centrala blir i stället den prövning om dels rättslig grund, dels nödvändighet och proportionalitet som alltid ska göras innan personuppgifter får behandlas för ett nytt ändamål.

Som anges i avsnitt 7.5 bör bestämmelserna i de brottsbekämpande myndigheternas registerförfattningar om primära och sekundära ändamål inte ses som ändamålsbestämmelser, utan snarare bestämmelser om rättslig grund för behandling av personuppgifter. I avsnittet anges även att regeringen kommer att ta ställning till frågan om bestämmelserna bör behållas i samband med att registerförfattningarna anpassas till ramlagen. Oavsett om bestämmelserna kommer att behållas eller inte gör regeringen bedömningen att den nya regleringen inte kommer att påverka möjligheten för myndigheterna att lämna ut uppgifter i de fall som räknas upp i de sekundära ändamålsbestämmelserna. Syftet med de bestämmelserna är att underlätta för tillämparen genom att han eller hon endast behöver avgöra om det är nödvändigt att lämna information som behövs i en annan brottsbekämpande myndighets verksamhet, utan att behöva ta ställning till om utlämnandet är förenligt med finalitetsprincipen. Lagstiftaren har bedömt att det är förenligt med det ursprungliga ändamålet med behandlingen att vidarebehandla personuppgifterna i de angivna situationerna. Enligt regeringen måste det som regel anses både nödvändigt och proportionerligt att behandla personuppgifter för att tillhandahålla information i de situationer som i dag räknas upp i de sekundära ändamålsbestämmelserna. Att någon prövning i vissa fall inte behövs behandlas i avsnitt 7.6.5.

7.6.3 Nya ändamål utanför ramlagens tillämpningsområde – dataskyddsförordningen är tillämplig

Regeringens bedömning: Det behövs inte någon upplysningsbestämmelse i ramlagen om att dataskyddsförordningen gäller vid behandling för ändamål som ligger utanför ramlagens tillämpningsområde.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att ramlagen ska innehålla en upplysningsbestämmelse om att dataskyddsförordningen gäller vid behandling för ändamål som ligger utanför ramlagens tillämpningsområde.

Remissinstanserna: Den enda remissinstans som framför synpunkter i denna del är *Kriminalvården* som anser att det är otydligt om, hur och i vilken utsträckning uppgifter som behandlas med stöd av ramlagen kommer att kunna behandlas för ändamål som faller utanför lagen. Enligt Kriminalvården är det även oklart om ett utlämnande med anledning av en uppgiftsskyldighet för ett ändamål som inte ryms inom ramlagen, ska anses falla in under ramlagen eller dataskyddsförordningen.

Skälen för regeringens bedömning

Från ramlagen till dataskyddsförordningen

Som anges i avsnitt 7.6.1 finns den nuvarande regleringen av vidarebehandling av personuppgifter dels i 9 § första stycket d personuppgiftslagen där finalitetsprincipen slås fast, dels i de sekundära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar. De sekundära ändamålsbestämmelserna reglerar behandling för ändamål som ligger både inom och utanför den föreslagna ramlagens tillämpningsområde. I detta avsnitt diskuteras behandling för nya ändamål utanför ramlagens tillämpningsområde.

Behöriga myndigheter kan ha behov av att behandla personuppgifter som behandlas med stöd av ramlagen för ändamål som ligger utanför ramlagens tillämpningsområde, framför allt för att lämna ut dem till myndigheter och andra aktörer som inte är behöriga myndigheter för deras behov. Ett exempel på det kan vara att Kustbevakningen lämnar personuppgifter till Sjöfartsverket, Transportstyrelsen eller en miljömyndighet efter en fartygskollision. Ett annat exempel är att Polismyndigheten lämnar personuppgifter till Försäkringskassan inom ramen för myndighetsöverskridande samverkan, om syftet med utlämnandet är att kontrollera riktigheten av bidrag eller andra utbetalningar. Personuppgifter som en behörig myndighet behandlar enligt ramlagen kan också behöva lämnas till en enhet inom myndigheten som bedriver verksamhet utanför lagens tillämpningsområde. Personuppgifter som behandlas i Polismyndighetens brottsbekämpande verksamhet kan exempelvis behöva lämnas till den inom myndigheten som beslutar i fråga om pass eller vapenlicens.

I artikel 9 regleras vad som gäller när personuppgifter som behandlas med stöd av direktivet ska behandlas för ändamål utanför direktivets tillämpningsområde. Där anges att personuppgifter som har samlats in för ändamål inom direktivets tillämpningsområde inte får behandlas för

andra ändamål, såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål eller av någon som inte är en behörig myndighet ska dataskyddsförordningen tillämpas, utom när behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. I skäl 34 framhålls att dataskyddsförordningen är tillämplig på överföring av personuppgifter för ändamål som inte omfattas av direktivet. Dataskyddsförordningen är därmed tillämplig redan på de behöriga myndigheternas behandling för att tillhandahålla personuppgifter till andra myndigheter, om ändamålet med behandlingen ligger utanför ramlagens tillämpningsområde.

Vad innebär det att dataskyddsförordningen är tillämplig?

För behandling av personuppgifter i verksamhet som omfattas av unionsrätten kommer antingen direktivets eller dataskyddsförordningens reglering att gälla. Direktivet och förordningen kan vara tillämpliga parallellt om samma personuppgift behandlas för olika syften, men de kan aldrig tillämpas samtidigt på personuppgiftsbehandling som bara har ett syfte (se avsnitt 6.4.4).

Regleringen i artikel 9 i direktivet innebär att direktivets, och därmed ramlagens, bestämmelser över huvud taget inte ska tillämpas vid behandling för ändamål utanför direktivets tillämpningsområde. Prövningen av om sådan behandling är tillåten ska som regel enbart göras med utgångspunkt i bestämmelserna i dataskyddsförordningen. Enligt förslaget till en ny dataskyddslag ska bestämmelserna i dataskyddsförordningen, med vissa undantag, gälla även i verksamhet utanför unionsrättens tillämpningsområde (prop. 2017/18:105 s. 28 f.). Eftersom behandlingen för ett nytt ändamål som inte omfattas av direktivet i de flesta fall blir en ny behandling enligt förordningen är det inte fråga om någon vidarebehandling, vilket gör att finalitetsprincipen inte ska tillämpas på den behandlingen. Det innebär att finalitetsprincipen aldrig blir tillämplig när personuppgifter som behandlas med stöd av ramlagen ska behandlas för nya ändamål (se även avsnitt 7.6.2).

Utredningen anser att ramlagen bör innehålla en bestämmelse som upplyser om att det är dataskyddsförordningen som ska tillämpas när personuppgifter behandlas för ändamål som inte omfattas av ramlagens tillämpningsområde. Regeringen gör dock bedömningen att någon sådan upplysningsbestämmelse inte behövs. Vilken personuppgiftsbehandling som omfattas av ramlagen kommer att framgå av bestämmelsen om lagens tillämpningsområde (se avsnitt 6.4.1). Personuppgiftsbehandling för ändamål som faller utanför ramlagen kommer att regleras av dataskyddsförordningen eller i undantagsfall av viss sektorspecifik reglering.

När personuppgifter lämnas ut med anledning av en uppgiftsskyldighet för ändamål som faller utanför ramlagen, ett exempel som *Kriminalvården* tar upp, ska alltså i de flesta fall dataskyddsförordningen tillämpas. Av avsnitt 7.6.4 framgår att det utöver reglerna i förordningen bör finnas en bestämmelse i ramlagen enligt vilken en särskild prövning krävs innan personuppgifter som behandlas med stöd av ramlagen behandlas för nya ändamål som inte omfattas av lagen.

Dataskyddsförordningen utgår, på samma sätt som direktivet, från att varje behandling av personuppgifter måste vila på en rättslig grund. De rättsliga grunderna räknas uttömmande upp i artikel 6.1 i förordningen. Om ingen av dem är tillämplig är behandlingen inte laglig och får därmed inte utföras. Regeringen håller med utredningen om att det är punkterna c, d och e som i de flesta fall aktualiseras när behöriga myndigheter lämnar ut personuppgifter för ändamål utanför ramlagens tillämpningsområde. De rättsliga grunderna enligt de punkterna är:

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Förutom att behandlingen för att lämna ut uppgifter ska vara rättsligt grundad enligt artikel 6 behöver den även i övrigt ske i enlighet med bestämmelserna i förordningen. Förordningens regler om bl.a. principer för behandling av personuppgifter, registrerades rättigheter och personuppgiftsansvarigas skyldigheter måste alltså också iakttas.

7.6.4 Nya ändamål utanför ramlagens tillämpningsområde – en prövning ska göras innan personuppgifter behandlas för nya ändamål

Regeringens förslag: Innan personuppgifter som behandlas med stöd av ramlagen behandlas för ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* avstyrker förslaget. Enligt Datainspektionen krävs det särskilda överväganden för att placera en bestämmelse om personuppgiftsbehandling på dataskyddsförordningens område i ramlagen. *Domstolsverket* ifrågasätter om det är möjligt att införa en bestämmelse i ramlagen som reglerar personuppgiftsbehandling utanför lagens tillämpningsområde. *Polismyndigheten* anser att det kommer att bli mer svårbedömt i vilka situationer uppgifter kan lämnas för nya ändamål och efterfrågar därför klargöranden i det avseendet. Övriga remissinstanser har inget att invända mot förslaget.

Skälen för regeringens förslag

Finns det utrymme och behov av att inom dataskyddsförordningens tillämpningsområde ha specifik reglering i svensk rätt om behandling av personuppgifter för att tillhandahålla information?

Regeringen instämmer i utredningens bedömning att det inte råder någon tvekan om att det enligt dataskyddsförordningen är tillåtet att i nationell rätt reglera utlämnandefrågor och andra former av behandling för nya ändamål på det område som det nu är fråga om. Det handlar om behöriga myndigheters behandling av personuppgifter för nya ändamål utanför ramlagens tillämpningsområde för att främst fullgöra rättsliga förpliktelser eller utföra uppgifter av allmänt intresse. Frågan är då om det finns behov av att i svensk rätt specificera villkoren för sådan personuppgiftsbehandling. I avsnitt 7.6.2 föreslår regeringen att det ska göras en särskild prövning innan personuppgifter som behandlas enligt ramlagen ska behandlas för nya ändamål inom lagens tillämpningsområde. Genom prövningen ska det säkerställas dels att det finns en tillåten rättslig grund för den nya behandlingen, dels att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Om motsvarande prövning inte skulle krävas vid behandling för nya ändamål utanför ramlagens tillämpningsområde, skulle det enligt utredningens mening uppstå en omotiverad skillnad mellan de två situationerna. Regeringen håller med utredningen om det. Det vore inte rimligt att kräva en noggrannare prövning för behandling för nya ändamål inom ramlagens tillämpningsområde än utanför det.

Det kan tilläggas att personuppgifter som behandlas med stöd av dataskyddsförordningen i regel endast får behandlas för nya ändamål om behandlingen är förenlig med finalitetsprincipen. Det måste således göras en prövning av om det nya ändamålet är förenligt med det ändamål som uppgifterna samlades in för, när personuppgifter vidarebehandlas enligt förordningen. Som anges i avsnitt 7.6.3 blir finalitetsprincipen inte tillämplig när personuppgifter som behandlas med stöd av ramlagen ska behandlas för nya ändamål inom dataskyddsförordningens tillämpningsområde, eftersom det då blir fråga om en ny behandling enligt förordningen.

Även om det är olika prövningar som ska göras krävs det alltså en prövning innan personuppgifter behandlas för nya ändamål både inom ramlagens och inom dataskyddsförordningens tillämpningsområde. Mot den bakgrunden anser regeringen, i likhet med utredningen, att det är rimligt att kräva en prövning även när personuppgifter som behandlas med stöd av ramlagen ska behandlas för ändamål utanför lagens tillämpningsområde. En bestämmelse om det bör föras in i ramlagen. Med anledning av *Datainspektionens* och *Domstolsverkets* tveksamhet till att placera en sådan bestämmelse i ramlagen kan påpekas att prövningen ska göras innan behandlingen av personuppgifterna för det nya ändamålet påbörjas. Vidare är syftet med bestämmelsen att personuppgifter som behandlas med stöd av ramlagen inte används på ett integritetskränkande sätt. Mot den bakgrunden och då det inte finns någon annan naturlig placering av bestämmelsen anser regeringen att den bör införas i ramlagen.

Som framgår av avsnitt 7.6.1 innehåller de sekundära ändamålsbestämmelserna som i dag finns i de brottsbekämpande myndigheternas registerförfattningar särskilda regler om vad som gäller när redan insamlade uppgifter ska behandlas för nya ändamål. Dagens reglering innebär att det ska prövas om det är nödvändigt att tillhandahålla personuppgifterna i de situationer som räknas upp i de sekundära ändamålsbestämmelserna. För att Polismyndigheten och Tullverket ska få lämna information till andra verksamheter inom respektive myndighet krävs det också särskilda skäl (se 2 kap. 8 § första stycket 4 polisdatalagen och 2 kap. 6 § första stycket 4 tullbrottsdatalagen). I förarbetena framhålls att kravet på särskilda skäl innebär att information inte får tillhandahållas rutinmässigt utan att det i det enskilda fallet måste finnas särskilda skäl som talar för att informationen bör tillhandahållas den andra verksamheten (prop. 2009/10:85 s. 322 och prop. 2016/17:91 s. 102).

Som nyss nämnts föreslår regeringen i avsnitt 7.6.2 att det ska prövas om det är nödvändigt och proportionerligt att personuppgifter behandlas för ett nytt ändamål inom ramlagens tillämpningsområde. Syftet med kravet på proportionalitet är att det ska göras en bedömning av behovet av att behandla personuppgifter för nya ändamål ställt i relation till intrånget i den personliga integriteten.

Oavsett om man ställer krav på särskilda skäl eller nödvändighet och proportionalitet är det centrala att det görs en prövning av skälen för att behandla personuppgifter för ett nytt ändamål innan uppgifterna behandlas för det ändamålet. Det skulle skapa en enhetlig tillämpning och underlätta för myndigheterna om den prövning som ska göras innan personuppgifter behandlas för nya ändamål är densamma oavsett om det nya ändamålet ligger inom eller utanför ramlagens tillämpningsområde.

Regeringen håller därför med utredningen om att den prövning som bör krävas innan personuppgifter behandlas för nya ändamål utanför ramlagens tillämpningsområde bör avse om det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. En sådan prövning utgör en lämplig avvägning mellan mottagarens behov av personuppgifterna och skyddet för enskildas personliga integritet. Eftersom prövningen är ett krav som ställs när personuppgifter som behandlas med stöd av ramlagen ska behandlas för ändamål utanför den lagen, kommer kravet inte i konflikt med regleringen i dataskyddsförordningen.

Innan personuppgifter behandlas för ett nytt ändamål inom ramlagens tillämpningsområde ska det enligt förslaget i avsnitt 7.6.2 även säkerställas att det finns en tillåten rättslig grund för den nya behandlingen. Att det ska finnas en rättslig grund för behandlingen när personuppgifter behandlas för ändamål utanför ramlagens tillämpningsområde kommer i de allra flesta fall att regleras i artikel 6 i dataskyddsförordningen och bör inte upprepas i den nationella regleringen. Det bör därför framgå att det innan behandling påbörjas för ett nytt ändamål utanför ramlagens tillämpningsområde – utöver de krav som gäller enligt förordningen – ska säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

Lagrådet anser att det är oklart hur den nu aktuella prövningen förhåller sig rättsligt och praktiskt till den nya prövning som ska göras enligt dataskyddsförordningen och påpekar att den föreslagna regleringen saknar stöd i direktivet och dataskyddsförordningen. Lagrådet kan därför inte tillstyrka den föreslagna paragrafen utan anser att den ska utgå. Som det har konstaterats ovan innebär prövningen att innan behandling påbörjas för ett nytt ändamål utanför ramlagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Regeringen bedömer därför att prövningen inte kommer i konflikt med regleringen i dataskyddsförordningen. Enligt regeringen hindrar inte heller regleringen i direktivet att en sådan prövning införs. Direktivet medger tvärtom att medlemsstaterna har starkare skyddsåtgärder än vad som krävs enligt direktivet (se bl.a. avsnitt 8.1.4).

Som anförts ovan föreslår regeringen i avsnitt 7.6.2 att det ska göras en särskild prövning innan personuppgifter som behandlas enligt ramlagen ska behandlas för nya ändamål inom ramlagens tillämpningsområde. Genom prövningen ska det bl.a. säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Enligt dataskyddsförordningen ska i motsvarande situation en prövning enligt finalitetsprincipen göras. Som anges i avsnitt 7.6.3 blir finalitetsprincipen dock inte tillämplig när personuppgifter som behandlas med stöd av ramlagen ska behandlas för nya ändamål inom dataskyddsförordningens tillämpningsområde, eftersom det då blir fråga om en ny behandling enligt förordningen. Om en prövning av nödvändighet och proportionalitet inte skulle krävas vid behandling för nya ändamål utanför ramlagens tillämpningsområde, skulle det uppstå en omotiverad skillnad mellan de två situationerna och en lucka i dataskyddsregelverket i den här delen. Regeringen föreslår mot denna bakgrund inte någon ändring i förhållande till lagrådsremissens lagförslag i det här avseendet. Hur prövningen ska göras i praktiken bör överlämnas till rättstillämpningen.

Polismyndigheten efterfrågar klargöranden i fråga om i vilka situationer uppgifter kan lämnas för nya ändamål. I avsnitt 7.6.2 utvecklas vad kraven på nödvändighet och proportionalitet innebär. Som exempel på när det skulle kunna vara nödvändigt och proportionerligt att behandla uppgifter för nya ändamål utanför ramlagens tillämpningsområde kan följande nämnas. Det kan finnas information i Polismyndighetens brottsbekämpande verksamhet om att en person har sådana kontakter i kriminella kretsar att han eller hon vid en helhetsbedömning t.ex. ter sig olämplig för att få en viss befattning eller tillstånd att bedriva viss verksamhet. Det kan då anses vara nödvändigt och proportionerligt att informationen tillhandahålls för att användas vid prövningen av anställnings- eller tillståndsärendet. Det kan på motsvarande sätt vara nödvändigt och proportionerligt att lämna information om det i Tullverkets brottsbekämpande verksamhet kommer fram uppgifter om hur personer kringgår regelverket som har betydelse för hur verksamheten Effektiv handel bör inrikta sina kontroller. Vidare får det anses både nödvändigt och proportionerligt att personuppgifter som behandlas i brottsbekämpande verksamhet behandlas för arkivering.

Av avsnitt 7.5 framgår att dagens bestämmelser i de brottsbekämpande myndigheternas registerförfattningar om primära och sekundära ändamål

inte bör ses som ändamålsbestämmelser, utan snarare bestämmelser om rättslig grund för behandling av personuppgifter. Av avsnittet framgår även att regeringen avser att ta ställning till frågan om bestämmelserna bör behållas i samband med att registerförfattningarna anpassas till ramlagen. Oavsett om bestämmelserna kommer att behållas eller inte gör regeringen samma bedömning i fråga om utlämnanden för ändamål utanför ramlagens tillämpningsområde som i fråga om utlämnanden för ändamål inom ramlagens tillämpningsområde, nämligen att den nya regleringen inte kommer att påverka möjligheterna för myndigheterna att lämna ut uppgifter i de fall som räknas upp i de sekundära ändamålsbestämmelserna. Som anges i avsnitt 7.6.2 måste det enligt regeringen som regel anses både nödvändigt och proportionerligt att behandla personuppgifter för att tillhandahålla information i de situationer som i dag räknas upp i de sekundära ändamålsbestämmelserna.

7.6.5 Uppgiftsskyldighet ersätter prövningen

Regeringens förslag: I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning av om det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet inte göras.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att en prövning av om behandlingen är nödvändig och proportionerlig för det nya ändamålet ska göras innan uppgifter lämnas med stöd av 6 kap. 5 § offentlighets- och sekretesslagen (2009:400).

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt om förslaget.

Skälen för regeringens förslag

Författningsreglerad uppgiftsskyldighet

Enligt de sekundära ändamålsbestämmelserna är det i dag tillåtet att lämna uppgifter i den utsträckning det finns skyldighet att göra det enligt lag eller förordning. Sådana skyldigheter kan avse ändamål både inom och utanför ramlagens tillämpningsområde.

Både i förundersöknings- och brottmålsförfarandet finns det omfattande skyldigheter att informera myndigheter och andra. I förundersökningskungörelsen (1947:948) finns ingående bestämmelser om uppgiftsskyldighet. Sådana skyldigheter föreskrivs också i bl.a. förordningen (1996:271) om mål och ärenden i allmän domstol, förordningen (1990:893) om underrättelse om dom i vissa brottmål, m.m. och 12 § strafföreläggandekungörelsen (1970:60), där det regleras till vilka fysiska eller juridiska personer domar, beslut och underrättelser i brottmål ska expedieras. Liknande skyldigheter finns även på andra områden. Enligt 36 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården har Polismyndigheten en vidsträckt skyldighet att lämna underrättelser till Kriminalvården.

Även i andra fall är behöriga myndigheter skyldiga att lämna viss information. Ett exempel är 14 kap. 1 § 2 socialtjänstlagen (2001:453)

enligt vilken rättspsykiatrisk undersökningsverksamhet, Kriminalvården, Polismyndigheten och Säkerhetspolisen är skyldiga att genast anmäla till socialnämnden om de i sin verksamhet får kännedom om eller misstänker att barn far illa. Ett annat exempel är 2 § lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet enligt vilken myndigheter som samverkar enligt lagen i vissa fall är skyldiga att lämna uppgifter till varandra.

När det i lag eller förordning föreskrivs att uppgifter ska lämnas har lagstiftaren tagit ställning till att det dels är så viktigt att det ska införas en skyldighet att lämna information, dels att eventuell sekretess ska brytas. Lagstiftaren får då också anses ha tagit ställning till att uppgiftslämnandet är nödvändigt och proportionerligt. Enligt regeringens mening bör sådan uppgiftsskyldighet ersätta den föreslagna prövningen av om det är nödvändigt och proportionerligt att personuppgifter behandlas för nya ändamål, oavsett om det gäller ändamål inom eller utanför ramlagens tillämpningsområde. Det bör tydliggöras i bestämmelserna.

Om det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna uppgifter ska myndigheten däremot pröva om det är nödvändigt och proportionerligt att lämna dem, eftersom lagstiftaren då inte har gjort den prövningen. En annan sak är att myndighetens prövning i sådana fall ofta torde mynna ut i att det är nödvändigt och proportionerligt att lämna uppgifterna.

Uppgiftslämnande enligt 6 kap. 5 § offentlighets- och sekretesslagen

En särskild fråga är hur man ska se på uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen. Enligt den paragrafen ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. Bestämmelsen anses innebära en skyldighet att lämna uppgifter (se t.ex. Behandling av personuppgifter inom studiestödsområdet, prop. 2008/09:96 s. 80 och prop. 2009/10:85 s. 120 f.). Trots att uppgiftslämnande enligt paragrafen betraktas som en uppgiftsskyldighet anser utredningen att den inte gör prövningen av nödvändighet och proportionalitet enligt ramlagen obehövlig. Som skäl för ställningstagandet anges att bestämmelser om sekretess har ett annat syfte än bestämmelser om skydd av personuppgifter. Enligt regeringen bör dock en myndighets skyldighet enligt 6 kap. 5 § offentlighets- och sekretesslagen att på begäran av en annan myndighet lämna ut uppgift som den förfogar över omfattas av undantaget när en prövning av om det är nödvändigt och proportionerligt att personuppgifter behandlas för nya ändamål inte ska göras. I annat fall finns risk att det uppstår en normkollision mellan 6 kap. 5 § offentlighets- och sekretesslagen och den nu föreslagna bestämmelsen.

7.7 Behandling för vetenskapliga, statistiska och historiska ändamål inom ramlagens tillämpningsområde

Regeringens förslag: En behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom ramlagens tillämpningsområde.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* tillstyrker förslaget. *Uppsala universitet* ställer sig frågande till förslaget då det ger intryck av att det författningsstöd som finns för att behandla personuppgifter i den ordinarie verksamheten skulle vara tillräckligt för att behandla uppgifterna även för vetenskapliga, statistiska och historiska ändamål, samtidigt som EU:s dataskyddsreform kräver att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter och svenska regler inom forskningsområdet kräver att forskning på personuppgifter om lagöverträdelser genomgår etikprövning av en etikprövningsnämnd. *Dataskydd.net* anser att lagförslaget bör kompletteras med ett krav på att uppgifterna ska pseudonymiseras om det inte finns särskilda skäl till varför detta vore olämpligt. Övriga remissinstanser yttrar sig inte särskilt om förslaget.

Skälen för regeringens förslag: Enligt artikel 4.3 kan behandling inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som omfattas av direktivets tillämpningsområde, under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter. Generella frågor om arkivering tas upp i avsnitt 8.2. Som framgår av det avsnittet faller behandling av personuppgifter för arkivändamål av allmänt intresse in under dataskyddsförordningen. I detta avsnitt diskuteras enbart behandling för vetenskapliga, statistiska och historiska ändamål inom direktivets tillämpningsområde.

Att det i direktivet lyfts fram att behandling kan inbegripa vetenskaplig, statistisk eller historisk användning gör det tydligt att direktivets övriga bestämmelser ska tillämpas även vid behandling för sådana ändamål. Det ska alltså finnas en rättslig grund för behandlingen (se avsnitt 7.2). De personuppgifter som behandlas ska vidare vara adekvata och relevanta och de får inte heller vara för omfattande i förhållande till de vetenskapliga, statistiska eller historiska ändamålen (se avsnitt 8.1.2). På samma sätt som den personuppgiftsansvarige vid behandling för andra ändamål inom ramlagens tillämpningsområde ska se till att personuppgifterna inte behandlas under längre tid än vad som behövs för de ändamålen (se avsnitt 8.2.2), får behandling för historiska, statistiska eller vetenskapliga ändamål inte heller pågå längre än vad som behövs för dessa ändamål. En bestämmelse som genomför artikel 4.3 bör tas in i ramlagen.

Artikel 4.3 reglerar bara behandling för historiska, statistiska och vetenskapliga ändamål inom direktivets tillämpningsområde. Eftersom endast behöriga myndigheter får behandla personuppgifter enligt ramlagen är det bara dessa myndigheters behandling av uppgifter för sådana ändamål som kan omfattas av ramlagen. Det gäller dock bara behöriga

myndigheters vetenskapliga, statistiska eller historiska användning av personuppgifter för sådana ändamål som rör brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Som exempel kan nämnas statistikbehandling som en uppföljande åtgärd till brottsbekämpande verksamhet. Statistikbehandling som rör t.ex. vapenärenden eller ärenden enligt ordningslagen ligger däremot utanför ramlagens tillämpningsområde. Andra myndigheters behandling av statistik rörande brottsbekämpning, lagföring och straffverkställighet, exempelvis Brottsförebyggande rådets sammanställning av rättsstatistik, ligger också utanför ramlagens tillämpningsområde.

Som *Uppsala universitet* påpekar ställer artikel 4.3 krav på lämpliga skyddsåtgärder för de registrerades rättigheter och friheter. Eftersom direktivets övriga bestämmelser ska tillämpas även vid behandling för historiska, statistiska och vetenskapliga ändamål kommer bl.a. de bestämmelser som föreslås om grundläggande krav på behandling av personuppgifter, personuppgiftsansvarigas skyldigheter och enskildas rättigheter att vara tillämpliga vid behandling för sådana ändamål. Vidare kommer det sökförbud som föreslås gälla i fråga om känsliga personuppgifter att vara tillämpligt även vid behandling för nu nämnda ändamål (avsnitt 8.1.4). Enligt regeringen är kravet på lämpliga skyddsåtgärder därmed uppfyllt.

Uppsala universitet väcker även frågan hur den föreslagna bestämmelsen förhåller sig till regelverket på forskningsområdet. Som framgått ovan gäller bestämmelsen behöriga myndigheters historiska, statistiska eller vetenskapliga användning av personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. När de behöriga myndigheterna behandlar personuppgifter för syften utanför ramlagens tillämpningsområde ska i de flesta fall dataskyddsförordningen tillämpas (avsnitt 7.6.3). I dataskyddsförordningen finns bestämmelser som rör behandling av personuppgifter för vetenskapliga och historiska forskningsändamål och förordningen både förutsätter och gör det möjligt att införa nationella bestämmelser som närmare preciserar förutsättningarna för behandling av personuppgifter för sådana forskningsändamål (se bl.a. artikel 9.2 j och 89.1 i dataskyddsförordningen). Den personuppgiftsbehandling som avses i bestämmelsen i ramlagen ska alltså skiljas från personuppgiftsbehandling för forskningsändamål. När t.ex. statistiska undersökningar utgör en integrerad del av ett forskningsprojekt där behandlingen av personuppgifter sker för vetenskapliga eller historiska forskningsändamål blir ramlagen inte tillämplig. Viss ledning till vad som avses med forskningsändamål enligt dataskyddsförordningen finns i skäl 159 och 160 i förordningen. I Forskningsdatautredningens betänkande Personuppgiftsbehandling för forskningsändamål (SOU 2017:50) föreslås en forskningsdatalag som ska komplettera dataskyddsförordningen och gälla vid behandling av personuppgifter för forskningsändamål. Förslaget bereds inom Regeringskansliet.

Vad gäller synpunkten från *Dataskydd.net* så anser regeringen av samma skäl som anges i avsnitt 7.3 att det saknas behov av att införa ett krav på pseudonymisering i den föreslagna bestämmelsen.

8 Övriga principer för behandling av personuppgifter

8.1 Grundläggande krav på behandlingen

8.1.1 Ingen generell bestämmelse om grundläggande principer

Regeringens förslag: Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Regeringens bedömning: Ramlagen bör inte innehålla någon generell bestämmelse om de grundläggande principerna för behandling av personuppgifter. Principerna bör i stället regleras i sitt sammanhang.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: Den enda remissinstans som yttrar sig i denna del är *Havs- och vattenmyndigheten* som tycker att ordet korrekt i lagförslaget bör ersättas med skäligt eller rimligt eller något annat ord som bättre speglar syftet med bestämmelsen.

Skälen för regeringens förslag och bedömning

De grundläggande principerna regleras i sitt sammanhang

Som framgår av avsnitt 7 krävs det en rättslig grund för att personuppgifter överhuvudtaget ska få behandlas. Är behandlingen rättsligt grundad ska särskilda, uttryckligt angivna och berättigade ändamål bestämmas för den. Utifrån de ändamålen får det sedan avgöras vilka personuppgifter som får behandlas och vilka övriga krav som ställs.

I artikel 4.1 anges allmänna principer för behandling av personuppgifter. Artikeln överensstämmer i allt väsentligt med artikel 6 i 1995 års dataskyddsdirektiv. Den artikeln har genomförts i 9 § personuppgiftslagen, som reglerar de grundläggande principerna för personuppgiftsbehandling. Stora delar av paragrafen gäller för de behöriga myndigheterna, antingen för att deras registerförfattningar gäller utöver personuppgiftslagen eller för att det uttryckligen hänvisas till delar av paragrafen i de registerförfattningar som gäller i stället för personuppgiftslagen. Regleringen i 9 § har således tillämpats länge och är väl inarbetad i myndigheternas verksamhet. Mot den bakgrunden skulle det kunna finnas skäl att ta in en motsvarande bestämmelse i ramlagen.

Paragrafer som är allmänt hållna och bygger på uppräkningar av grundläggande principer med ett påtagligt abstrakt innehåll blir emellertid lätt intetsägande och riskerar därigenom att inte i alla avseenden tillämpas på det sätt som är avsett. För att regleringen ska bli klar och tydlig håller regeringen med utredningen om att artikel 4.1 vid genomförandet bör delas upp och principerna i de olika punkterna bör behandlas i direkt anslutning till regleringen av de frågor som respektive princip tar sikte på. På det sättet blir det uppenbart att principerna utgör materiella bestämmelser, vilket både förbättrar skyddet för den enskilde och underlättar för tillämparen.

Enligt regeringen bör det alltså inte tas in någon motsvarighet till personuppgiftslagens generella bestämmelse om grundläggande krav på behandlingen i ramlagen. De grundläggande kraven på behandling av personuppgifter bör i stället behandlas i sitt sammanhang.

Ändamålen med behandlingen regleras i artikel 4.1 b. Principen har ett konkret och viktigt innehåll som bör lyftas fram. Den behandlas i avsnitt 7.4.

Kvaliteten på och omfattningen av de personuppgifter som behandlas regleras i artikel 4.1 c och d. Uppgifterna ska vara adekvata, relevanta och korrekta. Den principen bör behandlas tillsammans med artikel 6, enligt vilken åtskillnad ska göras mellan personuppgifter som rör olika kategorier av registrerade, och artikel 7.1, enligt vilken personuppgifter som grundar sig på fakta så långt möjligt ska skiljas från personuppgifter som grundar sig på personliga bedömningar. Frågorna behandlas i avsnitt 8.1.2 och 8.1.3.

I artikel 4.1 d föreskrivs även att alla rimliga åtgärder måste vidtas för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål. Den principen tas upp i anslutning till artiklarna 7.2 och 7.3, som behandlar åtgärder för att säkerställa att felaktiga, ofullständiga eller inaktuella personuppgifter inte överförs eller görs tillgängliga. Frågorna behandlas i avsnitt 8.1.6.

Personuppgifter ska enligt artikel 4.1 e inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas. Den principen hänger nära samman med artikel 5 som reglerar tidsgränser för lagring. Hur länge personuppgifter får behandlas tas upp i avsnitt 8.2.2.

Artikel 4.1 f behandlar säkerheten för personuppgifter och bör genomföras tillsammans med artikel 29, som också reglerar säkerhet i samband med behandling. Den frågan diskuteras i avsnitt 9.3.

Krav på författningsenlig och korrekt behandling

Enligt artikel 4.1 a ska personuppgifter behandlas på ett lagligt och korrekt sätt. De grundläggande kraven på lagenlighet, saklighet och opartiskhet i offentlig verksamhet finns i regeringsformen. Att en myndighet ska agera i enlighet med lag framstår som en självklarhet och är djupt förankrat i den svenska förvaltningstraditionen. Det gäller också att handläggningen ska ske på ett korrekt sätt. Det bör emellertid tydliggöras i ramlagen att personuppgifter alltid ska behandlas lagligt och på ett korrekt sätt.

Principen om laglighet innefattar att det ska finnas en rättslig grund för behandlingen (se avsnitt 7.2 och 7.3). Att använda ordet laglig kan lätt leda till motsatsslut. Eftersom det finns behov av att i andra bestämmelser i ramlagen reglera att behandlingen ska stå i överensstämmelse inte bara med lag utan även med föreskrifter på lägre nivåer anser regeringen, i likhet med utredningen, att uttrycket ”författningsenlig” är lämpligare att använda i ramlagen.

När det gäller principen om korrekthet kan det vid en jämförelse med andra språkversioner ifrågasättas om den svenska termen korrekt motsvarar avsikten med bestämmelsen. I den danska språkversionen anges i stäl-

let att uppgifterna ska behandlas ”rimeligt”. I den engelska används termen ”fairly”, vilket betyder rättvist, skäligt eller rimligt. Den franska språkversionen använder termen ”loyale” som har motsvarande betydelse. Användningen av dessa termer tyder enligt utredningens mening på att en intresseavvägning ska göras, vilket inte lika tydligt framgår av den svenska termen ”korrekt”. Utredningen tolkar artikeln så att det som avses med korrekt sätt är att behandlingen inte bara formellt ska vara i enlighet med regleringen utan också spegla intentionerna med lagstiftningen. Regeringen tolkar artikeln på samma sätt. Eftersom ordet ”korrekt” används i både direktivet och i motsvarande bestämmelse i artikel 5.1 a i dataskyddsförordningen bör ordet dock inte, som *Havs- och vattenmyndigheten* tycker, ersättas med något annat ord.

8.1.2 Personuppgifter ska vara korrekta och adekvata

Regeringens förslag: De personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

De personuppgifter som behandlas ska också vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans invänder mot förslaget.

Skälen för regeringens förslag

Personuppgifter ska vara korrekta och uppdaterade

Enligt artikel 4.1 d ska personuppgifter vara korrekta och, om nödvändigt, uppdaterade. Motsvarande bestämmelse finns i artikel 6.1 d i 1995 års dataskyddsdirektiv. Artikeln har genomförts i 9 § första stycket g personuppgiftslagen, enligt vilken personuppgifter som behandlas ska vara riktiga och, om nödvändigt, aktuella. En bestämmelse med det innehållet bör tas in i ramlagen. Regeringen anser att direktivets formulering bör användas.

En uppgift är korrekt om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är som personuppgifterna ska spegla får man söka ledning i ändamålen med behandlingen. I vissa fall är avsikten med behandlingen bara att registrera uppgifter som kommit in, t.ex. i en brottsanmälan. De behandlade personuppgifterna får då betraktas som korrekta om de stämmer överens med de inkomna uppgifterna, oavsett hur de förhåller sig till de verkliga förhållandena (jfr Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen, En kommentar, 4:e uppl. 2011, i fortsättningen Öman m.fl., s. 206).

Bedömningen av om en personuppgift är korrekt ska inte bara utgå från ändamålen för behandlingen. Att uppgifter som förekommer i bl.a. brottsbekämpande verksamhet och vid annan behandling av uppgifter om

lagöverträdelser har en särskild karaktär måste också beaktas. Frågan om en uppgift är korrekt måste därför även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. Om t.ex. en person anmäler en annan för brott är uppgifterna i anmälan korrekta om de återspeglar vad anmälaren har uppgett. Det förhållandet att det senare hålls ett förhör vid vilket vissa uppgifter tas tillbaka eller ändras innebär inte att de först nedtecknade uppgifterna i anmälan är felaktiga. Om det sedan vid en rättegång visar sig att personen i fråga lämnar nya uppgifter eller ändrar tidigare påståenden återspeglar ändå en uppteckning av tidigare förhör vad som sades vid det tillfället och är därigenom korrekt. Särskilt när det gäller utsagor från personer som hörs under en förundersökning eller vid en rättegång och som har ett personligt intresse av resultatet av handläggningen utgår lagstiftningen från att uppgifterna kan komma att ändras. Det krav på korrekthet som kan ställas när det gäller personuppgifter som behandlas vid utsagor måste därför inskränkas till att utsagorna återges så som de har lämnats och att dokumentationen av dem följer gällande regler.

För att kunna avgöra om uppgifterna är korrekta är det också av stor betydelse att veta om de grundar sig på fakta eller på personliga bedömningar. Att uppgifter som grundar sig på fakta i så stor utsträckning som möjligt ska skiljas från uppgifter som grundar sig på personliga bedömningar behandlas i avsnitt 8.1.3.

De behandlade uppgifterna behöver bara vara uppdaterade om det är nödvändigt. Frågan om det är nödvändigt att uppgifterna är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen (jfr Öman m.fl. s. 206). Exempelvis kan adressuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras. När ärendet har avslutats är det dock inte nödvändigt att uppdatera en adressuppgift.

I flera av myndigheternas registerförfattningar anges att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt och med respekt för människovärdet. En bestämmelse med motsvarande innehåll bör tas in i ramlagen. Bestämmelserna finns i dag i de paragrafer som reglerar användningen av känsliga personuppgifter (se bl.a. 2 kap. 10 § tredje stycket polisdatalagen och 2 kap. 7 § tredje stycket kustbevakningsdatalagen). Regleringen har lett till viss osäkerhet om signalementsuppgifter är känsliga personuppgifter. Bestämmelsen i ramlagen bör därför placeras tillsammans med reglerna om personuppgifters kvalitet för att tydliggöra att uppgifter om utseende inte i sig ska betraktas som känsliga personuppgifter. Ett signalement kan dock innehålla uppgifter ur vilka man kan utläsa uppgifter om t.ex. hälsa eller etniskt ursprung. Sådana uppgifter ska hanteras enligt reglerna om känsliga personuppgifter (se avsnitt 8.1.4).

Personuppgifter ska vara adekvata och relevanta

Enligt artikel 4.1 c ska personuppgifter vara adekvata och relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas. En bestämmelse med det innehållet bör tas in i ramlagen. Att uppgifterna ska vara adekvata och relevanta innebär att ovidkommande uppgifter inte får behandlas. Vilka uppgifter som är adekvata och relevanta ska bedömas i förhållande till ändamålen med behandlingen. Detsamma gäller hur

många personuppgifter det finns behov av att behandla. Det får betydelse för hur s.k. överskottsinformation ska hanteras, dvs. uppgifter som samlas in och som visar sig inte vara adekvata eller relevanta för det bestämda ändamålet. Om uppgifterna inte behöver behandlas för något annat tillåtet ändamål får de inte lagras för framtida behov. Det finns regler om i vilken utsträckning överskottsinformation över huvud taget får behandlas i vissa sammanhang (se t.ex. 27 kap. 23 a § rättegångsbalken).

8.1.3 Olika typer av personuppgifter ska skiljas från varandra

Regeringens förslag: Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

Personuppgifter som grundar sig på fakta ska så långt det är möjligt särskiljas från personuppgifter som grundar sig på personliga bedömningar. Om det inte framgår av sammanhanget eller på annat sätt vad uppgiften grundas på ska det tydliggöras genom en särskild upplysning.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* anser att det bör övervägas att införa en ny särskild beteckning för den kategori av registrerade som, utan att vara misstänkta för brott, är misstänkta för att ha utövat eller komma att utöva brottslig verksamhet och uttryckligen nämna den kategorin i lagtexten. Syftet skulle vara att uppnå en tillfredställande åtskillnad mellan sådana personer och personer som det inte finns några som helst misstankar mot. *Polismyndigheten* tycker däremot inte att det bör krävas olika kategorier av misstänkta, utan med misstänkta bör avses såväl de som är misstänkta för visst brott som de som är misstänkta för att ha utövat eller komma att utöva brottslig verksamhet. *Datainspektionen* saknar resonemang kring innebörden av förslaget att uppgifter som grundar sig på fakta ska skiljas från uppgifter som grundar sig på bedömning och betonar att förslaget inte får innebära någon försämring jämfört med dagens reglering. *Hovrätten för Västra Sverige* anser att formuleringen ”så långt det är möjligt” inte tillför något och ifrågasätter därför om den behöver finnas i lagtexten.

Skälen för regeringens förslag

Särskiljande mellan olika typer av personuppgifter

Enligt artikel 6 ska den personuppgiftsansvarige i tillämpliga fall och så långt det är möjligt skilja mellan personuppgifter som rör olika kategorier av registrerade. Som exempel på olika kategorier av registrerade nämns personer som har begått eller är på väg att begå brott, personer som har dömts för brott, brottsoffer eller personer som p.g.a. vissa om-

ständigheter kan antas vara brottsoffer och andra som berörs av ett brott, t.ex. vittnen, personer som kan lämna information om brott eller personer som har kontakter med eller band till personer som misstänks för eller är dömda för brott. Enligt artikel 7.1 ska personuppgifter som grundar sig på fakta så långt det är möjligt skiljas från personuppgifter som grundar sig på personliga bedömningar.

Syftet med bestämmelserna är att säkerställa att den som söker eller får del av information också får veta varför uppgifter om en viss person behandlas. Inom ramlagens tillämpningsområde är det särskilt viktigt att det framgår om en uppgift rör en icke misstänkt person och hur tillförlitlig en underrättelseuppgift bedöms vara. Ofta framgår det redan av det sammanhang i vilket personuppgifterna behandlas, men om en uppgift tas ur sitt sammanhang för att behandlas för ett nytt ändamål blir informationen viktig (jfr prop. 2009/10:85 s. 146 f.).

Ju längre ett brottmålsförfarande fortskrider, desto tydligare blir det vilken roll olika personer har och varför deras personuppgifter behandlas. Vid handläggningen i domstol anges det tydligt vem som är misstänkt, tilltalad, målsägande, vittne eller anhörig till någon av dessa. En sådan uppdelning uppfyller enligt regeringen kravet på särskiljande. I förundersökningsprotokoll görs på motsvarande sätt skillnad mellan olika personkategorier (se 20 och 21 §§ förundersökningskungörelsen [1947:948]).

Det är framför allt i det inledande skedet av en förundersökning och i underrättelseverksamhet som det kan vara otydligt vilken roll en person har och varför uppgifter om honom eller henne behandlas. I 3 kap. 3 § polisdatalagen anges därför att det vid behandling av gemensamt tillgängliga uppgifter genom en särskild upplysning eller på annat sätt ska framgå för vilket närmare ändamål personuppgifter behandlas och om en personuppgift har gjorts gemensamt tillgänglig som ett led i övervakningen av en allvarligt kriminellt belastad person. Om uppgifterna kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat brottslig verksamhet ska det enligt 3 kap. 4 § framgå att personen inte är misstänkt. Vidare föreskrivs att uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet, dvs. där ändamålet inte är att utreda ett konkret brott, ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av särskilda omständigheter är onödigt. Motsvarande gäller i Kustbevakningens brottsbekämpande verksamhet enligt 4 kap. 2 och 3 §§ kustbevakningsdatalagen samt för Tullverket och Skatteverket i deras brottsbekämpande verksamhet (se 3 kap. 3 och 4 §§ i både tullbrottsdatalagen och skattebrottsdatalagen). Även enligt 3 kap. 3 § åklagardatalagen ska det framgå om de uppgifter som behandlas rör en person som inte är misstänkt.

De bestämmelser som finns i dessa registerförfattningar är inarbetade men uppfyller inte helt direktivets krav. Det krävs också regler för övriga behöriga myndigheter. Det bör därför tas in en bestämmelse i ramlagen om att den personuppgiftsansvarige så långt det är möjligt ska skilja mellan personuppgifter som rör olika kategorier av registrerade. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori en person hör bör det tydliggöras genom en särskild upplysning.

Det är framför allt när uppgifter behandlas utanför sitt ursprungliga sammanhang som en särskild upplysning kan behövas (jfr prop.

2009/10:85 s. 146 f.). Kraven på särskild upplysning i de brottsbekämpande myndigheternas registerförfattningar gäller uppgifter som har gjorts gemensamt tillgängliga. Om uppgifter behandlas av en liten, klart avgränsad grupp vet de inblandade personerna som regel varifrån uppgifterna kommer, varför de behandlas och om en omnämnd person är misstänkt för brott eller för att utöva brottslig verksamhet eller om han eller hon tillhör någon annan kategori. Mot den bakgrunden kan det finnas skäl att göra undantag från kravet på särskild upplysning för uppgifter som inte har gjorts gemensamt tillgängliga. Regeringen återkommer till den frågan i samband med att de brottsbekämpande myndigheternas registerförfattningar anpassas till den nya ramlagen.

Det bör också tas in en bestämmelse i ramlagen om att personuppgifter som grundar sig på fakta bör skiljas från uppgifter som grundar sig på personliga bedömningar. Om det inte framgår av sammanhanget eller på annat sätt vad uppgiften grundas på bör det tydliggöras genom en särskild upplysning. Det som nyss sagts om att det kan finnas skäl att göra undantag från kravet på särskilda upplysningar bör gälla även för nu aktuella uppgifter som inte gjorts gemensamt tillgängliga.

Äldre personuppgifter

Det utvidgade kravet på särskilda upplysningar väcker frågan om de behöriga myndigheterna blir skyldiga att förse alla äldre personuppgifter som saknar sådana upplysningar med det. Eftersom kravet är att så långt möjligt skilja mellan olika typer av uppgifter anser regeringen, i likhet med utredningen, att det inte kan krävas av myndigheterna att de går igenom alla äldre personuppgifter för att kontrollera om det finns särskilda upplysningar. Om tveksamhet uppstår i ett enskilt fall och det är möjligt att tillfoga en särskild upplysning bör det dock göras. Formuleringen ”så långt det är möjligt” kan alltså få betydelse i bl.a. de fall då det är fråga om äldre personuppgifter. Med det i beaktande, och då direktivet endast kräver att åtskillnad görs mellan olika typer av uppgifter så långt det är möjligt, anser regeringen till skillnad mot *Hovrätten för Västra Sverige* att formuleringen behövs.

Kategorin misstänkta

Säkerhets- och integritetsskyddsnämnden och *Polismyndigheten* framför synpunkter som rör den kategori av registrerade som benämns misstänkta. Den föreslagna uppräkningen i lagtexten av olika kategorier av registrerade är endast exemplifierande, varför det enligt regeringen saknas skäl att lägga till ytterligare kategorier. Som Säkerhets- och integritetsskyddsnämnden påpekar är det av stor vikt att det framgår om en person inte är misstänkt vare sig för brott eller för att utöva brottslig verksamhet. Om den bestämmelse som nu föreslås i ramlagen därför bör kompletteras av bestämmelser i registerförfattningarna motsvarande den bestämmelse som i dag finns i 3 kap. 4 § polisdatalagen, är en fråga som regeringen avser att återkomma till när anpassningen av registerförfattningarna sker. Som *Datainspektionen* betonar är tanken inte att förslaget ska innebära någon försämring för enskilda jämfört med dagens reglering. Med det som utgångspunkt kommer regeringen, när registerförfatt-

ningarna anpassas till den nya regleringen, även att se över övriga bestämmelser om särskilda upplysningar som finns i dem.

Lagrådet föreslår att ”tilltalad” läggs till i lagtexten som exempel på en kategori av registrerade. Som just har nämnts är uppräkningen av kategorier av registrerade exemplifierande och därför finns det enligt regeringen inte skäl att lägga till tilltalad som ytterligare en kategori. Detta hindrar dock inte att det i sammanhang där det är relevant tydliggörs att personuppgifter som behandlas rör tilltalade.

8.1.4 Känsliga personuppgifter

Regeringens förslag: Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas. Om uppgifter om en person behandlas får de dock kompletteras med sådana personuppgifter när det är absolut nödvändigt för ändamålet med behandlingen.

Biometriska uppgifter och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får alltid behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser kommenterar inte förslaget. *Norrköpings kommun* anser att ordet ras kan ersättas med formuleringen nationellt eller etniskt ursprung. *Hovrätten för Västra Sverige* anser att ordet ”absolut” inte tillför något. *Justitiekanslern* ifrågasätter, mot bakgrund av att andra författningar ska innehålla bestämmelser om behandling av biometriska och genetiska uppgifter, om ramlagen bör innehålla ett krav på att sådan behandling ska vara absolut nödvändig eller om förutsättningarna för att behandla sådana uppgifter i stället uttömmande bör anges i de andra författningarna. *Polismyndigheten* menar att det saknas skäl för att utvidga begreppet känsliga personuppgifter till att omfatta biometriska och genetiska uppgifter och att samlingsbegreppet i stället bör vara särskilda kategorier av personuppgifter. Polismyndigheten tillstyrker vidare förslaget om ett generellt sökförbud, men påpekar att myndighetens registerförfattning kommer att behöva innehålla omfattande undantag från förbudet och att ramlagen bör innehålla ett generellt undantag för sökningar som sker i registervårdande syfte. Även *Säkerhets- och integritetsskyddsnämnden* understryker vikten av att registervårdande åtgärder regleras i de författningar som genomför direktivet. *Domstolsverket* ser problem med att förbjuda sökningar som sker i ett visst syfte, eftersom det enligt verket kan vara svårt att såväl när en sökning genomförs som i efterhand bedöma syftet med sökningen. Enligt *Datainspektionen* får det föreslagna sökförbudet inte innebära någon

utvidgning i förhållande till dagens möjligheter att söka på känsliga personuppgifter. Inspektionen ser det även som viktigt att syftet med sökningar på känsliga personuppgifter dokumenteras, både ur ett verksamhets- och tillsynsperspektiv. *Statens institutionsstyrelse* anser att sökförbudet blir mer ändamålsenligt och träffsäkert när det utgår från syftet med sökningen. Myndigheten lyfter samtidigt fram att det föreslagna förbudet torde öka möjligheterna att söka på känsliga personuppgifter på så sätt att det blir möjligt att söka på sådana uppgifter om sökningen begränsas till en viss person. Vid sökningar på känsliga personuppgifter i en persons journal går det inte att få fram något urval av personer.

Skälen för regeringens förslag

Nuvarande reglering

I lagstiftning om behandling av personuppgifter har känsliga personuppgifter en särställning. Med känsliga personuppgifter avses enligt 13 § personuppgiftslagen uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och uppgifter som rör hälsa eller sexualliv. Som huvudregel är det förbjudet att behandla känsliga personuppgifter. Från förbudet görs i 14–19 §§ personuppgiftslagen undantag för vissa situationer, t.ex. när den enskilde har samtyckt till behandlingen eller om behandlingen är nödvändig på grund av vissa särskilt angivna skäl. Enligt 8 § personuppgiftsförordningen (1998:1191) får känsliga personuppgifter behandlas av en myndighet i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

Definitionen av känsliga personuppgifter i personuppgiftslagen bildar utgångspunkten för regleringen i de behöriga myndigheternas registerförfattningar. Enligt registerförfattningarna får känsliga personuppgifter inte behandlas enbart på grund av vad som är känt om en person i dessa avseenden (se t.ex. 2 kap. 8 § åklagardatalagen). Om uppgifter om en person redan behandlas på någon annan grund, får de dock enligt de flesta registerförfattningarna kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen (se t.ex. 2 kap. 10 § polisdatalagen). Innebörden av bestämmelserna är att det t.ex. inte är tillåtet att föra särskilda register över personer baserat på deras politiska åsikter. Förekommer en person i en förundersökning eller något annat ärende, får dock uppgifter om politisk åskådning behandlas, om det bedöms vara absolut nödvändigt för syftet med behandlingen. Det kan t.ex. vara fallet om motivet för ett brott är politiskt. Något krav på att behandlingen är absolut nödvändig gäller enligt 13 § domstolsdatalagen inte i domstolarnas rättskipande och rättsvårdande verksamhet.

Fler kategorier av uppgifter blir känsliga personuppgifter

Enligt artikel 10 ska behandling av vissa kategorier av personuppgifter vara tillåten endast om det är absolut nödvändigt och om det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Dessutom krävs det att behandlingen är tillåten enligt unionsrätten eller nationell rätt, utförs för att skydda intressen som är av grundläggande

betydelse för den registrerade eller en annan fysisk person eller rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

De kategorier av personuppgifter som räknas upp i artikel 10 är till största delen de som i dag betecknas som känsliga personuppgifter, dvs. personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa eller sexualliv. Dessutom anges biometriska uppgifter för att unikt identifiera en fysisk person, genetiska uppgifter och uppgifter om sexuell läggning i artikeln. De nya kategorierna behandlas i det följande. Det finns även skäl att diskutera om ordet ras bör användas i ramlagen.

I artikel 10 benämns uppgifterna ”särskilda kategorier av personuppgifter”. Samma uttryck används i 1995 års dataskyddsdirektiv. I personuppgiftslagen benämns sådana personuppgifter ”känsliga personuppgifter”. *Polismyndigheten* förespråkar att ”särskilda kategorier av personuppgifter” används som samlingsbegrepp i stället för att begreppet ”känsliga personuppgifter” utvidgas. Regeringen håller dock med utredningen om att uttrycket ”känsliga personuppgifter” är tydligare än ”särskilda kategorier av uppgifter” och därför bör användas i ramlagen. (jfr prop. 2017/18:105 s. 75).

Genetiska uppgifter

Med genetiska uppgifter avses enligt den definition som föreslås i avsnitt 6.2 personuppgifter som rör sådana nedärvda eller förvärvade kännetecken för en fysisk person som kan tas fram ur ett prov från personen. Det handlar framför allt om information som kan tas fram vid dna-analyser, men även motsvarande information som tas fram genom andra analyser omfattas. Eftersom nedärvda eller förvärvade genetiska kännetecken för en fysisk person kan framgå av ett spår som påträffas vid utredning av ett brott omfattas även analys av spåren, trots att de då inte går att härleda till en identifierad person.

Genetiska uppgifter behandlas vid dna-analyser för att ta fram dna-profiler eller forensiska uppslag. Sådan behandling förekommer enbart i den forensiska verksamheten, som i Polismyndigheten sköts av Nationellt forensiskt centrum. Även Rättsmedicinalverket kan göra sådana analyser på begäran av Polismyndigheten eller en annan myndighet som omfattas av ramlagens tillämpningsområde. Behandlingen kan avse genetiska uppgifter från såväl identifierade som oidentifierade personer.

Själva dna-profilen, som behandlas i framför allt Polismyndighetens dna-register, är endast en sifferkombination och är därmed ingen genetisk uppgift.

Biometriska uppgifter

Med biometriska uppgifter avses enligt den föreslagna definitionen personuppgifter som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen. Som konstateras i avsnitt 6.2 omfattas inte fotografier och filmer som inte bearbetas tekniskt i det syftet av definitionen av biometriska uppgifter. Vidare kan nämnas att de personuppgifter, t.ex. fingeravtryck,

som förekommer i ett rättsutlåtande eller som bevisuppgift och som baseras på en teknisk bearbetning av biometriska uppgifter, inte i sig utgör biometriska uppgifter. Inte heller utgör uppgifter som beskriver förhållanden mellan detaljer i olika fingeravtryck, dna-analyser eller andra jämförelsematerial biometriska uppgifter.

Definitionen omfattar brottsbekämpande myndigheters hantering av fingeravtryck. Fingeravtryck som har tagits med stöd av rättegångsbalken eller lagen (1991:572) om särskild utlänningskontroll får behandlas i de fingeravtrycks- och signalementsregister som förs enligt 4 kap. 11 § polisdatalagen. Uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person får också behandlas om uppgiften kommit fram vid utredning om brott. Även oidentifierade fingeravtryck omfattas således av definitionen av biometriska uppgifter, eftersom det är möjligt att med hjälp av sådana identifiera den person som har avsatt dem.

Uppgifter om huruvida någon förekommer i Polismyndighetens fingeravtrycks- och signalementsregister eller dna-register är inte biometriska uppgifter. Däremot är den behandling som utförs vid jämförelse mellan olika fingeravtryck eller dna-profiler behandling av biometriska uppgifter.

Uppgifter om sexualliv och sexuell läggning

Enligt direktivet är uppgifter om fysiska personers sexualliv och sexuella läggning känsliga personuppgifter. I artikel 8 i 1995 års dataskyddsdirektiv och i 13 § personuppgiftslagen föreskrivs att uppgifter om sexualliv är en känslig personuppgift. Uppräkningen i ramlagen av känsliga personuppgifter bör omfatta uppgifter om både sexualliv och sexuell läggning.

Ordet ras

Ras har länge ansetts vara en känslig personuppgift. I uppräkningen i direktivet av vad som utgör känsliga personuppgifter nämns också ras. I skäl 37 klargörs att användningen av ordet ras inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser.

Frågan om utmönstring av ordet ras ur svensk lagstiftning har länge varit aktuell. Riksdagen har uttalat att det inte finns någon vetenskaplig grund för att dela in människor i skilda raser och ur biologisk synpunkt följaktligen inte heller någon grund för att använda ordet ras om människor. Enligt vad riksdagen anförde riskerar användningen av ordet ras i författningstext att underblåsa fördomar. Riksdagen konstaterade dock, i anledning av en motion, att det inte var möjligt att utmönstra ordet ras ur all lagstiftning, eftersom det så gott som uteslutande används i författningar som grundas på internationella konventioner eller författningar som genomför direktiv. Regeringen uppmanades att gå igenom i vilken utsträckning ordet ras förekom i författningar som inte grundas på internationella texter och där så var möjligt föreslå en annan definition (bet. 1997/98:KU29 s. 7).

Ordet ras har på senare år ersatts med andra uttryck i regeringsformen och i diskrimineringslagen (2008:567) och medvetet utelämnats i ett antal lagar. Exempelvis ersattes ordet ras i regeringsformen genom att uttrycket ”annat liknande förhållande” lades till efter etniskt ursprung och hudfärg. Med ”annat liknande förhållande” åsyftas i första hand

sådana föreställningar om ras som omfattas av ordet ras enligt den tidigare lydelsen (prop. 2009/10:80 s. 152).

Den omständigheten att direktivet använder ordet ras hindrar, som utredningen påpekar, inte att det i ramlagen används ett annat ord eller uttryck, förutsatt att det har samma betydelse. Att använda uttrycket ”etniskt ursprung, hudfärg eller annat liknande förhållande” som finns i bl.a. regeringsformen skulle emellertid inte fungera i ramlagen. Om hudfärg skulle räknas upp bland känsliga personuppgifter skulle det skapa problem för de brottsbekämpande myndigheterna, eftersom det skulle leda till att bilder på identifierbara personer skulle utgöra känsliga personuppgifter om hudfärgen syns. Avsikten med dataskyddsreformen kan inte rimligen vara att alla bilder på personer ska anses utgöra känsliga personuppgifter. Det får stöd av skäl 51 i dataskyddsförordningen där det bl.a. anges att behandling av foton inte systematiskt bör anses utgöra behandling av känsliga personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Det är enligt regeringen inte heller lämpligt att använda formuleringen ”etniskt ursprung eller annat liknande förhållande”. Det skulle för det första leda till osäkerhet om det är någon skillnad mellan de olika uttryckssätten. För det andra skulle det lämna ett alltför stort tolkningsutrymme och kunna leda till att de behöriga myndigheterna antingen behandlar känsliga personuppgifter i för stor utsträckning eller inte behandlar sådana uppgifter trots att det är sakligt motiverat. Regeringen anser därför i likhet med utredningen att det är nödvändigt att även fortsättningsvis använda ordet ras. Den formulering som *Norrköpings kommun* föreslår, ”nationellt eller etniskt ursprung”, ser regeringen alltså inte heller som något gångbart alternativ. Detta innebär att regleringen i ramlagen kommer att överensstämma med artikel 9 i dataskyddsförordningen.

Känsliga personuppgifter bör som huvudregel inte få behandlas i större utsträckning än i dag

Enligt direktivet ska behandling av särskilda kategorier av personuppgifter vara tillåten endast om den är absolut nödvändig och om det finns lämpliga skyddsåtgärder. Dessutom ska behandlingen vara tillåten enligt unionsrätt eller nationell rätt, alternativt ska den göras för att skydda intressen av grundläggande betydelse för den registrerade eller någon annan fysisk person eller avse uppgifter som har offentliggjorts av den som personuppgifterna rör.

Enligt gällande rätt får flertalet av de behöriga myndigheterna behandla känsliga personuppgifter om de behandlar uppgifter om personen i fråga på någon annan grund, men då bara om det är absolut nödvändigt för syftet med behandlingen. Domstolarna får emellertid behandla känsliga personuppgifter i större utsträckning. Enligt 13 § domstolsdatalagen får känsliga personuppgifter inte utgöra den enda grunden för behandlingen. Det behöver dock inte vara uppgifter om den person som de känsliga personuppgifterna rör som behandlas, utan det är enligt förarbetena tillräckligt att det finns en annan konkret grund för behandlingen. Det ställs inte heller något krav på att behandlingen ska vara absolut nödvändig. Skälet till denna mer generösa reglering är att det av principiella skäl

ansågs uteslutet att genom bestämmelser i lag inskränka domarnas frihet att formulera domskäl i syfte att undvika att känsliga personuppgifter behandlas. Det anges vidare att det strängt taget inte är någon skillnad mellan i vilken utsträckning domstolarna behöver behandla känsliga personuppgifter och andra personuppgifter (Domstolsdatalag, prop. 2014/15:148, s. 49).

Dagens regelverk är således betydligt mer restriktivt än direktivets reglering, eftersom känsliga personuppgifter i de flesta fall endast får behandlas tillsammans med andra uppgifter om personen i fråga. *Hovrätten för Västra Sverige* ifrågasätter behovet av ordet ”absolut” i bestämmelsen. Att behandlingen ska vara absolut nödvändig är ett krav som direktivet ställer och som därför bör komma till uttryck i ramlagen.

Enligt artikel 1.3 är det tillåtet att ha starkare skyddsåtgärder än de som fastställs i direktivet. Den nuvarande regleringen har fungerat väl för de berörda myndigheterna och kravet på att känsliga personuppgifter bara får behandlas om uppgifter om personen behandlas av annat skäl är enligt regeringens mening en sådan lämplig skyddsåtgärd som direktivet fordrar. Känsliga personuppgifter bör därför bara få behandlas om uppgifter om personen samtidigt behandlas på någon annan grund och det är absolut nödvändigt för ändamålet med behandlingen. Regleringen i ramlagen bör dock utformas på ett något annorlunda sätt än i myndigheternas registerförfattningar för att det ska bli tydligare vilka uppgifter som utgör känsliga personuppgifter och när dessa får behandlas.

De behöriga myndigheterna behandlar i stor utsträckning vissa typer av känsliga personuppgifter. Det gäller framför allt uppgifter om hälsa, t.ex. i förundersökningar och mål om vålds- och sexualbrott och i personutredningar. För sådana ändamål är behandling av uppgifter om hälsa givetvis absolut nödvändig. Regeringen vill därför understryka att någon förändring av synen på vad som är absolut nödvändigt vid behandling av känsliga personuppgifter inte är avsedd. Känsliga personuppgifter ska alltjämt användas restriktivt och en bedömning av om kravet är uppfyllt ska göras i det enskilda fallet. Den närmare innebörden av uttrycket kan dock variera mellan myndigheterna, eftersom deras verksamheter och behov av att behandla känsliga personuppgifter skiljer sig åt.

Som framgår av avsnitt 6.4.4 kommer flera myndigheter och andra aktörer att tillämpa ramlagen. Flera av dem har ingen särskild registerförfattning utan tillämpar i dag personuppgiftslagen med tillhörande förordning. Eftersom huvudregeln enligt personuppgiftslagen är att det är förbjudet att behandla känsliga personuppgifter och 8 § personuppgiftsförordningen bara medger undantag för vissa typer av behandling kan det inte undvikas att dessa myndigheter och aktörer sannolikt kommer att kunna behandla känsliga personuppgifter i större utsträckning med den nya regleringen. Det gäller dock bara när de utför uppgifter inom ramlagens tillämpningsområde och är en rimlig konsekvens av att de anses vara behöriga myndigheter i ramlagens mening.

Behandling av genetiska och biometriska uppgifter

Som nyss nämnts har genetiska och biometriska uppgifter inte tidigare ingått i uppräkningen av vad som är känsliga personuppgifter. I förarbetena till lagen (2006:351) om genetisk integritet m.m. uttalas att genetisk

information kan avslöja såväl hälsotillstånd som etnisk tillhörighet och därför är att betrakta som känsliga personuppgifter (Genetisk integritet m.m., prop. 2005/06:64, s. 63). Det är osäkert vilket genomslag det uttalandet har fått i praktiken och om de särskilda restriktioner som gäller för behandlingen av känsliga personuppgifter därför tillämpas på genetiska och biometriska uppgifter.

Fingeravtryck och framför allt dna-spår får en allt större betydelse i den brottsutredande verksamheten. Tekniken utvecklas hela tiden och möjliggör i dag dels analyser av oerhört små mängder dna, dels att nya typer av uppgifter kan tas fram ur dna-spår. Det är därför viktigt att behandling av personuppgifter i samband med hanteringen av fingeravtryck, dna-spår och dna-profiler är tydligt reglerad.

Det är vanligt att polisen hittar fingeravtryck eller dna-spår från någon som inte förekommer i fingeravtrycks- eller dna-registren. Som tidigare nämnts utgör sådana oidentifierade fingeravtryck eller dna-spår som genomgår särskild teknisk behandling för att möjliggöra unik identifiering biometriska uppgifter. Regeln om att känsliga personuppgifter endast får behandlas om någon annan uppgift om personen i fråga samtidigt behandlas fungerar därmed inte när det gäller oidentifierade avtryck eller spår. Det finns därför skäl att reglera behandlingen av genetiska och biometriska uppgifter särskilt. Sådana uppgifter bör få behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen. Att dessa kategorier av uppgifter regleras särskilt är en lagteknisk fråga och innebär inte att de ska betraktas på något annat sätt än övriga kategorier av känsliga personuppgifter. När det gäller frågan som *Justitiekanslern* väcker, om inte förutsättningarna för att få behandla biometriska och genetiska uppgifter uttömmande bör anges i andra författningar än ramlagen, håller regeringen med utredningen om att ramlagen bör innehålla en sådan bestämmelse som föreslås. Eftersom det är fråga om grundläggande krav för att få behandla två kategorier av känsliga personuppgifter hör bestämmelsen hemma i ramlagen, dessutom ska kravet på absolut nödvändighet som anges i bestämmelsen gälla generellt för alla behöriga myndigheter.

Behandling för diarieföring eller liknande

Som framgår av avsnitt 7.3 måste en myndighet alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande anmälningar, ansökningar och andra liknande handlingar. De som ska tillämpa ramlagen föreslås därför få behandla personuppgifter för diarieföring och för att utföra andra nödvändiga handläggningsuppgifter. Det bör gälla även i de fall där sådana handlingar innehåller känsliga personuppgifter, eftersom det ligger utanför myndighetens kontroll om sådana uppgifter finns i handlingarna. Det bör framgå att sådan behandling är tillåten.

Lagrådet förordar att bestämmelserna om känsliga personuppgifter formuleras annorlunda än i lagrådsremissens förslag. Det rör sig om en redaktionell ändring som bl.a. innebär att benämningen känsliga personuppgifter flyttas från 2 kap. 13 § till 2 kap. 11 §. Regeringen anser dock att de olika förutsättningarna för att behandla biometriska och genetiska uppgifter respektive övriga kategorier av känsliga personuppgifter fram-

kommer tydligare med den formulering av bestämmelserna som följer av lagrådsremissens förslag. Bestämmelserna bör därför inte omformuleras på det sätt som Lagrådet föreslår. Däremot anser regeringen att en mindre redaktionell ändring bör göras i 2 kap. 13 § jämfört med förslaget i lagrådsremissen.

Ett generellt sökförbud

Sökning på känsliga personuppgifter kan möjliggöra exempelvis kartläggning av personer med viss politisk ståndpunkt eller religiös uppfattning. Sökningar för sådana ändamål bör som huvudregel inte tillåtas. I flera av de behöriga myndigheternas registerförfattningar finns förbud mot att som sökbegrepp använda uppgifter som avslöjar känsliga personuppgifter (se t.ex. 3 kap. 5 § polisdatalagen). Det kan dock i vissa fall vara befogat att använda känsliga personuppgifter vid sökningar. Flera registerförfattningar ger därför möjlighet att i begränsad utsträckning använda sådana uppgifter som sökbegrepp (se t.ex. 14 och 15 §§ domstolsdatalagen). För Polismyndigheten, Kustbevakningen, Åklagarmyndigheten och Ekobrottsmyndigheten gäller förbuden att använda känsliga personuppgifter som sökbegrepp endast vid sökningar i personuppgifter som har gjorts gemensamt tillgängliga. De får alltså använda känsliga personuppgifter som sökbegrepp vid sökningar i uppgifter som endast ett fåtal personer har tillgång till. Detsamma gäller för Tullverket och Skatteverket i deras brottsbekämpande verksamhet.

Enligt direktivet krävs det inget förbud mot att använda känsliga personuppgifter vid sökning, men sådana uppgifter får behandlas endast om det finns lämpliga skyddsåtgärder för behandlingen. En verkningsfull skyddsåtgärd är att som huvudregel förbjuda att känsliga personuppgifter används vid sökning och att sedan reglera eventuella undantag från den regeln. Det bör därför som utredningen föreslår även i fortsättningen vara förbjudet att utföra sökningar som avslöjar känsliga personuppgifter. Eftersom inte alla behöriga myndigheter har en registerförfattning bör ett generellt sökförbud tas in i ramlagen.

Användningen av ordet sökbegrepp i bestämmelserna om sökförbud har lett till problem i tillämpningen. Vid en strikt tolkning av dessa bestämmelser skulle t.ex. en sökning på ordet islam inte få göras, eftersom uppgifter som avslöjar religiös övertygelse inte får användas som sökbegrepp. Islam är emellertid också ett vanligt personnamn som det måste vara möjligt att få använda vid sökning. Ett annat exempel är att ett sjukhus eller en kyrka, där ett brott begåtts, används som sökbegrepp av utredningsskäl. Sökningen kan ge träff på personer och därigenom avslöja uppgifter som rör hälsa eller religiös uppfattning samtidigt som det finns utredningsskäl att använda platsen som sökbegrepp. Regeringen håller därför med utredningen om att förbudet i ramlagen i stället bör utgå från syftet med sökningen. Det bör inte vara tillåtet att göra sökningar i syfte att få fram urval av personer grundade på känsliga personuppgifter. Detta stämmer enligt regeringens bedömning väl överens med syftet med dagens reglering (se t.ex. prop. 2009/10:85 s. 155). Med en sådan utformning överensstämmer sökförbudet i ramlagen även med sökförbudet i den föreslagna dataskyddslagen som ska innehålla kom-

pletterande bestämmelser till EU:s dataskyddsförordning (prop. 2017/18:105 s. 90 f.).

Datainspektionen ser det som viktigt att det föreslagna sökförbudet inte utökar möjligheterna att söka på känsliga personuppgifter. Att förbudet utformas på ett annat sätt än i dag är inte tänkt att utvidga möjligheterna att använda känsliga personuppgifter för sökning. Genom att sökförbudet placeras i ramlagen kommer det tvärtom att gälla i större utsträckning än i dag, eftersom sökförbuden i flera av registerförfattningarna enbart gäller vid sökningar i uppgifter som har gjorts gemensamt tillgängliga. När syftet blir avgörande för om en sökning är tillåten eller inte kommer vidare olika former av kodning av personuppgifter för att möjliggöra sammanställningar grundade på känsliga personuppgifter inte att vara tillåtna, vilket innebär ett skydd mot missbruk.

Däremot kommer sökningar på t.ex. egennamn som också kan avslöja känsliga personuppgifter att vara tillåtna, eftersom syftet med sökningen då är att få fram närmare information om en person med ett visst namn, inte att få fram ett urval av personer grundat på känsliga personuppgifter. Det blir därför, som Datainspektionen påpekar, viktigt att dokumentera syftet med en sökning av det slaget såvida inte syftet med sökningen framgår av sammanhanget. Det underlättar både intern kontroll och tillsyn över verksamheten.

Det kommer också att, som *Statens institutionsstyrelse* lyfter fram, vara tillåtet att söka på känsliga personuppgifter om sökningen begränsas till att gälla en viss person, eftersom sökresultatet då inte kommer att utvisa något urval av personer. Skyddet för enskilda tillgodoses i de fallen genom bestämmelsen om under vilka förutsättningar känsliga personuppgifter överhuvudtaget får behandlas. Inte heller dagens sökförbud syftar till att förbjuda den typen av begränsade sökningar. Vidare kommer det att vara tillåtet att utföra sökningar i registervårdande syfte och i syfte att utöva tillsyn, något som *Polismyndigheten* och *Säkerhets- och integritetsskyddsnämnden* betonar vikten av, eftersom sökningar för sådana syften inte träffas av förbudet.

Även vid tillåtna sökningar kan sökningen resultera i ett urval av personer grundat på känsliga personuppgifter. I exemplet med namnet Islam kan en sökning på egennamnet ge träffar både på personer med det namnet och personer som bekänner sig till en viss tro. I vilken utsträckning det sedan är tillåtet att behandla uppgifterna i sammanställningen får prövas mot huvudregeln för behandling av känsliga personuppgifter.

Domstolsverket ser problem med det sökförbud som föreslås eftersom det enligt verket kan vara svårt att bedöma syftet med en viss sökning. Det exempel Domstolsverket tar upp är att om allmänheten begär att en behörig myndighet ska ta fram vissa uppgifter för ett utlämnande, får myndigheten som regel inte efterfråga vad syftet med begäran är. Regeringen gör här följande överväganden. Vid utlämnande av en allmän handling som sker på begäran av en enskild har tryckfrihetsförordningens bestämmelser företräde framför dataskyddsregelverket (prop. 2017/18:105 s. 40 f.). Den behöriga myndigheten har att i varje enskilt fall bedöma om de uppgifter som efterfrågas utgör en allmän handling hos myndigheten. Utgör uppgifterna en allmän handling ska de lämnas ut såvida de inte omfattas av sekretess. Detta gäller även om det är fråga om känsliga personuppgifter som har sammanställts genom sökning. Sekre-

tessbestämmelser som kan vara tillämpliga i sammanhanget är bl.a. 18 kap. 1–2 §§ och 35 kap. 1 § offentlighets- och sekretesslagen.

I de behöriga myndigheternas registerförfattningar tillåts i viss utsträckning användning av känsliga personuppgifter vid sökning. Bestämmelserna kommer att behöva anpassas till att sökförbudet i ramlagen är annorlunda utformat än dagens reglering. Utgångspunkten är att de behöriga myndigheterna inte ska få använda känsliga personuppgifter vid sökning i större utsträckning än i dag. För någon eller några av de behöriga myndigheterna kan dock förbudet i dag vara för snävt. Vid utredning av brott kan de brottsbekämpande myndigheterna ha behov av att kunna söka på andra uppgifter än brottsrubriceringar eller uppgifter som beskriver en persons utseende, exempelvis uppgifter om sexualliv vid utredningen av en våldtäkt. Regeringen återkommer till frågan om sökning med användande av känsliga personuppgifter i samband med att registerförfattningarna anpassas till ramlagen.

8.1.5 Inga ytterligare regler om vilka personuppgifter som får behandlas

Regeringens bedömning: Utöver reglerna om känsliga personuppgifter bör det inte tas in några regler i ramlagen om vilka personuppgifter som får behandlas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: De remissinstanser som uttalar sig om bedömningen är *Polismyndigheten* som tillstyrker den och *Datainspektionen* som ställer sig tveksam till om direktivets krav blir uppfyllda då det inte närmare anges i ramlagen vilka personuppgifter som får behandlas.

Skälen för regeringens bedömning

Ingen uttömmande reglering av vilka personuppgifter som får behandlas

Enligt artikel 8.2 ska det i nationell rätt bl.a. föreskrivas vilka personuppgifter som ska behandlas. Ur ett integritetsperspektiv är det naturligtvis väsentligt att en myndighet inte behandlar andra personuppgifter än vad som behövs för myndighetens verksamhet. Regeringen håller med utredningen om att det inte är rimligt att tolka artikeln på det sättet att det i ramlagen eller i de särskilda registerförfattningarna måste räknas upp exakt vilka personuppgifter som får behandlas. Att i författning uttömmande reglera vilka personuppgifter, eller ens alla kategorier av personuppgifter, som får behandlas är en närmast omöjlig uppgift, eftersom det inte på förhand går att bedöma vilka uppgifter som kan få betydelse. Särskilt i mångfacetterade verksamheter som polisens och domstolarnas skulle det behövas mycket omfångsrika uppräkningar av vilka uppgifter som skulle få behandlas. Inte bara för dessa utan även för övriga behöriga myndigheter skulle det krävas omfattande och grundliga undersökningar innan det skulle kunna slås fast vilka personuppgifter som bör få behandlas. Saken kompliceras dessutom av att det skulle behöva preciseras beträffande varje enskild personkategori vilka personuppgifter som får behandlas för just den kategorin.

Behovet av att behandla personuppgifter skiljer sig åt beroende på om det är fråga om förundersökning, brottmålsrättegång, verkställighet av påföljd eller att upprätthålla allmän ordning och säkerhet. Vissa behöriga myndigheter har behov av att behandla fler typer av personuppgifter än andra. En allmängiltig förteckning skulle därför inte fungera. Skulle någon personkategori eller kategori av uppgifter saknas skulle det inte finnas rättsligt stöd för behandlingen även om den var nödvändig. Förutom att en detaljbetonad uppräkning av det slaget skulle strida mot svensk lagstiftningstradition skulle den försvåra möjligheterna för behöriga myndigheter att bedriva en effektiv verksamhet. Den som behöver behandla personuppgifter skulle nämligen alltid behöva konsultera en omfattande förteckning för att kunna avgöra om behandlingen av en viss personuppgift var tillåten. En uppräkning av det slaget skulle också riskera att snabbt bli inaktuell och skulle därför behöva uppdateras ofta.

Eftersom ett av syftena med direktivet enligt artikel 1.2 b är att säkerställa att behöriga myndigheters utbyte av personuppgifter inte begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter kan avsikten med artikel 8.2 enligt regeringens mening inte vara att det i nationell rätt ska finnas uttömmande uppräkningar av vilka personuppgifter som får behandlas.

Som framgår av avsnitt 7.4 och 8.1.2 föreslås att vissa grundläggande bestämmelser motsvarande dem som i dag finns i 9 § personuppgiftslagen ska tas in i ramlagen. Förslagen innebär att personuppgifter enbart får behandlas för särskilda, uttryckliga och berättigade ändamål. Personuppgifterna ska vidare vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen får inte behandlas och de personuppgifter som behandlas ska vara korrekta och, om nödvändigt, uppdaterade. Att behandla ovidkommande eller onödigt många personuppgifter i förhållande till de bestämda ändamålen strider därmed mot regelverket. Dessa grundläggande krav – tillsammans med bl.a. rättegångsbalkens och brottsbalkens regler – innebär därför såväl en kvantitativ som en kvalitativ begränsning av vilka personuppgifter som får behandlas.

Till skillnad mot *Datainspektionen* håller regeringen med utredningen om att de föreslagna grundläggande kraven och regleringen av när känsliga personuppgifter får behandlas, tillsammans med andra tillämpliga regler, därför innebär en tillräcklig avgränsning av vilka slags personuppgifter som behöriga myndigheter får behandla. Det finns därför inget behov av ytterligare regler om det i ramlagen.

Avidentifiering bör användas i så stor utsträckning som möjligt

En fråga som särskilt bör uppmärksammas är det faktiska behovet av att använda namnuppgifter eller andra uppgifter som direkt identifierar en person, t.ex. personnummer. Kan en uppgift utföras tillfredsställande även om personuppgifterna utelämnas är de grundläggande kraven på adekvans och personuppgifternas omfattning inte uppfyllda (jfr SOU 2015:39 s. 285).

Prövningen av om en personuppgift är nödvändig för en viss behandling måste göras kontinuerligt av myndigheterna och inte bara då uppgif-

ten registreras eller på annat sätt samlas in i verksamheten. Även vid en senare hantering ska personuppgiften behövas för ändamålet med just den hanteringen. Det innebär exempelvis att även om uppgiften om en persons namn måste behandlas vid handläggningen av ett ärende i vilket personen är part eller annars direkt berörd, är det inte säkert att namnuppgiften behöver behandlas i ett senare skede, t.ex. vid verksamhetsuppföljning eller vid publicering på myndighetens webbplats för att informera allmänheten om ett principiellt viktigt avgörande. Det ska alltså vid all behandling prövas om det går att avstå från att använda uppgifter som direkt går att hänföra till en viss person. Möjligheten till avidentifiering bör användas i så stor utsträckning som möjligt.

8.1.6 Åtgärder för att säkerställa personuppgifternas kvalitet

Regeringens förslag: Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga rättas utan onödigt dröjsmål. Detsamma gäller för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

När personuppgifter lämnas ut till en behörig myndighet, ska mottagaren så långt det är möjligt ges information som gör att det går att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga.

Alla rimliga åtgärder ska också vidtas för att personuppgifter som behandlas på ett otillåtet sätt utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

I stället för att personuppgifterna raderas, ska behandlingen av uppgifterna begränsas utan onödigt dröjsmål om uppgifterna behöver finnas kvar av bevisskäl.

Regeringens bedömning: Skyldigheten att underrätta mottagare av personuppgifterna om att de är felaktiga eller behandlas på otillåtet sätt kan regleras i förordning.

Utredningens förslag överensstämmer i sak med regeringens förslag och bedömning.

Remissinstanserna: *Hovrätten för Västra Sverige* anser att formuleringen ”så långt det är möjligt” inte tillför något konkret när det gäller informationsskyldigheten som gör det möjligt för mottagare av personuppgifter att bedöma uppgifternas kvalitet, och är därför tveksam till om den behövs. *Domstolsverket* efterlyser en ingående analys av när det kan bli aktuellt med radering inom ramlagens tillämpningsområde, mot bakgrund av att lagen nästan uteslutande kommer att tillämpas av myndigheter och det följaktligen i de flesta fall kommer att bli fråga om att radera personuppgifter som finns i allmänna handlingar. Domstolsverket efterfrågar också ett klargörande resonemang om vad som avses med rättelse och begränsning. Enligt *Sveriges advokatsamfund* finns det en överhängande risk för att brottsbekämpande myndigheter inte kommer

att kontrollera riktigheten av personuppgifter som behandlas i brottsutredande verksamhet. Sveriges advokatsamfund anser därför att det bör införas regler om kontrollåtgärder i förordning.

Skälen för regeringens förslag och bedömning

Felaktiga uppgifter ska rättas och uppgifter som behandlas på otillåtet sätt ska raderas

Av artikel 4.1 d framgår att alla rimliga åtgärder ska vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas utan dröjsmål raderas eller rättas. Av artikeln framgår inte i vilka fall uppgifterna ska rättas och i vilka fall de ska raderas. När det gäller korrigering på begäran av registrerade görs det däremot skillnad mellan vilka åtgärder som ska vidtas med felaktiga uppgifter respektive med uppgifter som behandlas på ett otillåtet sätt. Enligt artikel 16.1 ska felaktiga personuppgifter rättas, medan uppgifter som behandlas i strid med vissa uppräknade bestämmelser i direktivet enligt artikel 16.2 ska raderas. Regeringen anser i likhet med utredningen att de två korrigeringsalternativen bör användas under samma förutsättningar oavsett om korrigering görs på den personuppgiftsansvariges eget initiativ eller på begäran av registrerade. Regleringen i ramlagen bör därför utgå från att felaktiga personuppgifter ska rättas och att personuppgifter som behandlas på otillåtet sätt ska raderas.

Korrigeringsalternativen

Enligt artikel 4.1 d är det enbart felaktiga personuppgifter som omfattas av kravet på korrigering. Med hänsyn till att den personuppgiftsansvarige enligt artikel 7.2 ska se till att inte bara felaktiga utan även ofullständiga och inaktuella personuppgifter inte överförs eller görs tillgängliga, bör kravet på rättelse i ramlagen även omfatta ofullständiga och inaktuella uppgifter. I avsnitt 8.1.2 föreslås att personuppgifter bara behöver vara uppdaterade om det är nödvändigt. Därför bör det inte krävas att inaktuella uppgifter korrigeras annat än om det är nödvändigt.

Radering anges som ett korrigeringsalternativ i artikel 4.1 d. Regeringen anser som nyss nämnts att de förutsättningar som gäller för radering på begäran av enskild bör gälla även när frågan om radering väcks av den personuppgiftsansvarige. Av artikel 16.2 framgår att radering kan komma i fråga dels om behandlingen av personuppgifter står i strid med de bestämmelser som genomför artiklarna 4, 8 och 10, dels om det krävs för att den personuppgiftsansvarige ska uppfylla en rättslig förpliktelse. Frågan som *Domstolsverket* väcker, när det i praktiken kan bli aktuellt att använda radering inom ramlagens tillämpningsområde, utvecklas i avsnitt 10.4.2.

Enligt artikel 16.3 ska den personuppgiftsansvarige begränsa behandlingen av personuppgifterna i stället för att radera dem, om den registrerade bestrider att de är korrekta och det inte kan fastställas eller om personuppgifterna behöver sparas som bevisning. Begränsning av behandlingen nämns inte som ett korrigeringsalternativ i artikel 4.1 d. Som tidigare nämnts medger direktivet att medlemsstaterna har starkare skyddsåtgärder än vad som krävs enligt direktivet. Mot den bakgrunden bör be-

gränsning av behandlingen läggas till som ett korrigeringsalternativ, eftersom personuppgifter kan behöva sparas som bevisning till skydd för den registrerade även när den personuppgiftsansvarige själv upptäcker att uppgifterna behandlas på otillåtet sätt. Begränsning av behandlingen på den grunden att det inte kan fastställas om personuppgifterna är korrekta blir däremot inte aktuell när korrigering görs på den personuppgiftsansvariges eget initiativ (jfr avsnitt 10.4.3).

Domstolsverket efterfrågar ett klargörande av vad som avses med rättelse och begränsning. I avsnitt 8.1.2 diskuteras vad som avses med att en uppgift är korrekt. Som redogörs för närmare i avsnitt 10.4.1 kan rättelse innebära att en felaktig eller ofullständig personuppgift ersätts av en annan uppgift som är korrekt ur ett objektivt perspektiv eller kompletteras med en uppgift om de rätta förhållandena så att den blir fullständig i objektiv mening. En felaktig uppgift kan också rättas på det sättet att den tas bort utan att ersättas. Begränsning av behandling kan, som beskrivs i avsnitt 10.4.3, ske bl.a. genom att uppgifterna avskiljs från det datasystem där de behandlas eller genom att tillgången till uppgifterna inskränks. Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas utom för det ändamål som föranledde begränsningen.

Spridning av felaktiga uppgifter och uppgifter som behandlas på otillåtet sätt ska förhindras

Enligt artikel 7.2 ska de behöriga myndigheterna vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska också, i den mån det är praktiskt möjligt, kontrollera kvaliteten på personuppgifterna innan de överförs eller görs tillgängliga. Regleringen hänger naturligt samman med kravet på rättelse av felaktiga personuppgifter. I kravet på att den personuppgiftsansvarige ska göra allt för att rätta felaktiga, ofullständiga eller inaktuella personuppgifter i den egna verksamheten ligger också ett ansvar för att se till att sådana uppgifter inte lämnas ut eller görs tillgängliga. Det bör tydliggöras genom en bestämmelse i ramlagen. Däremot finns det inget behov av att särskilt reglera att den personuppgiftsansvarige ska kontrollera kvaliteten på personuppgifter innan de lämnas ut eller görs tillgängliga. Det får anses följa av det generella kravet på att den personuppgiftsansvarige ska vidta alla rimliga åtgärder för att rätta felaktiga uppgifter.

Artikel 7.2 gäller felaktiga, ofullständiga eller inaktuella personuppgifter, medan artikel 7.3 föreskriver att mottagaren omedelbart ska underrättas om det visar sig att felaktiga personuppgifter har överförts eller att personuppgifter har överförts olagligen. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16. Vad som avses med att uppgifter olagligen överförts är inte helt klart, men i och med att radering och begränsning av behandlingen nämns som korrigeringsalternativ bör, som utredningen konstaterar, underrättelseskyldigheten omfatta också personuppgifter som behandlas på otillåtet sätt. Den personuppgiftsansvarige bör alltså vara skyldig att se till att inte heller personuppgifter som behandlas på ett otillåtet sätt lämnas ut eller görs tillgängliga.

Om det upptäcks att felaktiga personuppgifter eller personuppgifter som behandlas på otillåtet sätt har lämnats ut är det naturligt att den som har fått uppgifterna underrättas, så att uppgifterna kan rättas eller raderas eller behandlingen av dem begränsas. Skyldigheten för mottagaren att rätta, radera eller begränsa behandlingen av uppgifterna behöver inte regleras särskilt, eftersom alla behöriga myndigheter omfattas av den föreslagna skyldigheten att korrigera uppgifter som är felaktiga eller behandlas på otillåtet sätt. Underrättelseskyldigheten kan regleras i förordning.

Sveriges advokatsamfund ser en risk för att de brottsbekämpande myndigheterna inte kommer att efterkomma de regler som nu föreslås om personuppgifters kvalitet och förespråkar därför regler om kontrollåtgärder på förordningsnivå. Det är naturligtvis viktigt att de föreslagna reglerna kommer att få genomslag i praktiken. Regeringen förutsätter att behöriga myndigheter kommer att följa regelverket och anser inte att det, utöver den kontroll som kommer att ligga i tillsynsmyndighetens uppdrag (se avsnitt 11), behöver införas några förordningsbestämmelser om kontrollåtgärder.

Information i samband med utlämnande eller tillgängliggörande av personuppgifter

Vid all överföring av personuppgifter ska enligt artikel 7.2 så långt möjligt sådan nödvändig information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad uppgifterna är korrekta, fullständiga och tillförlitliga och i vilken utsträckning de är aktuella. Bestämmelsen kompletterar skyddet för den enskilde när det gäller kvaliteten på personuppgifter genom att den som tar emot uppgifterna ges möjlighet att göra en egen bedömning av deras kvalitet. Mottagaren kan då fullgöra sin skyldighet att kontrollera kvaliteten på personuppgifter som kommer från andra behöriga myndigheter. En bestämmelse om att sådan information så långt det är möjligt ska lämnas i samband med att personuppgifter lämnas ut bör tas in i ramlagen. Informationen till mottagaren kan exempelvis avse information om var personuppgifterna kommer från, vad man vet om uppgiftslämnaren, när och för vilket ändamål uppgifterna hämtades in och om uppgifterna grundar sig på fakta eller personliga bedömningar. Det kan också vara av värde för mottagaren att få veta om personuppgifterna är eller har varit föremål för domstolsbehandling och om förfarandet i så fall är avslutat. *Hovrätten för Västra Sverige* är tveksam till om formuleringen ”så långt det är möjligt” behövs. Eftersom formuleringen finns i artikel 7.2 ställer direktivet inte något krav på att informationsskyldigheten är absolut. Regeringen gör bedömningen att skyldigheten att lämna information bara bör gälla så långt det är möjligt, eftersom det torde variera från fall till fall i vilken utsträckning den utlämnande myndigheten har information som gör det möjligt att bedöma personuppgifternas kvalitet.

8.2 Längsta tid som personuppgifter får behandlas

8.2.1 Terminologin bör renodlas

Regeringens bedömning: För att skilja mellan arkivrättsliga regler och regler om dataskydd bör orden bevarande och gallring bara användas i den betydelse de har i arkivlagstiftningen. Regleringen i ramlagen bör utgå från hur länge personuppgifter får behandlas för ändamål inom lagens tillämpningsområde.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten*, *Datainspektionen*, *Umeå tingsrätt* och *Riksarkivet* är positiva till att terminologin renodlas och anser att det bidrar till ett tydligare regelverk. Övriga remissinstanser yttrar sig inte särskilt om bedömningen.

Skälen för regeringens bedömning: Regleringen av bevarande av personuppgifter är komplex. Arkivreglerna innebär att allmänna handlingar ska bevaras i arkiv och bär på så sätt upp handlingsoffentligheten. Enligt 3 § arkivlagen (1990:782) ska myndigheters arkiv bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättsskipningen och förvaltningen och forskningens behov. Allmänna handlingar får enligt 10 § samma lag gallras, men det ska då beaktas att det arkivmaterial som återstår ska kunna tillgodose ändamålen med arkiven. Enligt 14 § arkivförordningen (1991:446) får statliga myndigheter gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet eller enligt särskilda gallringsföreskrifter i lag eller förordning. Gallring enligt Riksarkivets föreskrifter görs för att begränsa arkivens omfattning. Med gallring avses att handlingar eller uppgifter sorteras ut och förstörs. Gallring av elektroniska upptagningar innebär normalt att information raderas från databäraren. Som gallring räknas enligt Riksarkivets föreskrifter förstöring av allmänna handlingar och uppgifter i allmänna handlingar (se t.ex. 2 kap. 1 § RA-FS 2009:1). Överföring till annan databärare räknas som gallring om överföringen medför informationsförlust, förlust av sökmöjligheter eller förlust av möjligheter att fastställa informationens autenticitet (SOU 2015:39 s. 526). Informationen behöver således inte förstöras för att det ska vara fråga om gallring.

Regeringen gav i oktober 2017 en särskild utredare i uppdrag att göra en bred översyn av arkivområdet, bl.a. mot bakgrund av den ökande digitaliseringen. Utredaren ska bl.a. se över arkivlagstiftningen och närliggande lagstiftning och vid behov lämna förslag på hur lagstiftningen kan anpassas till utvecklingen på området. Uppdraget ska redovisas senast den 18 november 2019 (dir 2017:106).

I flertalet registerförfattningar finns det bestämmelser om bevarande och gallring (se bl.a. 3 kap. 9–15 §§ polisdatalagen, 2 kap. 10 § åklagardatalagen, 4 kap. 8–14 §§ kustbevakningsdatalagen och 7 § lagen om behandling av personuppgifter inom kriminalvården). Gallring enligt dessa författningar görs för att skydda den enskildes integritet. Sådana regler finns också i 4 kap. tullbrottsdatalagen och 4 kap. skattebrottsdatalagen.

De personuppgifter som behöriga myndigheter behandlar ingår i mycket stor utsträckning i upptagningar som är eller kommer att bli allmänna handlingar. Utgångspunkten i det arkivrättsliga regelverket är att uppgifter ska bevaras, medan presumtionen enligt reglerna om skydd för personuppgifter är den motsatta. I 8 § andra stycket personuppgiftslagen har arkivlagstiftningen getts företräde genom att det anges att bestämmelser om längsta tid för bevarande inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Den principen bör som utredningen föreslår, som utgångspunkt, gälla även fortsättningsvis.

Som nyss nämnts syftar gallringsbestämmelserna i myndigheternas registerförfattningar till att skydda enskildas integritet. För att tydligare skilja mellan arkivrättsliga regler och regler om skydd för personuppgifter bör begreppen bevarande och gallring enbart användas i den betydelse de har i arkivlagstiftningen. I ramlagen bör regleringen i stället utgå från hur länge personuppgifter får behandlas för ändamål inom ramlagens tillämpningsområde. Regeringen återkommer till de ändringar som kan behövas i registerförfattningarna i samband med att dessa anpassas till ramlagen.

8.2.2 Hur länge får personuppgifter behandlas?

Regeringens förslag: Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för ändamål inom ramlagens tillämpningsområde, ska den personuppgiftsansvarige årligen se över behovet av att fortsätta behandla personuppgifterna.

Regeringens bedömning: Att behöriga myndigheter ska ha rutiner för att säkerställa att reglerna om längsta tid för behandling av personuppgifter respekteras kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna: *Domstolsverket* ifrågasätter att behandling av personuppgifter för arkivändamål ska omfattas av dataskyddsförordningens tillämpningsområde. Enligt Domstolsverket är det inte lämpligt att olika regler ska gälla beroende på om domstolarna behandlar uppgifterna medan målet fortfarande pågår eller efter det att målet har avlutats och arkiverats. Domstolsverket efterfrågar också en närmare diskussion om vad det innebär att den personuppgiftsansvarige årligen ska se över behovet av att fortsätta behandla personuppgifter. Eftersom ramlagen endast kommer att vara tillämplig på pågående mål och ärenden kan inte verket se att det kan komma att finnas personuppgifter som behandlas av domstolarna under längre tid än nödvändigt. *Umeå tingsrätt* anser, mot bakgrund av att det ofta finns behov av att få tillgång till personuppgifter som finns i avslutade mål, att det noga bör analyseras om en årlig över-

syn är ändamålsenlig i de allmänna domstolarnas verksamhet. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet och nuvarande reglering

Enligt artikel 4.1 e ska personuppgifter inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas. Det ska enligt artikel 5 föreskrivas lämpliga tidsgränser för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna efterlevs. Behandling kan enligt artikel 4.3 inbegripa arkivändamål av allmänt intresse.

En bestämmelse som motsvarar artikel 4.1 e finns i artikel 6.1 e i 1995 års dataskyddsdirektiv, som har genomförts genom 9 § första stycket i personuppgiftslagen. Där anges att personuppgifter inte får bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Bestämmelsen är inte tillämplig för polisen, Kustbevakningen och åklagarväsendet. Den är inte heller tillämplig för Tullverket eller Skatteverket i deras brottsbekämpande verksamhet. I dessa myndigheters registerförfattningar finns det i stället särskilda bestämmelser med motsvarande innehåll.

Personuppgifter får bara behandlas så länge de behövs för ändamål inom ramlagens tillämpningsområde

För de behöriga myndigheterna gäller redan i dag att personuppgifter inte får bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas. Det gäller antingen för att de tillämpar 9 § personuppgiftslagen eller för att deras registerförfattningar innehåller en motsvarande bestämmelse. En motsvarande bestämmelse om hur länge personuppgifter får behandlas bör tas in i ramlagen. För att tydliggöra att det inte är fråga om bevarande i arkivlagens mening bör ordet behandlas användas i stället för bevaras. Personuppgifter bör alltså inte få behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Om en behörig myndighet behandlar en personuppgift för flera ändamål samtidigt varierar tiden för hur länge uppgiften behöver behandlas. Att det inte längre finns behov av att behandla personuppgiften för ett visst ändamål medför inte att behandlingen av den måste upphöra för alla andra ändamål samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål inte att den får fortsätta att behandlas för alla ändamål lika länge.

Artikel 5 ger två möjligheter när det gäller att säkerställa att personuppgifter inte behandlas längre än nödvändigt. Enligt artikeln ska det fastställas lämpliga tidsgränser för antingen radering av personuppgifter eller periodisk översyn av behovet av att lagra personuppgifter. Eftersom det enligt artikel 4.3 är tillåtet att behandla personuppgifter för arkivändamål av allmänt intresse kan det inte rimligen krävas att uppgifterna ska raderas. Enligt regeringen bör artikeln tolkas så att det ska finnas frister för när behandlingen av personuppgifterna för ändamål inom direktivets tillämpningsområde ska upphöra.

De flesta registerförfattningar föreskriver som nyss nämnts frister för när behandlingen av personuppgifterna för ändamål som anges i författningarna ska upphöra. I bestämmelserna anges att personuppgifterna ska gallras senast vid en viss tidpunkt. Regeringen avser att se över terminologin för att renodla den i samband med att registerförfattningarna anpassas till ramlagen (se avsnitt 8.2.1).

De frister som finns täcker dock inte all personuppgiftsbehandling som utförs av de behöriga myndigheterna. Regeringen håller med utredningen om att det varken är möjligt eller lämpligt att i ramlagen ställa upp en generell frist för när behandlingen av personuppgifter för ändamål inom ramlagens tillämpningsområde ska upphöra, eftersom det varierar hur länge myndigheterna behöver kunna behandla olika typer av personuppgifter. Regleringen i ramlagen bör därför utgå från möjligheten att föreskriva tidsgränser för periodisk översyn av behovet av att behandla personuppgifter.

Enligt huvudregeln får personuppgifter inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Om den regeln kompletteras med en bestämmelse om att den behöriga myndigheten – om det saknas frist för när uppgifter inte längre får behandlas för ändamål inom ramlagens tillämpningsområde – en gång om året ska se över behovet av att fortsatt behandla personuppgifterna, säkerställs att behandlingen upphör när det inte längre finns behov av den. För de behöriga myndigheter som inte har en registerförfattning, eller där registerförfattningen inte innehåller någon särskild frist för när personuppgifter inte längre får behandlas, kommer sistnämnda regel att gälla.

Det är viktigt att de behöriga myndigheterna ser till att de frister för längsta tid för behandling som finns respekteras och skapar rutiner för att se över behovet av att fortsatt behandla personuppgifter. Regeringen anser, i likhet med utredningen, att de särskilda fristerna och den föreslagna bestämmelsen om periodisk översyn kan kompletteras med föreskrifter på lägre nivå om att de behöriga myndigheterna ska ha rutiner för att se till att bestämmelserna efterlevs. Direktivets krav på procedurrelaterade åtgärder blir därmed uppfyllt.

Domstolsverket och *Umeå tingsrätt* har väckt frågan hur kravet på årlig översyn förhåller sig till domstolarnas verksamhet. Kravet på årlig översyn gäller endast om det saknas frist för hur länge personuppgifter får behandlas för ändamål inom ramlagens tillämpningsområde. Som framgår ovan är syftet med både årlig översyn och fastställda frister för när personuppgiftsbehandling ska upphöra, att säkerställa att behöriga myndigheter följer huvudregeln att personuppgifter inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Om det är nödvändigt för domstolarna att behandla personuppgifter så länge mål och ärenden pågår, torde den årliga översynen för domstolarnas del kunna vara mycket generell. Av direktivets krav på fastställda tidsgränser för antingen radering eller periodisk översyn är det senare alternativet det minst ingripande.

Enligt 8 § andra stycket personuppgiftslagen hindrar lagens bestämmelser om hur länge personuppgifter får bevaras inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Bestämmelsen gäller för några av de behöriga myndigheterna. Arkivlagstiftningen har alltså i fråga om allmänna handlingar företräde framför personuppgiftslagens bestämmelser om längsta bevarandetid. För polisen, åklagarväsendet och Kustbevakningen har det gjorts undantag från 8 § andra stycket. I de myndigheternas registerförfattningar finns i stället som nyss nämnts särskilda regler om gallring. Motsvarande reglering finns för Tullverkets och Skatteverkets brottsbekämpande verksamhet.

Enligt artikel 4.3 kan behandling inbegripa arkivändamål av allmänt intresse. För att tydliggöra att personuppgifter får arkiveras när de inte längre behövs för något av de andra i ramlagen tillåtna ändamålen bör det tas in en bestämmelse i ramlagen som motsvarar 8 § andra stycket personuppgiftslagen. I vilken utsträckning personuppgifterna ska gallras regleras i det arkivrättsliga regelverket.

Det bör anmärkas att behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde, oavsett om det är den behöriga myndigheten som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet. *Domstolsverket* har ifrågasatt detta, men eftersom dataskyddsdirektivet och följaktligen den föreslagna ramlagen endast gäller för behöriga myndigheters personuppgiftsbehandling för vissa syften (se avsnitt 6), faller behandling av personuppgifter för arkivändamål av allmänt intresse in under dataskyddsförordningen. *Umeå tingsrätt* har påpekat att domstolarna ofta har behov av att få tillgång till personuppgifter som finns i avslutade mål. Om ett avslutat brottmål har arkiverats blir dataskyddsförordningen tillämplig på de arkiverade personuppgifterna. Det hindrar inte att de arkiverade personuppgifterna hämtas för att behandlas i ett nyinkommet brottmål. Det blir då ramlagen och eventuell annan lagstiftning som genomför dataskyddsdirektivet som ska tillämpas på de hämtade personuppgifterna.

8.3 Automatiserade beslut

Regeringens förslag: Om ett beslut har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne och beslutet enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet prövat på nytt av någon person. Automatiserade beslut får inte enbart grundas på känsliga personuppgifter.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt om förslaget.

Skälen för regeringens förslag: I artikel 11 föreskrivs att det ska införas förbud mot automatiserade beslut som inbegriper profilering, såvida

inte sådana beslut är tillåtna enligt unionsrätten eller nationell rätt och det är föreskrivet lämpliga skyddsåtgärder för den enskilde. Skyddsåtgärderna ska åtminstone ge den enskilde rätt till personlig kontakt med någon hos den personuppgiftsansvarige. Enligt skäl 38 ska skyddsåtgärderna innefatta särskild information till den registrerade och rätt till personlig kontakt för att möjliggöra för honom eller henne att framföra synpunkter, att få beslutet förklarat för sig och att överklaga beslutet. Sådana beslut som avses i artikel 11 får inte grundas på känsliga personuppgifter, om inte lämpliga skyddsåtgärder har vidtagits.

Med automatiserade beslut avses beslut som inte fattas av någon tjänsteman utan som blir den automatiska följden av t.ex. att en viss handling ges in eller inte inkommer inom viss tid. Automatiserade beslut förekommer i viss utsträckning inom den svenska förvaltningen, men det rör sig främst om beslut i skattefrågor och i frågor som regleras i socialförsäkringsbalken. Inom ramlagens tillämpningsområde förekommer det i dag inga automatiserade beslut, men med teknikutvecklingen kan det inte uteslutas att det i framtiden kommer att finnas sådana. Eftersom direktivet sätter gränser för beslut som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne och som enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, bör ramlagen innehålla en bestämmelse om sådana beslut. Det finns dock inget skäl att öppna för möjligheten att meddela automatiserade beslut som enbart grundar sig på känsliga personuppgifter. Sådana beslut bör därför inte tillåtas.

I 29 § personuppgiftslagen finns en liknande bestämmelse om automatiserade beslut. Den bör tjäna som utgångspunkt för hur bestämmelsen i ramlagen utformas.

Information avseende automatiserade beslut behandlas i avsnitt 10.2.9 och överklagande i avsnitt 13.4.

8.4 Användningsbegränsning

Regeringens förslag: Om det inte är särskilt föreskrivet får villkor för behandlingen av personuppgifter inte ställas upp i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om det inte i motsvarande fall får ställas upp samma typ av villkor i förhållande till en svensk mottagare.

Regeringens bedömning: Att mottagaren ska informeras om sådana villkor kan regleras i förordning.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag och bedömning. Utredningen föreslår att det i vissa författningar som innehåller bestämmelser om användningsbegränsningar ska införas en upplysning om att det i ramlagen finns bestämmelser om att villkor om hur personuppgifter får behandlas inte får ställas upp i vissa fall.

Remissinstanserna: Ingen remissinstans invänder mot förslaget och bedömningen.

Skälen för regeringens förslag och bedömning: I artikel 9.3 föreskrivs skyldighet för behöriga myndigheter att informera mottagare av

personuppgifter om att det har ställts upp begränsningar för hur uppgifterna får behandlas och att sådana användningsbegränsningar måste respekteras. Enligt artikel 9.4 ska fastställda villkor för behandlingen av personuppgifter inte tillämpas i förhållande till mottagare i andra medlemsstater eller på byråer eller organ som har inrättats i enlighet med bestämmelserna om straffrättsligt samarbete och polissamarbete i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), med undantag för sådana villkor som är tillämpliga när personuppgifter i motsvarande fall lämnas ut nationellt.

Rätten att ställa upp användningsbegränsningar ska enligt artikel 9.3 framgå av unionsrätten eller av nationell rätt. Artikeln skapar ingen rätt för behöriga myndigheter att ställa upp användningsbegränsningar, utan innebär endast en skyldighet att informera när sådana villkor har ställts upp på grund av andra regler. Informationsskyldigheten kan regleras i förordning.

Användningsbegränsningar ska enligt artikel 9.4 inte tillämpas i förhållande till mottagare i andra medlemsstater eller EU-organ, utom sådana villkor som är tillämpliga när personuppgifter i motsvarande fall lämnas ut nationellt. Artikeln torde innebära att användningsbegränsningar inte får ställas upp i större utsträckning i förhållande till mottagare i andra medlemsstater än vad som är tillåtet i förhållande till mottagare i den egna medlemsstaten.

Det bör regleras att användningsbegränsningar inte får ställas upp i större utsträckning i förhållande till mottagare i en annan medlemsstat eller ett EU-organ än vad som gäller i förhållande till mottagare i Sverige, om det inte är särskilt föreskrivet. Bestämmelser om när användningsbegränsningar får ställas upp finns inom ramlagens tillämpningsområde i lagen (2000:562) om internationell rättslig hjälp i brottmål, lagen (2000:1219) om internationellt tullsamarbete, lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar, förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen, lagen (2017:496) om internationellt polisiärt samarbete och lagen (2017:1000) om en europeisk utredningsorder.

Av artikel 60 framgår att direktivet inte ska påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området som trädde i kraft den 6 maj 2016 eller tidigare, vilka gäller behandling mellan medlemsstater eller tillgång till informationssystem som inrättats på grundval av fördragen och som är relevanta för direktivets tillämpningsområde (se avsnitt 6.3). Dataskyddsbestämmelser i sådana rättsakter ska alltså gälla framför direktivet. Om det enligt en sådan rättsakt är tillåtet att ställa upp användningsbegränsningar i förhållande till andra medlemsstater, trots att motsvarande möjlighet inte finns när det gäller nationella mottagare, bör därför bestämmelser om det kunna behållas. Bestämmelserna om användningsbegränsningar i de författningar som nämns ovan kommer således att gälla framför den bestämmelse som nu föreslås. Mot den bakgrunden bör sådana upplysningsbestämmelser som utredningen föreslår inte införas i aktuella författningar. Artikel 9.4 får tolkas som att den avser användningsbegränsningar i samband med uppgiftsutbyte i andra fall.

8.5 Uppgifter till rättsstatistiken

Regeringens förslag: Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om förslaget.

Skälen för regeringens förslag: I avsnitt 6.1.2 anges att de brottsbekämpande myndigheternas registerförfattningar kommer att gälla utöver ramlagen och att en konsekvens av den ändrade strukturen är att vissa bestämmelser som i dag finns i registerförfattningarna kommer att behöva flyttas till ramlagen, om de är av den arten att de bör gälla för all verksamhet inom direktivets tillämpningsområde.

I 9 § lagen om behandling av personuppgifter inom kriminalvården, 2 kap. 14 § polisdatalagen, 2 kap. 12 § åklagardatalagen, 2 kap. 15 § tullbrottsdatalagen och 2 kap. 14 § skattebrottsdatalagen föreskrivs att personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik. Eftersom regleringen är av generell natur håller regeringen med utredningen om att en bestämmelse om det i stället bör införas i ramlagen.

Kustbevakningen har i dag ingen skyldighet att lämna sådan statistik och det finns därför ingen bestämmelse om uppgiftslämnande till rättsstatistiken i kustbevakningsdatalagen. Det hindrar inte att regleringen placeras i ramlagen.

9 Personuppgiftsansvariga och personuppgiftsbiträden

9.1 Vad innebär personuppgiftsansvar?

9.1.1 Definition av personuppgiftsansvarig

Regeringens förslag: Personuppgiftsansvarig ska i ramlagen definieras som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Personuppgiftsansvar är ett centralt begrepp i dataskyddslagstiftningen. Utgångspunkten är att det alltid ska finnas någon som bär ansvaret för att dataskyddsreglerna följs vid behandling av personuppgifter och som den enskilde kan vända sig till för att göra sina rättigheter gällande. Den personuppgiftsansvarige har det ansvaret. Det är viktigt att det tydligt framgår vem som är personuppgiftsansvarig och därför bör det i ramlagen definieras vad som avses med det.

Personuppgiftsansvarig definieras i artikel 3.8 i direktivet som en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Definitionen i direktivet motsvarar den som finns i 3 § personuppgiftslagen (1998:204). Definitionen är väl inarbetad och bör därför användas även i ramlagen. Det bör dock framgå att endast behöriga myndigheter kan vara personuppgiftsansvariga. Personuppgiftsansvarig bör följaktligen definieras som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Av artikel 3.8 i direktivet följer även en möjlighet att i nationell rätt bestämma vem som är personuppgiftsansvarig för en viss behandling av personuppgifter. I de brottsbekämpande myndigheternas registerförfattningar anges i dag vem som är personuppgiftsansvarig för den aktuella verksamheten. Regeringen återkommer till hur detta ska regleras i samband med att registerförfattningarna anpassas till den nya ramlagen. När det gäller de verksamheter där endast ramlagen är tillämplig instämmer regeringen i utredningens bedömning att definitionen i ramlagen ger tillräcklig vägledning för vem som är personuppgiftsansvarig.

9.1.2 Personuppgiftsansvarets omfattning

Regeringens förslag: Den personuppgiftsansvarige ska vara ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Hovrätten för Västra Sverige* anser att bestämmelsen om personuppgiftsansvarigas allmänna ansvar knappast handlar om deras skyldigheter och därför bör flyttas till kapitel 1. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Av ramlagen ska det framgå vad den personuppgiftsansvarige är skyldig att göra i olika situationer, t.ex. samarbeta med tillsynsmyndigheten, vidta säkerhetsåtgärder och utse dataskyddsombud. Detta bör regleras i ett eget kapitel i lagen som även omfattar personuppgiftsbiträden och deras skyldigheter.

Enligt artikel 4.4 i direktivet ska den personuppgiftsansvarige inte bara ansvara för att personuppgiftsbehandlingen utförs på ett lagligt och korrekt sätt och i övrigt i enlighet med de grundläggande principer som gäller för behandlingen, utan även kunna visa att principerna efterlevs. Det bör i ramlagen klargöras hur långt personuppgiftsansvaret sträcker sig. I en sådan grundläggande bestämmelse bör den personuppgiftsansvariges helhetsansvar slås fast. I likhet med utredningen anser regeringen att den bestämmelsen bör placeras först i det kapitel som gäller personuppgiftsansvariga, personuppgiftsbiträden och deras skyldigheter.

Enligt skäl 50 i direktivet bör personuppgiftsansvariga åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. På så sätt kommer personuppgiftsansvaret att omfatta dels den personuppgiftsbehandling som förekommer vid den behöriga myn-

digheten, dels den personuppgiftsbehandling som ett personuppgiftsbiträde utför på den personuppgiftsansvariges vägnar.

Den personuppgiftsansvariges helhetsansvar får också betydelse för det skadeståndsrättsliga ansvaret och ansvaret för eventuella sanktionsavgifter. Regeringen återkommer till dessa frågor (se avsnitt 13.3.2 och 12.4).

Den omständigheten att det har utsetts ett dataskyddsombud påverkar inte personuppgiftsansvaret, eftersom ett dataskyddsombud inte har något ansvar för personuppgiftsbehandlingen (se avsnitt 9.5.3).

Enligt artikel 23 ska den som får tillgång till personuppgifter endast behandla dem enligt instruktion från den personuppgiftsansvarige. Varje medarbetare måste därför vid behandling av personuppgifter se till att regelverket för sådan behandling följs, men ansvaret för att medarbetarna får tillräckliga instruktioner och den utbildning som krävs vilar på den personuppgiftsansvarige.

9.2 Skyldigheten att säkerställa författningsenlig behandling

9.2.1 Tekniska och organisatoriska åtgärder

Regeringens förslag: Den personuppgiftsansvarige ska genom lämpliga tekniska och organisatoriska åtgärder säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

Den personuppgiftsansvarige ska också genom lämpliga tekniska och organisatoriska åtgärder se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd). I automatiserade behandlingssystem ska det som regel inte vara möjligt att behandla andra personuppgifter än de som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

Regeringens bedömning: Vilka omständigheter som ska beaktas när den personuppgiftsansvarige beslutar om tekniska och organisatoriska åtgärder kan regleras i förordning.

Att den personuppgiftsansvarige ska anta interna strategier för dataskydd kan också regleras i förordning.

Utredningens förslag överensstämmer i sak med regeringens förslag och bedömning.

Remissinstanserna: *Datainspektionen* invänder att artikel 20.2 i direktivet inte medger att kravet på dataskydd som standard begränsas till automatiserade behandlingssystem. Vidare anser inspektionen att uppräkningen i artikel 20.2 bör tas in i ramlagen. *Malmö kommun* anför att de utökade säkerhetskraven är betungande och ställer sig frågande till att de införs, särskilt när endast en begränsad del av myndighetens verksamhet omfattas av ramlagens tillämpningsområde. *Norrköpings kommun* framhåller att det med hänsyn till upphandlingsreglerna kan finnas praktiska svårigheter med att byta ut eller justera befintliga standardprogram inför ikraftträdandet av lagförslaget. *Polismyndigheten* anser att begreppet dataskydd som standard ingår i begreppet inbyggt dataskydd. Myndigheten anför vidare att begreppsbildningen bör ses över och göras

konsekvent i det fortsatta lagstiftningsarbetet. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 19.1 ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med direktivet. Åtgärderna ska vidtas med beaktande av behandlingens art, omfattning, sammanhang och ändamål och riskerna för fysiska personers rättigheter och friheter. Åtgärderna ska ses över och uppdateras vid behov. Enligt artikel 19.2 ska åtgärderna, om det står i proportion till behandlingen, omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

I artikel 20.1 regleras principen om inbyggt dataskydd. Inbyggt dataskydd innebär att den personuppgiftsansvarige, både vid beslut om vilka medel behandlingen ska utföras med och vid själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder som återspeglar dataskyddsprinciper och integrerar nödvändiga skyddsåtgärder i behandlingen. Åtgärderna ska vidtas med beaktande av den senaste utvecklingen, kostnader för genomförandet, behandlingens art, omfattning, sammanhang och ändamål och risken för fysiska personers rättigheter och friheter. Pseudonymisering anges som exempel på en åtgärd som bör vidtas och uppgiftsminimering som exempel på en dataskyddsprincip som bör genomföras.

I artikel 20.2 kommer principen om dataskydd som standard till uttryck. Enligt artikeln ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast de personuppgifter behandlas som är nödvändiga för varje specifikt ändamål med behandlingen. Skyldigheten avser mängden insamlade uppgifter, behandlingens omfattning, hur länge uppgifterna får lagras och uppgifternas tillgänglighet. Framför allt ska åtgärderna säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal andra personer.

Bestämmelserna om tekniska och organisatoriska åtgärder saknar motsvarighet i 1995 års dataskyddsdirektiv och i personuppgiftslagen. I 31 § personuppgiftslagen finns dock bestämmelser om säkerhetsåtgärder.

Lämpliga tekniska och organisatoriska åtgärder ska vidtas

Artikel 4.1 i direktivet innehåller allmänna och grundläggande principer för behandling av personuppgifter. Av artikel 4.4 framgår att den personuppgiftsansvarige ska ansvara för och kunna visa efterlevnaden av dessa grundläggande principer. Enligt artikel 19.1 är den personuppgiftsansvarige skyldig att vidta lämpliga åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med gällande rätt. Den artikeln tar sikte på de åtgärder som behövs för att bl.a. de grundläggande principerna om behandling av personuppgifter i artikel 4.1 ska kunna efterlevas.

Artikel 19.1 bör genomföras, men det är inte möjligt att i ramlagen ange vilka tekniska och organisatoriska åtgärder som den personupp-

giftsansvarige bör vidta. Det får avgöras i varje enskilt fall beroende på vilken verksamhet det rör sig om. Vilka omständigheter som den personuppgiftsansvarige ska beakta vid beslut om åtgärder kan regleras i förordning. Vilka tekniska och organisatoriska åtgärder som kan krävas varierar också beroende på vilka personuppgifter som ska behandlas. Det kan vara lämpligt att regeringen eller den myndighet som regeringen bestämmer vid behov utfärdar närmare riktlinjer på området.

Enligt artikel 19.1 ska den personuppgiftsansvarige inte bara säkerställa att behandlingen utförs författningsenligt utan också kunna visa att så är fallet. Det bör innebära att den personuppgiftsansvarige bl.a. ska se till att behandlingar och vidtagna åtgärder dokumenteras och att det är tekniskt möjligt att spåra behandlingar genom loggning och att loggningen följs upp. Den personuppgiftsansvariges generella ansvar att vidta åtgärder bör tydliggöras i en särskild bestämmelse.

Enligt artikel 19.2 ska den personuppgiftsansvarige, om det står i proportion till behandlingen, anta lämpliga strategier för dataskydd. I skäl 53 anges att det är interna strategier som avses. Eftersom både direktivet och dataskyddsförordningen använder termen strategier bör den användas i regleringen på nationell nivå.

Direktivet ger ingen vägledning i fråga om vad som krävs för att skyldigheten att anta strategier ska vara proportionerlig. Enligt utredningens mening bör i vart fall personuppgiftsansvariga under vars ansvar det dagligen behandlas en större mängd personuppgifter eller hanteras behandlingssystem av större omfattning åläggas att anta interna strategier för skydd av personuppgifter. Det omfattar merparten av de behöriga myndigheterna inom ramlagens tillämpningsområde. Om en myndighet endast i liten omfattning behandlar personuppgifter inom ramlagens tillämpningsområde finns det inte samma behov av sådana strategier. Mot den bakgrunden anser regeringen att alla personuppgiftsansvariga bör vara skyldiga att anta interna strategier för dataskydd, om det inte är uppenbart obehövligt med hänsyn till verksamhetens begränsade omfattning. En bestämmelse om det kan tas in i förordning.

Inbyggt dataskydd

Begreppet inbyggt dataskydd innebär att integritetsfrågor ska påverka itsystemen från förstudie och kravställning via design och utveckling till användning och avveckling. Genom krav på att integritetsfrågor ska beaktas under hela tidsperioden kan säkerheten i systemen höjas och författningsenlig och korrekt behandling underlättas. Artikel 20.1 bör mot den bakgrunden genomföras i ramlagen.

På samma sätt som när det gäller artikel 19.1 är det inte möjligt att i ramlagen ange vilka tekniska och organisatoriska åtgärder som den personuppgiftsansvarige bör vidta för att leva upp till principen om inbyggt dataskydd. Det får avgöras i varje enskilt fall beroende på vilken verksamhet det rör sig om och vilka personuppgifter som ska behandlas. Det handlar främst om åtgärder för att minimera mängden personuppgifter, begränsa åtkomsten till uppgifterna och på olika sätt skydda dem. Vilka omständigheter som ska beaktas vid beslut om sådana åtgärder kan regleras i förordning.

Begreppen inbyggt dataskydd och dataskydd som standard är svårtillgängliga, vilket *Polismyndighetens* remissynpunkt belyser. Regeringen har dock svårt att se att begreppen skulle bli enklare att förhålla sig till med en annan begreppsbildning än den som utredningen har använt och som utgår från direktivets lydelse. Regeringen använder därför begreppen på samma sätt som utredningen.

Dataskydd som standard kan, som utredningen angett, sägas innebära att arbetsflödena i ett system automatiskt ska styra användaren mot ett integritetssäkert arbetssätt och att grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas. Direktivet föreskriver att personuppgiftsansvariga ska vidta lämpliga åtgärder för att i standardfallet säkerställa att så sker. Ramlagen bör innehålla en bestämmelse om detta.

Regeringen instämmer i utredningens bedömning att skyldigheten bör gälla oavsett omständigheterna. Den personuppgiftsansvarige ska alltså säkerställa dataskydd som standard oavsett vilken behandling eller vilka personuppgifter det rör sig om och utan hänsyn till vad åtgärderna kostar. Dataskydd som standard bör i princip gälla i alla system där personuppgifter behandlas, men det måste finnas visst utrymme för avsteg från huvudregeln i de fall där den personuppgiftsansvarige inte har rätt att införa sådana åtgärder. Som exempel kan nämnas standardprogram som Word och Outlook, där användaren inte råder över de tekniska lösningarna. De behöriga myndigheterna måste dock kunna använda även sådana system. Mot den bakgrunden instämmer regeringen i utredningens bedömning att kravet på dataskydd som standard endast bör gälla i automatiserade behandlingssystem. En sådan ordning kan, till skillnad från vad *Datainspektionen* har anfört, inte anses vara oförenlig med direktivet. Vad som avses med automatiserade behandlingssystem behandlas i avsnitt 9.2.2.

Även om kravet på dataskydd som standard endast gäller i automatiserade behandlingssystem måste de behöriga myndigheterna säkerställa att även behandling i de standardprogram som används lever upp till de grundläggande kraven på behandling av personuppgifter.

I artikel 20.2 anges att den personuppgiftsansvariges skyldighet gäller mängden insamlade uppgifter, behandlingens omfattning, lagringstiden och uppgifternas tillgänglighet. Regleringen avser alltså inte enbart tillgången till personuppgifter i sig, utan åtgärder ska även vidtas för att säkerställa att inte fler personuppgifter än nödvändigt behandlas, att uppgifterna endast behandlas på ett sådant sätt och så länge som det är nödvändigt och uppgifterna inte görs tillgängliga för fler personer än vad som är nödvändigt. Datainspektionen anser att uppräkningen i artikel 20.2 bör tas in i ramlagen. Regeringen instämmer dock i utredningens bedömning en sådan uppräkning i lagen kan riskera att låsa myndigheterna vid viss utformning av automatiserade behandlingssystem. Direktivets uppräkning bör därför inte föras över till lagen.

9.2.2 Loggning

Regeringens förslag: Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning som det är särskilt föreskrivet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Domstolsverket* anser att det med utredningens förslag är svårt för en personuppgiftsansvarig att veta när skyldigheten att t.ex. föra loggar är uppfylld och menar att detta är särskilt allvarligt med hänsyn till risken för att drabbas av sanktionsavgift. *Säkerhetspolisen* anför att kraven på loggning är nya och kostnadsdrivande och att det därför finns ett stort behov av en övergångsbestämmelse avseende bestämmelserna om loggning. *Datainspektionen* avstyrker förslaget om att kravet på loggning ska begränsas till automatiserade behandlingssystem och anför att begränsningen riskerar att försämra skyddet för den enskildes personliga integritet i förhållande till nuvarande regelverk. Datainspektionen anser vidare att det bör författningsregleras hur loggarna får användas. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Artikel 25.1 föreskriver att loggar, dvs. dokumentation, ska föras över vissa typer av behandlingar i automatiserade behandlingssystem. Loggningen ska avse insamling, ändring, läsning, utlämning (inklusive överföringar), sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling, vem som har läst eller lämnat ut personuppgifter och vilka som har fått tillgång till dem. Av artikel 25.2 framgår att loggarna bara bör användas för att kontrollera om behandlingen är tillåten, för att säkerställa personuppgifternas integritet och säkerhet, för egenkontroll och för straffrättsliga förfaranden. Här avses med att säkerställa personuppgifternas integritet att de ska skyddas mot förvanskning eller förändring. Loggarna ska, enligt artikel 25.3, på begäran göras tillgängliga för tillsynsmyndigheten. Bestämmelsen riktar sig även till personuppgiftsbiträden.

Som tidigare nämnts ställs krav på säkerhetsåtgärder i 31 § personuppgiftslagen. De anses även omfatta loggning och liknande åtgärder. Av Datainspektionens allmänna råd om säkerhet för personuppgifter framgår att det, beroende på känsligheten hos personuppgifterna, bör finnas en behandlingshistorik (logg) som sparas viss tid så att åtkomsten till uppgifterna kan kontrolleras. Enligt råden bör en behandlingshistorik normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Historiken bör, beroende på hur känsliga personuppgifterna är, ange t.ex. läsning, ändring, utplåning eller kopiering av personuppgifter (Säkerhet för personuppgifter, Datainspektionens allmänna råd, november 2008, s. 22). Bestämmelser om loggning kan även finnas i myndighetsföreskrifter.

Loggning är en säkerhetsåtgärd som innebär att behandlingshistorik sparas under en viss tid. Det är en teknisk funktion i systemet som fungerar automatiskt och som inte går att ändra eller påverka på annat sätt. Loggning fyller flera olika funktioner. Den ger den personuppgiftsansvarige information både om hur behandlingssystemen används och om externa och interna angrepp mot systemen. Loggning är således mycket viktig för det interna säkerhetsarbetet. Den ger också tillsynsmyndigheten nödvändig information för granskning i efterhand av hur personuppgifter har behandlats. Det bör finnas en bestämmelse i ramlagen som slår fast att det krävs loggning. I vilken utsträckning som loggning bör göras kan regleras i förordning.

Direktivet föreskriver att loggar ska föras över behandlingar i automatiserade behandlingssystem men uttrycket definieras inte. Det används endast i artikel 25.1 som handlar om loggning och i artikel 29.2 som räknar upp olika säkerhetsåtgärder. I den sistnämnda artikeln används uttrycket i samband med behörig åtkomst till automatiserade behandlingssystem och loggning av aktivitet i sådana system. Att uttrycket ”automatiserade behandlingssystem” bara används i dessa sammanhang talar för att det är en viss typ av system som avses och således inte it-system generellt. Den tolkningen framstår också som mest rimlig med tanke på vilka krav som ställs på loggning. Ser man till syftet med loggningen framstår behovet av den som störst vid användning av verksamhetsspecifika behandlingssystem.

Loggar bör alltså föras i automatiserade behandlingssystem. Regeringen anser i likhet med utredningen att automatiserade behandlingssystem i detta sammanhang bör avse för verksamheten särskilt utformade eller anpassade behandlingssystem där personuppgifter behandlas mer eller mindre strukturerat, t.ex. verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. Däremot bör standardprogram som Word, Outlook och Excel, av samma skäl som anges när det gäller dataskydd som standard, inte omfattas av de i direktivet preciserade kraven på loggning. Olika lagringsytor, som t.ex. usb-minnen och anställdas personliga mappar på den egna datorn, bör också undantas från de kraven. Personuppgiftsregleringen i övrigt gäller däremot för behandling som utförs i sådan programvara och på sådana lagringsytor även om de inte omfattas av de preciserade kraven på loggning. De närmare detaljerna kan regleras på lägre normgivningsnivå.

Förslaget att de mer preciserade kraven på loggning i direktivet ska begränsas till automatiserade behandlingssystem ska inte uppfattas som att kraven på annan behandling av personuppgifter i sådana system är lägre än vad som gäller för behandling i andra system.

Loggning är ett viktigt inslag i det övergripande kravet på att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna, vilket innebär att loggning kan krävas även i andra fall. Vilka uppgifter som kan behöva loggas kan dock variera. Det kan t.ex. vara viktigare med loggning i system som ett flertal personer använder än i system som enbart ett fåtal har tillgång till. Mot bakgrund av att alla de detaljkrav på loggning som direktivet ställer upp inte alltid är möjliga att leva upp till i alla system, bör regleringen i ram-

lagen begränsas till vad som krävs enligt direktivet. Som utredningen konstaterar riskerar respekten för regleringen att urholkas om det ställs detaljkrav som den personuppgiftsansvarige inte kan leva upp till.

Även om ramlagens krav på loggning inte gäller i andra system än automatiserade behandlingssystem bör de personuppgiftsansvariga när det är tekniskt möjligt ha loggning även i sådana system. Loggning krävs normalt även där för att ge tillräckligt underlag för intern kontroll. Dessutom måste personuppgiftsansvariga se till att behandling av integritetskänsliga personuppgifter inte utförs vid sidan av automatiserade behandlingssystem i syfte att kringgå ramlagens krav. Tillsynsmyndigheten bör också i enskilda fall kunna ställa krav på loggning om det är en skydds- eller säkerhetsåtgärd som är nödvändig för att behandlingen ska omgärdas med tillräckligt skydd.

Sammanfattningsvis anser regeringen, trots att *Datainspektionen* har avstyrkt förslaget, att kravet på loggning ska begränsas till automatiserade behandlingssystem.

Det kommer att behövas tid för myndigheterna att göra de verksamhets- och systemanalyser som krävs för att klarlägga i vilken utsträckning dagens system för loggning uppfyller regleringen och vilka eventuella förändringar som kan behövas. Som *Säkerhetspolisen* anför kan de nya kraven också komma att bli kostnadsdrivande. I avsnitt 17.2.3 redogör regeringen för behovet av övergångsbestämmelser, bl.a. när det gäller bestämmelserna om loggning i automatiserade behandlingssystem.

Vad ska loggas?

Loggar bör föras över de typer av behandlingar som anges i artikel 25.1. Därutöver bör även överföringar till tredjeland eller internationella organisationer loggas.

En behandlingshistorik bör normalt vara utformad så att den avslöjar felaktig eller obehörig användning av personuppgifter. När det gäller läsning och utlämning av personuppgifter ska enligt direktivet loggarna göra det möjligt att få fram viss typ av information. Eftersom loggning är ett automatiskt förfarande kan endast viss information om behandlingen dokumenteras. Det rör sig främst om datum och tidpunkt för behandlingen. Information om vem som har behandlat personuppgiften går också att få fram om de anställda har tilldelats behörigheter och det krävs inloggning i systemen. När det gäller utlämnande av uppgifter kan identiteten på den som har lämnat ut uppgifterna endast fastställas om de lämnats ut elektroniskt via systemet. Detsamma gäller överföringar till tredjeland eller internationella organisationer. Det bör dock vara möjligt att logga om en medarbetare har överfört, laddat ner eller skrivit ut uppgifter. Det är däremot inte möjligt att logga om uppgifterna sedan lämnas ut på annat sätt än elektroniskt, t.ex. muntligen eller på papper. Det kan också vara svårt att logga om uppgifterna lämnas ut via e-post.

Loggarna över läsning och utlämning ska enligt direktivet göra det möjligt att fastställa motiveringen för behandlingen. I skäl 57 anges att identiteten på den person som läst eller lämnat ut uppgifter bör loggas och från den identifieringen skulle det kunna vara möjligt att fastställa motiveringen till behandlingen. Skälen till att någon i ett visst fall tar del av eller lämnar ut en viss personuppgift kan dock knappast fastställas

automatiskt genom loggning. En skyldighet att automatiskt logga motiveringen till varför personuppgifter behandlas bör därför inte införas.

I artikel 25 anges att loggarna över läsning och utlämning även ska visa vilka som har fått tillgång till personuppgifterna. Kravet skulle kunna avse både intern och extern tillgång. Det som avses här torde dock framför allt vara de personer eller myndigheter till vilka uppgifterna har lämnats ut. Sådan information kan bara loggas om utlämnandet görs elektroniskt via systemet. Det kan t.ex. göras om någon har direktåtkomst till vissa uppgifter i ett system eller om uppgifter överförs elektroniskt efter förfrågan. Den utlämnande myndigheten bör genom loggning kunna fastställa vilken annan myndighet som har fått tillgång till viss information, men knappast få fram information om vilken medarbetare hos den andra myndigheten som har tagit del av informationen. Sådan information bör dock finnas hos mottagaren, om detta är en behörig myndighet. Detta bör vara tillräckligt för att uppfylla kraven i direktivet. *Domstolsverket* anser att det är svårt att veta när skyldigheten att föra loggar är uppfylld. Vad som ska loggas bör regleras i förordning eller genom föreskrifter på lägre normgivningsnivå eftersom behov, arbetssätt och tekniska möjligheter att logga varierar. Genom införandet av sådana föreskrifter bör tillräcklig vägledning vad gäller skyldigheten att föra loggar finnas.

Hur ska loggarna användas?

De flesta behöriga myndigheter för redan i dag loggar som en del av informationssäkerhetsarbetet. Tanken är inte att de behöriga myndigheterna ska åläggas att föra ytterligare en logg enbart för personuppgiftsbehandlingen. De system för loggning som i dag används främst i informationssäkerhetssyfte bör normalt kunna användas även för kontroll ur ett integritetsskyddsperspektiv. Av artikel 25.2 framgår att loggar endast får användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet och för straffrättsliga förfaranden. Det innebär att loggarna bara får användas i informationssäkerhetssyfte.

Syftet med loggning är att åtkomsten till personuppgifterna ska kunna kontrolleras, bl.a. för att göra det möjligt att utreda felaktig eller obehörig användning av uppgifterna. För att det ska kunna göras måste loggarna sparas en viss tid. Loggning kan också ha en förebyggande funktion. Det förutsätter att användarna informeras om att det förs loggar och att de kontrolleras. Loggningen bör alltså följas upp och loggarna skyddas mot otillåtna ändringar.

Det är viktigt att skilja mellan själva loggningen och uppföljning av loggningen. Logguppföljning bör göras systematiskt och återkommande i syfte att upptäcka och motverka obehörig åtkomst. Uppföljning bör också göras vid misstanke om att någon obehörigen tagit del av personuppgifter. Det kan vidare finnas anledning att följa upp behandlingshistoriken t.ex. på områden där det finns särskilt integritetskänsliga personuppgifter eller behörigheter som ger stora möjligheter till åtkomst. Det kan också finnas skäl att kontrollera vissa inloggningsmönster. Myndigheterna bör ha rutiner för logguppföljningen. Den personuppgiftsansvarige bör exempelvis ge riktlinjer och vägledning till den som kontrollerar

loggarna beträffande vad som kan vara obehörig åtkomst. Vid logguppföljning måste också reglerna om meddelarfrihet och efterforskningsförbud i tryckfrihetsförordningen och yttrandefrihetsgrundlagen beaktas, vilket innebär att möjligheten till uppföljning i vissa fall begränsas eller kan vara otillåten.

Det är av största vikt att loggningssystem inte missbrukas eller används för andra syften än som varit avsett. I likhet med utredningen anser dock regeringen att det inte bör författningsregleras hur loggarna får användas, eftersom detta skulle riskera att låsa fast myndigheterna vid ett visst arbetssätt eller omöjliggöra användning som kan visa sig vara nödvändig. Detta innebär inte att användningen av loggar bör vara helt oreglerad. Utöver myndigheternas interna föreskrifter och riktlinjer får tillsynsmyndigheten ge vägledning för användningen av loggar, t.ex. genom allmänna råd och riktlinjer.

Loggarna utgör sådan dokumentation som tillsynsmyndigheten har rätt att på begäran få del av. Någon särskild bestämmelse som föreskriver att loggarna ska göras tillgängliga för tillsynsmyndigheten behövs därför inte.

9.2.3 Tillgången till personuppgifter

Regeringens förslag: Den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Nuvarande reglering

I de flesta registerförfattningar inom ramlagens tillämpningsområde finns det bestämmelser som begränsar medarbetarnas tillgång till personuppgifter. Så är fallet i exempelvis 2 kap. 11 § polisdatalagen (2010:361), 2 kap. 9 § åklagardatalagen (2015:433) och 8 § domstolsdatalagen (2015:728). Av paragraferna framgår att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Tillgången till personuppgifter ska begränsas

I artikel 4.1 c, som anger de grundläggande principerna för behandling, föreskrivs att personuppgifter inte får vara för omfattande i förhållande till de syften för vilka de behandlas. Av artikel 29.2 e, som behandlar säkerhetsåtgärder, framgår att den personuppgiftsansvarige eller personuppgiftsbiträdet ska säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet. Frågan är om det i ramlagen bör tas in en generell bestämmelse om tillgången till personuppgifter.

När stora informationsmängder är samlade på ett sådant sätt att integritetskänsliga personuppgifter är enkelt sökbara på elektronisk väg finns

det uppenbara risker för intrång i den personliga integriteten. I förarbetena till flera av registerförfattningarna påtalas vikten av att det säkerställs att integritetskänsliga personuppgifter görs tillgängliga bara för dem som behöver uppgifterna för sitt arbete. Vem som har rätt att använda personuppgifterna och hur uppgifterna sprids är omständigheter som påverkar risken för intrång i den personliga integriteten (se bl.a. prop. 2009/10:85 s. 94 och prop. 2011/12:45 s. 87 f.). I förarbetena till åklagardatalagen konstateras att det är en hörnsten i skyddet av enskildas integritet att åtkomst endast medges till de personuppgifter som den enskilde tjänstemannen behöver för att kunna utföra sina arbetsuppgifter (prop. 2014/15:63 s. 59).

Ju fler personer i en myndighet som har tillgång till personuppgifter, desto större är risken för obehörig åtkomst eller spridning av uppgifterna. Att utbilda användarna i informationssäkerhets- och dataskyddsfrågor är en viktig organisatorisk säkerhetsåtgärd, men det är ofta inte tillräckligt. Att tillgången till personuppgifter i så stor utsträckning som möjligt faktiskt begränsas till vad var och en behöver för att utföra sitt arbete är viktigt för att skapa ett tillfredsställande internt skydd för personuppgifter vid myndigheters informationshantering.

Mot den bakgrunden finns det ett generellt behov av att begränsa tillgången till personuppgifter. En bestämmelse om detta bör därför tas in i ramlagen. Den personuppgiftsansvarige ska alltid vara skyldig att pröva anställdas och uppdragstagares behov av tillgång till personuppgifter utifrån vad arbetsuppgifterna kräver och begränsa tillgången i enlighet med det. Bestämmelsen bör gälla personuppgifter i både den behöriga myndighetens egna system och system som myndigheten får tillgång till genom direktåtkomst eller andra former av informationsutbyte.

Eftersom bestämmelsen bör vara generell kan det finnas behov av närmare riktlinjer för hur tillgången till personuppgifter bör avgränsas för de enskilda tjänstemännen. Det kan regleras i myndigheternas registerförfattningar eller i föreskrifter på myndighetsnivå. Det kan också regleras i interna styrdokument hos den behöriga myndigheten.

9.2.4 Konsekvensbedömning

Regeringens förslag: Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska den personuppgiftsansvarige innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Regeringens bedömning: Vad en konsekvensbedömning ska innehålla och kraven i övrigt på bedömningen kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna yttrar sig inte särskilt i dessa delar.

Skälen för regeringens förslag och bedömning: I artikel 27.1 i direktivet föreskrivs att den personuppgiftsansvarige i vissa fall ska göra en bedömning av konsekvenserna för skyddet av personuppgifter när det

gäller planerad personuppgiftsbehandling. En konsekvensbedömning ska göras om en typ av behandling, särskilt med användning av ny teknik och med beaktande av behandlingens art, omfattning, sammanhang och ändamål, sannolikt leder till hög risk för fysiska personers rättigheter och friheter. Enligt artikel 27.2 ska en konsekvensbedömning innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter och uppgift om dels vilka åtgärder som planeras för att hantera dessa risker, dels skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att direktivet efterlevs.

Det behövs en bestämmelse i ramlagen som reglerar personuppgiftsansvarigas skyldighet att göra konsekvensbedömningar. En konsekvensbedömning bör göras om det kan antas att en ny typ av behandling kommer att medföra särskild risk för intrång i registrerades personliga integritet. En konsekvensbedömning bör också göras om betydande förändringar av redan pågående behandlingar förväntas leda till sådan risk. Det framgår av artikel 27.1 vilka omständigheter som särskilt ska beaktas vid bedömningen av risken.

I skäl 58 anges att konsekvensbedömningarna bör omfatta relevanta system och processer för behandlingen men inte enskilda fall. Det tydliggörs i artikeln genom att det ska röra sig om en typ av behandling. Samma uttryck bör, som utredningen föreslår, användas i ramlagen.

Konsekvensbedömningen ska innehålla viss i direktivet angiven information. Det följer indirekt av det kravet att konsekvensbedömningen ska dokumenteras, exempelvis i en skriftlig rapport. Det bör regleras vilken information konsekvensbedömningen ska innehålla och att den ska dokumenteras, men detta kan göras i förordning.

Det finns inte något som hindrar att personuppgiftsansvariga gör konsekvensbedömningar även i andra fall, t.ex. om en typ av behandling förväntas leda till risk för intrång i registrerades personliga integritet men risken inte är så påtaglig att en konsekvensbedömning krävs enligt lagen. Sådana konsekvensbedömningar kan vara nödvändiga vid bedömningar av bl.a. vilka säkerhets- och skyddsåtgärder som krävs.

9.2.5 Förhandssamråd med tillsynsmyndigheten

Regeringens förslag: Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (förhandssamråd).

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser, med hänvisning till uttalanden på dataskyddsförordningens område från den s.k. artikel 29-gruppen, att den personuppgiftsansvarige inte bör vara skyldig att samråda med tillsynsmyndigheten om åtgärder har vidtagits för att minska risken för intrång i den registrerades personliga integritet i tillräcklig omfattning.

Innehållet i direktivet

I artikel 28.1 föreskrivs att den personuppgiftsansvarige eller personuppgiftsbiträdet under vissa förutsättningar ska samråda med tillsynsmyndigheten inför behandling av personuppgifter som kommer att ingå i ett nytt register, s.k. förhandssamråd. Sådant samråd ska bl.a. äga rum om en konsekvensbedömning visar att behandlingen skulle leda till hög risk för de registrerades rättigheter och friheter om den personuppgiftsansvarige inte vidtar åtgärder för att minska risken.

Tillsynsmyndigheten får enligt artikel 28.3 upprätta en förteckning över vilka typer av behandlingar som kräver förhandssamråd. Den personuppgiftsansvarige ska enligt artikel 28.4 lämna in konsekvensbedömningen till tillsynsmyndigheten tillsammans med eventuell övrig information som myndigheten behöver för att kunna bedöma behandlingen.

I artikel 28.5 regleras förfarandet hos tillsynsmyndigheten. Myndigheten ska, om den anser att den planerade behandlingen inte är förenlig med direktivet, inom viss tid lämna skriftliga råd till den personuppgiftsansvarige eller personuppgiftsbiträdet. Tillsynsmyndigheten får då utnyttja alla de befogenheter som den har.

Nuvarande reglering

Enligt artikel 20 i 1995 års dataskyddsdirektiv ska medlemsstaterna bestämma vilka behandlingar som kan innebära särskilda risker för de registrerades fri- och rättigheter och säkerställa att dessa kontrolleras innan de påbörjas. Sådana förhandskontroller ska utföras av tillsynsmyndigheten efter anmälan från den personuppgiftsansvarige. Artikeln har genomförts i 41 § personuppgiftslagen. Där föreskrivs att regeringen får meddela föreskrifter om att sådana behandlingar som innebär särskilda risker för intrång i den personliga integriteten ska anmälas till tillsynsmyndigheten för förhandskontroll.

I 2 § polisdataförordningen (2010:1155) regleras när Polismyndigheten och Säkerhetspolisen ska samråda med Datainspektionen. Sådant samråd ska äga rum när myndigheterna planerar nya it-system av större omfattning eller nya it-system som kan innebära särskilda risker för intrång i den personliga integriteten och när det genomförs betydande förändringar i sådana system. Samråd ska äga rum i god tid innan beslut i frågan fattas. Paragrafen föreskriver även samråd med Säkerhets- och integritetsskyddsnämnden i vissa frågor. En likadan bestämmelse om samråd med Datainspektionen finns i 2 § kustbevakningsdataförordningen (2012:146).

En generell samrådsskyldighet för alla personuppgiftsansvariga

Enligt direktivet ska den personuppgiftsansvarige vara skyldig att samråda med tillsynsmyndigheten vid planering av behandling av personuppgifter i ett nytt register på ett sätt som kan leda till hög risk för intrång i registrerades personliga integritet. Samråd ska äga rum om en konsekvensbedömning visar att behandlingen kommer att medföra sådan risk om åtgärder inte vidtas för att minska risken eller om typen av behand-

ling i sig kan anses innebära sådan risk. Vid bedömningen ska särskilt användandet av ny teknik, nya rutiner eller nya förfaranden beaktas.

Samrådsskyldigheten enligt artikel 28.1 ska gälla för alla personuppgiftsansvariga. Det bör därför i ramlagen tas in en bestämmelse som riktar sig till de personuppgiftsansvariga och som ålägger dem skyldighet att samråda med tillsynsmyndigheten i vissa situationer. Personuppgiftsbiträdens skyldigheter vid förhandssamråd behandlas i avsnitt 9.6.5.

I direktivet krävs det bara konsekvensbedömning och samråd inför helt nya former av behandling. Det måste dock anses vara lika viktigt med samråd inför betydande förändringar av redan pågående behandlingar som kan antas medföra särskild risk för intrång i den personliga integriteten. Skyldigheten att upprätta konsekvensbedömningar bör därför även omfatta den situationen (se avsnitt 9.2.4). Motsvarande bör gälla för samrådsskyldigheten. För att underlätta för den personuppgiftsansvarige och för att säkerställa att förhandssamrådet träffar rätt situationer bör tillsynsmyndigheten genom föreskrifter kunna ange vilka typer av behandlingar som ska omfattas av förhandssamråd.

Samråd blir främst aktuellt när den personuppgiftsansvarige har gjort en konsekvensbedömning som visar att behandlingen innebär en särskild risk för intrång i registrerades personliga integritet. Vid samrådet bör den personuppgiftsansvarige redovisa vilka åtgärder som planeras för att minska risken. *Datainspektionen* anser att samråd inte ska behöva hållas när den personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att minska risken för intrång. Som utredningen påpekar kan det vara svårt för den personuppgiftsansvarige att på egen hand avgöra vilka åtgärder som är tillräckliga. Regeringen utesluter dock inte att vidtagna åtgärder från den personuppgiftsansvariges sida kan befria från samrådsskyldigheten. I vilken utsträckning samråd inte bör krävas för att den personuppgiftsansvarige har vidtagit åtgärder som minskat risken för intrång till en godtagbar nivå, bör överlämnas åt rättstillämpningen att avgöra.

Samråd aktualiseras också om typen av behandling, särskilt med beaktande av ny teknik, nya rutiner eller nya förfaranden, i sig innebär särskild risk för intrång i registrerades personliga integritet och en konsekvensbedömning med anledning av det har gjorts. I sådana fall är resultatet av konsekvensbedömningen inte avgörande för om samråd med tillsynsmyndigheten ska äga rum.

Det är viktigt att samrådet äger rum så tidigt i utvecklingsprocessen som möjligt. Då kan frågor om integritetsskydd beaktas på ett bättre sätt. Samtidigt bör förhandssamrådet inte äga rum så tidigt att det inte finns något konkret förslag på teknisk lösning för tillsynsmyndigheten att ta ställning till. Samrådet bör äga rum i god tid innan behandlingen påbörjas eller större förändringar av redan pågående behandlingar genomförs.

Vid förhandssamråd bör den personuppgiftsansvarige lämna in konsekvensbedömningen och eventuell annan information som tillsynsmyndigheten kan behöva för sin prövning.

Tillsynsmyndighetens befogenheter

Enligt artikel 28.5 ska tillsynsmyndigheten inom ramen för förhandssamrådet använda sina befogenheter, om den anser att den planerade behandlingen inte är författningsenlig. Tillsynsmyndigheten bör i dessa situatio-

ner ha möjlighet att använda sina förebyggande befogenheter gentemot den personuppgiftsansvarige. Myndigheten ska inom ramen för förhandssamrådet ge den personuppgiftsansvarige skriftliga råd. Myndigheten har också möjlighet att utfärda varning för att behandla personuppgifterna på det planerade sättet (se avsnitt 11.7.5). Om den personuppgiftsansvarige ignorerar råden och varningen och påbörjar behandlingen kan tillsynsmyndigheten vidta andra åtgärder, t.ex. utfärda ett föreläggande eller besluta om sanktionsavgift (se avsnitt 11.7.6 och 12.5.2). Korrigerande åtgärder ska dock inte vidtas inom ramen för förhandssamrådet utan är i stället ett led i tillsynsmyndighetens allmänna tillsynsuppgifter enligt ramlagen.

Direktivet innehåller vissa detaljbestämmelser om tillsynsmyndighetens roll vid förhandssamråd. De skriftiga råden till den personuppgiftsansvarige ska lämnas inom sex veckor från det att begäran om samråd mottogs. Tiden får förlängas med en månad om den planerade behandlingen är komplicerad. I så fall ska tillsynsmyndigheten inom en månad från det att begäran om samråd mottogs informera den personuppgiftsansvarige om förlängningen och om orsakerna till den. Detaljerna kring detta kan regleras i förordning.

9.2.6 Samarbete med tillsynsmyndigheten

Regeringens förslag: Den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför sina uppgifter enligt ramlagen och föreskrifter som har meddelats i anslutning till lagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna har inte något att invända mot förslaget.

Skälen för regeringens förslag: Enligt artikel 26 ska den personuppgiftsansvarige på begäran samarbeta med tillsynsmyndigheten när den utför sina uppgifter. Personuppgiftsbiträden har samma skyldighet (se avsnitt 9.6.5). Det finns i dag ingen uttrycklig regel om personuppgiftsansvarigas samarbete med tillsynsmyndigheten.

Direktivets krav på samarbete med tillsynsmyndigheten måste anses gå utöver det som ryms i den allmänna samverkansskyldigheten enligt förvaltningslagen. Regleringen av tillsynsmyndighetens undersökningsbefogenheter täcker inte heller helt den samarbetsskyldighet som krävs enligt direktivet. Samarbetsskyldigheten innebär inte bara att den personuppgiftsansvarige ska ge tillsynsmyndigheten tillgång till det material och de resurser som den har rätt till. Bestämmelsen innebär även att den personuppgiftsansvarige ska underlätta för tillsynsmyndigheten att utöva sina tillsynsbefogenheter på ett effektivt sätt.

Som framgår av avsnitt 11.7.3 får tillsynsmyndigheten inte använda tvång mot den personuppgiftsansvarige för att kunna utöva sin tillsyn. Även mot den bakgrunden är det viktigt att den personuppgiftsansvarige ges en uttrycklig skyldighet att samarbeta med tillsynsmyndigheten. Det bör därför tas in en bestämmelse i ramlagen som slår fast att den personuppgiftsansvarige är skyldig att samarbeta med tillsynsmyndigheten.

Samarbetsskyldigheten aktualiseras när tillsynsmyndigheten utför sina uppgifter enligt ramlagen och de föreskrifter som utfärdas i anslutning

till den. Den personuppgiftsansvarige ska alltså vara skyldig att samarbeta med tillsynsmyndigheten när den utövar allmän tillsyn över personuppgiftsbehandling, handlägger klagomål från registrerade, på begäran kontrollerar om personuppgifter behandlas författningsenligt, vidtar åtgärder för att bistå en tillsynsmyndighet i en annan medlemsstat och ger råd inom ramen för bl.a. förhandssamråd.

Vad samarbetsskyldigheten mer konkret kommer att innebära för den personuppgiftsansvarige hör samman med vilka befogenheter som tillsynsmyndigheten ges. Den frågan behandlas i avsnitt 11.7.

9.2.7 Skyldighet att förteckna behandlingar

Regeringens bedömning: Den personuppgiftsansvariges skyldighet att förteckna de kategorier av behandlingar som denne ansvarar för får regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

Enligt artikel 24.1 ska personuppgiftsansvariga föra register över alla kategorier av verksamheter i samband med behandling som de ansvarar för. I artikeln anges i detalj vilka uppgifter som registret ska innehålla. I artikel 24.2 föreskrivs motsvarande skyldighet för personuppgiftsbiträden (se avsnitt 9.6.4).

Registren ska enligt artikel 24.3 upprättas skriftligen, vilket även innefattar elektronisk form, och på begäran göras tillgängliga för tillsynsmyndigheten.

Nuvarande reglering

Personuppgiftsansvariga har i dag ingen skyldighet att föra register över de behandlingar som de ansvarar för. I stället är de enligt artikel 18.1 i 1995 års dataskyddsdirektiv skyldiga att anmäla behandling av personuppgifter som är helt eller delvis automatiserad till tillsynsmyndigheten. Tillsynsmyndigheten ska enligt artikel 21.2 föra ett register över de behandlingar som har anmälts till myndigheten. Enligt artikel 18.2 behöver dock någon anmälan till tillsynsmyndigheten inte göras om den personuppgiftsansvarige utser ett personuppgiftsombud, som bl.a. ska ha till uppgift att föra register över de behandlingar som utförs av den personuppgiftsansvarige. Artiklarna har genomförts i 36, 37 och 39 §§ personuppgiftslagen och i 3–7 §§ personuppgiftsförordningen (1998:1191). Anmälningsskyldigheten regleras i 36 § första stycket personuppgiftslagen. Av 7 § personuppgiftsförordningen framgår att Datainspektionen ska föra register över de behandlingar av personuppgifter som anmälts till inspektionen.

Myndigheterna i rättskedjan är dock inte anmälningsskyldiga enligt 36 § personuppgiftslagen. Enligt 3 § 3 personuppgiftsförordningen gäller undantag från anmälningsskyldigheten bl.a. för behandling av person-

uppgifter som regleras genom särskilda föreskrifter i lag eller förordning. Myndigheternas registerförfattningar är sådana särskilda föreskrifter. Datainspektionen för således inget register över dessa behandlingar.

För några av myndigheterna föreskrivs att ett personuppgiftsombud ska utses och, genom hänvisning till 39 § personuppgiftslagen, att ombudet ska föra en förteckning över de behandlingar som utförs (se exempelvis 2 kap. 2 § 9 och 5 § polisdatalagen och 2 kap. 2 § 9 och 4 § åklagardatalagen). Detsamma gäller för domstolarna, men ombudets skyldighet att föra en förteckning över behandlingarna regleras i 11 § domstolsdatalagen.

En dokumentationsskyldighet införs

I direktivet läggs uppgiften att föra register över de behandlingar som utförs på de personuppgiftsansvariga och, i tillämpliga fall, personuppgiftsbiträdena (se avsnitt 9.6.4 om personuppgiftsbiträden).

Av skäl 56 framgår att de personuppgiftsansvariga bör föra register för att visa att behandlingen sker i överensstämmelse med direktivet och att dessa register bör tjäna som grund för övervakningen av behandlingen. Ett av syftena med dokumentationen är alltså att underlätta tillsynsmyndighetens kontroll, men även att underlätta intern kontroll och granskning av den personuppgiftsbehandling som utförs. Dokumentationen bör också kunna vara till hjälp när information ska lämnas till registrerade. Det behövs en bestämmelse som reglerar skyldigheten att dokumentera behandlingen men den kan tas in i förordning.

Av artikel 24 framgår att personuppgiftsansvariga och personuppgiftsbiträden ska föra register över de kategorier av behandling som de ansvarar för. Vad som avses med kategorier av behandling framgår inte. Begreppet bör dock inte tolkas så att alla typer av behandlingar som förekommer ska dokumenteras. En sådan tolkning skulle leda till en alltför omfattande dokumentationsskyldighet. En kategori av behandlingar kan i stället vara behandling av personuppgifter i ett specifikt register eller inom ramen för ett särskilt projekt eller behandling av personuppgifter för en typ av ändamål, t.ex. registrering av brottsanmälningar och handläggning av brottmål.

Vad ska dokumenteras?

I artikel 24.1 räknas det upp vilka uppgifter som ska anges i registret. Registret bör innehålla samtliga dessa uppgifter, vilket kan regleras i förordning.

Tillsynsmyndigheten föreslås på begäran få upplysningar om och dokumentation av behandling av personuppgifter från den personuppgiftsansvarige (se avsnitt 11.7.3). Det register över behandlingar som den personuppgiftsansvarige ska föra utgör sådan dokumentation. Någon särskild bestämmelse om att registret ska göras tillgänglig för tillsynsmyndigheten behövs därför inte.

9.2.8 Anmälan av överträdelser

Regeringens bedömning: Att den personuppgiftsansvarige ska ha interna rutiner för anmälan av överträdelser av bestämmelserna om behandling av personuppgifter, får regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.

Remissinstanserna: *Norrköpings kommun* anför att offentliga myndigheter inte kan garantera fullständig anonymitet för enskilda som lämnar in handlingar där den enskildes identitet går att utläsa.

Skälen för regeringens bedömning: Enligt artikel 48 ska behöriga myndigheter inrätta effektiva mekanismer för att uppmuntra konfidentiell rapportering av överträdelser av bestämmelserna som genomför direktivet. Någon motsvarande reglering finns inte i dag.

Regeringen anser i likhet med utredningen att bestämmelsen får uppfattas som ett krav på att behöriga myndigheter ska ha en särskild ordning för interna anmälningar av överträdelser av bestämmelser om personuppgiftsbehandling. Detta kan regleras i förordning.

Som utvecklas i avsnitt 9.5.3 ingår det i dataskyddsombudens arbetsuppgifter att övervaka efterlevnaden av tillämpliga dataskyddsbestämmelser. I det ingår att genomföra de granskningar som behövs för myndighetens interna kontroll. Det är därför naturligt att låta dataskyddsombuden ta emot interna anmälningar om överträdelser och avgöra om de bör bli föremål för kontroll. Dataskyddsombud har som regel tillgång till de flesta behandlingssystem och personuppgifter. Ombuden bör också ha den kunskap som krävs för att utreda en eventuell överträdelse och kunna bedöma vad en anmälan bör leda till. Det kan t.ex. vara en rekommendation till den personuppgiftsansvarige att vidta åtgärder eller att dataskyddsombudet själv anmäler överträdelsen till tillsynsmyndigheten, om den negligeras av den personuppgiftsansvarige.

Det kan inte uteslutas att anställda i vissa fall avhåller sig från att anmäla iakttagelser om överträdelser på grund av rädsla för repressalier från kollegor, chefer eller arbetsgivaren. Kravet på konfidentiell rapportering innebär enligt utredningens mening att den interna ordningen ska skydda anmälaren. Till skillnad från vad som kan vara fallet vid anmälningar om allvarliga missförhållanden av annat slag i verksamheten, bör det underlag som krävs för utredningen av överträdelsen i princip finnas i behandlingssystemen. En anmälan torde därför kunna göras anonymt utan att det äventyrar möjligheterna att utreda frågan.

Direktivet ställer inte upp några krav på hur anmälan ska göras. Ordningen kan därmed bestå av allt från en enkel manuell brevlådefunktion till ett avancerat systemstöd. Enligt utredningens mening bör det överlämnas till de behöriga myndigheterna att bestämma hur anmälan om överträdelser av bestämmelser om personuppgiftsbehandling bör göras. Det måste dock säkerställas att anmälan kan göras på ett sådant sätt att anmälarens identitet inte avslöjas. Eftersom det är fråga om interna anmälningar och inte ingivande av handlingar som därmed blir allmänna handlingar bör det inte, som *Norrköpings kommun* anför, vara omöjligt att garantera enskildas anonymitet.

9.3 Säkerheten för personuppgifter

Regeringens förslag: Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Regeringens bedömning: Vilka omständigheter som ska beaktas för att uppnå en lämplig skyddsnivå kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna: *Polismyndigheten* anför att det torde underlätta vid tillämpningen om skillnaden mellan vad som är skyddsåtgärder och vad som är säkerhetsåtgärder tydliggörs. *Datainspektionen* anser att de faktorer som anges i artikel 29.1 i direktivet bör komma till uttryck i lagen i stället för i förordning.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 29.1 ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller känsliga personuppgifter. Åtgärderna ska vara lämpliga med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål och riskerna för fysiska personers rättigheter och friheter. I artikel 29.2 ställs mer konkreta krav på vilka typer av åtgärder som ska vidtas för att förhindra att uppgifterna hamnar i orätta händer och säkerställa att det går att kontrollera viss behandling och att de system som används fungerar tillfredsställande.

Artikel 29 kompletterar det grundläggande kravet på säkerhet i artikel 4.1 f. Där framgår att personuppgifter, med användning av lämpliga tekniska eller organisatoriska åtgärder, ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse.

Nuvarande reglering

Säkerhetsåtgärder regleras i artikel 17.1 i 1995 års dataskyddsdirektiv. Den bestämmelsen motsvarar i stort innehållet i artikel 29.1 i det nya direktivet, men det ställs inte lika konkreta krav som i artikel 29.2.

Artikel 17.1 i 1995 års direktiv har genomförts i 31 § första stycket personuppgiftslagen. Där föreskrivs att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas och att åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur känsliga de behandlade personuppgifterna är. Vidare föreskrivs i 32 § person-

uppgiftslagen att tillsynsmyndigheten i enskilda fall får besluta om säkerhetsåtgärder enligt 31 §.

Datainspektionen ges i 16 § personuppgiftsförordningen möjlighet att meddela föreskrifter om bl.a. säkerhetsåtgärder. Inspektionen har dock inte meddelat några sådana föreskrifter utan har i stället valt att ge närmare vägledning genom allmänna råd.

Myndigheternas registerförfattningar hänvisar antingen till personuppgiftslagens bestämmelser (t.ex. 2 kap. 2 § första stycket 7 polisdatalagen) eller saknar sådana bestämmelser, vilket innebär att personuppgiftslagens bestämmelser ändå är tillämpliga (t.ex. 2 § lagen [2001:617] om behandling av personuppgifter inom kriminalvården). I några registerförfattningar finns det dock bestämmelser som preciserar de allmänna kraven i personuppgiftslagen.

Bestämmelser om informationssäkerhet finns även i andra författningar, t.ex. i arkivlagen (1990:782) och säkerhetsskyddslagen (1996:627) med tillhörande förordningar och i föreskrifter meddelade av Myndigheten för samhällsskydd och beredskap (exempelvis MSBFS 2016:1 Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet).

Bara en bestämmelse om säkerhetsåtgärder

Det bör tas in en bestämmelse om skyddet för personuppgifter i ramlagen. Frågan är inledningsvis hur man ska se på förhållandet mellan artikel 4.1 f och artikel 29 i direktivet.

Artikel 4.1 f slår fast en grundläggande princip för all behandling av personuppgifter och riktar sig till personuppgiftsansvariga. Bestämmelserna i artikel 29 är mer konkreta och riktar sig även till personuppgiftsbiträden. Båda artiklarna föreskriver dock en skyldighet att säkerställa lämplig säkerhet för personuppgifter med hjälp av tekniska och organisatoriska åtgärder. I artikel 29 utvecklas hur det ska uppnås och vilka åtgärder som ska vidtas. Artikel 29 får därför ses som en precisering av den grundläggande princip som anges i artikel 4.1 f. Det behövs följaktligen inte två olika bestämmelser om säkerhetsåtgärder i ramlagen.

Kraven på säkerhetsåtgärder

Artikel 29.1 motsvarar i princip 31 § första stycket personuppgiftslagen. Frågan är om artikel 29.2, som anger mer konkreta åtgärder, kräver några särskilda lagstiftningsåtgärder. Dataskyddsrambeslutet innehåller en likadan uppräkning av åtgärder. Vid genomförandet av rambeslutet bedömdes att personuppgiftslagens bestämmelser, även om de var mer generellt utformade, motsvarade rambeslutets bestämmelser om säkerhet och att dess mer preciserade bestämmelser därför inte krävde några lagändringar (prop. 2008/09:16 s. 52). Motsvarande bedömning gjordes när Schengenkonventionen genomfördes i svensk rätt (prop. 1999/2000:64 s. 148). Även vid genomförandet av motsvarande bestämmelser om säkerhet i det rådsbeslut som ersatte konventionens bestämmelser om Schengens informationssystem gjordes bedömningen att det inte krävdes några författningsändringar (prop. 2009/10:86 s. 25).

Regeringen anser att det saknas anledning att göra en annan bedömning i fråga om artikel 29.2 i direktivet än vad som gjorts tidigare. En

generellt utformad regel om grundläggande krav på åtgärder får alltså anses vara tillräcklig för att uppfylla kraven i direktivet. Som utredningen har framhållit är det med hänsyn till den tekniska utvecklingen och förändringar i samhället knappast lämpligt eller möjligt att på ett ändamålsenligt och långsiktigt sätt författningsreglera detaljerade krav på säkerhetsåtgärder. Det bör dock framgå att sådana åtgärder ska vidtas för att skydda personuppgifterna, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom oavsiktliga händelser. Härigenom kommer också de mer preciserade åtgärderna i artikel 29.2 tydligare till uttryck. Punkterna a–h behandlar olika sätt att skydda personuppgifter mot obehörig eller otillåten behandling. Punkterna i och j behandlar åtgärder för att förhindra förlust, förstöring eller skada bl.a. genom olyckshändelse. Även ramlagens bestämmelser om loggning och begränsning av tillgången till personuppgifter kan ses som förtydliganden av de åtgärder som anges i artikel 29.2.

Regeringen anser i likhet med utredningen, men till skillnad från *Datainspektionen*, att vilka omständigheter som bör beaktas för att uppnå en lämplig skyddsnivå kan regleras i förordning. Utöver de omständigheter som anges i 31 § personuppgiftslagen bör behandlingens art, omfattning, sammanhang och ändamål beaktas. Särskild hänsyn bör tas till i vilken utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är.

Polismyndigheten anför att innebörden av begreppen skyddsåtgärder och säkerhetsåtgärder bör tydliggöras. Regeringen anser dock att det, utifrån de förslag som nu lämnas, inte är lämpligt att utveckla begreppens innebörd närmare i detta sammanhang.

Om det uppstår behov av att ytterligare precisera vilka åtgärder som den personuppgiftsansvarige bör vidta kan det göras genom föreskrifter i förordning eller på myndighetsnivå. Riktlinjer kan också lämnas genom allmänna råd.

Personuppgiftsbiträdenas skyldigheter tas upp i avsnitt 9.6.5.

9.4 Personuppgiftsincidenter

9.4.1 Vad är en personuppgiftsincident?

Regeringens förslag: Personuppgiftsincident ska i ramlagen definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: En personuppgiftsincident är enligt artikel 3.11 en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Personuppgiftsincident är ett nytt begrepp när det gäller dataskydd. På informationssäkerhetsområdet är ordet incident dock etablerat. Med en incident avses att något allvarligt och oplanerat har inträffat.

En personuppgiftsincident motsvarar till viss del vad som i dagligt tal brukar kallas dataintrång. Med personuppgiftsincident avses dock inte bara ett sådant avsiktligt intrång, utan även olyckshändelser och andra oavsiktliga händelser som får oönskade effekter, t.ex. brand. I 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och i 10 a § säkerhetsskyddsförordningen (1996:633) används uttrycket it-incident för att beskriva i princip samma sak. Eftersom personuppgiftsincident används i dataskyddsförordningen bör det ordet användas i ramlagen. Ordet tydliggör att det rör sig om en händelse som får oönskade effekter för skyddet av personuppgifter.

En incident kan inträffa genom yttre påverkan, men kan också bero på interna brister eller otillåtet handlande av någon inom organisationen. Det som är väsentligt för definitionen av personuppgiftsincident är inte hur händelsen uppkommit eller vem som åstadkommit den utan effekten av den.

Både direktivet och dataskyddsförordningen innehåller regler om personuppgiftsincidenter och definierar dem på samma sätt. Motsvarande begrepp bör användas i ramlagen. Personuppgiftsincident bör således definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.

9.4.2 Anmälan till tillsynsmyndigheten

Regeringens förslag: Den personuppgiftsansvarige ska inom 72 timmar anmäla en personuppgiftsincident till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen. Någon anmälan behöver inte göras om det är osannolikt att incidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

Regeringens bedömning: Anmälningsförfarandet och vad anmälan ska innehålla kan regleras i förordning.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag och bedömning. Utredningen föreslår att någon anmälan inte ska behöva göras om det kan antas att en incident inte har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

Remissinstanserna: *Säkerhetspolisen* och *Försvarets radioanstalt* instämmer i bedömningen att det bör införas ett undantag från skyldigheten att anmäla en personuppgiftsincident till tillsynsmyndigheten om händelsen ska anmälas enligt säkerhetsskyddsförordningen (1996:633). *Datainspektionen* framhåller att begreppet ”osannolikt” används i direktivet och föreslår att det begreppet används i stället för ”kan antas”, eftersom det enligt inspektionen är en stor skillnad mellan att något kan antas och att något anses vara osannolikt. *Norrköpings kommun* önskar vägledning i fråga om dels hur tidsfristen ska beräknas om en incident inträffar på en helgdag, dels hur en personuppgiftsansvarig ska anses ha

fått kännedom om en incident. *Dataskydd.net* invänder mot att den personuppgiftsansvarige själv får avgöra om en incident ska anmälas till tillsynsmyndigheten eller inte.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 30.1 ska den personuppgiftsansvarige vid en personuppgiftsincident, utan onödigt dröjsmål och om möjligt inom 72 timmar, anmäla incidenten till tillsynsmyndigheten. Någon anmälan behöver emellertid inte göras om det är osannolikt att incidenten medför risk för fysiska personers rättigheter och friheter. I artikel 30.3 anges vad en anmälan till tillsynsmyndigheten ska innehålla. En anmälan ska bl.a. beskriva personuppgiftsincidentens art, de sannolika konsekvenserna av incidenten och vilka åtgärder som har vidtagits för att åtgärda den. Om det inte är möjligt att tillhandahålla all information samtidigt får den enligt artikel 30.4 tillhandahållas i omgångar.

Nuvarande reglering

Det finns inga bestämmelser om personuppgiftsincidenter i personuppgiftslagen eller myndigheternas registerförfattningar. Incidenter behandlas inte heller i Datainspektionens allmänna råd om säkerhet. Däremot ska incidenter i it-system rapporteras av andra skäl. I 20 § första stycket förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap föreskrivs att en myndighet skyndsamt ska rapportera it-incidenter som inträffat i myndighetens it-system till Myndigheten för samhällsskydd och beredskap. Det gäller om incidenten allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. En myndighet som tillhandahåller it-tjänster åt en annan organisation ska informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

Rapporteringsskyldigheten omfattar inte it-incidenter som enligt 10 a § säkerhetsskyddsförordningen ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Exempel på sådana incidenter är incidenter i informationssystem där hemliga uppgifter som gäller Sveriges säkerhet behandlas eller i it-system som särskilt behöver skyddas mot terrorism. Säkerhetskyddsförordningen gäller för myndigheter, kommuner och landsting och för vissa bolag, föreningar, stiftelser och enskilda.

Anmälningsskyldigheten bör regleras i ramlagen

Som framgått är myndigheter skyldiga att rapportera it-incidenter, men den rapporteringen görs till andra myndigheter än tillsynsmyndigheten och har ett annat syfte. Regleringen i artikel 30 tar sikte på skyddet för de personuppgifter som påverkas av incidenten och konsekvenserna för registrerade. En personuppgiftsincident som inte snabbt åtgärdas kan leda till att registrerade drabbas av såväl ekonomisk skada som personlig kränkning. I skäl 61 nämns som exempel på skador som kan uppkomma vid en personuppgiftsincident bl.a. identitetsstöld och identitetsbedrägeri,

diskriminering, skadat anseende och röjande av personuppgifter som är sekretesskyddade.

I ramlagen bör det föreskrivas att den personuppgiftsansvarige inom viss tid ska anmäla personuppgiftsincidenter till tillsynsmyndigheten. Undantaget från anmälningsskyldighet vid incidenter som inte medfört risk för registrerade bör också framgå. Någon anmälan behöver t.ex. inte göras om incidenten har påverkat få personuppgifter som inte är av känslig art eller om skyddet för personuppgifterna påverkats under så kort tid att obehörig åtkomst inte varit möjlig. Regeringen anser i likhet med *Datainspektionen* att formuleringen av bestämmelsen bör följa direktivets lydelse. Av skäl 61 framgår att det är den personuppgiftsansvarige som ska visa att det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

Regeringen instämmer vidare i utredningens bedömning att behovet av att skydda hemliga uppgifter som rör Sveriges säkerhet är så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av sådan information Eftersom nationell säkerhet ligger utanför direktivets tillämpningsområde hindrar inte direktivet att sådana uppgifter som ska anmälas enligt 10 eller 10 a § säkerhetsskyddsförordningen undantas från anmälningsskyldigheten till tillsynsmyndigheten. Motsvarande undantag kommer att gälla enligt den föreslagna lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Undantaget i brottsdatalagen bör utformas i linje med formuleringen i dataskyddslagen, dvs. anmälningsskyldigheten bör inte gälla personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen (prop. 2017/18:105 s. 7).

Vad ska anmälan innehålla?

Det bör regleras vad en anmälan till tillsynsmyndigheten ska innehålla, men det kan göras i förordning. En anmälan av en personuppgiftsincident ska enligt artikel 30.3 beskriva personuppgiftsincidentens art, dvs. vad det är som har inträffat. Om det är möjligt bör det också anges vilka kategorier av och ungefärligt antal registrerade och personuppgiftsposter som berörs. Beroende på vad som har inträffat kan det ibland vara svårt att överblicka hur många personuppgifter som berörs av incidenten och hur många registrerade som kan ha drabbats. Den personuppgiftsansvarige bör dock åtminstone redovisa en ungefärlig uppskattning. Dessutom bör anmälan innehålla en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten och vilka åtgärder som har vidtagits eller föreslagits för att åtgärda incidenten. En preliminär bedömning av konsekvenserna av incidenten bör göras av den personuppgiftsansvarige. Beskrivningen av vilka åtgärder som vidtagits bör även omfatta åtgärder för att mildra personuppgiftsincidentens negativa effekter. Anmälan bör också innehålla namnet på och kontaktuppgifter till dataskyddsombud eller annan kontaktpunkt hos den personuppgiftsansvarige.

En anmälan till tillsynsmyndigheten bör göras så snabbt som möjligt och senast inom 72 timmar, vilket bör framgå av ramlagen. *Norrköpings kommun* har efterfrågat klargöranden i fråga om när fristen börjar löpa om en incident inträffar på en helgdag. Avgörande är enligt direktivet när den personuppgiftsansvarige har fått kännedom om incidenten och inte när den har inträffat. Det är dock inte möjligt att i detta sammanhang närmare ange kriterierna för när en personuppgiftsansvarig ska anses ha fått kännedom om en incident. Eftersom det är fråga om regler till skydd för enskildas integritet är det dock av största vikt att anmälan görs så snart det kan ske.

Anmälningsförfarandet kan i övrigt regleras i förordning. Om anmälan görs senare än 72 timmar efter det att den personuppgiftsansvarige har fått kännedom om personuppgiftsincidenten, bör anmälan innehålla en förklaring till förseningen. Senare anmälan bör komma ifråga endast i särskilda fall där längre tid krävs för att överblicka personuppgiftsincidenten och dess konsekvenser. Informationen bör få lämnas i omgångar om det inte är möjligt att lämna all information samtidigt. Det bör således inte fördröja anmälan.

Om en anmälan av en personuppgiftsincident innebär att sekretessbelagda uppgifter behöver lämnas till tillsynsmyndigheten måste sekretessen kunna brytas. En bestämmelse som föreskriver att personuppgiftsansvariga ska anmäla en personuppgiftsincident till tillsynsmyndigheten innebär en sådan uppgiftsskyldighet som avses i 10 kap. 28 § offentlighets- och sekretesslagen (2009:400). Sekretess hindrar då inte att uppgifterna lämnas.

I 11 kap. 1 § offentlighets- och sekretesslagen regleras överföring av sekretess vid tillsyn. Där anges att om en myndighet i verksamhet som avser tillsyn, får en sekretessreglerad uppgift från en annan myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten. Vid anmälan av en personuppgiftsincident överförs således eventuell sekretess som gäller för uppgiften till tillsynsmyndigheten.

9.4.3 Underrättelse till den registrerade

Regeringens förslag: Om en personuppgiftsincident har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten. Underrättelseskyldigheten gäller inte om den personuppgiftsansvarige har vidtagit vissa skyddsåtgärder eller om den skulle kräva oproportionerligt stora ansträngningar. Den registrerade behöver inte heller underrättas om incidenten om det gäller sekretess eller tystnadsplikt för uppgifterna.

Regeringens bedömning: Vilken information en underrättelse ska innehålla kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 31.1 ska den personuppgiftsansvarige, om en personuppgiftsincident sannolikt kommer att leda till hög risk för fysiska personers rättigheter och friheter, utan onödigt dröjsmål informera registrerade om incidenten. Informationen ska enligt artikel 31.2 innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och beskriva de sannolika konsekvenserna av incidenten och vilka åtgärder som har vidtagits eller föreslagits för att åtgärda incidenten. Kontaktuppgifter till dataskyddsombudet eller annan kontaktpunkt ska också uppges.

I vissa fall behöver registrerade inte underrättas. Det gäller enligt artikel 31.3 om den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten eller om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risken för registrerades rättigheter och friheter inte längre kommer att finnas. Underrättelseskyldigheten gäller inte heller om den skulle kräva en oproportionerlig ansträngning. Då ska i stället allmänheten informeras eller en liknande åtgärd vidtas som innebär att den registrerade informeras på ett lika effektivt sätt. Underrättelse till den registrerade får också, enligt artikel 31.5, senareläggas, begränsas eller utelämnas på de villkor och av de skäl som anges i artikel 13.3.

Om den personuppgiftsansvarige inte har underrättat den registrerade, men tillsynsmyndigheten anser att personuppgiftsincidenten medför så hög risk att han eller hon bör underrättas, får tillsynsmyndigheten enligt artikel 31.4 kräva att den personuppgiftsansvarige gör det. Tillsynsmyndigheten kan också besluta att någon underrättelse inte krävs därför att något av de villkor som anges i artikel 31.3 är uppfyllt.

I vilka fall ska registrerade underrättas?

Skyldigheten att underrätta registrerade om en personuppgiftsincident och undantagen från skyldigheten bör regleras i ramlagen, medan detaljerna i förfarandet kan regleras i förordning. Underrättelse bör lämnas utan onödigt dröjsmål om personuppgiftsincidenten kan antas leda till särskild risk för otillbörligt intrång i registrerades personliga integritet. Av skäl 62 framgår att syftet med underrättelsen bl.a. är att den registrerade ska kunna vidta nödvändiga försiktighetsåtgärder.

Hur snabbt den personuppgiftsansvarige kan informera de registrerade beror på omständigheterna i det enskilda fallet. I skäl 62 framhålls att behovet av att mildra en omedelbar skaderisk kräver att de registrerade underrättas omgående, medan behovet av att vidta lämpliga åtgärder vid fortlöpande eller likartade incidenter kan motivera längre tid för underrättelsen. Framför allt bör personuppgiftsincidentens art och den registrerades intresse av och möjlighet att själv vidta åtgärder för att begränsa skadan beaktas. Även den tid det tar för den personuppgiftsansvarige att vidta akuta åtgärder för att begränsa skadan, avhjälpa fel och liknande bör beaktas.

I ramlagen bör det också regleras under vilka omständigheter någon underrättelse till den registrerade inte behöver lämnas. Underrättelseskyldighet bör inte gälla om något av de villkor som anges i artikel 31.3 är

uppfyllda. Det innebär att den registrerade inte behöver underrättas om den personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder. Om t.ex. personuppgifter gått förlorade vid en brand men det finns tillfredsställande back-up-rutiner kan risken vara så låg att någon underrättelse inte krävs. Någon underrättelse krävs inte heller om den personuppgiftsansvarige har vidtagit åtgärder som säkerställer att det inte längre finns särskild risk för otillbörligt intrång. Det kan t.ex. vara fråga om att tillgången till ett register har begränsats till dess att den personuppgiftsansvarige har kunnat överblicka konsekvenserna av incidenten. Den registrerade behöver inte heller underrättas om det skulle kräva en oproportionerlig ansträngning av den personuppgiftsansvarige. Det skulle kunna vara fallet om en personuppgiftsincident t.ex. påverkar ett mycket stort antal registrerade. Då bör i stället allmänheten informeras på lämpligt sätt eller en liknande åtgärd vidtas för att de registrerade ska få nödvändig information.

Vilken information ska lämnas?

Det bör regleras vilken information som ska lämnas till den registrerade vid en personuppgiftsincident. Det kan göras i förordning.

Begränsning av information till den registrerade

Informationen till den registrerade får senareläggas, begränsas eller utelämnas i vissa fall. Syftet är enligt direktivet att undvika att rättsliga utredningar, förundersökningar eller andra förfaranden hindras eller att undvika menlig inverkan på brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder och att skydda allmän eller nationell säkerhet eller andra personers rättigheter och friheter. Informationen får begränsas endast i den utsträckning och så länge som begränsningen är nödvändig och proportionerlig. Vid bedömningen ska hänsyn tas till den berörda personens grundläggande rättigheter och berättigade intressen.

Bestämmelser som begränsar rätten till information är nödvändiga för att de behöriga myndigheterna ska kunna utföra sina uppdrag på ett effektivt sätt. Det är framför allt regleringen i offentlighets- och sekretesslagen som tillgodoser det behovet. Även den relativt begränsade information som ska lämnas till den registrerade vid en personuppgiftsincident skulle t.ex. kunna skada en förundersökning i ett initialt skede eller avslöja att uppgifter om personen finns i ett sekretessreglerat register. I ramlagen bör det därför tas in en regel som klargör att sekretess och tystnadsplikt har företräde framför rätten till information vid personuppgiftsincidenter.

Tillsynsmyndighetens befogenheter

Enligt artikel 31.4 ska tillsynsmyndigheten ha möjlighet att förelägga den personuppgiftsansvarige att informera den registrerade, om det inte har gjorts. Det skulle kunna bli aktuellt om tillsynsmyndigheten gör en annan bedömning av behovet av att underrätta de registrerade. Den skyldigheten behöver inte regleras särskilt, eftersom den ryms i förslaget om tillsynsmyndighetens korrigerande befogenheter (se avsnitt 11.7.6).

9.4.4 Dokumentations- och underrättelseskyldighet

Regeringens bedömning: Den personuppgiftsansvariges skyldighet att dokumentera personuppgiftsincidenter kan regleras i förordning. Även skyldigheten att i vissa fall underrätta behöriga myndigheter i andra medlemsstater kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens bedömning

Dokumentation av personuppgiftsincidenter

Enligt artikel 30.5 ska den personuppgiftsansvarige dokumentera alla personuppgiftsincidenter som avses i artikel 30.1, inbegripet omständigheterna rörande incidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationsskyldigheten bör regleras i förordning.

Eftersom dokumentationsskyldigheten är knuten till artikel 30.1 är det oklart om det endast är sådana incidenter som ska anmälas till tillsynsmyndigheten som ska dokumenteras eller om tanken är att även sådana mindre allvarliga incidenter som inte behöver anmälas ska dokumenteras. I motsvarande bestämmelse i dataskyddsförordningen, artikel 33.5, anges att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter.

Regeringen instämmer i utredningens bedömning att en dokumentationsskyldighet endast för sådana personuppgiftsincidenter som anmäls till tillsynsmyndigheten skulle vara av begränsat värde, eftersom dokumentation om dem ska finnas i anmälan. I direktivet anges att dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av artikeln. För att det ska vara möjligt bör därför alla personuppgiftsincidenter dokumenteras.

Underrättelseskyldighet

Om personuppgiftsincidenten rör personuppgifter som kommer från eller har lämnats till en personuppgiftsansvarig i en annan medlemsstat, ska samma information som lämnas till tillsynsmyndigheten utan onödigt dröjsmål lämnas till den som lämnade eller tog emot uppgifterna i den andra medlemsstaten. Det framgår av artikel 30.6.

En bestämmelse om underrättelseskyldighet bör tas in i förordning. Skyldigheten bör korrespondera med skyldigheten att göra en anmälan till tillsynsmyndigheten. Det innebär att om någon anmälan inte görs dit, antingen på grund av att incidenten medfört så låg risk att anmälan inte krävs eller på grund av att incidenten rör nationell säkerhet, gäller inte underrättelseskyldigheten.

Utgångspunkten är att en uppgift för vilken sekretess gäller enligt offentlighets- och sekretesslagen inte får röjas för en utländsk myndighet eller en mellanfolklig organisation. I 8 kap. 3 § 1 offentlighets- och sekretesslagen görs dock undantag från huvudregeln om uppgiftslämnandet regleras särskilt i lag eller förordning. Eftersom det föreslås en bestämmelse om att behöriga myndigheter i andra medlemsstater ska underrättas i vissa fall, kommer sekretess inte att hindra att informationen lämnas.

Ett personuppgiftsbiträde har enligt direktivet ingen skyldighet att anmäla personuppgiftsincidenter till tillsynsmyndigheten eller att underrätta registrerade om incidenter. Eftersom den personuppgiftsansvarige ska anmäla personuppgiftsincidenter till tillsynsmyndigheten behöver den personuppgiftsansvarige även få kännedom om incidenter som inträffat hos personuppgiftsbiträdet. Det bör därför införas en skyldighet för personuppgiftsbiträden att underrätta den personuppgiftsansvarige om sådana incidenter (se avsnitt 9.6.5).

9.5 Dataskyddsombud

9.5.1 Definition av dataskyddsombud

Regeringens förslag: Dataskyddsombud ska i ramlagen definieras som den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att endast fysiska personer ska kunna utses till dataskyddsombud.

Remissinstanserna: *Datainspektionen* anser att definitionen av dataskyddsombud i ramlagen bör inkludera juridiska personer.

Skälen för regeringens förslag: I direktivet talas det på flera ställen om dataskyddsombud, men det finns inte någon definition av den termen. I 3 § personuppgiftslagen definieras personuppgiftsombud, som motsvarar det som i direktivet kallas dataskyddsombud. Där anges att ett personuppgiftsombud är den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Personuppgiftsombud är visserligen ett inarbetat begrepp men dataskyddsombud är den term som används både i direktivet och i dataskyddsförordningen. Den termen bör, som utredningen föreslår, användas även i ramlagen.

Dataskyddsombud bör definieras i ramlagen. Definitionen av personuppgiftsombud i personuppgiftslagen kan då tjäna som förebild. För att terminologin i ramlagen ska bli enhetlig bör uttrycket författningsenlig användas. *Datainspektionen* anser, med hänvisning till artikel 29-gruppens vägledning om dataskyddsombud, att även juridiska personer bör inkluderas i definitionen. Regeringen håller med Datainspektionen om det. Dataskyddsombud bör därför definieras som den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i ramlagen.

9.5.2 Krav på dataskyddsombud

Regeringens förslag: Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* framhåller att om en personuppgiftsansvarig utser flera dataskyddsombud måste det vara tydligt för den registrerade hur denne ska kunna utöva sina rättigheter. Inspektionen anser vidare att de krav på dataskyddsombudets kvalifikationer som följer av artikel 32.2. i direktivet bör anges i ramlagen eller förordningen. *Justitiekanslern* påpekar att det är något oklart hur brottsdatalagens och dataskyddsförordningens regler om dataskyddsombud förhåller sig till varandra och anför att frågan kan behöva belysas närmare. Justitiekanslern tolkar reglerna som att en myndighet som tillämpar båda regelverken ska utse och anmäla dataskyddsombud dels enligt brottsdatalagen, dels enligt dataskyddsförordningen. *Sveriges advokatsamfund* anför att det med hänsyn till intresset av dataskyddsombudens oberoende ställning kan vara lämpligt att dessa normalt anlitas externt.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 32 ska den personuppgiftsansvarige utnämna ett dataskyddsombud, offentliggöra ombudets kontaktuppgifter och meddela tillsynsmyndigheten vem som har utsetts och hans eller hennes kontaktuppgifter. Domstolars och andra oberoende rättsliga myndigheters dömande verksamhet får undantas från skyldigheten att utnämna dataskyddsombud.

Dataskyddsombud ska utnämnas på grundval av sina yrkesmässiga kvalifikationer, sin sakkunskap om lagstiftning och praxis rörande dataskydd och sin förmåga att fullgöra de uppgifter som åläggs dataskyddsombud. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter med hänsyn tagen till organisationsstruktur och storlek.

Alla personuppgiftsansvariga ska utse dataskyddsombud

Eftersom direktivet föreskriver en skyldighet för personuppgiftsansvariga att utnämna dataskyddsombud bör en bestämmelse om det tas in i ramlagen.

I dataskyddsförordningen finns inte någon allmän skyldighet för personuppgiftsansvariga att utse dataskyddsombud. Däremot gäller enligt artikel 37.1 en sådan skyldighet för myndigheter och andra offentliga organ. Dataskyddsombud ska också utses av personuppgiftsansvariga eller personuppgiftsbiträden vilkas kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning. Detsamma gäller om kärnverksamheten består av behandling i stor omfattning av känsliga personuppgifter och personuppgifter som rör fällande domar i brottmål och överträdelser.

Det föreslås nu att endast behöriga myndigheter ska kunna vara personuppgiftsansvariga. Som framgår av avsnitt 6.4.4 kan en behörig myn-

dighet vara antingen en myndighet som har de i ramlagen angivna uppgifterna eller en annan aktör som utövar myndighet för något av dessa syften. Myndigheter som bedriver verksamhet inom ramlagens tillämpningsområde bör vara skyldiga att utse dataskyddsombud. Frågan är om även andra aktörer än myndigheter bör vara skyldiga att utse dataskyddsombud.

I direktivet görs ingen skillnad mellan myndigheter och andra organ när det gäller att utse dataskyddsombud. Det talar för att alla personuppgiftsansvariga ska utse dataskyddsombud. Aktörer som bedriver verksamhet inom ramlagens tillämpningsområde, oavsett om det rör sig om en myndighet eller ett privat organ, behandlar ofta integritetskänsliga personuppgifter för relativt känsliga ändamål och det är av stor vikt att den interna kontrollen i sådana verksamheter fungerar tillfredsställande. Om en privat aktör inte behöver utse ett dataskyddsombud enligt förordningen kan det ifrågasättas om det behövs ett ombud enbart för ett begränsat uppdrag inom ramlagens tillämpningsområde. Behandlingen enligt ramlagen är emellertid av sådan art att det bör finnas ett dataskyddsombud som övervakar personuppgiftsbehandlingen. Regeringen anser därför i likhet med utredningen att alla personuppgiftsansvariga bör vara skyldiga att utse ett eller flera dataskyddsombud.

Bestämmelserna om dataskyddsombud i dataskyddsförordningen respektive brottsdatalagen bör, i enlighet med *Justitiekanslerns* tolkning, uppfattas som att en myndighet som tillämpar båda regelverken är skyldig att utse och anmäla dataskyddsombud enligt såväl förordningen som lagen. Det finns ingenting som hindrar att samma ombud utses för båda regelverken.

Ett eller flera dataskyddsombud ska utses

I artikel 32.1 anges att den personuppgiftsansvarige ska utse ett dataskyddsombud. Bestämmelsen bör inte tolkas så att endast ett ombud får utses. I större myndighetsorganisationer kan det vara svårt för en enda person att ensam utföra de uppgifter som ett dataskyddsombud ska ha i framtiden. Flera dataskyddsombud bör därmed kunna utses för en behörig myndighet.

Man kan tänka sig att det finns behöriga myndigheter som bedriver likartad verksamhet i nära anslutning till varandra och att det av den anledningen skulle kunna vara lämpligt att utse ett gemensamt ombud. Så skulle exempelvis kunna vara fallet med vissa domstolar. När myndigheter samarbetar i informationssystem som är gemensamma för flera myndigheter kan det också finnas behov av ett dataskyddsombud som kan se till helheten och eventuellt hjälpa enskilda registrerade i förhållande till samtliga inblandade myndigheter. I skäl 63 nämns som exempel att flera personuppgiftsansvariga gemensamt kan utse ett dataskyddsombud t.ex. vid gemensamma resurser i centralenheter. Mot den bakgrunden är det tydligt att det bör vara möjligt att utnämna samma dataskyddsombud för flera behöriga myndigheter. Detta behöver dock inte författningsregleras.

Dataskyddsombudens kvalifikationer

Vilka kvalifikationer och vilken kunskap den som utses till dataskyddsombud bör ha varierar naturligtvis. Enligt artikel 32.2 ska dataskyddsombudet utnämnas på grundval av sina yrkesmässiga kvalifikationer och, i synnerhet, sin sakkunskap om lagstiftning och praxis i fråga om dataskydd samt förmåga att fullgöra de uppgifter som avses i artikel 34. *Datainspektionen* anser att kraven på dataskyddsombudets kvalifikationer bör anges i ramlagen eller i förordning. Enligt regeringens bedömning kan sådana krav anges i förordning.

Enligt skäl 63 bör den nödvändiga nivån på sakkunskap fastställas med utgångspunkt i den personuppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas. Det kan således krävas mer av ett dataskyddsombud i en stor organisation som behandlar många känsliga personuppgifter och för olika ändamål än av ett ombud i en mindre organisation där en begränsad mängd uppgifter behandlas. Det ligger i varje personuppgiftsansvarigs intresse att dataskyddsombudet har tillräcklig kunskap, erfarenhet och förmåga att utföra sina uppgifter.

Som *Sveriges advokatsamfund* anför vore det en fördel med hänsyn till intresset av oberoende dataskyddsombud om ombuden kunde rekryteras externt. Enligt skäl 63 kan dock dataskyddsombudet vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning beträffande lagstiftning och praxis i fråga om dataskydd. Det är alltså möjligt att anlita dataskyddsombud såväl inom som utanför den egna organisationen. Uppgiften att vara dataskyddsombud kan utföras på deltid eller heltid.

Information om dataskyddsombuden

Den personuppgiftsansvarige bör anmäla till tillsynsmyndigheten vem som har utsetts till dataskyddsombud och när ombudet entledigas. Det är viktigt att tillsynsmyndigheten får information om det, eftersom ombuden bl.a. ska ha till uppgift att samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den i vissa fall (se avsnitt 9.5.3).

I avsnitt 10.2.6 behandlas den personuppgiftsansvariges skyldighet att göra information om dataskyddsombudets kontaktuppgifter tillgänglig.

9.5.3 Dataskyddsombudens arbetsuppgifter

Regeringens förslag: Dataskyddsombud ska ha vissa i ramlagen angivna arbetsuppgifter.

Regeringens bedömning: Skyldigheten att underlätta dataskyddsombudens verksamhet kan regleras i förordning.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag och bedömning. Enligt utredningens förslag ska dataskyddsombud vara skyldiga att anmäla till tillsynsmyndigheten om personuppgiftsansvariga bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

I artikel 34 anges vilka arbetsuppgifter som ett dataskyddsombud ska ha. Dataskyddsombud ska informera och ge råd till den personuppgiftsansvarige och de anställda som utför personuppgiftsbehandling om deras skyldigheter enligt direktivet och annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd. Ombuden ska också övervaka efterlevnaden av dessa regler och av den personuppgiftsansvariges strategier för skyddet av personuppgifter. I arbetsuppgifterna ingår vidare att på begäran ge råd beträffande konsekvensbedömningar och att övervaka genomförandet av dem. Dataskyddsombud ska samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den i frågor som rör behandling av personuppgifter, särskilt när det gäller förhandssamråd enligt artikel 28. Ombuden ska, om det är lämpligt, samråda med tillsynsmyndigheten även i andra frågor.

Enligt artikel 33.1 ska den personuppgiftsansvarige säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Den personuppgiftsansvarige ska enligt artikel 33.2 stödja dataskyddsombudet i utförandet av de arbetsuppgifter som anges i artikel 34. Det ska göras genom att den personuppgiftsansvarige tillhandahåller de resurser som krävs för att ombudet ska kunna fullgöra uppgifterna och ger ombudet tillgång till personuppgifter och itsystem. Den personuppgiftsansvarige ska också se till att dataskyddsombudets kunskaper upprätthålls.

I skäl 63 framhålls att dataskyddsombud bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt.

Nuvarande reglering

Enligt 38–40 §§ personuppgiftslagen ska personuppgiftsombud självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed och påpeka eventuella brister. Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter, och vidtas inte rättelse efter påpekande, ska ombudet anmäla det till tillsynsmyndigheten. Personuppgiftsombud ska även i övrigt samråda med tillsynsmyndigheten. Personuppgiftsombuden ska också föra förteckning över de behandlingar som den personuppgiftsansvarige utför och som skulle ha omfattats av anmälningsskyldighet om inte ombudet hade funnits. Personuppgiftsombud ska dessutom hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

Ombudens arbetsuppgifter enligt direktivet

Dataskyddsombudens roll påminner i stora delar om personuppgiftsombudens. Dataskyddsombuden har dock genom direktivet fått delvis nya arbetsuppgifter och en något förändrad roll. Flertalet av de arbetsuppgifter som ska anförtros dataskyddsombud har t.ex. karaktären av intern rådgivning, vilket inte är fallet i dag. Dataskyddsombuden har också fått ett tydligare uppdrag att bistå tillsynsmyndigheten.

Det bör i ramlagen föreskrivas att dataskyddsombud självständigt ska kontrollera att de personuppgiftsansvariga behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör de skyldigheter som åligger personuppgiftsansvariga. Kravet på självständighet infördes i personuppgiftslagen eftersom 1995 års dataskyddsdirektiv anger att ombudet ”på ett oberoende sätt” ska kunna kontrollera den personuppgiftsansvarige. I skäl 63 uttrycks samma sak. Självständighetskravet innebär att den personuppgiftsansvarige inte bör utse ett ombud som har en alltför underordnad ställning i organisationen. För att ombuden ska vara oberoende på det sätt som direktivet förutsätter måste han eller hon också ha tillräckliga kvalifikationer och kunskaper för att kunna utföra sina arbetsuppgifter på ett självständigt sätt.

I artikel 34 b anges att dataskyddsombudens kontroll ska omfatta ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning. Regeringen anser i likhet med utredningen att det inte är lämpligt att i detalj författningsreglera vad ombuden ska granska. Hur omfattande ombudens kontroll bör vara får som i dag avgöras efter omständigheterna i det enskilda fallet. Uppräkningen i direktivet kan dock tjäna som vägledning. Ombuden bör också påpeka eventuella brister för de personuppgiftsansvariga så att de blir medvetna om dem och har möjlighet att vidta lämpliga åtgärder.

Dataskyddsombud bör informera och ge råd till personuppgiftsansvariga och de som behandlar personuppgifter under dennes ledning om deras skyldigheter enligt ramlagen och andra författningar som rör personuppgiftsbehandling. Det handlar främst om att göra den personuppgiftsansvarige och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att informera registrerade, att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Om den personuppgiftsansvarige begär det ska ombudet ge råd vid en konsekvensbedömning och kontrollera att bedömningen genomförs på rätt sätt.

Dataskyddsombud ska även samarbeta med och fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter. Det gäller särskilt vid sådant förhandssamråd som avses i artikel 28 (se avsnitt 9.2.5). Samarbetet innebär också att ombuden, när det är lämpligt, ska samråda med tillsynsmyndigheten även i andra frågor som rör personuppgiftsbehandling.

Dataskyddsombudens roll påminner om internrevisorers. För att ombuden ska kunna utöva intern kontroll bör de inte ges arbetsuppgifter som kan komma i konflikt med kontrolluppgiften. Det kan t.ex. vara olämpligt att låta dataskyddsombud utbilda personalen eller ansvara för att den får annan information, eftersom det är åtgärder som omfattas av den interna granskningen. I större myndigheter torde det inte innebära några svårigheter att hålla isär dessa arbetsuppgifter. I mindre organisationer kan det dock vara svårare. Det är då viktigt att dataskyddsombudet trots sin dubbla roll kan utöva kontrollen på ett oberoende sätt. En lösning kan vara att anlita ett dataskyddsombud utanför den egna organisationen.

Dagens personuppgiftsombud ska enligt 40 § personuppgiftslagen hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Det framgår inte av förarbetena vad hjälpen innebär och frågan är om dataskyddsombud bör ha den arbetsuppgiften.

Personuppgiftsombud fungerar enligt uppgift främst som kontaktpunkt för registrerade i frågor om rättelse och är normalt inte den som i praktiken rättar personuppgifter. Personuppgiftsombud verkar emellertid också användas som kontaktpunkt för registrerade i andra frågor som rör behandling av personuppgifter. I förarbetena till polisdatalagen påtalas vikten av att registrerade enkelt kan vända sig till rätt person hos myndigheten bl.a. i frågor om information om behandling och om rättelse av felaktiga uppgifter (prop. 2009/10:85 s. 93). Liknande uttalanden finns också i förarbetena till andra registerförfattningar (se t.ex. prop. 2014/15:148 s. 91). Det förefaller således finnas behov av att ombudet hjälper registrerade även med andra frågor.

Det är naturligt att dataskyddsombuden fungerar som kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter på samma sätt som personuppgiftsombuden. Den personuppgiftsansvarige ska också enligt artikel 13.1 självmant göra dataskyddsombudens kontaktuppgifter tillgängliga för registrerade. Det talar för att dataskyddsombuden bör ha samma roll i förhållande till enskilda som personuppgiftsombud har i dag. Regeringen anser dock inte att det bör författningsregleras vad dataskyddsombud ska göra i egenskap av kontaktpunkt för enskilda.

Enligt personuppgiftslagen ska ett personuppgiftsombud anmäla till tillsynsmyndigheten om han eller hon misstänker att den personuppgiftsansvarige bryter mot gällande bestämmelser och inte vidtar rättelse. Någon sådan skyldighet föreskrivs inte i direktivet. Som utredningen påpekar är det viktigt att dataskyddsombud uppmärksammar tillsynsmyndigheten på eventuella problem och brister, särskilt om den personuppgiftsansvarige inte rättar sig efter ombudets påpekanden. Till skillnad från utredningen anser regeringen dock inte att dataskyddsombuden bör ha en sådan författningsreglerad skyldighet att anmäla eventuella överträdelser till tillsynsmyndigheten som personuppgiftsombuden har i dag. Någon motsvarande anmälningsskyldighet gäller inte på dataskyddsförordningens område och enligt regeringen är det inte motiverat att införa en sådan skyldighet endast inom ramlagens tillämpningsområde.

Dataskyddsombudens verksamhet ska underlättas

För att dataskyddsombuden ska kunna utföra sina arbetsuppgifter krävs det att de personuppgiftsansvariga gör det möjligt och tillhandahåller de resurser som ombuden behöver. Den personuppgiftsansvarige ska t.ex. göra ombudet delaktig i frågor och beslut som rör behandling av personuppgifter. Ombuden bör också få tillgång till all dokumentation gällande personuppgiftsbehandlingen och, i den utsträckning det behövs, tillgång till de personuppgifter som behandlas. Den personuppgiftsansvarige bör även se till att ombudet ges utrymme för vidareutbildning och annan kunskapsinhämtning. Bestämmelser om det som nu har sagts kan tas in i förordning.

9.6 Personuppgiftsbiträden

9.6.1 Definition av personuppgiftsbiträde

Regeringens förslag: Personuppgiftsbiträde ska i ramlagen definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska personuppgiftsbiträde definieras som den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.

Remissinstanserna: *Datainspektionen* och *Sveriges advokatsamfund* påpekar att artikel 3.9 i direktivet inte innehåller något krav på skriftliga avtal eller skriftliga överenskommelser vid anlitande av personuppgiftsbiträden och anför att denna skillnad mellan direktivets och lagens lydelser kan leda till oklarheter vid tillämpningen. De anser därför att direktivets definition ska användas.

Skälen för regeringens förslag: Personuppgiftsbiträde definieras i artikel 3.9 som en fysisk eller juridisk person, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det motsvarar i sak definitionen i 3 § personuppgiftslagen. Utredningen anser att det ska framgå av definitionen att det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse mellan personuppgiftsbiträdet och den personuppgiftsansvarige. Som *Datainspektionen* och *Sveriges advokatsamfund* invänder, ställer direktivets definition av personuppgiftsbiträde inte något krav på en skriftlig överenskommelse. Mot den bakgrunden anser regeringen, till skillnad från utredningen, att inte heller ramlagens definition bör innehålla något krav på en skriftlig överenskommelse. Personuppgiftsbiträde bör mot den bakgrunden definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Därmed kommer definitionen att överensstämma med den som finns i dataskyddsförordningen.

Ett personuppgiftsbiträde måste alltid finnas utanför den personuppgiftsansvariges organisation. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

9.6.2 Anlitande av personuppgiftsbiträden

Regeringens förslag: Den personuppgiftsansvarige ska, om det är lämpligt, få anlita personuppgiftsbiträden. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde ska försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde ska inte få anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från den personuppgiftsansvarige.

Regeringens bedömning: Vad avtalet eller överenskommelsen ska innehålla kan regleras i förordning.

Det som i övrigt ska gälla för tillstånd från den personuppgiftsansvarige att få anlita ett annat personuppgiftsbiträde kan regleras i förordning.

Utredningens förslag överensstämmer i sak med regeringens förslag och bedömning.

Remissinstanserna: *Eskilstuna tingsrätt* anser att det saknas en analys av när det kan anses vara lämpligt att anlita privata underbiträden. *Sveriges advokatsamfund* efterfrågar en ytterligare analys av riskerna vid anlitande av personuppgiftsbiträden som bedriver sin verksamhet utomlands, särskilt eftersom sådana biträden kan behöva lämna uppgifter till utländska myndigheter.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 22.1 får den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att vidta lämpliga tekniska och organisatoriska åtgärder, så att behandlingen uppfyller kraven i direktivet och säkerställer att den registrerades rättigheter skyddas.

Personuppgiftsbiträdets behandling ska enligt artikel 22.3 regleras genom ett avtal eller annan rättsakt enligt unionsrätten eller nationell rätt. Avtalet ska enligt artikel 22.4 vara skriftligt.

Av artikel 22.3 framgår att föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter, kategorier av registrerade och den personuppgiftsansvariges skyldigheter och rättigheter ska regleras i avtalet eller motsvarande. Därutöver ska vissa krav och villkor särskilt anges, t.ex. att personuppgiftsbiträdet säkerställer att personer som har tillstånd att behandla personuppgifterna har tystnadsplikt. Personuppgiftsbiträdet ska också radera eller återlämna alla personuppgifter till den personuppgiftsansvarige när uppdraget har avslutats och radera befintliga kopior av personuppgifterna, om inte lagring av dem krävs enligt unionsrätten eller nationell rätt.

Enligt artikel 22.2 får personuppgiftsbiträdet inte anlita ett annat personuppgiftsbiträde utan skriftligt förhandstillstånd av den personuppgiftsansvarige. Om ett allmänt tillstånd har erhållits, ska personuppgiftsbiträdet alltid informera den personuppgiftsansvarige om planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden.

Nuvarande reglering

Regler om personuppgiftsbiträden finns i artikel 17.2 och 17.3 i 1995 års dataskyddsdirektiv, som har genomförts i 30 och 31 §§ personuppgiftslagen. Enligt 31 § andra stycket ska den personuppgiftsansvarige, när denne anlitar ett personuppgiftsbiträde, förvissa sig om att biträdet kan vidta de säkerhetsåtgärder som krävs och se till att biträdet gör det. Det är dock den personuppgiftsansvarige som har ansvaret gentemot den registrerade även när ett personuppgiftsbiträde anlitas (prop. 1997/98:44

s. 93). Det ska enligt 30 § andra stycket personuppgiftslagen finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet ska vidta de säkerhetsåtgärder som avses i 31 § första stycket för att skydda personuppgifterna.

Myndigheternas registerförfattningar hänvisar antingen till dessa paragrafer eller saknar avvikande bestämmelser.

Personuppgiftsbiträden ska kunna anlitas

På direktivets område är det ovanligt att myndigheter anlitar utomstående privata aktörer för behandling av personuppgifter, men det kan förekomma. Ibland träffas också överenskommelser mellan myndigheter där en myndighet agerar personuppgiftsbiträde åt en annan. Det behövs därför bestämmelser i ramlagen som reglerar anlitandet av personuppgiftsbiträden.

På samma sätt som i dag bör det krävas att den personuppgiftsansvarige försäkrar sig om att personuppgiftsbiträdet ska vidta nödvändiga säkerhetsåtgärder och ser till att det görs. Artikel 22.1 omfattar inte bara säkerhetsåtgärder, utan även andra tekniska och organisatoriska åtgärder som säkerställer att behandlingen är författningsenlig och utförs på ett korrekt sätt och att personuppgifterna skyddas. Den personuppgiftsansvarige bör innan ett personuppgiftsbiträde anlitas bl.a. förhöra sig om hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna har hos biträdet. Bestämmelsen måste anses gå längre än de nu gällande kraven på personuppgiftsansvariga. Bestämmelsen i ramlagen bör därför ha en något vidare formulering än motsvarande bestämmelse i personuppgiftslagen.

Ansvarsfördelningen mellan den personuppgiftsansvarige och personuppgiftsbiträdet

Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs på dennes vägnar. Den personuppgiftsansvarige ansvarar således både i förhållande till tillsynsmyndigheten och i förhållande till registrerade för att reglerna i ramlagen och andra tillämpliga författningar följs vid personuppgiftsbehandling hos ett personuppgiftsbiträde. Den personuppgiftsansvarige kan uppdra åt biträdet att utföra viss behandling av personuppgifter, men kan inte avsäga sig personuppgiftsansvaret och de skyldigheter som följer med det. Den personuppgiftsansvarige är också skadeståndsskyldig gentemot enskilda vid felaktig behandling av personuppgifter hos personuppgiftsbiträdet. Att biträdet kan bli skadeståndsskyldigt gentemot den personuppgiftsansvarige är en annan sak.

Den omständigheten att flera bestämmelser i direktivet riktar sig direkt till personuppgiftsbiträden innebär ingen förändring av ansvarsfördelningen mellan personuppgiftsansvariga och personuppgiftsbiträden. Tillsynsmyndigheten får dock i vissa fall utkräva ansvar även av personuppgiftsbiträden. Om ett personuppgiftsbiträde t.ex. inte vidtar nödvändiga säkerhetsåtgärder kan tillsynsmyndigheten vidta åtgärder mot både

biträdet och den personuppgiftsansvarige. Likaså kan båda åläggas sanktionsavgift för sådana brister hos biträdet.

Personuppgiftsbiträdets roll ska regleras i en överenskommelse

På samma sätt som i dag bör det krävas ett skriftligt avtal eller någon annan skriftlig överenskommelse mellan personuppgiftsbiträdet och den personuppgiftsansvarige. I artikel 22.3 anges relativt utförligt vad ett sådant avtal ska innehålla. I jämförelse med motsvarande bestämmelse i 1995 års dataskyddsdirektiv ställs det väsentligt högre krav på innehållet. Ramlagen bör dock inte tyngas av alltför detaljerade bestämmelser. Även om det i dag anges i personuppgiftslagen vad ett personuppgiftsbiträdesavtal ska innehålla anser regeringen därför att den mer detaljbetonade regleringen bör finnas i förordning.

Anlitande av underbiträden

Varken 1995 års dataskyddsdirektiv eller personuppgiftslagen reglerar förutsättningarna för när ett personuppgiftsbiträde får anlita ett annat personuppgiftsbiträde, ett underbiträde.

Det är av grundläggande betydelse att den personuppgiftsansvarige känner till vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning. Av ramlagen bör det därför framgå att ett personuppgiftsbiträde inte får anlita ett annat personuppgiftsbiträde utan att den personuppgiftsansvarige har lämnat skriftligt tillstånd till det. Att personuppgiftsbiträden som har fått ett generellt tillstånd att anlita underbiträden ska vara skyldiga att informera den personuppgiftsansvarige när underbiträden anlitas kan regleras i förordning. Syftet med informationen är att den personuppgiftsansvarige ska ha möjlighet att invända mot anlitandet av nya biträden.

Eskilstuna tingsrätt har efterfrågat en analys av när det kan anses vara lämpligt att anlita privata underbiträden. Regeringen anser dock inte att det är lämpligt att utöver regleringen i direktivet ställa upp några särskilda kriterier för när biträden får anlitas. Vid tveksamheter kring det tilltänkta biträdets förmåga att uppfylla sina skyldigheter bör biträdet inte anlitas. *Sveriges advokatsamfund* har för sin del väckt frågor kring riskerna med att anlita utländska personuppgiftsbiträden. Sådana eventuella risker måste också vägas in av den personuppgiftsansvarige när biträden anlitas, men det är knappast möjligt att generellt utesluta möjligheten att anlita biträden som har sin verksamhet utomlands.

9.6.3 Behandling enligt den personuppgiftsansvariges instruktioner

Regeringens förslag: Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt artikel 23 får personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandla uppgifterna enligt instruktion från den personuppgiftsansvarige. Undantag gäller dock om någon enligt unionsrätten eller nationell rätt är skyldig att behandla personuppgifter. Om så är fallet får personuppgiftsbiträdet göra det även utan instruktion från den personuppgiftsansvarige.

En likadan bestämmelse finns i artikel 16 i 1995 års dataskyddsdirektiv. Den har genomförts i 30 § första stycket personuppgiftslagen. Där föreskrivs att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det allmännas verksamhet i sådana frågor, gäller emellertid de bestämmelserna i stället för 30 § första stycket. Det som främst avses är bestämmelser om tystnadsplikt och sekretess (prop. 1997/98:44 s. 136).

I artikel 22.5 föreskrivs att ett personuppgiftsbiträde som i strid med direktivet fastställer ändamålen med och medlen för behandlingen ska anses vara personuppgiftsansvarig avseende den behandlingen. Någon motsvarande bestämmelse finns inte i dag.

Behandling enligt den personuppgiftsansvariges instruktioner

Det bör framgå av ramlagen att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Det framgår inte av direktivet hur utförliga instruktioner som ska lämnas till biträdet. Instruktionerna bör givetvis vara så tydliga att otillåten behandling inte utförs (jfr SOU 1997:39 s. 336). Den överenskommelse som styr personuppgiftsbiträdets uppdrag ska innehålla viss information som ger instruktioner till biträdet, bl.a. om behandlingens varaktighet, art och ändamål. Instruktionerna kan också gälla exempelvis hur tillgången till personuppgifter hos biträdet ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för dataskydd. Enligt skäl 64 bör ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation om biträdet fått i uppdrag att göra det. Sådana uppdrag bör också framgå av de instruktioner som den personuppgiftsansvarige lämnar till biträdet.

Eftersom ramlagen är subsidiär kommer avvikande bestämmelser i annan författning att gälla framför bestämmelserna i ramlagen, vilket framgår av den föreslagna bestämmelsen i lagens 1 kap. 5 §. Om det finns avvikande regler i annan lagstiftning som anger att någon är skyldig att utföra en viss behandling, exempelvis att lämna ut allmänna hand-

lingar, innebär det att behandlingen får utföras utan särskilda instruktioner.

Att den som bestämmer ändamålen med och medlen för behandlingen är att anse som personuppgiftsansvarig framgår av definitionen av personuppgiftsansvarig. Det bör i ramlagen tydliggöras att ett personuppgiftsbiträde som går utanför sin befogenhet och behandlar personuppgifter för något annat ändamål än enligt sina instruktioner är personuppgiftsansvarig för den behandlingen. I sådana fall kan biträdet bli skadeståndsskyldig eller påföras sanktionsavgift på grund av den behandlingen.

Trots att personuppgiftsbiträdet kanske inte är en behörig myndighet enligt definitionen i ramlagen bör den behandling som biträdet utför i egenskap av personuppgiftsansvarig omfattas av lagens regler. Bestämmelsen i direktivet om att personuppgiftsbiträden blir personuppgiftsansvariga i den nu aktuella situationen har till syfte att säkerställa att behandlingen av personuppgifterna utförs enligt direktivets bestämmelser. Direktivet är skräddarsytt för behandlingen av personuppgifter för vissa ändamål. Det skulle innebära ett sämre skydd för enskilda om personuppgiftsbiträdenas behandling inte skulle följa den regleringen om de går utanför sina instruktioner. Det som nu har sagts kan dock bara gälla så länge syftet med behandlingen ligger inom ramlagens tillämpningsområde. Skulle personuppgiftsbiträdet behandla uppgifterna för helt andra ändamål blir dataskyddsförordningen tillämplig.

9.6.4 Skyldighet att förteckna behandlingar

Regeringens bedömning: Personuppgiftsbiträdets skyldighet att förteckna de kategorier av behandling som utförs för en personuppgiftsansvarigs räkning får regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens bedömning: Enligt artikel 24.2 ska personuppgiftsbiträden föra register över de kategorier av behandling som utförs för en personuppgiftsansvarigs räkning, vilket är en nyhet. I artikeln räknas ett antal uppgifter upp som ska framgå av registret, som enligt artikel 24.3 på begäran ska göras tillgängligt för tillsynsmyndigheten.

Den dokumentationsskyldighet för personuppgiftsbiträden som artikeln föreskriver kan regleras i förordning. De uppgifter som anges i artikel 24.2 bör framgå av registret. Någon särskild bestämmelse om att dokumentationen ska göras tillgänglig för tillsynsmyndigheten behövs inte (jfr avsnitt 9.2.7).

9.6.5 Övriga skyldigheter för personuppgiftsbiträden

Regeringens förslag: Ett personuppgiftsbiträde ska ha samma skyldigheter som en personuppgiftsansvarig att logga vissa typer av behandlingar, begränsa tillgången till personuppgifter, vidta säkerhetsåtgärder och samarbeta med tillsynsmyndigheten.

Regeringens bedömning: Personuppgiftsbiträdets skyldighet att underrätta den personuppgiftsansvarige om personuppgiftsincidenter kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna: *Dataskydd.net* anser att ett personuppgiftsbiträde ska ha samma skyldighet som den personuppgiftsansvarige att genom tekniska åtgärder se till att dataskyddsprinciper säkerställs.

Skälen för regeringens förslag och bedömning: Flera av skyldigheterna för personuppgiftsansvariga gäller även för personuppgiftsbiträden. Det är samarbetsskyldigheten enligt artikel 26, skyldigheten enligt artikel 29 att vidta lämpliga säkerhetsåtgärder och skyldigheten enligt artikel 25 att föra loggar. När det gäller förhandssamråd enligt artikel 28 föreskrivs att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten.

Som anges i avsnitt 9.6.2 ska en personuppgiftsansvarig som anlitar ett personuppgiftsbiträde försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter. Regeringen anser, till skillnad från *Dataskydd.net*, att det saknas skäl att i ramlagen dessutom ange att ett personuppgiftsbiträde ska ha samma skyldighet som den personuppgiftsansvarige att genom tekniska åtgärder se till att dataskyddsprinciper säkerställs.

Den personuppgiftsansvariges skyldighet att logga vissa typer av behandlingar, samarbeta med tillsynsmyndigheten och vidta lämpliga åtgärder för att skydda personuppgifterna regleras i ramlagen. Det bör framgå av ramlagen att bestämmelserna i fråga gäller även för personuppgiftsbiträden.

Skyldigheten att begränsa tillgången till personuppgifter till vad varje tjänsteman behöver för att fullgöra sina arbetsuppgifter bör gälla även för personuppgiftsbiträden, vilket bör framgå av ramlagen.

Förhandssamråd med tillsynsmyndigheten bör dock bara vara en skyldighet för den personuppgiftsansvarige, eftersom denne är ansvarig även för den behandling som personuppgiftsbiträdet utför. Den föreslagna bestämmelsen om förhandssamråd bör därför inte gälla för personuppgiftsbiträden. Eftersom det i artikel 28 anges att den personuppgiftsansvarige *eller* personuppgiftbiträdet i vissa fall ska samråda med tillsynsmyndigheten kan en sådan reglering inte anses strida mot direktivet. Ett personuppgiftsbiträde kan dock behöva bistå den personuppgiftsansvarige under förhandssamrådet om samrådet t.ex. rör förändringar avseende redan pågående personuppgiftsbehandling som utförs av biträdet. Skyldigheten att samarbeta med tillsynsmyndigheten föreslås gälla även för personuppgiftsbiträden. Samarbetsskyldigheten gäller generellt och omfattar

därigenom även samarbete från biträdets sida vid förhandssamråd om det blir aktuellt.

Enligt artikel 30.2 ska ett personuppgiftsbiträde utan onödigt dröjsmål underrätta den personuppgiftsansvarige efter att ha fått vetskap om en personuppgiftsincident. Det som avses bör rimligen vara en incident hos personuppgiftsbiträdet eller något biträde som denne i sin tur anlitat. Syftet med bestämmelsen är att den personuppgiftsansvarige, efter att ha fått vetskap om incidenten, ska anmäla den till tillsynsmyndigheten om förutsättningarna för sådan anmälan är uppfyllda. Eftersom det är den personuppgiftsansvarige som ska anmäla personuppgiftsincidenter enligt ramlagen bör det föreskrivas att ett personuppgiftsbiträde ska underrätta den personuppgiftsansvarige om personuppgiftsincidenter hos biträdet. Det kan regleras i förordning.

Regleringen av personuppgiftsbiträdens skyldigheter medför inga större skillnader i förhållande till dagens reglering. Enligt 30 § andra stycket personuppgiftslagen är ett personuppgiftsbiträde skyldigt att vidta sådana säkerhetsåtgärder som avses i 31 § första stycket. Det ska också föreskrivas i biträdesavtalet. Personuppgiftsbiträden är alltså redan i dag skyldiga att vidta lämpliga åtgärder för att skydda de personuppgifter som behandlas. Det innebär ett indirekt krav på att begränsa tillgången till personuppgifter genom exempelvis behörighetstilldelning och att logga behandlingar för att kunna kontrollera åtkomsten till personuppgifterna. Den enda nyheten är att tillsynsmyndigheten kan vidta åtgärder mot både personuppgiftsansvariga och personuppgiftsbiträden om de brister i sina skyldigheter. Eftersom den personuppgiftsansvarige fortfarande är ansvarig för den behandling som personuppgiftsbiträdet utför torde det sällan bli aktuellt att utnyttja den möjligheten.

9.7 Gemensamt personuppgiftsansvar

9.7.1 Gemensamt personuppgiftsansvar i dag

Den personuppgiftsansvarige definieras i personuppgiftslagen som den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen. Två eller flera personuppgiftsansvariga kan därför vara gemensamt personuppgiftsansvariga för viss behandling av personuppgifter. Om så är fallet, och vad deras respektive ansvar då innebär, kan dock vara svårt att avgöra. Det finns ingen reglering av vad det innebär om flera tillsammans bestämmer ändamålen med och medlen för behandlingen.

Ett samarbete mellan två eller flera myndigheter medför inte automatiskt ett gemensamt ansvar för behandlingen av personuppgifter. Det avgörande är i stället om de deltagande myndigheterna i någon mån tillsammans bestämmer ändamålen med och medlen för behandlingen. I många fall då myndigheter samarbetar framgår det av de faktiska omständigheterna vem som är ansvarig för vilken personuppgiftsbehandling, t.ex. genom att det endast är en myndighet som har tillgång till personuppgifterna eller it-systemet, eller om myndigheterna agerar i olika skeden av en process. Det förhållandet att två myndigheter använder samma datasystem eller att en myndighet ger en annan myndighet direktåtkomst

till ett visst datasystem innebär inte heller per automatik att det uppstår ett gemensamt personuppgiftsansvar. Ibland förekommer dock att flera myndigheter är ansvariga för samma behandling, om samarbetet innebär att de deltagande myndigheterna tillsammans bestämmer exempelvis vilka uppgifter som ska läggas in, lagras eller tas bort.

Den oklarhet som råder i fråga om gemensamt personuppgiftsansvar innebär att det kan vara svårt för den enskilde att veta vem han eller hon ska vända sig till för att få information om personuppgiftsbehandlingen eller för att göra eventuella anspråk gällande. Vidare är det av stor betydelse för möjligheterna att utöva tillsyn att personuppgiftsansvaret är tydligt. Ett gemensamt personuppgiftsansvar som inte har reglerats tillräckligt tydligt kan också medföra svårigheter för de personuppgiftsansvariga själva. Det kan vara svårt för dem att på ett effektivt och ändamålsenligt sätt fullgöra sitt ansvar om det är oklart hur långt ansvaret sträcker sig och vad skyldigheterna omfattar.

Även om gemensamt personuppgiftsansvar mellan myndigheter är tillåtet, torde det i praktiken vara ovanligt. I de allra flesta fall är den personuppgiftsbehandling som förekommer väl avgränsad och går att härleda till en viss myndighet. De faktiska omständigheterna tillsammans med regelverken som gäller för myndigheterna innebär att gemensamt personuppgiftsansvar sällan aktualiseras. Det kan dock de facto uppstå vid behandling av personuppgifter i en viss situation eller på ett visst sätt. Eftersom personuppgiftslagen inte ger någon ledning för hur frågor om gemensamt personuppgiftsansvar ska hanteras får de personuppgiftsansvariga själva lösa dem.

9.7.2 En reglering av gemensamt personuppgiftsansvar

Regeringens förslag: Två eller flera personuppgiftsansvariga som gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen ska vara gemensamt personuppgiftsansvariga. Den registrerade ska få utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Regeringens bedömning: Det kan regleras i förordning att gemensamt personuppgiftsansvariga genom en skriftlig överenskommelse ska fastställa sina respektive ansvar.

Utredningens förslag överensstämmer delvis med regeringens förslag och bedömning. Utredningen föreslår att två eller flera behöriga myndigheter får vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det. Utredningen föreslår vidare att rätten för den registrerade att få utöva sina rättigheter mot var och en av de gemensamt personuppgiftsansvariga kan regleras i förordning.

Remissinstanserna: *Säkerhetspolisen* konstaterar att utredningens förslag inte har någon motsvarighet i direktivet. Säkerhetspolisen har inte några invändningar mot förslaget i sig men anför att förslaget förutsätter att det tydligt framgår vad som krävs för att ett gemensamt personuppgiftsansvar ska anses föreligga. *Försvarets radioanstalt* framhåller att det

varken i direktivet eller dataskyddsförordningen finns någon motsvarighet till den bestämmelse som utredningen föreslår.

Skälen för regeringens förslag och bedömning: Personuppgiftsansvarig definieras i artikel 3.8 som en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Redan av definitionen framgår det alltså att den personuppgiftsansvarige kan bestämma ändamål och medel för behandlingen tillsammans med andra.

Enligt artikel 21.1 är två eller flera personuppgiftsansvariga som gemensamt fastställer ändamålen med och medlen för behandlingen gemensamt personuppgiftsansvariga. De gemensamt personuppgiftsansvariga ska genom ett inbördes arrangemang under öppna former fastställa vars och ens ansvar för efterlevnaden av direktivet, särskilt när det gäller att enskilda ska kunna utöva sina rättigheter och skyldigheten att tillhandahålla information enligt artikel 13. I den mån de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller nationell rätt ska någon överenskommelse om fördelning av ansvaret inte ingås i den delen.

De gemensamt personuppgiftsansvariga ska också utse en kontaktpunkt för registrerade. Enligt artikeln kan medlemsstaterna fastslå vem av de gemensamt personuppgiftsansvariga som kan fungera som kontaktpunkt. I artikel 21.2 öppnas en möjlighet att föreskriva att den registrerade, oavsett det inbördes arrangemanget, får göra sina rättigheter gällande mot var och en av de personuppgiftsansvariga.

Utredningen föreslår att det i ramlagen ska tas in en bestämmelse som föreskriver att två eller flera behöriga myndigheter får vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning, eller om regeringen i enskilda fall beslutar om det. Sådant ansvar kan då inte uppstå de facto i en viss situation, utan endast i den utsträckning som riksdagen eller regeringen har beslutat om det. Ordningen för när gemensamt personuppgiftsansvar uppkommer skulle därmed bli tydligare.

Som *Säkerhetspolisen* och *Försvarets radioanstalt* anför finns det inte någon motsvarighet till utredningens förslag i direktivet. Inte heller i dataskyddsförordningen finns det något motsvarande formkrav för att ett gemensamt personuppgiftsansvar ska uppstå. Skillnaden mellan lydelsen i direktivet och lydelsen i utredningens förslag skulle kunna medföra att ett gemensamt personuppgiftsansvar i vissa fall föreligger enligt direktivet men inte enligt ramlagen. Detta kan leda till oklarheter vid rättstillämpningen, särskilt med hänsyn till att det är osäkert hur den EU-rättsliga tolkningen av begreppet gemensamt personuppgiftsansvar kan komma att utvecklas i framtiden. Trots de fördelar som finns med utredningens förslag, anser regeringen därför att bestämmelsens lydelse i ramlagen bör motsvara direktivets lydelse.

Det bör alltså i lagen införas en bestämmelse som innebär att två eller flera personuppgiftsansvariga som gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen ska vara gemensamt personuppgiftsansvariga.

Vidare bör det av bestämmelsen i lagen framgå att den registrerade ska få utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Motsvarande ordning gäller vid gemensamt personuppgiftsansvar enligt dataskyddsförordningen.

En skriftlig överenskommelse om fördelningen av ansvaret

Enligt artikel 21.1 ska gemensamt personuppgiftsansvariga på ett tydligt sätt fastställa sitt respektive ansvar, främst i förhållande till registrerade. I skäl 54 framhålls vikten av att det tydligt fastställs vem som bär ansvaret. Det ska ske under öppna former genom ett inbördes arrangemang mellan de personuppgiftsansvariga.

Det bör med hänsyn till innehållet i artikel 21.1 ställas krav på att en skriftlig överenskommelse träffas, men detta kan regleras i förordning. Även om det finns en skriftlig överenskommelse som reglerar ansvaret kan detta inte befria någon av avtalsparterna från det ansvar som följer av gällande rätt, exempelvis registrerades möjligheter att utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga. En överenskommelse ska enbart reglera hur ansvaret ska utövas i praktiken.

Kravet på öppenhet måste anses vara uppfyllt genom regleringen om tillgång till allmänna handlingar.

9.8 Föreskriftsrätt

Regeringens förslag: Regeringen bemyndigas att meddela föreskrifter om vissa skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Dataskydd.net* avstyrker förslaget.

Skälen för regeringens förslag: Ramlagen och den tillhörande förordningen kommer främst att tillämpas av myndigheter men även av privata aktörer. Även om registerlagstiftning inte tillhör det obligatoriska lagområdet har utvecklingen gått mot att sådan lagstiftning i allt större utsträckning ges lagform. Skyldigheter som åläggs personuppgiftsansvariga och personuppgiftsbiträden enligt ramlagen kan innebära skyldigheter för enskilda. Föreskrifter som gäller förhållandet mellan enskilda och det allmänna och som gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden ska enligt 8 kap. 2 § första stycket 2 regeringsformen som huvudregel meddelas i lag. Riksdagen kan dock enligt 8 kap. 3 § första stycket regeringsformen bemyndiga regeringen att meddela sådana föreskrifter.

I 8 kap. 7 § regeringsformen anges inom vilka områden regeringen utan delegering får meddela föreskrifter. Enligt paragrafen får regeringen bl.a. meddela föreskrifter om verkställighet av lag. Verkställighetsföreskrifter är i första hand tillämpningsföreskrifter av rent administrativ karaktär. Sådana bestämmelser kan fylla ut eller precisera lagbestämmelser. Lagregleringen får dock inte tillföras något väsentligt nytt genom verkställighetsföreskrifter. De får t.ex. inte innebära att enskilda åläggs ytterligare skyldigheter.

Ramlagen och den tillhörande förordningen är en offentligrättslig reglering och omfattas av det delegeringsbara lagområdet. Det är därmed möjligt att i vissa fall bemyndiga regeringen att meddela föreskrifter inom ramlagens tillämpningsområde. För att undvika en alltför detaljerad lagreglering bör vissa bestämmelser som kan innebära åligganden för enskilda finnas i förordning. Sådana bestämmelser kan ibland fylla ut eller precisera en lagbestämmelse och ses då som verkställighetsföreskrifter. Så kan exempelvis vara fallet om åtgärder ska vidtas för att en skyldighet i lag ska kunna uppfyllas, t.ex. dokumentation eller underrättelse. I övriga fall kan det krävas ett bemyndigande till regeringen för att sådana bestämmelser ska kunna meddelas i förordning.

Merparten av de skyldigheter som åläggs personuppgiftsansvariga och personuppgiftsbiträden föreslås regleras i ramlagen, men vissa detaljbestämmelser föreslås regleras i förordning. Eftersom det är mindre lämpligt att tynga en lag med utpräglade detaljföreskrifter bör vissa skyldigheter för personuppgiftsansvariga regleras i förordningen trots att de även kan träffa enskilda. Det gäller skyldigheten att föra register över kategorier av behandlingar av personuppgifter och skyldigheten att införa interna rutiner för anmälan av överträdelser. De bestämmelserna är inte heller så ingripande att de av den anledningen bör regleras i lag. Konsekvenserna av lagförslaget i sin helhet kan överblickas även om regeringen ges ett bemyndigande. Regeringen bör därför i ramlagen bemyndigas att meddela föreskrifter om dessa skyldigheter.

10 Enskildas rättigheter

10.1 Tydligare reglering av enskildas rättigheter

Rätten till skydd av personuppgifter är inte en absolut rättighet utan ska vägas mot andra intressen. En del i personuppgiftsskyddet är enskildas rätt att få veta hur deras personuppgifter behandlas. Information om den personuppgiftsbehandling som pågår är en förutsättning för att enskilda ska kunna kontrollera om behandlingen är författningsenlig och i övrigt kunna bevaka sina intressen. Direktivet medför att rättigheterna för enskilda tydliggörs. Den enskilde får utökade möjligheter att kontrollera hur hans eller hennes personuppgifter behandlas och att begära korrigering av felaktiga eller ofullständiga personuppgifter och åtgärder vid otillåten behandling. I skäl 7 betonas att skyddet för fysiska personers rättigheter och friheter ska vara likvärdigt i alla medlemsstater när personuppgifter behandlas inom direktivets tillämpningsområde. Det framhålls även att ett effektivt skydd av personuppgifter förutsätter stärkta rättigheter för enskilda och ökade skyldigheter för dem som behandlar personuppgifter.

10.2 Rätten till information

10.2.1 Allmänt om rätten till information

Tillgången till allmänna handlingar

Det finns regler inom olika områden som ger enskilda rätt till insyn i viss myndighetsverksamhet och rätt att ta del av handlingar som behandlas där. Det gäller även inom ramlagens tillämpningsområde. Reglerna om personuppgiftsbehandling, och den rätt till information som skapas genom dem, utgör bara en mindre del av den samlade rätten till information.

Vem som helst har rätt att med stöd av 2 kap. 1 § tryckfrihetsförordningen ta del av allmänna handlingar. Den rätten kan bara begränsas av sekretess och tystnadsplikt. I offentlighets- och sekretesslagen (2009:400) finns både sekretessbestämmelser och bestämmelser som anger när olika typer av sekretess får brytas. Sekretess till skydd för enskildas personliga eller ekonomiska intressen gäller normalt inte i förhållande till den person som uppgiften avser (12 kap. 1 §). Däremot kan sekretess till skydd för det allmännas intressen eller till skydd för annan enskilds intressen begränsa rätten att få del av allmänna handlingar. För de verksamheter där ramlagen kommer att tillämpas gäller framför allt sekretess enligt 18 och 35 kap. offentlighets- och sekretesslagen, som skyddar det allmännas respektive enskildas intressen i brottsbekämpande verksamhet. Även andra sekretessbestämmelser kan gälla i det enskilda fallet. Sådan sekretess som gäller hos alla myndigheter är inte sällan aktuell inom ramlagens tillämpningsområde, exempelvis sekretess till skydd för vissa adressuppgifter (21 kap. 3 §) eller för utlänningar (21 kap. 5 §).

Rätten till insyn

Den som är part i ett mål eller ärende hos en myndighet eller en domstol har i stor utsträckning rätt till insyn i förfarandet och rätt att ta del av den information som tillförs målet eller ärendet under handläggningen. Myndigheter och domstolar är i varierande utsträckning skyldiga att se till att en part får del av sådan information. Bestämmelser om det finns bl.a. i förvaltningslagen, förvaltningsprocesslagen (1971:291) och 45 kap. 9 § rättegångsbalken. Enligt 10 kap. 3 § offentlighets- och sekretesslagen hindrar sekretess inte den som är part och som på grund av sin partsställning har rätt till insyn i handläggningen att ta del av handlingar och material i målet eller ärendet. Insynen får bara begränsas under förutsättning att det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att en sekretessbelagd uppgift i en handling i målet eller ärendet inte lämnas ut till parten. Sekretess hindrar aldrig en part från att ta del av en dom eller ett beslut i målet eller ärendet. Sekretess innebär inte heller någon begränsning i en parts rätt enligt rättegångsbalken att få del av alla omständigheter som läggs till grund för ett avgörande.

Förvaltningslagens bestämmelser om partsinsyn och kommunikationsskyldighet gäller inte i polisens, åklagarnas, Tullverkets, Kustbevakningens och Skatteverkets brottsbekämpande verksamhet. Brottsförebyggande arbete är inte författningsreglerat och det finns inte heller några

särskilda regler om insyn eller tillgång till handlingar i sådan verksamhet. Underrättelseverksamhet är endast i mycket begränsad utsträckning författningsreglerad och några särskilda regler om insyn eller tillgång till handlingar i den verksamheten finns inte heller.

Särskilda regler gäller däremot om misstänktas rätt till insyn i förundersökningar enligt 10 kap. 3 a § offentlighets- och sekretesslagen och 23 kap. rättegångsbalken. Förundersökningar omfattas i de flesta fall åtminstone inledningsvis till stor del av sekretess, men den avklingar normalt ju längre utredningen kommer. Därför har regleringen av rätten till insyn i förundersökningar stor praktisk betydelse.

Tidpunkten för när en person underrättas om att han eller hon är skäligen misstänkt är utgångspunkten för rätten till insyn. Den som är skäligen misstänkt eller åtalad har rätt till insyn och tillgång till material enligt 23 kap. 18, 18 a och 21 §§ rättegångsbalken. Den som utsätts för ett straffprocessuellt tvångsmedel som kan prövas av domstol har vid domstolens handläggning partsrättigheter, men har inte någon insyn i t.ex. polisens eller åklagarens handläggning utöver vad som nyss har sagts. Vid domstolens handläggning av andra förprocessuella frågor, t.ex. frågor om offentlig försvarare eller målsägandebiträde, har den berörde på motsvarande sätt partsställning och den insyn som följer av det.

Det finns inga regler om målsägandens eller andra berördas rätt till insyn i förundersökningsförfarandet. Däremot finns det omfattande regler om underrättelseskyldighet som bl.a. tillgodoser målsägandenas intressen knutna till att en förundersökning slutförs.

Om åtal väcks blir som regel de flesta handlingar som rör åtalet offentliga. En domstols handläggning av brottmål är till största delen offentlig och för handlingarna i målet gäller bara i begränsad utsträckning sekretess. Det är framför allt i mål som rör underåriga eller särskilt känsliga frågor som exempelvis vissa sexualbrott och för viss personalia som det kan gälla sekretess.

Det är viktigt att skilja den rätt till information och tillgång till handlingar som skapas genom de nu nämnda regleringarna från den rätt till information och tillgång till personuppgifter som skapas genom reglerna om skydd för personuppgifter. Bestämmelserna har helt olika syften.

10.2.2 Reglerna om information i straffrättsliga förfaranden har företräde

Regeringens bedömning: Det behöver inte regleras att bestämmelser om personuppgiftsbehandling inte får inkräkta på reglerna om rätt till information vid förundersökning och andra straffrättsliga förfaranden, eftersom avvikande regler gäller i stället för ramlagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om bedömningen.

Skälen för regeringens bedömning

Innehållet i direktivet

Enligt artikel 18 får medlemsstaterna föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med medlemsstaternas nationella rätt, om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

Av skäl 49 och 107 framgår att direktivet inte hindrar medlemsstaterna att i nationell straffprocesslagstiftning genomföra bestämmelser dels om den registrerades rätt till information om behandlingen av hans eller hennes personuppgifter, rättelse och radering av personuppgifter och begränsning av behandlingen i samband med straffrättsliga förfaranden, dels om begränsningar av dessa rättigheter.

Behövs det någon ny reglering?

Det finns som nyss nämnts åtskilliga bestämmelser om enskildas rätt till insyn i brottsutredningar och straffrättsliga förfaranden. Av särskild betydelse är 23 kap. rättegångsbalken, som reglerar den misstänktes insyn under en förundersökning, 20 kap. rättegångsbalken som reglerar frågor som rör målsägande och förundersökningskungörelsen (1947:948) som framför allt reglerar underrättelseskyldigheter till misstänkt, målsägande och andra som berörs av en förundersökning.

Brottsförebyggande arbete, underrättelseverksamhet, förundersökningar och brottmålsprocesser kan i dag genomföras på ett ändamålsenligt sätt, eftersom den processrättsliga lagstiftningen tillsammans med bestämmelser om sekretess och tystnadsplikt – när det finns skäl för det – begränsar enskildas rätt till information.

Eftersom ramlagen föreslås vara subsidiär i förhållande till andra lagar och förordningar kommer reglerna i de processrättsliga regelverken och sekretessregleringen att ta över vid en konflikt mellan regelverken (se avsnitt 6.1.2). Det innebär att om reglerna om rätt till partsinsyn eller tillgång till handlingar enligt rättegångsbalken eller andra författningar eller reglerna om sekretess eller tystnadsplikt kommer i konflikt med ramlagens bestämmelser ska de förstnämnda reglerna tillämpas i stället för ramlagens.

I likhet med utredningen gör regeringen bedömningen att den ordning som gäller i dag för enskildas rätt till information och tillgång till uppgifter i brottsutredningar och straffrättsliga förfaranden således inte kommer att påverkas när ramlagen träder i kraft. Några ytterligare regler för att säkerställa att brottsutredningar eller straffrättsliga förfaranden kan genomföras på samma sätt som nu behövs därmed inte.

10.2.3 Innehållet i direktivet

I direktivet finns det tre artiklar som reglerar vilken information som den personuppgiftsansvarige ska tillhandahålla den registrerade, artiklarna 13.1, 13.2 och 14. För att kunna ta ställning till hur dessa artiklar ska genomföras i ramlagen krävs först en analys av vilka rättigheter och skyldigheter artiklarna slår fast och hur de förhåller sig till varandra.

Artikel 13.1 är utformad som minimikrav. Den anger vilken information som den personuppgiftsansvarige alltid ska göra tillgänglig för registrerade. Det är fråga om allmän information om den personuppgiftsansvarige och dataskyddsombudet, ändamålen med behandlingen, rätten att lämna in klagomål, rätten att begära tillgång till personuppgifter och rätten att begära rättelse, radering och begränsning av behandling.

Därutöver ska den personuppgiftsansvarige enligt artikel 13.2 i specifika fall lämna ytterligare information för att göra det möjligt för den registrerade att utöva sina rättigheter. Det gäller information om behandlingens rättsliga grund, hur länge personuppgifterna får behandlas, kategorier av mottagare av uppgifterna och den ytterligare information som det finns behov av.

Enligt artikel 14 ska den registrerade ha rätt att få bekräftelse av den personuppgiftsansvarige om hans eller hennes personuppgifter behandlas. Om så är fallet ska den registrerade få tillgång till personuppgifterna och information om vilka personuppgifter som behandlas och varifrån de har hämtats. Den registrerade ska också informeras om ändamålen med behandlingen och dess rättsliga grund, kategorier av personuppgifter, mottagare eller kategorier av mottagare, hur länge uppgifterna får behandlas, rätten att begära rättelse, radering eller begränsning av behandlingen och möjligheten att lämna in klagomål till tillsynsmyndigheten.

10.2.4 Nuvarande reglering

Information som den personuppgiftsansvarige ska lämna självmant

I 23–25 §§ personuppgiftslagen (1998:204) föreskrivs att den personuppgiftsansvarige självmant ska informera den registrerade om behandlingen av hans eller hennes personuppgifter. I 23 § regleras vad som gäller om uppgifterna lämnats av den registrerade själv och i 24 § om uppgifterna hämtats från något annat håll. I 25 § första stycket anges vilken information som den personuppgiftsansvarige ska lämna självmant. Uppgift om den personuppgiftsansvariges identitet ska alltid lämnas och uppgift om ändamålen med behandlingen. All annan information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen ska också lämnas, t.ex. information om mottagarna av uppgifterna, skyldigheten att lämna uppgifter och rätten att ansöka om information och att få rättelse.

Enligt 25 § andra stycket personuppgiftslagen behöver information inte lämnas om sådant som den registrerade redan känner till. Undantaget har stor praktisk betydelse för omfattningen av den personuppgiftsansvariges skyldighet.

Bestämmelserna i 23 och 25 §§ personuppgiftslagen gäller för myndigheterna i rättskedjan. För polisen och Kustbevakningen görs undantag från informationsskyldigheten i 23 § dels vid insamling av personuppgifter genom bilder eller ljud, dels om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen (2 kap. 2 § tredje stycket polisdatalagen [2010:361] och 2 kap. 2 § tredje stycket kustbevakningsdatalagen [2012:145]).

Myndigheternas registerförfattningar hänvisar däremot inte till 24 § personuppgiftslagen. Det beror på att informationsskyldigheten enligt

den paragrafen inte gäller om det finns avvikande bestämmelser i lag eller annan författning (prop. 2014/15:63 s. 52 f. och prop. 2014/15:148 s. 87).

Regeringen kan enligt 50 § e personuppgiftslagen meddela närmare föreskrifter om vilken information som ska lämnas till registrerade och hur den ska lämnas. Datainspektionen har motsvarande delegation enligt 16 § 5 personuppgiftsförordningen (1998:1191). Några sådana föreskrifter har inte utfärdats. Datainspektionen har dock gett ut allmänna råd om information (Information till registrerade, Datainspektionens allmänna råd, maj 2000).

Information som den personuppgiftsansvarige ska lämna efter ansökan

Enligt 26 § personuppgiftslagen är den personuppgiftsansvarige skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller inte. Om sådana uppgifter behandlas ska också skriftlig information lämnas om vilka uppgifter om den sökande som behandlas, varifrån dessa uppgifter har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Paragrafen gäller för myndigheterna i rättskedjan, antingen genom en uttrycklig hänvisning i registerförfattningarna eller genom att de registerförfattningar som gäller utöver personuppgiftslagen inte har några avvikande regler.

10.2.5 Innebörden av artiklarna om information

Regeringens bedömning: Artikel 13.1 avser allmän information som ska göras tillgänglig för registrerade. Artikel 13.2 avser personrelaterad information som den personuppgiftsansvarige på eget initiativ ska lämna till en registrerad i ett enskilt fall, medan artikel 14 avser personrelaterad information som ska lämnas på begäran.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans anför något i denna del.

Skälen för regeringens bedömning

Allmän eller personrelaterad information?

Artiklarna om information innehåller till viss del samma eller liknande krav på vilken information som den personuppgiftsansvarige ska tillhandahålla; t.ex. anges ”ändamålen med behandlingen” både i artiklarna 13.1 och 14 och ”behandlingens rättsliga grund” både i artiklarna 13.2 och 14. Bestämmelserna har emellertid enligt utredningens uppfattning olika syften. Regeringen har ingen annan uppfattning.

Artikel 13.1 avser allmän information som riktar sig till allmänheten eller en obestämd, större krets av registrerade. Det rör sig om upplysningar av generell karaktär som hänför sig till myndighetens personuppgiftsbehandling i allmänhet, exempelvis kontaktuppgifter till personuppgiftsansvarig, dataskyddsombud och tillsynsmyndigheten. Det rör sig också om allmänna upplysningar om hur man ansöker om rättelse, rade-

ring eller begränsning av behandlingen av personuppgifter. Artikel 14 tar sikte på information riktad till en enskild registrerad om behandlingen av hans eller hennes personuppgifter (personrelaterad information).

Eftersom artikel 13.2 avser information som ska lämnas i specifika fall för att göra det möjligt för den registrerade att utöva sina rättigheter, håller regeringen med utredningen om att artikeln inte kan syfta på upplysningar av generell karaktär. Regeringen bedömer därför att artikel 13.2, i likhet med artikel 14, avser personrelaterad information.

En annan möjlig tolkning är att artikel 13.2 riktar sig till lagstiftaren som i lag eller förordning ska föreskriva i vilka fall information enligt artikeln ska lämnas. En sådan tolkning är dock som utredningen påpekar inte rimlig, eftersom det inte är möjligt att i författning reglera specifika fall där information bör lämnas för att den registrerade ska kunna ta till vara sina rättigheter. Till det kommer att artikel 11.1 c i 1995 års dataskyddsdirektiv, som har liknande utformning, har genomförts genom 25 § första stycket c personuppgiftslagen som riktar sig till den personuppgiftsansvarige.

Ska informationen göras tillgänglig eller lämnas?

Artikel 13.1 föreskriver att informationen ska göras tillgänglig för den registrerade, medan det i artikel 13.2 föreskrivs att informationen ska lämnas till den registrerade. Som nyss nämnts avser artikel 13.1 allmän information som riktar sig till en obestämd krets av registrerade. I kravet på att information ska vara tillgänglig ligger att de registrerade i princip ska ha möjlighet att ta del av informationen när de önskar. Informationen kan t.ex. publiceras på myndighetens webbplats (jfr skäl 42) eller finnas i en broschyr, folder eller annan informationsskrift.

Informationen enligt artikel 13.2 avser som just konstaterats personrelaterad information som ska lämnas till den registrerade. Kravet får anses innebära att den personuppgiftsansvarige ska ge information riktat till den registrerade, t.ex. genom att skicka sådan information med post eller e-post eller lämna muntlig information. Det är således som utredningen konstaterar inte tillräckligt att enbart göra informationen tillgänglig på en webbplats, men den kan naturligtvis finnas där också.

Enligt artikel 14 ska personrelaterad information lämnas till den registrerade i samband med ett besked om att hans eller hennes personuppgifter behandlas.

Ska informationen lämnas på eget initiativ eller först på begäran?

En annan fråga är om artiklarna 13 och 14 förutsätter att den personuppgiftsansvarige informerar på eget initiativ eller om det krävs att den registrerade begär information. Eftersom artikel 13.1 avser allmän information som ska göras tillgänglig av den personuppgiftsansvarige på exempelvis en webbplats, framstår det som naturligt att den tillhandahålls på den personuppgiftsansvariges eget initiativ. Det som talar för att även personrelaterad information enligt artikel 13.2 ska lämnas ex officio är punkten d, som nämner personuppgifter som samlas in utan den registrerades vetskap. Om personuppgifter samlats in utan den registrerades vetskap saknar han eller hon förutsättningar att begära information om

behandlingen. Då krävs det att den personuppgiftsansvarige agerar för att se till att den registrerade får informationen.

Viss ledning för hur artiklarna 13.2 och 14 bör tolkas kan hämtas från motsvarande bestämmelser i personuppgiftslagen och i 1995 års dataskyddsdirektiv som har ett likartat innehåll och liknande struktur. Artikel 13 motsvaras av 25 § personuppgiftslagen, som tillsammans med 23 och 24 §§ genomför artiklarna 10 och 11 i 1995 års direktiv. I förarbetena anför regeringen att artiklarna, trots att det inte sägs uttryckligen, innebär att den personuppgiftsansvarige *självmant* ska lämna informationen till den registrerade (prop. 1997/98:44 s. 78). I 25 § personuppgiftslagen föreskrivs att informationen ska lämnas självmant. Mot den bakgrunden håller regeringen med utredningen om att den personuppgiftsansvarige på eget initiativ ska lämna sådan information som avses i artikel 13.2.

När det gäller artikel 14 är artikel 12 a i 1995 års direktiv och 26 § personuppgiftslagen, som genomför artikeln, av intresse. Paragrafen ger den registrerade rätt till information om de personuppgifter som rör honom eller henne. Regeringen anför i förarbetena att artikel 12 a innebär att informationen bara behöver lämnas på den registrerades begäran (prop. 1997/98:44 s. 81). I 26 § personuppgiftslagen föreskrivs därför att informationen ska lämnas efter ansökan. Artikel 12 a svarar mot artikel 14 i det nya direktivet, i vilken det anges att den registrerade ska få bekräftelse av den personuppgiftsansvarige om personuppgifter som rör den registrerade behandlas och, om så är fallet, viss information om dessa uppgifter. Ordet bekräftelse tyder på att information enligt artikel 14 bara behöver lämnas på begäran. I motsvarande artikel i dataskyddsförordningen, artikel 15, används också ordet bekräftelse. Av skäl 63 i förordningen framgår att den registrerade ska göra en framställan, vilket ger ytterligare stöd för tolkningen att informationen i fråga bara behöver lämnas på begäran. I likhet med utredningen anser regeringen mot den bakgrunden att artikel 14 i direktivet avser personrelaterad information som ska lämnas först när den efterfrågas.

10.2.6 Allmän information som ska göras tillgänglig

Regeringens förslag: Den personuppgiftsansvarige ska göra viss allmän information tillgänglig för den registrerade. Bland annat ska kategorier av ändamål för behandlingen göras tillgänglig.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska bl.a. ändamålen med behandlingen göras tillgänglig.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* och *Polismyndigheten* anser att det bör framgå av författningstexten att det är ändamålen med behandlingen på en övergripande nivå som avses. *Datainspektionen* välkomnar förslaget men anser att det finns en risk för att den personuppgiftsansvarige lämnar för lite information om ändamålen med behandlingen för det fall det skulle vara tillräckligt att, som utredningen menar, endast ge en god bild av personuppgiftsbehandlingen. Samtidigt framhåller Datainspektionen att för omfattande och detaljerad

information inte heller är bra eftersom informationen då riskerar att bli oläsbar och svår för de registrerade att ta till sig. Övriga remissinstanser yttrar sig inte om förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Artikel 13.1 anger vilken information den personuppgiftsansvarige alltid ska göra tillgänglig för registrerade. Det är fråga om den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter och ändamålen med behandlingen. Även information om rätten att begära tillgång till personuppgifter och att begära rättelse, radering och begränsning av behandlingen och möjligheten att lämna in klagomål till en tillsynsmyndighet och dess kontaktuppgifter ska göras tillgänglig.

Vilken information ska göras tillgänglig?

En bestämmelse i ramlagen bör reglera vilken allmän information som ska göras tillgänglig enligt artikel 13.1. Den bör lista de uppgifter som räknas upp i artikeln. Hur uppgifterna bör göras tillgängliga diskuteras i avsnitt 10.2.5.

Dataskyddsombudets kontaktuppgifter bör göras tillgängliga. Dataskyddsombud behandlas i avsnitt 9.5. Enligt utredningen behöver det inte vara en direkt kontaktuppgift till dataskyddsombudet, t.ex. hans eller hennes e-postadress, utan det är tillräckligt att ombudet går att nå via kontaktuppgiften. Regeringen instämmer i den bedömningen. Direktivet förutsätter inte att dataskyddsombudets identitet ska göras tillgänglig. I dag finns det inte någon skyldighet att informera allmänheten om personuppgiftsombudets identitet eller kontaktuppgifter, utan endast en skyldighet att anmäla uppgifterna till tillsynsmyndigheten. Det finns inte skäl att nu införa krav på att dataskyddsombudets identitet ska göras allmänt tillgänglig.

Vidare ska den personuppgiftsansvarige enligt artikeln göra information om ändamålen med behandlingen tillgänglig. Samma krav ställs i 25 § första stycket b personuppgiftslagen. Som utvecklas i avsnitt 10.2.5 anser regeringen att det är fråga om upplysningar av generell karaktär som gäller den behöriga myndighetens personuppgiftsbehandling i allmänhet. Det innebär att det inte är fråga om ändamålen för behandling i varje enskilt fall som avses utan för vilka kategorier av ändamål personuppgifter får behandlas t.ex. förundersökningar, ärenden om strafföreläggganden eller brottmål. Detta bör, som *Polismyndigheten* och *Säkerhets- och integritetsskyddsnämnden* påpekar, framgå av författningstexten. Regeringen håller med utredningen om att det inte bör krävas en uttömmande uppräkning av för vilka ändamål personuppgifter behandlas. Det bör vara tillräckligt att enskilda genom uppräkningen får en god bild av den personuppgiftsbehandling som den behöriga myndigheten utför. Regeringen anser inte, till skillnad från *Datainspektionen*, att det därmed finns risk att för lite information lämnas om ändamålen med behandlingen.

Slutligen bör informationen också omfatta rätten att få information om behandlingen och att få del av personuppgifterna och rätten att begära

rättelse, radering eller begränsning av behandlingen och möjligheten att lämna in klagomål till tillsynsmyndigheten. En allmän beskrivning av hur registrerade ska gå till väga för att kunna utöva dessa rättigheter, t.ex. hur man begär rättelse av personuppgifter, bör också göras tillgänglig av den personuppgiftsansvarige. Tillsynsmyndighetens kontaktuppgifter bör anges.

10.2.7 Information som ska lämnas i ett enskilt fall

Regeringens förslag: Den personuppgiftsansvarige ska i ett enskilt fall lämna viss personrelaterad information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* välkomnar förslaget men anser att utredningens tolkning av uttrycket ”specifika fall” riskerar att försvåra för registrerade att ta till vara sina rättigheter. Även *Kriminalvården* kommenterar uttrycket ”specifika fall”. Kriminalvården anser att uttrycket är otydligt och efterfrågar därför fler exempel samt ett tydliggörande av vad som ryms inom den nu aktuella informationsskyldigheten respektive informationsskyldigheten rörande personuppgiftsincidenter. *Dataskydd.net* förespråkar att formuleringen ”i specifika fall” utgår från lagtexten. Övriga remissinstanser yttrar sig inte om förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Utöver den allmänna information som avses i artikel 13.1, ska den personuppgiftsansvarige enligt artikel 13.2 i specifika fall lämna viss information för att göra det möjligt för den registrerade att utöva sina rättigheter. Det gäller information om behandlingens rättsliga grund, hur länge personuppgifterna får behandlas eller kriterierna för att fastställa det, kategorier av mottagare av uppgifterna och den ytterligare information som det finns behov av, i synnerhet om personuppgifterna samlas in utan den registrerades vetskap. I skäl 42 anges att den registrerade bör informeras i den utsträckning som ytterligare information är nödvändig för att garantera att hans eller hennes personuppgifter behandlas korrekt. Vid den avvägningen ska de särskilda omständigheter under vilka personuppgifterna behandlas beaktas.

Vad är specifika fall?

Ramlagen bör reglera vilken information som ska lämnas enligt artikel 13.2. Att informationen ska riktas till den registrerade och lämnas på den personuppgiftsansvariges eget initiativ behandlas i avsnitt 10.2.5. Det som då återstår att diskutera är vad som avses med specifika fall.

Information behöver endast lämnas i de fall där den registrerade behöver informationen för att kunna ta till vara sina rättigheter. Direktivet ger ingen ledning för när det kan bli aktuellt. Enligt utredningens uppfattning kan det vara om den enskilde riskerar att lida någon rättsförlust, t.ex. om känsliga personuppgifter har behandlats på otillåtet sätt. Ett annat exem-

pel som utredningen ger är att personuppgifter har lämnats till fel mottagare och att det kan komma att medföra negativa konsekvenser för den registrerade. Den personuppgiftsansvarige bör i sådana fall informera den registrerade om vad som har hänt och vilka åtgärder som han eller hon kan vidta, t.ex. att lämna in klagomål till tillsynsmyndigheten eller väcka talan om skadestånd. Enligt utredningen bör det inte krävas att den personuppgiftsansvarige informerar vid sådana fel som inte kan antas ha någon negativ inverkan. Utredningen anser att det normalt bör krävas att det är fråga om överträdelser av regelverket som skulle kunna föranleda skadeståndsansvar, allvarlig kritik eller ingripande från tillsynsmyndigheten eller någon annan liknande reaktion. *Datainspektionen* ser det som problematiskt att knyta rätten till information till en bedömning av sannolika effekter för den registrerade. Att informationsskyldigheten avser att göra det möjligt för den registrerade att ta till vara sina rättigheter, talar enligt regeringen för den tolkning av artikeln som utredningen gör. Regeringen anser därför i likhet med utredningen att skyldigheten att lämna information som regel bör inträda först när det är fråga om överträdelser av regelverket som kan antas få negativa följder för den registrerade. *Kriminalvården* efterfrågar mer vägledning för när bestämmelsen kan bli tillämplig. Som ytterligare exempel kan nämnas att personuppgifter har behandlats utan rättslig grund eller att personuppgifter har behandlats under längre tid än regelverket tillåter.

Information som rutinmässigt lämnas till en viss kategori av personer, t.ex. information till personer som lämnar salivprov för dna-analys enligt rättegångsbalken eller till vittnen om personuppgiftsbehandling i samband med ljud- och bildupptagning under domstolsförhandling, syftar i och för sig till att underlätta för dem att ta till vara sina rättigheter. Eftersom informationen i dessa fall lämnas till alla berörda är den inte personrelaterad. Det rör sig således inte om specifika fall. Datainspektionen invänder mot detta och anser att både de som lämnar salivprov och de som vittnar i en rättegång är betjänta av information enligt den nu aktuella bestämmelsen. Regeringen håller med om att de nämnda kategorierna av personer bör få information om personuppgiftsbehandlingen, men anser att den information som ska göras tillgänglig enligt förslaget i avsnitt 10.2.6. är tillräcklig i de fallen. Enligt regeringen är den gränsdragning som utredningen gör mellan allmän information som ska tillgängliggöras och personrelaterad information som ska lämnas i specifika fall välbalanserad och rimlig.

I avsnitt 9.4.3 föreslås att registrerade i vissa fall ska informeras om personuppgiftsincidenter. Kriminalvården väcker frågan hur den informationsskyldigheten förhåller sig till skyldigheten att lämna personrelaterad information i specifika fall. Information om personuppgiftsincidenter aktualiseras bara när det har inträffat en säkerhetsincident, medan informationsskyldighet enligt den bestämmelse som nu föreslås aktualiseras vid regelöverträdelser som kan antas få negativa konsekvenser för registrerade. Vidare syftar information om personuppgiftsincidenter till att de registrerade ska kunna vidta åtgärder för att skydda sig och sina personuppgifter, medan personrelaterad information i specifika fall syftar till att de registrerade ska kunna ta till vara sina rättigheter. De två informationsskyldigheterna inträder alltså under olika förutsättningar och tjänar olika syften. Det utesluter dock inte att en personuppgiftsincident

kan vara ett sådant specifikt fall som avses i artikel 13.2. Den registrerade ska i så fall få information både för att det är fråga om ett specifikt fall och på grund av personuppgiftsincidenten.

Lagrådet föreslår att uttrycket ”i specifika fall” utgår ur lagtexten. Enligt Lagrådet framgår det ändå av bestämmelsen att det rör sig om ett enskilt fall. Alternativt bör uttrycket enligt Lagrådets mening ersättas med ”i ett enskilt fall”. Även *Dataskydd.net* förespråkar att uttrycket ”i specifika fall” utgår ur lagtexten. Regeringen anser inte att uttrycket kan utgå. Det skulle kunna leda till oklarhet om hur bestämmelserna om rätt till information förhåller sig till varandra. Däremot håller regeringen med om att ”i ett enskilt fall” bör användas i stället för ”i specifika fall”. Även om det sistnämnda uttrycket används i direktivet är formuleringen ”i ett enskilt fall” tydligare och därför att föredra.

Vilken information ska lämnas?

Informationen som ska lämnas bör motsvara det som räknas upp i artikel 13.2. Den personuppgiftsansvarige bör således informera om den rättsliga grunden för behandlingen. Den personuppgiftsansvarige bör även informera om vilka kategorier som mottar personuppgifterna. Det bör räcka att ange vilken typ av myndighet som personuppgifterna lämnas ut till, t.ex. socialnämnd eller åklagare. Enligt kommentaren till 26 § personuppgiftslagen, där motsvarande uttryck diskuteras, kan förhållandevis allmän information om mottagare godtas (Öman m.fl. s. 401). Om mottagarkategorin finns i ett tredjeland eller är en internationell organisation bör det anges.

Vidare bör det framgå hur länge personuppgifterna får behandlas. Om det inte är möjligt att fastställa hur länge uppgifterna får behandlas i det enskilda fallet bör i stället kriterierna för att fastställa det anges. Det kan vara upplysningar om vilka omständigheter eller tidpunkter som styr hur länge personuppgifterna får behandlas, t.ex. nedläggning av förundersökning eller att ett visst antal år förflutit efter det att uppgifterna registrerades.

Den personuppgiftsansvarige bör också lämna övrig nödvändig information om behandlingen. Vad som är nödvändig information får bedömas med utgångspunkt i om den registrerade har behov av den för att kunna ta till vara sina rättigheter. Det kan t.ex. vara information om rätten att få del av personuppgifterna och rätten att begära rättelse, radering eller begränsning av behandlingen. Ett annat exempel är information om möjligheten att lämna in klagomål till tillsynsmyndigheten. Vid bedömningen av om sådan övrig information bör lämnas ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap. Det ligger i sakens natur att behovet av information är större om den registrerade inte känner till att hans eller hennes personuppgifter behandlas.

10.2.8 Information som ska lämnas på begäran

Regeringens förslag: Den personuppgiftsansvarige ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av uppgifterna och få viss skriftlig information om behandlingen.

Sökanden behöver inte få del av personuppgifter som han eller hon redan har tagit del av, om det inte begärs. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser att det är tveksamt om undantaget från kravet på att lämna information har stöd i dataskyddsdirektivet. *Umeå universitet* föreslår att tiden för att lämna ut information preciseras till utan onödigt dröjsmål och senast inom en månad från det att den personuppgiftsansvarige har mottagit begäran. Att inte ange någon exakt bortre tidsgräns riskerar enligt universitetet att det skriftliga beskedet i praktiken kommer att dröja länge. Övriga remissinstanser yttrar sig inte om förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 14 ska den registrerade ha rätt att få bekräftelse av den personuppgiftsansvarige om den registrerades personuppgifter behandlas. I så fall ska han eller hon få tillgång till personuppgifterna och viss annan information. Det gäller vilka personuppgifter som behandlas och all tillgänglig information om varifrån de härstammar. Den registrerade ska också få information om ändamålen med behandlingen och dess rättsliga grund, kategorier av personuppgifter, mottagare eller kategorier av mottagare, hur länge uppgifterna får behandlas eller kriterierna för att fastställa det, rätten att begära rättelse, radering eller begränsning av behandlingen och möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Rätten att få del av personuppgifter

För att den enskilde ska kunna hålla sig underrättad om hans eller hennes personuppgifter behandlas och kunna kontrollera om behandlingen utförs författningsenligt bör ramlagen innehålla en bestämmelse som motsvarar artikel 14. Den bör räkna upp de typer av information som anges i artikeln.

Enligt artikel 14 är det den registrerade som har rätt att få tillgång till personuppgifter som rör honom eller henne och information om behandlingen. Det uttrycks på samma sätt i artikel 12 i 1995 års dataskyddsdirektiv. I 26 § personuppgiftslagen har lagstiftaren i stället valt uttrycken ”var och en som ansöker” respektive ”den sökande”. Det är logiskt, eftersom den som begär besked om hans eller hennes personuppgifter behandlas kan få ett nekande svar. Vederbörande kan då inte betecknas som registrerad. Uttrycket ”sökanden” bör därför användas i ramlagen.

Enligt artikel 14 ska den registrerade få tillgång till personuppgifterna som behandlas och viss information om behandlingen. Artikel 15 i dataskyddsförordningen är utformad på motsvarande sätt. I likhet med utredningen anser regeringen att för att syftet med artikel 14 ska uppnås – att den registrerade ska kunna kontrollera om hans eller hennes personuppgifter behandlas författningsenligt – bör han eller hon kunna få del av uppgifterna och inte bara få information om behandlingen. Det bör därför föreskrivas att om uppgifter om sökanden behandlas ska han eller hon få del av dem och få viss skriftlig i paragrafen uppräknad information om behandlingen. Att information och uppgifter behöver lämnas först när den registrerade begär det behandlas i avsnitt 10.2.5. Begränsning av tillgången behandlas i avsnitt 10.3.

Vilka personuppgifter har sökanden rätt att få del av?

Om den personuppgiftsansvarige behandlar personuppgifter om sökanden ska alltså han eller hon få del av uppgifterna. Enligt förarbetena till personuppgiftslagen omfattar skyldigheten bara de behandlade uppgifter som den personuppgiftsansvarige har i behåll när informationen lämnas. Enligt förarbetena finns det inget som hindrar att den personuppgiftsansvarige under tiden från det att ansökan görs till dess att uppgifterna lämnas raderar uppgifterna eller slutar att behandla dem (prop. 1997/98:44 s. 132). Regeringen gör ingen annan bedömning nu. Det är alltså uppgifterna som behandlas vid tiden för utlämnandet som sökanden ska få del av, men samtidigt bör understrykas att det inte är acceptabelt att radera uppgifter som behandlades vid ansökan i syfte att undgå att behöva lämna ut dem.

EU-domstolen har i den s.k. Rijkeboer-domen behandlat frågan om rätten att få tillgång till uppgifter enligt artikel 12 a i 1995 års dataskyddsdirektiv endast avser nutid eller även förfluten tid. Domstolen slog fast att en enskilds rätt att få tillgång till uppgift om vilka personuppgifter som lämnats ut och till vilka mottagare eller mottagarkategorier även avser förfluten tid och innebär en skyldighet för den personuppgiftsansvarige att under viss tid spara sådan information. Enligt domstolen ankommer det på medlemsstaterna att fastställa den tiden, men domstolen uttalade att ett år inte är tillräckligt om det inte visas att en längre lagring av personuppgifterna utgör en orimlig börda för den personuppgiftsansvarige (dom av den 7 maj 2009, Rijkeboer, C-553/07). Av avsnitt 8.2.2 framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. EU-domstolens dom kan, vilket också utredningen menar, inte tolkas så att personuppgifter ska sparas enbart i syfte att vid behov kunna lämnas ut om en registrerad med stöd av reglerna om rätt till information frågar efter dem.

Enligt skäl 43 är det tillräckligt att den registrerade får en komplett sammanfattning av uppgifterna i begripligt format, dvs. ett format som gör det möjligt för den registrerade att få kännedom om uppgifterna och kontrollera att de behandlas korrekt. Det har slagits fast av EU-domstolen i ett mål där fråga var om artikel 12 a i 1995 års dataskyddsdirektiv innebar en skyldighet att till sökanden lämna ut en kopia av ett ansökningsprotokoll som innehöll personuppgifter om sökanden. Domstolen konsta-

terade att artikel 12 a inte innebär en sådan skyldighet, utan att det var tillräckligt att lämna ut en fullständig sammanställning i begriplig form av uppgifterna. Vidare konstaterade domstolen att, för att undvika att sökanden får tillgång till andra upplysningar än de personuppgifter som rör honom eller henne, sökanden kan få en kopia av den ursprungliga handlingen där de övriga upplysningarna har gjorts oläsbara (dom av den 17 juli 2014, YS m.fl., förenade målen C-141/12 och C-372/12). Regleringen i ramlagen bör mot den bakgrunden innebära att en kopia av en handling med de personuppgifter som rör sökanden kan lämnas ut till honom eller henne om det bedöms vara lämpligt, men det bör inte vara någon skyldighet. Om rättigheterna kan säkerställas genom någon annan form av utlämnande, t.ex. en sammanfattning av personuppgifterna, är det tillräckligt.

Vad krävs av den personuppgiftsansvarige?

En viktig fråga är hur långtgående den personuppgiftsansvariges undersökningsplikt bör vara och vad som måste göras för att få fram alla personuppgifter som behandlas om en registrerad. I förarbetena till personuppgiftslagen diskuterades vilka krav 1995 års dataskyddsdirektiv ställer. Regeringens slutsats var då att den personuppgiftsansvarige endast är skyldig att utnyttja alla de sök- och sammanställningsmöjligheter som han eller hon har tillgång till (prop. 1997/98:44 s. 82 f.). Det förarbetsuttalandet måste sättas i sitt historiska sammanhang, där tillgången till datorer och sökmöjligheterna i den samlade verksamheten var begränsade och myndigheterna var betydligt mindre än i dag.

Utgångspunkten är att sökanden ska få tillgång till all information som den personuppgiftsansvarige själv kan få fram om honom eller henne. Det förutsätter att det finns uppgifter som direkt kan hänföras till den person som begär informationen. Sökanden måste lämna sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen. Det kan vara fullständigt namn eller person- eller samordningsnummer eller någon annan lika unik identitet.

Utgångspunkten är att det är tillräckligt att den personuppgiftsansvarige använder de möjligheter till sökning som är tillgängliga och tillåtna i verksamheten. Som utredningen menar är det rimligt att sökningar görs i myndighetens verksamhetsspecifika behandlingssystem, t.ex. dokument- och ärendehanteringssystem, register och databaser. I den mån uppgifter är sökbara i standardprogram som Word, Outlook och Excel bör de också omfattas. Det är däremot inte rimligt att alla anställda i myndigheter med hundratals eller tusentals anställda var och en ska söka efter eventuella personuppgifter på egna lagringsytor vid varje förfrågan från en enskild (jfr avsnitt 9.2.2).

Det kan dock anmärkas att en registrerad genom att utnyttja sin rätt att begära information enligt ramlagen inte i något fall kommer att kunna få en fullständig bild av vilka personuppgifter om honom eller henne som den personuppgiftsansvarige behandlar. Det beror på den tudelning av regelverket för personuppgiftsbehandling som EU:s dataskyddsreform innebär. Den som vänder sig till t.ex. Polismyndigheten med en begäran om att få veta vilka personuppgifter som myndigheten behandlar om

honom eller henne måste därför utnyttja sin rätt till information enligt både dataskyddsförordningen och ramlagen.

Vilken övrig information ska lämnas?

Den registrerade ska också informeras om behandlingen av personuppgifterna. Informationen bör motsvara det som räknas upp i artikel 14. Informationen ska alltså omfatta vilka uppgifter om sökanden som behandlas och varifrån dessa kommer. Information om varifrån personuppgifterna kommer behöver bara avse den information som finns tillgänglig. Sådan information behöver alltså inte sparas i syfte att på begäran kunna lämnas till enskilda. Som utredningen anger bör informationen avse förhållandena vid tidpunkten för utlämnandet.

Enligt artikel 14 ska den registrerade informeras om de kategorier av personuppgifter som behandlingen gäller. Kategorier av personuppgifter kan t.ex. vara adressuppgifter eller fordonsuppgifter. Regeringen anser i likhet med utredningen att kategorier av personuppgifter ingår i det större begreppet personuppgifter som behandlas och därför, på samma sätt som i dag, inte kräver någon särskild reglering. Även behandlingens rättsliga grund bör framgå. Den personuppgiftsansvarige bör vidare informera om ändamålen med behandlingen. Det som avses är ändamålen med behandlingen i det enskilda fallet.

Information om mottagare eller kategorier av mottagare av personuppgifterna bör också lämnas. Med mottagare avses i ramlagen den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision (se avsnitt 6.2). Den personuppgiftsansvarige behöver således inte informera sökanden om att uppgifter har lämnats ut till myndigheter för tillsyn, t.ex. till Justitiekanslern eller Säkerhets- och integritetsskyddsnämnden. Eftersom en myndighet enligt 2 kap. 14 § tryckfrihetsförordningen varken får efterfråga eller dokumentera vilka som tar del av allmänna handlingar med personuppgifter behöver inte heller uppgifter om sådana mottagare lämnas ut (SOU 2015:39 s. 500).

För att uppfylla kravet i direktivet bör det räcka att information om kategorier av mottagare lämnas. Exempel på kategorier av mottagare kan vara åklagare eller domstol. Om mottagaren finns i ett tredjeland eller är en internationell organisation ska det anges.

Vidare bör det framgå hur länge personuppgifterna får behandlas. Om det inte är möjligt att ange hur länge de får behandlas i det enskilda fallet ska i stället kriterierna för att fastställa det anges. Det kan exempelvis vara den föreskrivna tidpunkten i en myndighets registerlagstiftning när de personuppgifter som saken gäller inte längre får behandlas.

Den personuppgiftsansvarige ska även underrätta den registrerade om rätten att begära rättelse, radering eller begränsning av behandlingen och om möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Regeringen instämmer i utredningens uppfattning att det inte i lag bör preciseras vad informationen bör innehålla eller hur den bör lämnas. Det kan göras av regeringen eller den myndighet som regeringen bestämmer.

Att en registrerads rätt till information om vilka personuppgifter om honom eller henne som behandlas inte gäller i den utsträckning person-

uppgifterna inte får lämnas ut behandlas i avsnitt 10.3.1. Personuppgifter i ofärdig text eller som utgör minnesanteckningar behandlas i avsnitt 10.3.3.

När ska informationen lämnas?

Artikel 14 anger inte när en ansökan senast ska besvaras av den personuppgiftsansvarige. Artikel 12.3 reglerar bl.a. skyldigheten för den personuppgiftsansvarige att utan onödigt dröjsmål informera den registrerade om uppföljningen av hans eller hennes begäran om information enligt artikel 14, men inte när informationen ska lämnas. Som framgår av avsnitt 10.5.6 anser regeringen att det inte bör införas någon särskild regel om information om handläggningen. Däremot anser utredningen att den personrelaterade informationen bör lämnas utan onödigt dröjsmål. Enligt *Umeå universitet* bör en bestämd bortre gräns anges i författningstexten så att inte informationslämnandet drar ut på tiden. Angivandet av en bortre gräns skulle dock kunna få motsatt effekt. I stället för att tjäna som en sällan utnyttjad maximigräns finns risk att behöriga myndigheter dröjer med att lämna information eftersom lagstiftningen skulle ge utrymme för det. Mot den bakgrunden, och då direktivet inte kräver att en exakt tidsgräns anges, instämmer regeringen i utredningens förslag.

Det framgår inte heller av artikel 14 hur ofta en enskild har rätt att få information om hur hans eller hennes personuppgifter behandlas. I skäl 43 anges att fysiska personer bör kunna utöva rätten till information med rimliga intervall. Eftersom det i artikel 12.4 bl.a. anges när en personuppgiftsansvarig får vägra att tillmötesgå en begäran om information på grund av att den är återkommande, behandlas frågan i samband med att den artikeln diskuteras (avsnitt 10.3.4).

Bör hanteringen av informationslämnandet underlättas?

Det har både i tidigare lagstiftningsärenden och vid utvärdering av 26 § personuppgiftslagen visat sig att personuppgiftsansvariga upplever det som betungande att lämna information till registrerade enligt paragrafen (se t.ex. Ds 2001:27 s. 65 f. och prop. 2005/06:173 s. 40 f.). För att underlätta de personuppgiftsansvarigas hantering föreslog Personuppgiftslagsutredningen att det skulle införas ett undantag från informationsskyldigheten om det var omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats för den personuppgiftsansvarige att lämna informationen (SOU 2004:6 s. 195 f.). Regeringen valde emellertid att inte genomföra förslaget. I stället begränsades informationsskyldigheten för uppgifter i ostrukturerat material genom att 5 a § personuppgiftslagen infördes (prop. 2005/06:173 s. 40 f. och 49 f.). Direktivet medger inte att informationsskyldigheten begränsas på det sättet. Informationsskyldigheten i ramlagen kommer således att omfatta även personuppgifter i ostrukturerat material, med undantag för personuppgifter i ofärdig löpande text eller som utgör minnesanteckningar (se avsnitt 10.3.3).

Som utredningen påpekar måste hänsyn ändå tas till att informationsskyldigheten i vissa fall kan vara betungande för myndigheterna. Det finns därför skäl att överväga om det finns någon annan möjlighet att underlätta för de personuppgiftsansvariga, utan att det inkräktar på den grundläggande rätten för enskilda att få information om hur deras per-

sonuppgifter behandlas. Rätten till information är nämligen som tidigare nämnts en förutsättning för att enskilda ska kunna kontrollera om behandlingen är författningsenlig och kunna begära rättelse eller radering av uppgifterna.

En möjlighet är att införa en begränsning som motsvarar nuvarande 3 kap. 2 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. Av bestämmelsen följer att uppgift i vissa elektroniska handlingar inte behöver lämnas ut till den registrerade i samband med att myndigheten fullgör sin informationsskyldighet enligt 26 § personuppgiftslagen, om han eller hon redan har tagit del av handlingens innehåll. Undantaget förutsätter att den registrerade får tydlig information om att handlingar som han eller hon har skickat in till eller fått från myndigheten finns registrerade samt att han eller hon får en förteckning över dessa handlingar. Den registrerade har också rätt att få information om uppgift i en sådan handling om han eller hon begär det (prop. 2000/01:33 s. 204). I förarbetena framhålls att förfarandet torde vara tillräckligt för att uppfylla 1995 års dataskyddsdirektivs krav på att den registrerade ska kunna kontrollera om uppgifterna är korrekta eller inte (a. prop. s. 106 f.).

Enligt utredningens uppfattning finns det inga sakliga skäl för att den registrerade ska behöva få del av personuppgifter som han eller hon redan har tagit del av, om uppgifterna inte har förändrats. Regeringen instämmer i den uppfattningen. Det kan t.ex. vara personuppgifter i handlingar som den registrerade själv har skickat in till myndigheten eller som har expedierats till honom eller henne av myndigheten, antingen elektroniskt eller på papper.

Regeringen håller med utredningen om att en ordning där den personuppgiftsansvarige inte behöver lämna ut personuppgifter som den registrerade redan tagit del av skulle bespara myndigheterna onödigt arbete. En bestämmelse som medger att informationen inte behöver omfatta personuppgifter som sökanden redan tagit del av bör därför tas in i ramlagen. I motsats till *Datainspektionen* anser regeringen att det inte råder någon tvekan om att en sådan bestämmelse är förenlig med dataskyddsdirektivet. Enskildas rätt till information är kopplad till att enskilda ska kunna bevaka sina intressen och bl.a. kunna kontrollera om behandlingen är författningsenlig. För att kunna bevaka sina intressen behöver enskilda inte få del av personuppgifter som de redan har tagit del av. För att leva upp till informationsskyldigheten bör dock den personuppgiftsansvarige tydligt ange vilka personuppgifter som behandlas och ge sökanden en förteckning över dem. Den personuppgiftsansvarige bör också lämna sådan övrig information om behandlingen som räknas upp i artikel 14, bl.a. information om rättslig grund, ändamål och mottagare. Om sökanden begär det, bör den personuppgiftsansvarige vara skyldig att låta honom eller henne få del även av personuppgifter som han eller hon tidigare tagit del av.

En förutsättning för att en sådan bestämmelse ska vara godtagbar är dock att den inte begränsar en parts rätt till insyn i mål och ärenden enligt de processrättsliga regelverken. Eftersom ramlagens bestämmelser om rätt till eller begränsning av information inte inverkar på en parts rätt till insyn enligt rättegångsbalken eller andra författningar bedömer regeringen, i likhet med utredningen, att det inte är något problem.

Regeringen återkommer i avsnitt 10.3 till andra undantag från informationsskyldigheten.

10.2.9 Information om automatiserade beslut

Regeringens förslag: Den som har varit föremål för ett automatiserat beslut ska ha rätt att på begäran få närmare information om beslutet av den personuppgiftsansvarige.

Utredningens förslag överensstämmer i sak med regeringens. Enligt utredningens formulering av lagtexten har dock den som varit föremål för ett automatiserat beslut endast rätt att begära närmare information om beslutet.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* anser att det bör övervägas att i bestämmelsen uttryckligen inte bara reglera en rätt att begära information utan också en rätt att få information.

Skälen för regeringens förslag: I artikel 11 regleras automatiserade beslut. Som anges i avsnitt 8.3 förekommer det i dag inga automatiserade beslut inom ramlagens tillämpningsområde, men regeringen föreslår ändå en bestämmelse om sådana beslut. Det innebär att det också bör tas in en bestämmelse i ramlagen om den information som den personuppgiftsansvarige är skyldig att på begäran lämna vid sådana beslut. Som *Säkerhets- och integritetsskyddsnämnden* påpekar bör det av bestämmelsen framgå att den enskilde inte bara har rätt att begära information, utan också rätt att få information av den personuppgiftsansvarige. Säkerhets- och integritetsskyddsnämnden väcker även frågan om rätten till information enligt bestämmelsen bör kunna begränsas med stöd av den bestämmelse som föreslås i avsnitt 10.3.1. Enligt regeringen bör rätten att få närmare information om automatiserade beslut inte gå att begränsa med stöd av den bestämmelse som föreslås i avsnitt 10.3.1.

10.3 Begränsning av rätten till information

10.3.1 Rätten till information får begränsas

Regeringens förslag: Skyldigheten att lämna personrelaterad information ska inte gälla i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning, att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans rättigheter och friheter skyddas.

Om det finns grund för att begränsa informationen ska den personuppgiftsansvarige inte heller vara skyldig att lämna ut skälen för be-

slut att begränsa informationen eller för beslut i fråga om begäran om rättelse, radering eller begränsning av behandlingen.

Om den personuppgiftsansvarige inte är en myndighet ska undantagen från informationsskyldigheten gälla även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Kammarrätten i Göteborg* föreslår att hänvisningen till de olika intressena utesluts alternativt att en hänvisning till ramlagen förs in i offentlighets- och sekretesslagen (2009:400), eftersom ramlagen ska vara subsidiär i förhållande till andra lagar och förordningar och offentlighets- och sekretesslagen således ska tillämpas i sin helhet. Övriga remissinstanser yttrar sig inte särskilt om förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Direktivet ger möjlighet att i nationell rätt begränsa den registrerades rätt till information om personuppgiftsbehandling som avser honom eller henne. Det framgår dels av artikel 13.3 som ger möjlighet att senarelägga, begränsa eller utelämna sådan information som den personuppgiftsansvarige ska lämna enligt artikel 13.2, dels av artikel 15.1 som ger möjlighet att begränsa den registrerades rätt till sådan information som avser behandling av hans eller hennes personuppgifter som den personuppgiftsansvarige ska lämna på begäran. I artikel 16.4 ges möjlighet att begränsa information till den registrerade om skälen för att den personuppgiftsansvarige inte har rättat, raderat eller begränsat behandlingen.

Syftet med att begränsa informationen ska enligt direktivet vara att undvika att officiella eller rättsliga utredningar, förundersökningar eller förfaranden hindras eller att undvika menlig inverkan på brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder och att skydda allmän eller nationell säkerhet eller andra personers rättigheter och friheter. Begränsning får vidtas endast i den utsträckning och så länge som den är nödvändig och proportionerlig. Vid bedömningen ska hänsyn tas till den berörda fysiska personens grundläggande rättigheter och berättigade intressen.

Nuvarande reglering

Enligt artikel 13.1 i 1995 års dataskyddsdirektiv får medlemsstaterna genom lagstiftning begränsa omfattningen av vissa skyldigheter och rättigheter som följer av direktivet. En sådan begränsning ska vara en nödvändig åtgärd med hänsyn till bl.a. statens säkerhet, allmän säkerhet, förebyggande, undersökning, avslöjande av brott eller åtal för brott och skydd av den registrerades eller andras fri- och rättigheter. Artikeln har åberopats till stöd för bl.a. undantaget i 27 § personuppgiftslagen från skyldigheten att lämna information enligt 23–26 §§ personuppgiftslagen till den registrerade vid sekretess och tystnadsplikt. Enligt förarbetena får bestämmelsen anses vara uppställd till skydd för sådana fri- och rättigheter som avses i artikel 13.1 g i 1995 års direktiv (prop. 1997/98:44 s. 84).

Vid en översyn av personuppgiftslagen åberopades artikel 13.1 även till stöd för en bestämmelse om delegation till regeringen. Enligt 8 a § personuppgiftslagen får regeringen meddela föreskrifter om undantag bl.a. från bestämmelserna om information till den registrerade i 23–26 §§, om det behövs med hänsyn till bl.a. rikets säkerhet, allmän säkerhet, förebyggande, undersökning eller avslöjande av brott, åtal för brott och skyddet av fri- och rättigheter.

Hur bör artiklarna om begränsning av information genomföras?

Bestämmelser som begränsar rätten till information är nödvändiga för att de behöriga myndigheterna ska kunna utföra sina uppdrag på ett effektivt sätt. Artiklarna 13.3, 15.1 och 16.4 ger möjlighet att begränsa rätten till information.

I förarbetena till 8 a § personuppgiftslagen diskuterades om undantagen i artikel 13.1 i 1995 års direktiv borde införas direkt i personuppgiftslagen. Regeringen ansåg att undantagen var alltför generella och vaga för att kunna ligga till grund för reglering. Bedömningen av om ett sådant undantag är tillämpligt borde enligt förarbetena inte göras av varje enskild personuppgiftsansvarig. Som huvudregel borde undantagsbestämmelser tas in i särlagstiftning med bestämmelser som avviker från personuppgiftslagen. I vissa fall krävs dock undantag och då behövs en möjlighet för regeringen att föreskriva om undantag, t.ex. i avvaktan på att särlagstiftning hinner utarbetas eller ändras (prop. 2005/06:173 s. 55 f.).

Förarbetsuttalandena är av intresse för hur artiklarna 13.3, 15.1 och 16.4 ska genomföras. De undantag som görs i artiklarna är lika generella och vaga som motsvarande bestämmelser i 1995 års direktiv. Regeringen håller med utredningen om att det därför inte är lämpligt att personuppgiftsansvariga med det som enda utgångspunkt avgör om det i ett enskilt fall kan finnas skäl för att begränsa informationen. Undantagen bör preciseras i lag eller förordning.

Begränsning av information enligt artiklarna 13.3, 15.1 och 16.4 får bara göras i syfte att undvika att förundersökningar eller andra rättsliga utredningar, brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder hindras eller i syfte att skydda allmän eller nationell säkerhet eller andra personers rättigheter och friheter.

Bestämmelser till skydd för bl.a. dessa intressen finns redan i offentlighets- och sekretesslagen och i vissa andra författningar. På samma sätt som i 27 § personuppgiftslagen bör möjligheten att begränsa information enligt ramlagen utgå från den regleringen. I ramlagen bör det tas in en regel om att den registrerades rätt till information inte gäller om det är särskilt föreskrivet att personuppgifterna inte får lämnas ut av hänsyn till något av de intressen som nyss nämnts. I likhet med utredningen anser regeringen att det inte finns något behov av en bestämmelse motsvarande 8 a § personuppgiftslagen.

Det är, som framgår av avsnitt 10.2.1, viktigt att hålla isär reglerna om rätt till information och tillgång till allmänna handlingar.

Syftet med reglerna i tryckfrihetsförordningen är att ge var och en insyn i den offentliga verksamheten, dvs. att skapa en möjlighet för alla, inte specifikt en viss person, att kunna ta del av handlingar och uppgifter som rör en viss fråga. Sekretessregleringen syftar till att värna viktiga intressen, bl.a. det allmännas intresse av brottsbekämpning, lagföring och straffverkställighet. Sekretess värnar också enskildas intresse av att känsliga uppgifter om deras personliga eller ekonomiska förhållanden inte sprids. De i sig mycket komplexa regelverken om tillgång till handlingar och begränsningen av rätten att ta del av dem har ett annat fokus än lagstiftningen om personuppgiftsbehandling.

Även om det i dag finns en koppling mellan de båda regelsystemen genom att 27 § personuppgiftslagen knyter an till regleringen i offentlighets- och sekretesslagen, kan det ifrågasättas om det har varit lagstiftarens avsikt att en begäran om personrelaterad information ska resultera i en formell prövning av om sekretessbelagda handlingar eller uppgifter ska kunna lämnas ut till personen i fråga.

Beslut att inte lämna ut personrelaterad information får överklagas enligt 52 § personuppgiftslagen. I ett mål där klaganden hade nekats att få personrelaterad information prövade Högsta förvaltningsdomstolen vilken överklagandebestämmelse som skulle tillämpas när beslutet hade motiverats med att det gällde sekretess enligt 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen. Domstolen fann att den ordning som gäller för överklagande i 6 kap. samma lag skulle tillämpas med motiveringen att i den utsträckning det gäller sekretess för personrelaterad information gäller inte den ordning för överklagande som föreskrivs i personuppgiftslagen (HFD 2014 ref. 55). Med den tolkning som gjorts i det målet väcks frågan om bestämmelsen i 52 § personuppgiftslagen angående överklagande av ett beslut enligt 26 § samma lag har någon funktion att fylla, vid sidan av de fall där den personuppgiftsansvarige inte lämnar ut uppgifterna inom de tidsfrister som anges i paragrafen eller inte lämnar ut uppgifter i text som inte har färdigställts. Det kan ifrågasättas om avsikten varit att överklagandebestämmelsen skulle ha ett så begränsat tillämpningsområde. Förekomsten av en särskild överklagandebestämmelse i personuppgiftslagen talar i stället för att den prövning som görs vid en begäran enligt 26 § inte är en formell sekretessprövning enligt offentlighets- och sekretesslagen. Det är snarare en annan typ av prövning där det materiella innehållet i sekretessreglerna är avgörande för resultatet men prövningen inte innefattar samma moment. Regeringen instämmer i utredningens bedömning att det inte är rimligt att likställa prövningen av om personrelaterad information kan lämnas ut med en prövning enligt offentlighets- och sekretesslagen.

Bestämmelserna som ger enskilda rätt till information om huruvida deras personuppgifter behandlas skapades i en annan tid, då behandlingen av personuppgifter fortfarande till stor del ägde rum i enskilda register. I avgränsade register är möjligheterna att överblicka informationen och att snabbt få bekräftat om uppgifter om en viss person behandlas betydligt större än i dagens automatiserade behandlingssystem. I de sist-

nämnda kan det finnas mycket stora mängder av information som i och för sig är sökbar men där det inte går att lika enkelt överblicka i vilket sammanhang personuppgifterna förekommer. Som utredningen påpekar medför det att bestämmelser om rätt till personrelaterad information delvis måste ses i ett annat ljus än tidigare, trots att direktivet utgår från samma synsätt som dataskyddsdirektivet från år 1995.

Rätten till personrelaterad information ger enligt regeringen inte den registrerade någon rätt att få del av annat än information om just behandlingen av personuppgifterna. Det handlar alltså inte om att pröva om den registrerade ska kunna få tillgång till all den information som finns i ett visst mål eller ärende. I stället ska det prövas om det förhållandet att personuppgifter behandlas i ett visst sammanhang – t.ex. i underrättelseverksamhet eller i förundersökningen om ett visst brott – kan avslöjas för den registrerade. Det förhållandet att det avslöjas att personuppgifterna behandlas kan i ett enskilt fall riskera att hindra underrättelseverksamheten eller förundersökningen i fråga och då bör informationen kunna begränsas. En sådan prövning kräver inte lika ingående överväganden som när det gäller att ta ställning till om en viss handling som innehåller sekretessbelagd information kan lämnas ut helt eller delvis utan att det vållar förundersökningen eller underrättelseverksamheten skada. Det innebär t.ex. att om en viss person pekas ut som gärningsman i en polisanmälan och det gäller sekretess för den uppgiften kommer personen i fråga – om han eller hon vänder sig till Polismyndigheten och begär besked om vilka personuppgifter som behandlas – inte att få någon upplysning om polisanmälan. Ett sådant beslut får enligt regeringens förslag överklagas enligt ramlagens regler (se avsnitt 13.4).

En begäran om att få besked om personuppgifter behandlas ska alltså besvaras utifrån regelverket om skydd för personuppgifter. I den prövningen ingår inte att ta ställning till om uppgifterna finns i en allmän handling och om den kan lämnas ut. Det finns givetvis inget som hindrar att en behörig myndighet gör en formell prövning enligt offentlighets- och sekretesslagen när den registrerade begär att få personrelaterad information. Om det görs och myndigheten i sitt beslut att inte lämna information motiverar det med att det gäller sekretess enligt någon eller några bestämmelser i offentlighets- och sekretesslagen, ska beslutet överklagas enligt de särskilda reglerna i den lagen (HFD 2014 ref. 55).

Mot denna bakgrund anser regeringen att hänvisningen till de olika intressena i den bestämmelse som nu föreslås inte bör uteslutas, som *Kammarrätten i Göteborg* föreslår. Hänvisningen till de olika intressena tydliggör att det är den nu föreslagna bestämmelsen som ska tillämpas vid prövningen av om personrelaterad information kan lämnas ut och att det inte är fråga om någon formell prövning enligt offentlighets- och sekretesslagen.

Eftersom ramlagen även kommer att vara tillämplig på andra aktörer än myndigheter bör även dessa kunna underlåta att lämna information till registrerade om behandlingen av deras personuppgifter (jfr 27 § andra meningen personuppgiftslagen och prop. 2017/18:105 sid. 103 f.).

Vilken typ av information får begränsas?

Frågan är vilken information som undantaget bör omfatta. Att den personuppgiftsansvarige ska ha rätt att begränsa eller inte lämna ut personrelaterad information står klart. Det gäller både information som ska lämnas självmant och på begäran. Det finns även behov av att kunna begränsa underrättelser om skälen för beslut i fråga om rättelse, radering eller begränsning av behandlingen. Om skälen skulle riskera att röja information som hänför sig till något av nyss nämnda intressen, t.ex. att rymning från ett fängelse planeras eller att hemlig avlyssning av elektronisk kommunikation pågår, bör underrättelsen till den registrerade kunna begränsas. Om så inte var fallet skulle enskilda kunna begära rättelse och därigenom få del av information som annars inte skulle lämnas ut.

I avsnitt 10.5.7 och 10.5.8 behandlas de formella kraven på besluten.

Rätten till kontroll när information inte har lämnats eller begränsats

För att den registrerade ska kunna ta till vara sina rättigheter när information inte har lämnats ut eller begränsats på grund av de intressen som anges i artiklarna 13.3, 15.1 och 16.4, föreskrivs i artikel 17.1 att tillsynsmyndigheten på den enskildes vägnar ska kunna kontrollera om personuppgifterna behandlas författningsenligt. Enskilda som har vänt sig till den personuppgiftsansvarige med en begäran om att få personrelaterad information eller att en korrigeringsåtgärd ska vidtas ska kunna vända sig till tillsynsmyndigheten med en begäran om kontroll. Kontrollerna behandlas i avsnitt 11.6.3.

10.3.2 Kategorier av behandling

Regeringens bedömning: Möjligheten att fastställa kategorier av behandling som undantas från enskildas rätt till information bör inte utnyttjas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om bedömningen.

Skälen för regeringens bedömning: Av artiklarna 13.4 och 15.2 framgår att det är möjligt att fastställa kategorier av behandling som helt eller delvis kan omfattas av möjligheten att begränsa enskildas rätt till information enligt artiklarna 13.3 respektive 15.1. Det är oklart vad som avses med uttrycket ”kategori av behandling”. Enligt utredningens mening skulle det kunna vara behandling av personuppgifter i ett visst register. Det skulle också, enligt utredningen, kunna vara fråga om behandling av en viss typ av personuppgifter, exempelvis dna-profiler, fordonsuppgifter eller fotografier. Regeringen har ingen annan uppfattning.

Sekretessen varierar under de olika stadierna av brottsbekämpning, lagföring och straffverkställighet. Normalt avklingar sekretessen till skydd för det allmänna ju längre utredningen når. En personuppgift som är föremål för sekretess eller tystnadsplikt under förundersökningen kan bli offentlig vid åtalet, under domstolsförhandlingen eller i domen. Det kan gälla allt från underrättelseinformation och uppgifter om hemliga tvångsmedel till uppgifter om hälsa eller andra känsliga personuppgifter. Ett

undantag för kategorier av behandling kan därför inte vara generellt utan måste anpassas till den sekretess som kan gälla i de olika behöriga myndigheternas verksamhet.

Det är framför allt i verksamheter där det förekommer många sekretessbelagda uppgifter som det skulle vara av intresse att peka ut sådana kategorier av behandling. De brottsbekämpande myndigheternas personuppgiftsbehandling utförs numera i liten utsträckning i särskilda register. Uppgifterna är i stället gemensamt tillgängliga i myndigheternas verksamhetsstöd. Det gör att det är svårt att peka ut en viss kategori av behandling som i sin helhet kan undantas. För de register som är specialreglerade, som Polismyndighetens dna- och fingeravtrycksregister, finns det som regel särskilda sekretessbestämmelser, vilket skulle göra att undantag för de kategorierna får begränsat värde. En kategori kan som utredningen anger bara undantas om det är rättsligt möjligt att avgränsa den. När det t.ex. gäller underrättelseuppgifter håller regeringen med utredningen om att det inte är möjligt att göra det, eftersom underrättelseverksamheten inte är reglerad och uppgifterna inte heller behandlas i särskilt reglerade register.

10.3.3 Ofärdig text och minnesanteckningar

Regeringens förslag: Rätten att få del av personrelaterad information ska inte gälla personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten ska dock gälla om uppgifterna

1. har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för vetenskapliga, statistiska eller historiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Tredje man ska definieras som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen föreslår att informationsskyldigheten ska gälla när uppgifterna har lämnats ut till myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Enligt utredningens förslag ska det även följa av bestämmelsen att informationsskyldigheten gäller om uppgifterna behandlas enbart för arkivändamål av allmänt intresse.

Remissinstanserna: *Uppsala universitet* efterfrågar ett förtydligande av från vilken tidpunkt ettårsfristen ska beräknas. *Säkerhets- och integritetsskyddsnämnden* påpekar att definitionen av tredje man inte undantar myndigheter som utövar tillsyn, kontroll eller revision.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Som framgår av avsnitt 10.3.1 ger artikel 15.1 möjlighet att begränsa den registrerades rätt till information i syfte att skydda rättigheter och friheter. En motsvarande regel finns i artikel 13.1 g i 1995 års dataskyddsdirektiv. I förarbetena till personuppgiftslagen hänvisade regeringen till skyddet för fri- och rättigheter som motiv för att införa begränsningen av informationsskyldigheten i 26 § tredje stycket personuppgiftslagen (prop. 1997/98:44 s. 83). Undantaget gäller för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran om information gjordes eller som utgör minnesanteckning eller liknande. Om uppgifterna redan har lämnats ut till tredje man eller om uppgifterna i den löpande texten ännu inte fått sin slutliga utformning efter ett års behandling, gäller inte undantaget. Det gäller inte heller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål.

Undantag för vissa typer av text

Att enskilda inte har någon rätt till insyn i utkast och koncept till skrivelser, beslut och domar under den tid som arbetet pågår värnar myndigheternas verksamhet och skyddar andra enskilda. Av samma skäl är minnesanteckningar eller liknande, t.ex. promemorior eller andra anteckningar som används under handläggningen, fredade från insyn så länge handläggningen pågår.

Utkast under arbete eller minnesanteckningar som inte ska bevaras för framtiden är inte allmänna handlingar enligt 2 kap. tryckfrihetsförordningen och lämnas därmed inte ut enligt offentlighetsprincipen. Det finns därför goda skäl att inte ge en sökande rätt till information om hur hans eller hennes personuppgifter behandlas i ofärdiga texter och minnesanteckningar. Ett undantag för sådan text bör därför tas in i ramlagen.

Artikel 15.1 e medger undantag från rätten till information för att skydda andra personers rättigheter och friheter. En begränsning enligt artikel 15.1 får dock endast göras i den utsträckning och så länge som den är nödvändig och proportionerlig. Vid bedömningen ska hänsyn tas till den berörda personens grundläggande rättigheter och berättigade intressen. Undantaget för handlingar som inte är färdigställda är av stor praktisk betydelse för myndigheterna. Det är också en förutsättning för ett fungerande rättsväsende – och för tilltron till det – att information om enskilda inte lämnas ut innan beslut och domar är färdigställda och meddelade, särskilt som de ofta innehåller personuppgifter om andra. I likhet med utredningen anser regeringen därför att en sådan begränsning – som har sin motsvarighet i 26 § tredje stycket personuppgiftslagen – är nödvändig.

När det gäller kravet på proportionalitet instämmer regeringen i följande överväganden som utredningen gör. Om personuppgifterna i utkasten har behandlats under längre tid än ett år utan att texten färdigställts väger den registrerades intresse av att kunna ta del av hur personuppgifterna behandlas tyngre än den personuppgiftsansvariges intresse av att fortsätta att behandla personuppgifterna utan insyn. Information om personuppgifterna bör därför lämnas till den registrerade, om inte den personuppgiftsansvarige väljer att i stället radera personuppgifterna i den

ofärdiga texten (jfr prop. 1997/98:44 s. 83 f.). Med anledning av *Uppsala universitets* förfrågan om ettårsfristen kan tydliggöras att om personuppgifterna har behandlats i utkastet under längre tid än ett år, räknat bakåt från den tidpunkt då begäran om information gjordes, så gäller inte undantaget för uppgifter i löpande text som inte fått sin slutliga utformning.

Om ett utkast eller en minnesanteckning endast används vid statistikproduktion eller för vetenskapliga eller historiska ändamål inom ramlagens tillämpningsområde bör information om personuppgiftsbehandlingen kunna lämnas. Undantaget bör därför inte gälla för personuppgifter i ofärdiga texter eller minnesanteckningar som enbart behandlas för vetenskapliga, statistiska eller historiska ändamål för de syften som omfattas av ramlagen. Som utredningen föreslår bör undantaget inte heller gälla för personuppgifter i utkast eller minnesanteckningar som enbart behandlas för arkivändamål av allmänt intresse. Till skillnad från utredningen anser regeringen dock inte att det behöver framgå av bestämmelsen i ramlagen. Som anges i avsnitt 8.2.2 faller behandling av personuppgifter för arkivändamål in under dataskyddsförordningen. Att personuppgifter i arkiverade utkast eller minnesanteckningar bör kunna lämnas ut följer av förslaget till en ny dataskyddslag (prop. 2017/18:105 s. 103 f).

Information bör också lämnas om uppgifterna i den ofärdiga texten eller minnesanteckningen har lämnats ut till tredje man. Information bör dock få lämnas till dataskyddsombud, personuppgiftsbiträden och andra personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar behandlar personuppgifter, utan att undantaget upphör att gälla (jfr 26 § tredje stycket andra meningen jämfört med 3 § personuppgiftslagen). För att det ska bli tydligt bör tredje man definieras i ramlagen som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Som *Säkerhets- och integritetsskyddsnämnden* påpekar bör information även få lämnas till myndigheter som utövar tillsyn, kontroll eller revision utan att undantaget upphör att gälla. Enligt regeringen bör det framgå tydligt av lagtexten.

Det bör alltså tas in en regel i ramlagen om att information bör lämnas om uppgifter i ofärdig text eller minnesanteckningar har lämnats ut till tredje man, med undantag för myndighet som med stöd av författning utövar tillsyn, kontroll eller revision, om uppgifterna behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller om uppgifterna har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning. Begränsningen av den registrerades rätt till information i ofärdiga texter och minnesanteckningar är då enligt regeringen såväl nödvändig som proportionerlig.

Ett beslut om att begränsa tillgången till denna typ av information får enligt regeringens förslag överklagas till allmän förvaltningsdomstol (se avsnitt 13.4).

10.3.4 Orimliga eller uppenbart ogrundade framställningar

Regeringens förslag: Om en begäran om personrelaterad information är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Om någon begär sådan information eller sådana uppgifter oftare än en gång per år, får den personuppgiftsansvarige ta ut en rimlig avgift eller avslå begäran.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Norrköpings kommun* ser framtida utmaningar i form av ett ökat antal framställningar om att få del av personrelaterad information och tillstyrker därför förslaget. *Datainspektionen* delar inte utredningens bedömning att en begäran om information kan anses orimlig på den grunden att den avser en större myndighets hela verksamhet. *Umeå tingsrätt* anser att avslagsgrunderna bör tydliggöras. Enligt tingsrätten ger det inte mycket ledning för beslutet att som avslagskriterium ange att en begäran är orimlig. Tingsrätten ifrågasätter också varför det måste vara uppenbart att ansökan är ogrundad. Övriga remissinstanser har inget att invända mot förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Om en registrerads begäran om information är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får den personuppgiftsansvarige enligt artikel 12.4 antingen ta ut en rimlig avgift för de administrativa kostnaderna för att tillhandahålla informationen eller vägra att tillmötesgå begäran. Den personuppgiftsansvarige har bevisbördan för att en begäran är uppenbart ogrundad eller orimlig.

En begäran som är orimlig eller uppenbart ogrundad ska avslås

Av skäl 40 framgår att en begäran om information kan vara orimlig om en sökande utan skäl och vid upprepade tillfällen begär uppgifter och uppenbart ogrundad om en sökande missbrukar sin rätt till information genom att exempelvis lämna felaktiga eller missvisande uppgifter i sin begäran. Regeringen håller med utredningen om att en begäran också kan vara orimlig om sökanden inte lämnar sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen utan ytterligare efterforskningar.

Andra omständigheter som enligt utredningen kan göra att en begäran anses vara orimlig är att den är så oprecis att det skulle vara närmast omöjligt att besvara den. Det kan enligt utredningen vara fallet t.ex. om begäran avser en större myndighets hela verksamhet, särskilt om myndigheten har många olika arbetsuppgifter. Utredningen menar att begäran i sådana fall normalt bör kunna preciseras till viss verksamhet, visst ärende eller någon annan liknande avgränsning. Till skillnad från *Datainspektionen* instämmer regeringen i utredningens överväganden i denna del. Det är av stor praktisk betydelse att myndigheterna inte åläggs att

besvara framställningar som är så obegränsade att det i princip är omöjligt att besvara dem.

Regeringen håller också med utredningen om att en myndighet aldrig bör vara skyldig att tillgodose en begäran om information som är uppenbart ogrundad. Detsamma bör gälla en begäran som är orimlig av något annat skäl än att den är repetitiv, dvs. återkommande. Möjligheten att mot avgift besvara en begäran som är uppenbart ogrundad eller orimlig på annat sätt än att den är återkommande, bör därför inte utnyttjas. I stället bör begäran om information avslås. En bestämmelse om det bör tas in i ramlagen. *Umeå tingsrätt* anser att lagtexten bör innehålla tydligare avslagsgrunder än uppenbart ogrundad eller orimlig. Mot bakgrund av att formuleringen ”uppenbart ogrundad eller orimlig” används i direktivet, vilket även tingsrätten konstaterar, anser regeringen att den formuleringen bör användas i ramlagens bestämmelse. Avslagskriterierna enligt ramlagen kommer då också att överensstämma med de som anges i artikel 12.5 i dataskyddsförordningen. Närmare ledning för hur uttrycket ”uppenbart ogrundad eller orimlig” ska tolkas får utvecklas i rättstillämpningen.

Upprepad begäran kan besvaras mot avgift eller avslås

En begäran om information som är orimlig på grund av att den återupprepas kan antingen besvaras mot avgift eller avslås. Utgångspunkten bör vara att den personuppgiftsansvarige i första hand tar ut en rimlig avgift för de kostnader som begäran förorsakar och i andra hand vägrar att lämna den begärda informationen. Om en myndighet avser att ta ut avgift för informationen bör den först underrätta sökanden om det och förhöra sig om han eller hon vidhåller sin begäran.

Frågan är hur ofta det är rimligt att sökanden ska kunna få information utan att betala avgift för det. I dag har den registrerade enligt 26 § personuppgiftslagen rätt till gratis information om behandlingen av hans eller hennes personuppgifter högst en gång per kalenderår. Paragrafen genomför artikel 12 a i 1995 års dataskyddsdirektiv, som föreskriver att den registrerade med rimliga intervall ska få viss information. Samma uttryck finns i skäl 43 i direktivet, där det framgår att fysiska personer med rimliga intervall bör ha rätt att få tillgång till insamlade uppgifter som rör dem för att kunna kontrollera att behandlingen är laglig.

I likhet med utredningen anser regeringen att dagens ordning med avgiftsfri information en gång per år tillgodoser den enskildes rätt att med rimliga intervall hålla sig underrättad om hans eller hennes personuppgifter behandlas och om behandlingen är författningsenlig. Tidsintervallet är samtidigt anpassat så att den personuppgiftsansvariges arbetsinsats inte blir orimligt betungande. Om information begärs oftare än en gång per år kan det däremot anses som orimligt på grund av att begäran är återkommande. En bestämmelse om att den personuppgiftsansvarige i dessa fall får ta ut rimlig avgift eller avslå begäran bör därför tas in i ramlagen. Det ger den enskilde möjlighet att begära information så ofta han eller hon önskar, men tvingar inte den personuppgiftsansvarige att behandla alla framställningar på samma sätt. Den personuppgiftsansvarige får med utgångspunkt i begäran avgöra om den ska besvaras mot avgift eller avslås. Närmare anvisningar för vad som gäller i fråga om avgifter bör kunna

meddelas av regeringen eller den myndighet som regeringen bestämmer. Vad som kan vara en rimlig avgift för att lämna information kan regleras t.ex. i avgiftsförordningen (1992:191).

Regeringen återkommer i avsnitt 10.5.7 och 10.5.8 till de formella kraven på besluten.

10.4 Rättelse, radering och begränsning av behandlingen

10.4.1 Rätten till rättelse och komplettering

Regeringens förslag: Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Den enda remissinstans som yttrar sig om förslaget är *Kriminalvården* som efterfrågar en utvecklad beskrivning av vilka krav som bör ställas på den personuppgiftsansvariges utredning kring personuppgifternas korrekthet.

Skälen för regeringens förslag

Innehållet i direktivet

Artikel 16.1 reglerar den registrerades rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade och – med beaktande av ändamålet med behandlingen – att få ofullständiga personuppgifter kompletterade. Enligt skäl 47 ska särskilt felaktiga faktauppgifter rättas. Rätten gäller oberoende av det grundläggande kravet i artikel 4.1 d att den personuppgiftsansvarige på eget initiativ ska rätta felaktiga personuppgifter.

Nuvarande reglering

I personuppgiftslagen finns det både en regel om skyldigheten för den personuppgiftsansvarige att självmant rätta felaktiga personuppgifter och en regel om rätten för den registrerade att begära rättelse. Enligt 28 § personuppgiftslagen, som genomför artikel 12 b i 1995 års dataskyddsdirektiv, är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen.

Det finns även regler om rättelse i förvaltningslagen, förvaltningsprocesslagen samt 30 kap. 13 § och 48 kap. 12 a § rättegångsbalken. Reglerna om rättelse i förvaltningslagen och de processrättsliga regelverken medför emellertid, till skillnad från regeln om rättelse i personuppgiftslagen, ingen skyldighet för myndigheten att rätta eller någon rätt för enskilda att begära rättelse. Reglerna gäller dessutom enbart rättelse av uppgifter i beslut och domar eller motsvarande (jfr SOU 2015:39 s. 564 f. och 569 f.).

Att de personuppgifter som behandlas är korrekta är av grundläggande betydelse både för myndigheternas verksamhet och för enskilda. I ramlagen bör det därför finnas en regel om rätt för den registrerade att begära rättelse. Skyldigheten för den personuppgiftsansvarige att självmant vidta åtgärder när det upptäcks att personuppgifter är felaktiga, ofullständiga eller inaktuella behandlas i avsnitt 8.1.6. Här diskuteras således enbart rätten för registrerade att begära att den personuppgiftsansvarige rättar felaktiga eller ofullständiga uppgifter.

Om en registrerad har begärt att få en ofullständig uppgift kompletterad ska han eller hon enligt direktivet ha rätt att lämna en kompletterande inlaga. Regeringen håller med utredningen om att det är oklart vad bestämmelsen syftar på. En möjlig tolkning är att den registrerade ska ha rätt att ge in en skrivelse till den personuppgiftsansvarige där den registrerade utvecklar skälen för begäran. Den rätten följer redan av förvaltningslagen och de processrättsliga regelverken och behöver därför inte regleras.

Den personuppgiftsansvarige ska enligt direktivet vidta den begärda åtgärden utan onödigt dröjsmål. Regeringen instämmer i utredningens ställningstagande att den personuppgiftsansvarige skyndsamt bör utreda frågan och, om det är motiverat, så fort som möjligt genomföra rättelse eller korrigering. Den personuppgiftsansvarige får således inte av bekvämlighetsskäl vänta med att rätta och korrigera uppgifter till dess att de ändå ska uppdateras, om det är möjligt att göra det tidigare (jfr Öman m.fl. s. 417). *Kriminalvården* efterfrågar en närmare beskrivning av vilka krav som bör ställas på den personuppgiftsansvariges utredning kring personuppgifters korrekthet. Enligt regeringen är det svårt att uppställa några generella krav på utredningen. Den information som finns tillgänglig för den personuppgiftsansvarige, bl.a. den information som framgår av begäran om rättelse, bör tas i beaktande, men vilka utredningsåtgärder som i övrigt bör vidtas får bedömas i varje enskilt fall.

Felaktiga och ofullständiga uppgifter

I avsnitt 8.1.2 diskuteras vad som avses med att en personuppgift är korrekt. Att en felaktig eller ofullständig personuppgift rättas eller kompletteras kan innebära att den ersätts av en annan uppgift som är korrekt ur ett objektivt perspektiv eller kompletteras med en uppgift om de rätta förhållandena så att den blir fullständig i objektiv mening. Det kan vara fråga om t.ex. ett felaktigt namn eller att endast delar av ett namn har återgetts i en handling. Det kan även vara fråga om något fel som uppstått på grund av ett tekniskt förfarande. Det ska alltså röra sig om ett fel eller en ofullständighet på grund av något som inte bygger på en bedömning.

I ramlagen bör det regleras att den personuppgiftsansvarige på begäran ska rätta eller komplettera personuppgifter som rör den registrerade om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Att den personuppgiftsansvarige ska ta hänsyn till ändamålet med behandlingen vid bedömningen av om felaktiga personuppgifter ska rättas framgår av artikel 4.1 d. Det är dessutom en nödvändig del av prövningen av om en personuppgift är felaktig.

Den registrerade bör inte ges rätt att kräva att den personuppgiftsansvarige rättar inaktuella uppgifter. Rätten till rättelse i artikel 16.1 omfattar nämligen inte inaktuella uppgifter. Däremot är den personuppgiftsansvarige skyldig att – om det är nödvändigt – självmant uppdatera uppgifter som är inaktuella (se avsnitt 8.1.6).

En felaktig uppgift kan också rättas på det sättet att den tas bort utan att ersättas. Om en uppgift om en person har antecknats felaktigt i ett register, t.ex. om förväxling med en annan person har lett till en felaktig anteckning i misstankeregistret eller belastningsregistret, ska uppgiften rättas genom att den tas bort från registret (jfr JO:s kritik mot bl.a. Säkerhetspolisen för passivitet i ett ärende om rättelse av uppgifter i belastningsregistret i JO 2007/08 s. 67).

10.4.2 Rätten till radering

Regeringens förslag: På begäran av den registrerade ska den personuppgiftsansvarige utan onödigt dröjsmål radera personuppgifter som rör honom eller henne om de behandlas på otillåtet sätt. Detsamma gäller om det krävs radering för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Den enda remissinstans som kommenterar förslaget är *Justitiekanslern* som anser att det är oklart vad som avses med att personuppgifter ska raderas om det krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt artikel 16.2 har den registrerade rätt att begära att den personuppgiftsansvarige utan onödigt dröjsmål raderar personuppgifter som rör den registrerade dels om behandlingen står i strid med de bestämmelser som antas enligt artiklarna 4, 8 och 10, dels om det krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. Enligt artikel 4.1 d är den personuppgiftsansvarige skyldig att på eget initiativ se till att vissa personuppgifter raderas.

Enligt 28 § personuppgiftslagen, som genomför artikel 12 b i 1995 års dataskyddsdirektiv, är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen.

Radering om personuppgifter behandlas i strid med ramlagen

På samma sätt som när det gäller rättelse bör radering kunna göras dels på den personuppgiftsansvariges eget initiativ, dels på begäran av registrerade. I avsnitt 8.1.6 behandlas den personuppgiftsansvariges skyldighet att självmant vidta åtgärder om personuppgifter behandlas i strid med vissa bestämmelser i ramlagen. Rätten för registrerade att i motsvarande

fall begära att den personuppgiftsansvarige raderar uppgifterna bör regleras i ramlagen.

Hur personuppgifter ska behandlas diskuteras i avsnitt 7 och 8. Där föreslås att det i ramlagen ska tas in bestämmelser om att personuppgifter ska vara adekvata och relevanta, att inte fler personuppgifter än nödvändigt får behandlas och att de bara får behandlas om det finns en rättslig grund och för särskilt angivna ändamål. Vidare föreslås att det ska regleras i vilken utsträckning känsliga personuppgifter får behandlas och hur länge personuppgifter får behandlas. Frågan om en personuppgift bör raderas får bedömas mot bakgrund av dessa bestämmelser. Vid bedömningen ska även 2 kap. tryckfrihetsförordningen och det arkivrättsliga regelverket beaktas.

Radering för att utföra en rättslig förpliktelse

Regeringen föreslår i avsnitt 8.1.6 att den personuppgiftsansvarige ska vara skyldig att på eget initiativ radera personuppgifter om det krävs för att utföra en rättslig förpliktelse. Den registrerade bör därför också kunna begära att personuppgifter raderas på denna grund, vilket bör framgå av ramlagen. *Justitiekanslern* anser att det är oklart vad som avses med radering på grund av en rättslig förpliktelse. I likhet med utredningen gör regeringen bedömningen att uttrycket ”rättslig förpliktelse” syftar på en skyldighet som åligger den personuppgiftsansvarige enligt ramlagen, den behöriga myndighetens registerförfattning eller andra författningar med bestämmelser om personuppgiftsbehandling. Ett domstolsbeslut som innebär att personuppgiften ska raderas kan också vara en rättslig förpliktelse (jfr Segerstedt-Wiberg mot Sverige). Vidare kan ett föreläggande från tillsynsmyndigheten om att uppgifter ska raderas vara en rättslig förpliktelse (se avsnitt 11.7.6). Även i dessa fall ska 2 kap. tryckfrihetsförordningen och det arkivrättsliga regelverket beaktas.

Uppgifter i allmänna handlingar

En grundläggande princip i svensk rätt är att allmänheten ska ha insyn i det allmännas verksamhet. I 2 kap. 18 § tryckfrihetsförordningen föreskrivs därför att grundläggande bestämmelser om hur allmänna handlingar ska bevaras och om gallring och annat avhändande av sådana handlingar ska meddelas i lag. Det som åsyftas är arkivlagen (1990:782), vilken kompletteras av arkivförordningen (1991:446) och Riksarkivets föreskrifter.

Många av de behöriga myndigheternas handlingar är allmänna och omfattas därmed av offentlighetsprincipen. Arkivlagstiftningen har som utgångspunkt företräde framför personuppgiftslagstiftningen på så sätt att intresset av att bevara allmänna handlingar har prioritet framför skyddet för personlig integritet. Det framgår av 8 § andra stycket personuppgiftslagen. I avsnitt 8.2.2 föreslås att en motsvarande bestämmelse ska tas in i ramlagen. Utrymmet för att radera uppgifter i allmänna handlingar begränsas därmed av arkivlagstiftningen. Eftersom radering av uppgifter innebär att personuppgifter tas bort från informationssamlingar på ett sådant sätt att de inte kan återskapas, bör en sådan åtgärd bara vidtas om den är förenlig med arkivlagstiftningen. För att radera personuppgifter i allmänna handlingar krävs därför författningsstöd för gallring. Utrymmet

för att radera personuppgifter i allmänna handlingar på grund av att personuppgifterna inte har behandlats författningsenligt förefaller därför vara begränsat (jfr bl.a. SOU 2015:39 s. 529 och 573 f.).

10.4.3 Begränsning av behandlingen

Regeringens förslag: Om förutsättningarna för att radera personuppgifter är uppfyllda, men uppgifterna behöver finnas kvar av bevisskäl, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av dem.

Om den registrerade bestrider att personuppgifter som rör honom eller henne är korrekta och det inte kan fastställas, ska den personuppgiftsansvarige utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 16.3 ska den personuppgiftsansvarige, i stället för att radera personuppgifterna, begränsa behandlingen av dem dels om den registrerade bestrider att personuppgifterna är korrekta och det rätta förhållandet inte kan fastställas, dels om personuppgifterna ska sparas som bevisning. Uttrycket begränsning av behandling definieras i artikel 3.3 som en markering av lagrade personuppgifter med syftet att begränsa behandlingen av dem i framtiden.

Som framgår av avsnitt 10.2.2 följer av artikel 18 att den rätt som avses i bl.a. artikel 16 kan utövas i enlighet medlemsstaternas nationella rätt, om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

Nuvarande reglering

Dagens motsvarighet till begränsning av behandling är blockering. Blockering av personuppgifter definieras i 3 § personuppgiftslagen som en åtgärd som vidtas för att personuppgifterna ska vara förknippade med information om att de är spärrade och om anledningen till spärren, för att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen. Det innebär att blockerade personuppgifter får användas internt av den personuppgiftsansvarige och av personuppgiftsbiträdet, under förutsättning att det framgår att uppgifterna är spärrade och anledningen till åtgärden. Däremot får personuppgifterna inte lämnas ut till tredje man, förutom enligt 2 kap. tryckfrihetsförordningen (prop. 1997/98:44 s. 117).

Enligt 28 § personuppgiftslagen är, som tidigare nämnts, den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i

enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen.

Vad avses med begränsning av behandling?

Frågan är vad som i direktivet åsyftas med att behandling av personuppgifter begränsas. Där definieras begränsning av behandling som en markering av lagrade personuppgifter i syfte att begränsa behandlingen av dem i framtiden. Det skiljer sig från blockering, som innebär att personuppgifterna förses med information om att de inte ska lämnas ut till tredje man (annat än med stöd av offentlighetsprincipen) och om anledningen till det. Sådana personuppgifter får dock fortfarande behandlas av den personuppgiftsansvarige eller av personuppgiftsbiträden.

Av skäl 47 framgår att om behandlingen av personuppgifter har begränsats i stället för att de raderas, bör uppgifterna endast behandlas för det ändamål som förhindrade raderingen. Som exempel på begränsning av behandling anges att personuppgifterna flyttas till ett annat databehandlingssystem, t.ex. ett system för arkivering, eller att uppgifterna görs otillgängliga med hjälp av tekniska medel. Det talar för att begränsning av behandling i direktivets mening är något utöver enbart en markering av personuppgifterna. Utredningen anser att behandlingen ska begränsas redan i samband med markeringen för att åtgärden ska bli effektiv. Regeringen har ingen annan uppfattning. Det innebär att direktivets definition blir missvisande. En definition som uttalar att begränsning av behandling är en åtgärd som visar att behandlingen av personuppgifter har begränsats tillför inte något i sak. Uttrycket bör därför inte definieras.

Begränsning när personuppgifterna behöver finnas kvar av bevisskäl

Begränsning av behandling kan aktualiseras om personuppgifterna behöver finnas kvar av bevisskäl. Begränsningen ska då göras i stället för att radera personuppgifterna. Radering kan bara komma i fråga om uppgifterna behandlas otillåtet (se avsnitt 10.4.2). I skäl 47 framhålls att behandlingen av personuppgifter bör begränsas snarare än att uppgifterna raderas, om det finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades legitima intressen. Ett exempel kan vara att uppgifterna kan behövas som bevisning i en rättsprocess om skadestånd för otillåten personuppgiftsbehandling.

Det kan ligga både i den registrerades och i det allmännas intresse att personuppgifter i vissa fall behålls en tid i stället för att raderas. Det är oklart vad som avses i direktivet med att personuppgifterna behöver sparas som bevisning. Det kan tolkas som att uppgifterna behövs som bevisning om vad som förekommit vid personuppgiftsbehandlingen. Det skulle dock även kunna syfta på att det är fråga om uppgifter som behövs som bevisning i det allmännas intresse, dvs. för något av direktivets huvudsyften brottsbekämpning, lagföring eller straffverkställighet. Mot det talar skäl 47, som enbart hänvisar till den registrerades legitima intressen. Regeringen instämmer i utredningens bedömning att begränsning av behandlingen i stället för radering därför bara bör komma ifråga när personuppgifterna behöver sparas som bevisning om hur de har behandlats. Om personuppgifter behålls i bevissyfte bör, som utgångspunkt,

uppgifterna endast få behandlas för det ändamål som förhindrade radering.

Ett exempel på att personuppgifter har sparats av bevisskäl är det s.k. kringresanderegistret där uppgifter enligt Säkerhets- och integritetsskyddsnämnden (uttalande den 15 november 2013, dnr 173-2013) behandlades i strid med polisdatalagen och där uppgifterna därför togs bort. Två kopior sparades dock för att myndigheten skulle kunna besvara frågor om vilka som förekom i registret och för att uppgifterna eventuellt skulle kunna användas som bevis (se bl.a. SOU 2015:39 s. 574 och 645 f.).

Begränsning när personuppgifternas korrekthet bestrids

Begränsning av behandlingen kan också komma i fråga om den registrerade bestrider att personuppgifterna är korrekta, men det inte är möjligt att fastställa om så är fallet. En felaktig personuppgift ska rättas utan onödigt dröjsmål. Om den personuppgiftsansvariges utredning om den omstridda personuppgiften inte kan slutföras tillräckligt snabbt bör behandlingen begränsas under utredningstiden. Uppgifterna får då inte behandlas av den personuppgiftsansvarige eller personuppgiftsbiträden annat än för det ändamål som föranledde begränsningen. Om det efter utredning visar sig att personuppgifterna är korrekta kan behandlingen av dem fortsätta som tidigare. Begränsningen bör då upphävas. Innan dess ska dock den registrerade underrättas om att begränsningen upphör (se avsnitt 10.5.8). Skulle det visa sig att personuppgifterna är felaktiga ska den personuppgiftsansvarige rätta dem, varefter begränsningen kan upphöra.

Begränsning på denna grund ska enligt direktivet användas i stället för radering. Åtgärden kan emellertid som utredningen konstaterar inte vara ett alternativ till radering, eftersom den ska användas när uppgifters korrekthet bestrids och därför knyter an till rättelseförfarandet.

Åtgärd som visar att behandlingen har begränsats

Den personuppgiftsansvarige ska vidta en åtgärd med personuppgifterna som visar att behandlingen har begränsats. Hur begränsningen bör göras får bedömas med utgångspunkt i vad som är lämpligt i det enskilda fallet. En naturlig åtgärd kan vara att avskilja uppgifterna från det datasystem där de behandlas. Begränsningen kan också ha formen av en teknisk begränsning, vilket kan vara en lämplig åtgärd medan personuppgifternas korrekthet utreds. En tredje möjlighet att begränsa behandlingen är att inskränka tillgången till uppgifterna.

Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av vare sig den personuppgiftsansvarige eller ett personuppgiftsbiträde utom för det syfte som har föranlett begränsningen. Har en personuppgift behandlats på otillåtet sätt måste den ändå kunna behandlas inom ramen för en utredning av om brott har begåtts i samband med behandlingen eller om någon tjänsteman vid behandlingen gjort sig skyldig till fel som kan föranleda disciplinansvar eller skadestånd. Det beror på felets karaktär om all behandling av personuppgiften måste upphöra eller om det bara gäller behandlingen i viss verksamhet. Vidare bör beaktas vad som följer av artikel 18 och skäl 49

att nationella bestämmelser om straffrättsliga förfaranden kan påverka rätten till begränsning av behandling.

Oavsett vilken åtgärd som vidtas för att begränsa behandlingen är den inte avsedd att vara permanent. När personuppgifterna inte längre behöver finnas kvar som bevisning ska de raderas och när utredningen om personuppgifternas korrekthet är avslutad ska begränsningen av behandlingen upphöra och uppgifterna antingen fortsätta att behandlas eller rättas.

Begränsning av behandlingen bör i likhet med de andra korrigerande åtgärderna genomföras utan onödigt dröjsmål.

Rätten att begära begränsning av behandlingen

Det är inte tydligt i direktivet om enskilda ska ha rätt att begära begränsning av behandlingen. Av artikel 16.3 kan inte en sådan rätt utläsas. Å andra sidan föreskrivs det i artiklarna 13.1 e och 14 e att den registrerade ska informeras om rätten att begära begränsning av behandlingen. Även skäl 40 och 42 ger intryck av att den registrerade ska ha en sådan rätt. Regeringen håller med utredningen om att registrerade bör ha den rätten om personuppgifterna behöver finnas kvar som bevis. Registrerade får i sådana fall begära radering och bör därför också kunna begära den mindre ingripande åtgärden begränsning av behandlingen. Det är tillåtet att ha starkare skyddsåtgärder än dem som fastställs i direktivet och i det här fallet anser regeringen att det är motiverat. I ramlagen bör det således tas in en bestämmelse om rätt för den registrerade att begära begränsning av behandlingen i de fall där personuppgifterna behöver finnas kvar som bevis.

10.4.4 Val av åtgärd

Regeringens förslag: Den personuppgiftsansvarige avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* tillstyrker förslaget. *Dataskydd.net* anser att bestämmelsen inte tillför någonting till de förslag som behandlas i avsnitten 10.4.1–10.4.3 och ser därför inget behov av den. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt förarbetena till personuppgiftslagen väljer den personuppgiftsansvarige själv vilket alternativ som ska användas av rättelse, utplånande eller blockering (prop. 1997/98:44 s. 87). Den ordningen bör även gälla i fråga om rättelse, radering eller begränsning av behandlingen enligt ramlagen. Den personuppgiftsansvarige bör därför inte endast pröva om den åtgärd som begärs av den registrerade ska vidtas eller inte, utan är fri att välja en annan åtgärd om den är lämpligare. Det följer av att den personuppgiftsansvarige ska vara skyldig att vidta alla rimliga åtgärder för att rätta personuppgifter som är felaktiga eller ofullständiga och för att radera eller begränsa behandlingen av personuppgifter som har behandlats otillåtet. För att det ska vara tydligt bör det, i motsats till vad *Dataskydd.net* tycker, framgå av

ramlagen att den personuppgiftsansvarige inte är bunden av begäran utan självständigt avgör vilken åtgärd som bör vidtas.

Den personuppgiftsansvarige ska alltså se till att den lämpligaste åtgärden vidtas oavsett vad som begärs. En åtgärd kan emellertid inte vidtas om den strider mot annan lagstiftning. Det innebär t.ex. att en myndighet inte kan radera uppgifter i en allmän handling utan författningsstöd för gallring.

10.5 Hur informationen ska begäras och lämnas

10.5.1 Kraven på informationen och på den som begär den

I direktivet anges vissa allmänna krav på hur den personuppgiftsansvarige ska tillhandahålla information. Det handlar om att den information som lämnas ska vara kortfattad, lättillgänglig och lättbegriplig och lämnas i lämplig form. Information om handläggningen ska lämnas. Vidare ska informationen som huvudregel vara avgiftsfri. Reglerna syftar till att underlätta den registrerades möjligheter att ta till vara sina rättigheter. Direktivet innehåller även bestämmelser om den personuppgiftsansvariges skyldighet att underrätta såväl enskilda som andra om vissa beslut.

Det ställs däremot få krav i direktivet på den som begär att få information av den personuppgiftsansvarige. Indirekt kan det utläsas vissa sådana krav, t.ex. genom att den personuppgiftsansvarige har rätt att vägra att lämna information i vissa fall.

10.5.2 Kraven på begäran

Regeringens bedömning: Kraven på en begäran om information eller att en åtgärd ska vidtas kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Direktivet innehåller som nyss nämnts inga direkta bestämmelser om vad som krävs av den som begär information eller att en korrigeringsåtgärd ska vidtas. I 26 § andra stycket personuppgiftslagen föreskrivs att en ansökan ska göras skriftligen hos den personuppgiftsansvarige och vara undertecknad av sökanden. Kravet på egenhändigt undertecknande innebär att ett ombud inte kan underteckna ansökan. Däremot kan vårdnadshavare och andra ställföreträdare underteckna ansökan för den som inte har rätt att själv begära information eller åtgärder. Något krav på egenhändigt undertecknad ansökan ställs inte i 1995 års dataskyddsdirektiv. Det härrör i stället från en bestämmelse om registerutdrag i 10 § datalagen (1973:289). Syftet med kravet är att säkerställa att det är den registrerade som får tillgång till informationen (SOU 1997:39 s. 389 och prop. 1997/98:44 s. 82).

I dagens informationssamhälle, där allt fler privatärenden utförs elektroniskt, är det enligt regeringen av vikt att en ansökan kan göras på olika sätt. Regeringen anser därför att en ansökan bör kunna göras både

på papper och elektroniskt. Det ligger också i linje med avsikten att underlätta för den registrerade att utöva sina rättigheter (jfr artikel 12). Regleringen bör således vara teknikneutral. Vilka närmare krav som bör ställas på en begäran om information eller att en åtgärd ska vidtas kan regleras i förordning och myndighetsföreskrifter.

10.5.3 Åtgärder för att säkerställa att begäran görs av en behörig person

Regeringens bedömning: Det kan regleras i förordning att det ska säkerställas att begäran görs av en behörig person.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna: Ingen remissinstans anför något i den här delen.
Skälen för regeringens bedömning: Om det finns skäl att ifrågasätta den registrerades identitet vid en begäran om information eller en korrigeringsåtgärd, får den personuppgiftsansvarige enligt artikel 12.5 kräva den ytterligare information som är nödvändig för att bekräfta identiteten. Sådan information bör endast behandlas för det specifika ändamålet och inte lagras längre än vad som krävs för det ändamålet.

Som nyss nämnts är syftet med dagens krav på egenhändigt undertecknande att garantera att det är den registrerade som får tillgång till personuppgifter och information eller begär att en åtgärd ska vidtas med personuppgifter som behandlas. Det bör givetvis undvikas att obehöriga får kännedom om integritetskänslig information om andra. Det finns emellertid möjlighet att fastställa den registrerades identitet på annat sätt än genom en egenhändigt undertecknad handling, t.ex. genom avancerad elektronisk underskrift. En annan möjlighet att säkerställa från vem begäran kommer kan vara att kontakta den registrerade.

Regeringen håller med utredningen om att det bör ställas krav på att den personuppgiftsansvarige på lämpligt sätt säkerställer att begäran gjorts av en behörig person. Den personuppgiftsansvarige kan exempelvis ställa kontrollfrågor som bekräftar identiteten vid direktkontakt med den registrerade. Hur det närmare bör göras finns det inte anledning att gå in på här, men utgångspunkten bör vara att dels underlätta för den registrerade, dels ha en teknikneutral lösning. Det kan regleras i förordning att den personuppgiftsansvarige bör säkerställa att begäran görs av en behörig person.

10.5.4 Lättbegriplig information i lämplig form

Regeringens bedömning: Det kan regleras i förordning vilka krav som ställs på information till enskilda.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

Enligt artikel 12.1 är den personuppgiftsansvarige skyldig att vidta rimliga åtgärder för att informationen till den registrerade om hans eller hennes rättigheter tillhandahålls i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Det handlar om den information som den registrerade har rätt till enligt dels artikel 13, dels artiklarna 11, 14–18 och 31.

Informationen ska tillhandahållas på lämpligt sätt. Den personuppgiftsansvarige ska i allmänhet lämna informationen i samma form som begäran. Av skäl 39 framgår att information till den registrerade bör vara lättåtkomlig, t.ex. genom att tillhandahållas på den personuppgiftsansvariges webbplats.

Nuvarande reglering

I dag ställs inte några särskilda krav på hur information till den registrerade ska utformas och lämnas, utöver att den i vissa fall ska lämnas på den personuppgiftsansvariges eget initiativ. I Datainspektionens allmänna råd om information till registrerade framhålls att det är den personuppgiftsansvarige som har bevisbördan för att den registrerade har fått den information som krävs och att det därför ligger i den personuppgiftsansvariges intresse att informationen är tydlig och begriplig. Om informationen bör lämnas muntligen eller skriftligen avgörs av omständigheterna i det enskilda fallet. Datainspektionen ger råd om hur information bör lämnas i olika situationer beroende på hur personuppgifterna samlas in. Inspektionen rekommenderar att den personuppgiftsansvarige utformar tydliga rutiner för hur information ska lämnas.

Förvaltningslagen innehåller bestämmelser om förvaltningsmyndigheternas serviceskyldighet och allmänna krav på handläggning av ärenden. Bland annat ska myndigheter se till att kontakterna med enskilda blir smidiga och enkla och ärenden ska handläggas så enkelt, snabbt och kostnadseffektivt som möjligt utan att rättssäkerheten eftersätts. Enligt 11 § språklagen (2009:600) ska språket i offentlig verksamhet vara vårdat, enkelt och begripligt.

Behövs det särskild reglering?

Regleringen i förvaltningslagen och språklagen innebär att det redan finns generella krav på begriplighet och klart och tydligt språk som gäller i offentlig verksamhet. Det innebär att kraven i direktivet är uppfyllda för större delen av den verksamhet som ramlagen omfattar. Det kan dock ändå finnas skäl att ha en särskild bestämmelse om att information till registrerade om personuppgiftsbehandling ska vara lättillgänglig och lättbegriplig samt lämnas i lämplig form, eftersom det är ett så komplext ämne. I att den ska vara lättillgänglig och lättbegriplig ligger att den normalt bör vara kortfattad. Frågan kan regleras i förordning.

10.5.5 Åtgärder som underlättar utövandet av rättigheterna

Regeringens bedömning: Att den personuppgiftsansvarige ska underlätta för den registrerade att ta till vara sina rättigheter kräver inga lagstiftningsåtgärder.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om bedömningen.

Skälen för regeringens bedömning: Enligt artikel 12.2 ska den personuppgiftsansvarige underlätta utövandet av den registrerades rättigheter. I skäl 40 framhålls särskilt rutiner för att kostnadsfritt begära och få tillgång till personuppgifter, rättelse, radering och begränsning av behandling.

Alla myndigheter har en i förvaltningslagen fastlagd serviceskyldighet. Det finns också allmänna krav på myndigheternas och domstolarnas handläggning. Även de förfaranderegler som gäller i mål- och ärendehantering hos de behöriga myndigheterna innehåller sådana bestämmelser. Enligt 6 § (2017:900) förvaltningslagen ska varje myndighet se till att kontakterna med enskilda blir smidiga och enkla och lämna sådan hjälp till enskilda att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Det innebär att myndigheten ska hjälpa enskilda att ta till vara sin rätt i angelägenheter inom dess verksamhetsområde. Det kan gälla exempelvis upplysningar om hur man gör en ansökan, råd om vilka handlingar som bör bifogas och hjälp med att fylla i blanketter. Det finns delvis likartade bestämmelser för domstolarna.

Bestämmelsen i artikel 12.2 är generellt utformad och närmast att se som en inledande bestämmelse till de efterföljande punkterna i artikeln, som preciserar vad den personuppgiftsansvarige ska göra för att underlätta för den registrerade att utöva sina rättigheter. Regeringen instämmer i utredningens uppfattning att artikel 12.2 därför inte behöver genomföras i svensk rätt.

10.5.6 Skyldighet att informera om handläggningen

Regeringens bedömning: Skyldigheten att informera om handläggningen kräver inga lagstiftningsåtgärder.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans kommenterar bedömningen.

Skälen för regeringens bedömning: Den personuppgiftsansvarige ska enligt artikel 12.3 utan onödigt dröjsmål skriftligen informera den registrerade om uppföljningen av hans eller hennes begäran.

Regeringen instämmer i utredningens bedömning att artikel 12.3 syftar till att förhindra att den personuppgiftsansvarige dröjer alltför länge med att behandla en registrerads begäran om information eller om en korrigeringsåtgärd. Vilken information som ska lämnas i de fall där den personuppgiftsansvarige är skyldig att lämna svar framgår inte av direktivet,

utöver att svaret ska vara en uppföljning av begäran. I artiklarna 12.3 och 12.4 i dataskyddsförordningen föreskrivs i motsvarande bestämmelser att informationen ska avse de åtgärder som har vidtagits eller orsaken till att åtgärderna inte har vidtagits. Eftersom det inte finns motsvarande regler i direktivet skulle det, som också utredningen menar, leda för långt att begära att den personuppgiftsansvarige ska ange vilka åtgärder som har vidtagits eller motivera varför några åtgärder inte vidtagits i anledning av begäran. I likhet med utredningen tolkar regeringen artikeln så att det som krävs av den personuppgiftsansvarige är att den registrerade informeras om hur begäran hanteras, dvs. status för handläggningen av den. Det ligger också i linje med svensk förvaltningstradition att kräva att den personuppgiftsansvarige när det begärs bekräftar att en handling tagits emot och anger om den är under handläggning eller inte.

När det gäller begäran om rättelse, radering eller begränsning av behandlingen föreskrivs att åtgärderna ska vidtas utan onödigt dröjsmål (se avsnitt 10.4.1–3). Detsamma gäller begäran om personrelaterad information (se avsnitt 10.2.8). Det kommer därför inte att finnas något behov av att informera om handläggningen annat än om det uppstår något oförutsett dröjsmål. Att den registrerade vid behov ska hållas informerad om handläggningen följer av allmänna förvaltningsrättsliga principer och den allmänna serviceskyldigheten i förvaltningslagen och kräver därför enligt regeringen inte några lagstiftningsåtgärder.

10.5.7 Beslut ska vara skriftliga och motiverade

Regeringens bedömning: Att beslut ska vara skriftliga och i vissa fall motiverade kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens bedömning: Enligt artikel 15.3 ska den personuppgiftsansvarige skriftligen informera den registrerade om sådan information som avses i artikel 14 vägras eller begränsas och om skälen för att det görs. Av skäl 45 framgår att beslut om begränsning av information ska inkludera de faktiska och rättsliga skäl som beslutet grundar sig på. Det bör därför föreskrivas att beslut att inte lämna personrelaterad information ska vara skriftliga och motiverade.

Att den personuppgiftsansvarige kan vägra att lämna information om en begäran är orimlig eller uppenbart ogrundad eller ta ut avgift om begäran är återkommande behandlas i avsnitt 10.3.4. Beslut om att ta ut avgift eller att inte lämna information bör vara skriftliga och motiverade.

Enligt artikel 16.4 ska den personuppgiftsansvarige underrätta den registrerade skriftligen om beslut att inte rätta, radera eller begränsa behandlingen. Besluten ska vara motiverade. Det bör därför föreskrivas att beslut i fråga om rättelse, radering eller begränsning av behandlingen ska vara skriftliga. Beslut som går den registrerade emot ska också vara motiverade. Att skälen för besluten inte behöver lämnas ut i vissa fall behandlas i avsnitt 10.3.1.

Att besluten ska vara skriftliga och i vissa fall motiverade kan regleras i förordning.

10.5.8 Underrättelseskyldighet

Regeringens bedömning: Underrättelseskyldigheter knutna till enskildas rättigheter kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens bedömning.
Remissinstanserna: Ingen remissinstans anför något i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

Som nyss nämnts ska den personuppgiftsansvarige enligt artikel 15.3 utan onödigt dröjsmål skriftligen informera den registrerade om sådan information som avses i artikel 14 vägras eller begränsas och om skälen för det. En sådan underrättelse kan enligt artikeln utelämnas om den skulle undergräva ändamålet med åtgärden. Den personuppgiftsansvarige ska även underrätta den registrerade om möjligheten att lämna in klagomål till en tillsynsmyndighet eller begära rättslig prövning. Enligt artikel 15.4 ska den personuppgiftsansvarige dokumentera de sakliga och rättsliga grunderna för beslutet. Informationen ska göras tillgänglig för tillsynsmyndigheterna.

Om den personuppgiftsansvarige inte har lämnat information till den registrerade eller inte uppgett skälen för beslut att avslå begäran om rättelse, radering eller begränsning av behandling ska enligt artikel 17.2 den registrerade underrättas om möjligheten att utöva rättigheterna genom tillsynsmyndigheten.

I de fall där behandlingen begränsas för att den registrerade bestrider att personuppgifterna är korrekta och det rätta förhållandet inte kan fastställas, ska enligt artikel 16.3 den personuppgiftsansvarige underrätta den registrerade innan begränsningen av behandlingen upphävs. Enligt artikel 16.4 ska den personuppgiftsansvarige underrätta den registrerade skriftligen om ett beslut att inte rätta, radera eller begränsa behandlingen. Han eller hon ska också underrättas om möjligheten att lämna in klagomål till en tillsynsmyndighet eller begära rättslig prövning. Om en oriktig personuppgift har rättats ska enligt artikel 16.5 den personuppgiftsansvarige underrätta den behöriga myndighet från vilken personuppgiften kommer. Artikel 16.6 föreskriver att om personuppgifter har rättats, raderats eller behandlingen av dem har begränsats ska den personuppgiftsansvarige underrätta mottagarna om åtgärden. Mottagarna ska rätta eller radera personuppgifterna eller begränsa den behandling som utförs under deras ansvar.

Underrättelser till enskilda

Enligt förvaltningslagen, som tillämpas när en myndighet agerar i egenskap av personuppgiftsansvarig, ska beslut som regel motiveras. Det gäller även för brottsbekämpande myndigheter och för domstolar i fråga om administrativa beslut. En myndighet som meddelar ett beslut ska även så snart som möjligt underrätta den som är part om det fullständiga innehållet i beslutet. Det krävs således inte någon lagstiftningsåtgärd för att uppfylla det kravet i artikel 15.3. Artikeln innehåller dock ett undantag från denna skyldighet, nämligen att den registrerade inte behöver

underrättas om underrättelsen skulle undergräva ändamålet med åtgärden. Det kan vara fallet om skälen för beslutet skulle riskera att röja information som hänför sig till något av de intressen som enligt direktivet får läggas till grund för att begränsa informationen. Regeringen håller med utredningen om att ett sådant undantag är nödvändigt för att sökanden inte genom avslagsbeslutet ska kunna få del av information som han eller hon annars inte har rätt att få. Kraven på sådana beslut behandlas i avsnitt 10.5.7. Sökanden bör utan onödigt dröjsmål underrättas om ett sådant beslut, om det inte skulle skada det intresse som föranleder att information inte har lämnats. Det kan regleras i förordning.

Att den personuppgiftsansvarige ska underrätta sökanden om möjligheten att begära rättslig prövning kräver inte någon lagstiftningsåtgärd, eftersom skyldigheten att upplysa enskilda om huruvida ett beslut är överklagbart och hur det går till att överklaga följer av förvaltningslagen. Sökanden bör dock underrättas om möjligheten att lämna in klagomål till tillsynsmyndigheten och att begära att den kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt. Det kan regleras i förordning. Underrättelsen kan lämpligen lämnas i det beslut där den efterfrågade informationen begränsas eller inte lämnas ut.

Regeringen instämmer i utredningens uppfattning att det inte heller krävs någon bestämmelse om att den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslut och göra informationen tillgänglig för tillsynsmyndigheten. Grunderna för ett beslut ska enligt förvaltningslagen framgå av skälen. Tillsynsmyndighetens rätt att få tillgång till dokumentation för att kunna utöva tillsyn behandlas i avsnitt 11.7.3.

Att den personuppgiftsansvarige kan vägra att lämna information om en begäran är orimlig eller uppenbart ogrundad eller ta ut avgift för den om begäran är återkommande behandlas i avsnitt 10.3.4 och kraven på sådana beslut i avsnitt 10.5.7. Sökanden bör underrättas om beslutet. Det kan regleras i förordning.

I avsnitt 10.5.7 behandlas också kraven på beslut om rättelse, radering eller begränsning av behandlingen. Den registrerade ska underrättas om beslutet och om möjligheten att lämna in klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige inte har angett skälen för beslutet att inte lämna information ska den registrerade också underrättas om möjligheten att begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt. Det kan regleras i förordning.

Även skyldigheten att informera innan en begränsning av behandling av personuppgifter upphör kan regleras i förordning.

Underrättelser till andra

Enligt 28 § personuppgiftslagen ska i vissa fall tredje man underrättas om att personuppgifter har rättats. Den personuppgiftsansvarige ska på begäran av den registrerade underrätta tredje man som fått uppgifterna om rättelsen. Någon underrättelse behöver dock inte lämnas om det skulle visa sig vara omöjligt eller skulle kräva en oproportionerligt stor arbetsinsats. Paragrafen genomför artikel 12 c i 1995 års dataskyddsdirektiv, som också gör undantag från kravet på underrättelse till tredje man om det

visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning.

När det gäller underrättelse till tredje man enligt artikel 16.6 medger direktivet inte ett sådant undantag som finns i 28 § personuppgiftslagen. En underrättelse bör således alltid skickas på den personuppgiftsansvariges eget initiativ till mottagaren, om en personuppgift har rättats eller raderats eller behandlingen av den har begränsats. Underrättelseskyldigheten kan regleras i förordning. Vilka åtgärder som bör vidtas behandlas i avsnitt 8.1.6.

Någon underrättelse bör inte krävas i den personuppgiftsansvariges egen verksamhet. Det följer av de grundläggande kraven på behandling att den personuppgiftsansvarige ska se till att felaktiga personuppgifter inte behandlas. Den personuppgiftsansvarige har därför intresse av att inom den egna organisationen på lämpligt sätt sprida kännedom om de rättelser och ändringar som görs.

Enligt artikeln ska mottagare av personuppgifter som har rättats, raderats eller där behandlingen har begränsats vidta motsvarande åtgärder med personuppgifter som behandlas under deras ansvar. Om en behörig myndighet underrättas om att en personuppgift som den har tagit emot har rättats, raderats eller att behandlingen av den har begränsats av den myndighet som överlämnat den, ska den behöriga myndigheten pröva om motsvarande åtgärd även bör göras där. Skyldigheten att agera följer av förslaget om att den personuppgiftsansvarige ska vara skyldig att på eget initiativ rätta personuppgifter som är felaktiga eller ofullständiga, uppdatera personuppgifter som är inaktuella och radera eller begränsa behandlingen av personuppgifter som har behandlats på ett otillåtet sätt (se avsnitt 8.1.6). Någon ytterligare reglering behövs därför inte. Eftersom myndigheter kan ha olika ändamål för behandlingen behöver dock en korrigeringsåtgärd hos en myndighet inte alltid leda till samma åtgärd hos en annan, trots att det är fråga om samma personuppgift.

Om en felaktig eller ofullständig personuppgift har rättats eller kompletterats ska den personuppgiftsansvarige underrätta den myndighet från vilken personuppgiften kommer. En bestämmelse om det bör tas in i förordning.

10.5.9 Information ska inte avgiftsbeläggas

Regeringens förslag: Information om behandlingen av personuppgifter som den personuppgiftsansvarige ska lämna på eget initiativ och information om automatiserade beslut ska lämnas utan avgift. Information som ska lämnas på begäran är avgiftsfri en gång per år.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om förslaget.

Skälen för regeringens förslag: Enligt artikel 12.4 ska den registrerades rättigheter vara kostnadsfria. Det handlar dels om kostnadsfri information om behandlingen av den registrerades personuppgifter enligt artikel 13, dels om att meddelanden eller åtgärder enligt artiklarna 11, 14–18 och 31 ska vara kostnadsfria.

Myndigheters information och beslut är som huvudregel kostnadsfria, om inte annat föreskrivs. För att tydliggöra att så är fallet bör det i ramlagen föreskrivas att information som den personuppgiftsansvarige lämnar på eget initiativ om behandlingen av den registrerades personuppgifter ska vara avgiftsfri. Detsamma gäller den personuppgiftsansvariges information till den registrerade om automatiserade beslut. Som framgår av avsnitt 10.3.4 anser utredningen att personrelaterad information som lämnas på begäran ska vara avgiftsfri en gång per år. Begär någon information oftare föreslås att den personuppgiftsansvarige ska få ta ut rimlig avgift eller avslå begäran.

Enligt direktivet ska även beslut, underrättelser och åtgärder vara kostnadsfria. Regeringen gör samma bedömning som utredningen att det inte behöver regleras särskilt utan följer av huvudregeln att ingen avgift tas ut för myndigheters beslut och meddelanden.

I likhet med utredningen anser regeringen att uttrycket ”utan avgift” bör väljas i stället för direktivets ”kostnadsfri” för att korrespondera med uttrycket ”rimlig avgift”.

11 Tillsyn

11.1 Dagens tillsyn över personuppgiftsbehandling

11.1.1 Datainspektionen

Datainspektionen utövar tillsyn över all behandling av personuppgifter, så länge ansvaret inte uttryckligen har anförtrotts någon annan myndighet. Uppdraget regleras i förordningen (2007:975) med instruktion för Datainspektionen (i det följande Datainspektionens instruktion). Datainspektionens tillsyn omfattar både behandling som regleras i personuppgiftslagen (1998:204) och i särskilda registerförfattningar och andra författningar som innehåller bestämmelser om behandling av personuppgifter.

Enligt 2 § personuppgiftsförordningen (1998:1191) är Datainspektionen tillsynsmyndighet enligt personuppgiftslagen. Datainspektionen har också utsetts till nationell tillsynsmyndighet enligt flera unionsrättsakter, bl.a. artikel 28.1 i 1995 års dataskyddsdirektiv, artikel 25.1 i rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete och artikel 30.5 i rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümrådsbeslutet).

Inspektionens uppgift är bl.a. att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Verksamheten ska särskilt inriktas på att informera om gällande regler och att ge råd och hjälp åt personuppgiftsombud. Vidare ska myndigheten följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik (1 § Datainspektionens instruktion).

Inspektionen har rätt att för sin tillsyn få tillgång till personuppgifter, upplysningar och dokument och tillträde till lokaler som används för behandling av personuppgifter (43 § personuppgiftslagen). Genom påpekanden och liknande förfaranden ska inspektionen i första hand försöka åstadkomma rättelse och i andra hand besluta om förbud mot annan behandling än lagring (45 § personuppgiftslagen) eller vid domstol ansöka om utplåning av personuppgifter som behandlats på ett olagligt sätt (47 § personuppgiftslagen). I vissa fall kan inspektionen förena sina förelägganden med vite (44 och 45 §§ personuppgiftslagen). Datainspektionens beslut i tillsynsfrågor får överklagas (51 § personuppgiftslagen).

Datainspektionen ingår i den s.k. Artikel 29-gruppen som inrättats med stöd av artikel 29.1 i 1995 års dataskyddsdirektiv. Arbetsgruppen består av en företrädare för tillsynsverksamheten i varje medlemsstat i EU. Arbetsgruppen har bl.a. till uppgift att bidra till en enhetlig tillämpning av nationella bestämmelser som genomför direktivet, att lämna råd till kommissionen inför ändringar av direktivet, att yttra sig till kommissionen om dataskyddsnivån inom EU och i tredjeland och att utarbeta gemensamma uppförandekoder.

En närmare redogörelse för Datainspektionens tillsynsverksamhet finns i betänkandet Ett samlat ansvar för tillsyn över den personliga integriteten (SOU 2016:65 s. 78 f.).

11.1.2 Säkerhets- och integritetsskyddsnämnden

Även Säkerhets- och integritetsskyddsnämnden utövar tillsyn över personuppgiftsbehandling inom direktivets tillämpningsområde. Nämndens uppdrag regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden (i det följande nämndens instruktion).

Nämnden utövar tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. De myndigheter vars verksamhet berörs av tillsynen är Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten och Tullverket. Nämnden utövar även tillsyn över Säkerhetspolisens och Polismyndighetens behandling av personuppgifter enligt polisdatalagen (2010:361). Tillsynen ska särskilt ta sikte på behandlingen av känsliga personuppgifter.

Nämnden inrättades i syfte att skapa ett fristående och självständigt organ som ska säkerställa rätten till effektivt rättsmedel som den garanteras i artikel 13 i Europakonventionen. Avsikten är att nämndens tillsyn ska komplettera den tillsyn som andra myndigheter ansvarar för, främst Justitiekanslern, Åklagarmyndigheten och Datainspektionen (prop. 2006/07:133 s. 61 f. och prop. 2009/10:85 s. 272 f.).

Nämnden utövar sin tillsyn genom inspektioner och andra undersökningar, som kan vara både föranmälda och oanmälda. Nämnden ska också på begäran av enskilda kontrollera om de har varit föremål för behandling av personuppgifter inom nämndens tillsynsområde och underrätta dem om att kontrollen genomförts. Nämnden har för sin tillsyn rätt att få tillgång till de uppgifter och den hjälp som den begär av den myndighet

som tillsynen avser. Om nämnden finner något att anmärka på får den lämna synpunkter på hur bristerna bör avhjälpas. Nämndens rekommendationer är inte bindande och kan inte överklagas.

Om nämnden upptäcker brott ska det enligt 20 § nämndens instruktion anmälas till Åklagarmyndigheten och om nämnden finner något som kan leda till skadeståndsansvar för staten ska det anmälas till Justitiekanslern. Finner nämnden omständigheter som Datainspektionen bör uppmärksammas på, ska nämnden anmäla det till inspektionen. Det har hittills inte funnits anledning för nämnden att göra någon anmälan till Datainspektionen, eftersom de brottsbekämpande myndigheterna följer nämndens uttalanden om regelefterlevnad. Nämndens rekommendationer om förbättringar följs dock inte alltid av myndigheterna (se Riksrevisionens rapport om Säkerhets- och integritetsskyddsnämndens tillsyn över brottsbekämpande myndigheter, skr. 2015/16:188, s. 49).

11.1.3 Riksdagens ombudsmän och Justitiekanslern

Riksdagens ombudsmän (JO) och Justitiekanslern utövar tillsyn över hur lagar och andra föreskrifter tillämpas i offentlig verksamhet. Deras tillsyn omfattar därmed även behandlingen av personuppgifter och skyddet av enskildas personliga integritet vid sådan behandling. Både JO och Justitiekanslern är extraordinära tillsynsorgan.

JO:s verksamhet regleras framför allt i regeringsformen, riksdagsordningen och lagen (1986:765) med instruktion för Riksdagens ombudsmän.

Justitiekanslerns verksamhet regleras huvudsakligen i lagen (1975:1339) om Justitiekanslerns tillsyn och i förordningen (1975:1345) med instruktion för Justitiekanslern.

De som står under JO:s och Justitiekanslerns tillsyn ska på begäran lämna upplysningar och yttranden och ge tillgång till handlingar och protokoll. Ett granskningsärende kan inledas både efter klagomål från enskilda och på JO:s eller Justitiekanslerns eget initiativ. Såväl JO som Justitiekanslern kan genomföra inspektioner som ett led i granskningen. Tillsynsärenden kan resultera i beslut som kan innehålla kritik eller vägledande uttalanden. Både JO och Justitiekanslern kan även väcka åtal mot någon som står under deras respektive tillsyn för brott som begåtts i tjänsten och har också rätt att väcka frågor om disciplinär bestraffning. Varken JO eller Justitiekanslern har däremot rätt att ompröva eller ändra beslut som har fattats av någon som står under deras tillsyn.

11.2 Utgångspunkter för överväganden om tillsyn

Frågor om tillsyn har fått ökat fokus

Frågor om tillsyn, t.ex. hur den ska bedrivas och vem som ska utöva tillsyn, har diskuterats inom många olika områden under senare år och lösningarna varierar. Regeringen har i skrivelsen En tydlig, rättssäker och effektiv tillsyn (skr. 2009/10:79, i det följande tillsynsskrivelsen) utvecklat sin syn på tillsynsfrågor. I skrivelsen framhålls att den offentliga tillsynen är viktig för att stärka efterlevnaden av de föreskrifter som riks-

dagen och regeringen har beslutat. Tillsynen bidrar till att upprätthålla grundläggande värden i samhället som bl.a. rättssäkerhet. Medborgarna ska genom tillsynen vara tillförsäkrade att deras intressen tas till vara.

Utgångspunkten i skrivelsen är att det krävs större enhetlighet i fråga om tillsyn. I skrivelsen framhålls bl.a. att den offentliga tillsynen bör präglas av tydlighet och enhetlighet. Ett sätt att uppnå det är att tillsynsmyndigheternas uppdrag preciseras i form av tillsynsuppgifter, regler och i förekommande fall mål och prioriteringar. I skrivelsen pekas också på behovet av enhetliga begrepp.

Vidare understryks att avsteg från de generella bedömningarna i skrivelsen kan leda till minskad tydlighet och enhetlighet, men att det inom vissa områden ändå kan finnas skäl att göra avsteg om det leder till en mer ändamålsenlig tillsyn inom det specifika området. Ett annat skäl för avsteg kan vara Sveriges skyldigheter att genomföra och anpassa lagstiftning till unionsrättsakter eller till internationella konventioner (skr. 2009/10:79 s. 13).

Utredningarnas olika uppdrag

Genomförandet av dataskyddsdirektivet när det gäller tillsynen kompliceras av flera faktorer. En har att göra med att Utredningen om 2016 års dataskyddsdirektivs uppdrag att utreda hur direktivet bör genomföras inte varit heltäckande. Uppdraget har, som tidigare nämnts, delvis fullgjorts av en annan utredning med ett annat fokus. Utredningen om tillsynen över den personliga integriteten (Ju 2015:02) har haft i uppdrag att kartlägga vilken tillsyn över behandling av personuppgifter som bedrivs i dag och överväga om den i större utsträckning kan samlas hos en myndighet. Den utredningen har också haft i uppdrag att peka ut vilken eller vilka myndigheter som bör vara tillsynsmyndighet enligt dataskyddsförordningen respektive dataskyddsdirektivet och representera Sverige i Europeiska dataskyddsstyrelsen (i det följande styrelsen). Även frågorna om hur företrädare för tillsynsmyndigheten ska utses och hur verksamheten ska organiseras har ingått i den utredningens uppdrag. Utredningen har avgett betänkandet Ett samlat ansvar för tillsyn över den personliga integriteten (SOU 2016:65). I det följande behandlas den utredningens slutsatser huvudsakligen såvitt gäller genomförandet av dataskyddsdirektivet i avsnitt 11.4. I de fall hänvisningar till den utredningens överväganden sker i andra delar av detta kapitel skrivs utredningens fullständiga namn eller SOU 2016:65 ut. För att ge en klarare bild av hur de olika utredningarnas uppdrag förhåller sig till och kompletterar varandra på tillsynsområdet tas några av de allmänna frågor som Utredningen om tillsynen över den personliga integriteten har behandlat upp redan här.

Reglerna i direktivet och dataskyddsförordningen har stora likheter

Direktivet har, bl.a. när det gäller tillsynen över behandlingen av personuppgifter, till stora delar samma innehåll som dataskyddsförordningen eller i vart fall liknande regler. Tillsynsuppgifterna är i princip desamma enligt direktivet och förordningen, men förordningen reglerar också frågor som inte aktualiseras på direktivets område. Förordningen innehåller fler och mer detaljerade regler om tillsynsmyndighetens befogenheter, men i sak motsvarar de i stort sett direktivets bestämmelser.

Frågan är då vilka utgångspunkter som regeringen bör ha när det gäller genomförandet av artiklar i direktivet som är likalydande eller har betydande likheter med artiklar i dataskyddsförordningen. Eftersom förordningen kommer att gälla som svensk lag saknas det utrymme för att justera i dess bestämmelser. I den mån bestämmelserna i dataskyddsdirektivet och dataskyddsförordningen behöver anpassas till varandra, t.ex. beträffande terminologin eller hur tillsynsverksamheten bör regleras, måste följaktligen den anpassningen göras vid genomförandet av direktivet.

Det är viktigt att samma begrepp används vid tillsyn av personuppgiftsbehandling på dataskyddsdirektivets respektive dataskyddsförordningens område. Därför finns det anledning att vara återhållsam med att använda annan terminologi än den som används i förordningen, om det inte finns goda sakliga skäl för det (se avsnitt 6.2).

Ett så enhetligt system för tillsyn över personuppgiftsbehandling som möjligt är också till fördel för både tillsynsmyndigheten och tillsynsobjekten. Reglerna om tillsyn på direktivets och förordningens område bör därför enligt regeringens mening så långt möjligt stämma överens, såvida det inte finns sakliga skäl för avvikelser.

En fri och oberoende tillsyn måste värnas

I skäl 4 i dataskyddsdirektivet framhålls att en hög skyddsnivå för personuppgifter förutsätter ett kraftfullt tillsynsarbete. Ett viktigt verktyg för det är en oberoende och effektiv tillsyn över behandlingen av personuppgifter. Direktivet medför bl.a. ökade krav på att tillsynsmyndigheternas oberoende värnas, att de får tillräckliga resurser och befogenheter att utöva sin tillsyn och att enskilda får möjlighet att reagera om tillsynsmyndigheten inte agerar tillräckligt snabbt.

Ett led i en effektivare tillsyn är, som framhålls i tillsynsskrivelsen, att skapa tydliga regler för verksamheten så att både tillsynsmyndigheten, tillsynsobjekten och enskilda som befarar att deras personuppgifter kan ha behandlats på ett otillåtet sätt vet vilka skyldigheter respektive rättigheter de har och vilka resultat som kan förväntas av tillsynen. Samtidigt är det lika viktigt att inte skapa detaljregler som riskerar att begränsa tillsynsmyndighetens möjligheter att arbeta oberoende och att prioritera bland sina arbetsuppgifter på det sätt som den anser bäst gagnar tillsynsverksamheten som helhet. Det är alltså en balansgång mellan att skapa tydliga regler och att inte åstadkomma ett regelsystem som riskerar att hämma tillsynsmyndighetens oberoende. Regeringens utgångspunkt är att en effektiv tillsyn bäst gagnas av att den som utövar tillsynen får så stor frihet att välja arbetsformer som möjligt, utan att avkall görs på rättssäkerheten. Den flexibilitet som den nuvarande, oreglerade, tillsynsverksamheten ger bör därför så långt möjligt värnas.

Direktivets dubbla syften

I avsnitt 6.1.3 redovisas att direktivet har dubbla syften. Det ska även prägla tillsynen. Tillsynsmyndigheten ska både skydda enskildas rättigheter och underlätta det fria flödet av personuppgifter inom EU. Vad det innebär behandlas i avsnitt 11.5.2. Mot den bakgrunden kan regleringen

som rör tillsynen inte byggas enbart utifrån enskildas perspektiv utan måste också beakta effekterna på det fria flödet av personuppgifter.

11.3 Tillsynsområdet

11.3.1 Tillsynsområdet bör slås fast i en definition

Regeringens förslag: I ramlagen ska tillsynsmyndigheten definieras som den myndighet som regeringen utser enligt direktivet för att utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: I avsnitt 6.1.2 föreslås att direktivet ska genomföras i en generellt tillämplig ramlag med tillhörande förordning. De kommer på samma sätt som i dag att kompletteras av myndigheternas registerförfattningar och författningar om särskilda register. Det finns även enstaka bestämmelser inom direktivets tillämpningsområde i andra författningar. Tillsynsmyndigheten ska enligt artikel 41.1 och artikel 46.1 övervaka tillämpningen av direktivet och de författningar som genomför det. Det innebär att tillsynsmyndigheten ska kunna utöva tillsyn över tillämpningen av både ramlagen och andra författningar som reglerar behandling av personuppgifter inom direktivets tillämpningsområde. En grundläggande fråga är hur det i ramlagen bör preciseras vad tillsynen ska omfatta.

Ett alternativ är att i ramlagen räkna upp de lagar som omfattas av tillsynen på samma sätt som i 1 § andra stycket lagen om tillsyn över viss brottsbekämpande verksamhet. Att all behandling av personuppgifter som utförs med stöd av ramlagen och den tillhörande förordningen ska omfattas av tillsynen är självklart. Eftersom det är syftet med behandlingen som är avgörande för om ramlagen eller dataskyddsförordningen är tillämplig (se avsnitt 6.4.1), och därigenom vilka tillsynsregler som ska tillämpas, kan tillsynsområdet inte avgränsas genom att det i ramlagen anges vilka författningar som omfattas av tillsynen. Dessutom reglerar flera av myndigheternas registerförfattningar i dag personuppgiftsbehandling inte bara inom direktivets tillämpningsområde utan även inom dataskyddsförordningens.

Av samma skäl – att det är syftet med behandlingen som är avgörande för om det ena eller andra regelverket ska tillämpas – bör tillsynsområdet inte heller knytas till en uppräkning av vissa myndigheter eller verksamheter. Tillsynsområdet måste därför, på samma sätt som ramlagens tillämpningsområde, bestämmas utifrån syftet med behandlingen av personuppgifter.

När det gäller definitionen av tillsynsmyndigheten noterar *Lagrådet* att ramlagen även innehåller bestämmelser om ”tillsynsmyndighet i en annan medlemsstat”, som inte bör omfattas av definitionen. Mot den bakgrunden och då den svenska tillsynsmyndigheten genomgående anges i

bestämd form i den föreslagna lagtexten, anser Lagrådet att tillsynsmyndigheten bör anges i bestämd form i definitionen. Regeringen håller med Lagrådet om detta. Vidare kan enligt Lagrådet den definition som regeringen föreslog i lagrådsremissen förkortas enligt följande: ”Myndighet som regeringen utser att utöva tillsyn över behandling av personuppgifter inom dataskyddsdirektivets tillämpningsområde”. Regeringen anser dock att det är viktigt att definitionen endast omfattar den tillsynsmyndighet som utses enligt dataskyddsdirektivet. Den får inte uppfattas som att den inkluderar andra myndigheter som kan komma att utöva tillsyn över behandling av personuppgifter inom dataskyddsdirektivets område, t.ex. Säkerhets- och integritetsskyddsnämnden. Definitionen av tillsynsmyndigheten bör därför vara den myndighet som regeringen utser enligt dataskyddsdirektivet för att utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

11.3.2 Undantag för dömande verksamhet

Regeringens förslag: Tillsynen ska inte omfatta behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet.

Utredningens förslag innehåller ingen särskild bestämmelse om tillsyn över behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet. Utredningen bedömer att dömande verksamhet redan skyddas genom bestämmelser i regeringsformen och att undantaget i direktivet därför inte kräver några lagstiftningsåtgärder.

Remissinstanserna: Vissa remissinstanser, bl.a. *Kammarrätten i Göteborg*, *Förvaltningsrätten i Stockholm* och *Domstolsverket*, anser att det är oklart om 11 kap. 3 § regeringsformen omfattar det som avses med dömande verksamhet i artikel 45.2 i direktivet och att det finns anledning att reglera undantaget för tillsyn över domstolar. Enligt Domstolsverket finns det goda skäl att anta att begreppet dömande verksamhet får en vidare betydelse i ett unionsrättsligt perspektiv jämfört med ett svenskt. *Umeå tingsrätt* framhåller att det är av stor betydelse att det i en lagstiftning av detta slag tydliggörs att tillsynen inte ska omfatta domstolarnas dömande verksamhet. Att det i regeringsformen finns skydd för domstolarnas beslutsfattande och rättstillämpning i enskilda fall är enligt tingsrätten inte tillräckligt.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 45.2 ska tillsynsmyndigheten inte vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet. Medlemsstaterna får även från tillsynsområdet undanta andra oberoende rättsliga instanser som behandlar personuppgifter inom ramen för sin rättsliga verksamhet. Av skäl 80 framgår att direktivet visserligen är tillämpligt på domstolars och andra rättsliga myndig-

heters verksamheter, men att tillsynsmyndigheterna inte bör ha behörighet att övervaka behandling av personuppgifter inom ramen för domstolars dömande verksamhet. Syftet är att garantera domares oberoende när de utför sina rättsliga uppgifter. Vidare framgår att undantaget bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare kan medverka i enlighet med sin nationella rätt. Slutligen anges att medlemsstaterna också bör kunna föreskriva att tillsynsmyndigheten inte ska vara behörig att övervaka andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet, exempelvis åklagarmyndigheter. Någon reglering som begränsar tillsynen över domstolarna på detta sätt finns inte i 1995 års dataskyddsdirektiv. Av artikel 55.3 i dataskyddsförordningen framgår också att tillsynsmyndigheterna inte ska vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

Hur utövas tillsyn över domstolarna i dag?

Enligt 11 kap. 3 § regeringsformen får ingen myndighet bestämma hur en domstol ska döma i det enskilda fallet eller hur en domstol i övrigt ska tillämpa en rättsregel i ett särskilt fall. Bestämmelsen ger uttryck för den centrala principen om domstolarnas självständighet i dömandet. Principen innebär att domstolarna i sitt dömande bara har att rätta sig efter rättsregler och inte får ta emot direktiv om hur de ska döma i ett enskilt fall.

Både JO och Justitiekanslern utövar tillsyn över domstolarna. Det har ansetts självklart att JO:s tillsyn över domstolarna inte får inkräkta på domstolarnas grundlagsfästa självständighet. Datainspektionen utövar tillsyn över domstolarnas personuppgiftsbehandling. I ett mål som rörde frågan om Datainspektionen kunde utöva tillsyn över den behandling av personuppgifter som ägt rum genom att en domstol publicerat upprops-listor på den egna webbplatsen uttalade Högsta förvaltningsdomstolen att 11 kap. 3 § regeringsformen inte omfattar sådana beslut som en domstol fattar i den egna verksamheten avseende domstolens administration. Det fanns därför inget som hindrade Datainspektionen att utöva tillsyn i det fallet (HFD 2014 ref. 32).

Frågan om det finns behov av att uttryckligen avgränsa tillsynsmyndighetens behörighet för att säkerställa domares självständiga ställning berördes varken när personuppgiftslagen eller domstolsdatalagen infördes.

Behövs det en ny reglering?

Den verksamhet som bedrivs av domstolarna är alltså inte generellt undantagen från tillsyn vare sig när det gäller personuppgiftsbehandling eller i övrigt. Det uttryckliga undantaget för dömande verksamhet är som ovan nämnts en nyhet i och med dataskyddsreformen. Tolkningen av begreppet dömande verksamhet är inte klar och därmed är det också osäkert hur stort område som ska vara undantaget från tillsyn. Utöver det nämnda HFD-avgörandet rörande domstolens administration saknas praxis kring tillämpningsområdet för 11 kap. 3 § regeringsformen när det gäller tillsyn över personuppgiftsbehandling. Som *Kammarrätten i Göteborg*, *Förvaltningsrätten i Stockholm* och *Domstolsverket* påpekar är det

därför oklart om undantaget i 11 kap. 3 § regeringsformen omfattar hela det område som avses med dömande verksamhet i artikel 45.2.

Det motsvarande undantaget för domstolarnas dömande verksamhet i artikel 55.3 i dataskyddsförordningen kommer att vara direkt tillämpligt på förordningens område. Enligt regeringen kan någon materiell skillnad mellan direktivet och förordningen inte vara avsedd i detta sammanhang. Det framstår därför som lämpligt att frågan om tillsyn över domstolarnas dömande verksamhet regleras på ett likartat sätt inom såväl direktivets som förordningens tillämpningsområde. En särskild reglering i ramlagen skulle tydliggöra att samma begränsning av tillsynsområdet gäller för all dömande verksamhet i domstolarna.

För att säkerställa ett korrekt genomförande av artikel 45.2 i direktivet och för att åstadkomma en tydlig reglering anser regeringen, i likhet med flera remissinstanser, att det i ramlagen bör tas in en bestämmelse som anger att tillsynen inte ska omfatta behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet. Uttrycket dömande verksamhet bör ges samma innebörd som i direktivet. Av skäl 80 till direktivet framgår att det aktuella undantaget bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka. Den närmare innebörden av begreppet får dock betraktas som oklar och bör överlämnas till rättstillämpningen att utveckla (se även prop. 2017/18:113, s. 23).

Enligt artikel 45.2 i direktivet finns det också en möjlighet att från tillsynsområdet undanta även andra rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet. En sådan reglering är dock frivillig och därför inte nödvändig för att genomföra direktivet. Något motsvarande undantag kommer inte att gälla på dataskyddsförordningens område. Regeringen anser därför att det inte bör införas något undantag avseende andra rättsliga myndigheter än domstolar.

11.4 Tillsynsmyndighet enligt direktivet och den fortsatta tillsynen över Polismyndighetens personuppgiftsbehandling

Regeringens bedömning: Datainspektionen bör utses till svensk nationell tillsynsmyndighet enligt dataskyddsdirektivet och bör delta i dataskyddsstyrelsens arbete.

Chefen för Datainspektionen bör anställas genom beslut av regeringen för en period om minst fyra år, med möjlighet till förlängning. I övrigt uppfyller svensk rätt dataskyddsdirektivets krav om tillsynsmyndighetens oberoende, organisation och utnämning respektive avsättande av tillsynsmyndighetens chef.

Det bör inte längre anges i Datainspektionens instruktion att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud.

Tillsynen över Polismyndighetens personuppgiftsbehandling inom dataskyddsdirektivets område bör även fortsättningsvis utföras både av Datainspektionen och Säkerhets- och integritetsskyddsnämnden.

Utredningens bedömning i betänkandet Ett samlat ansvar för tillsyn över den personliga integriteten (SOU 2016:65) överensstämmer delvis med regeringens bedömning. Utredningen föreslår att tillsynen över Polismyndighetens personuppgiftsbehandling ska utövas av Datainspektionen.

Remissinstanserna:

Ett samlat ansvar för tillsyn över den personliga integriteten (SOU 2016:65): Ingen remissinstans motsätter sig förslaget att peka ut Datainspektionen som nationell tillsynsmyndighet.

Endast ett fåtal remissinstanser yttrar sig särskilt över utredningens förslag om anställningsskydd, mandatperiod och möjlighet till förlängning för tillsynsmyndighetens chef och utredningens bedömning att svensk rätt i allt väsentligt motsvarar direktivets krav på tillsynsmyndighetens organisation och utnämningen respektive avsättandet av tillsynsmyndighetens chef. *Datainspektionen* tillstyrker att tillsynsmyndighetens chef anställs av regeringen för en period om minst fyra år men anför att anställningen lämpligen endast bör kunna förlängas två gånger och att myndighetens chef inte bör kunna förflyttas till annan statlig tjänst under pågående anställning. *Arbetsgivarverket* avstyrker förslaget om att tillsynsmyndighetens chef bör förordnas för en initial period om fyra år i stället för de gängse sex åren. *Sveriges advokatsamfund* ifrågasätter om inte anställningen som tillsynsmyndighetens chef bör tillsättas med fullmakt. Övriga remissinstanser som yttrar sig i dessa frågor har inte någon erinran mot utredningens förslag.

Datainspektionen och *Stockholms universitet* tillstyrker utredningens förslag om att myndighetens instruktion inte längre ska ange att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud. *IT&Telekomföretagen* menar dock att en sådan ändring vore olycklig med hänsyn till det stora behovet av information och vägledning till personuppgiftsombud. Övriga remissinstanser yttrar sig inte särskilt i denna fråga.

Ett fåtal remissinstanser, däribland *Polismyndigheten* och *Datainspektionen*, yttrar sig särskilt över utredningens förslag om att begränsa Säkerhets- och integritetsskyddsnämndens tillsynsansvar. De är i huvudsak positiva till utredningens förslag. *Säkerhets- och integritetsskyddsnämnden* anför dock att förslaget inte kan förväntas innebära en förstärkning av den enskildes personliga integritet.

Brottsdatalag (SOU 2017:29): *Förvaltningsrätten i Stockholm* anser att tillsynsmyndigheten bör anges i ramlagen.

Skälen för regeringens bedömning: I likhet med utredningen anser regeringen att Datainspektionen bör utses till svensk nationell tillsynsmyndighet enligt dataskyddsdirektivet (se artikel 41.1), och delta i dataskyddsstyrelsens arbete. Detta bör, till skillnad från vad *Förvaltningsrätten i Stockholm* anför, ske på förordningsnivå. Såsom utredningen anför finns det dock inget hinder mot att viss tillsyn även i fortsättningen utförs av andra myndigheter (SOU 2016:65 s. 146 f.).

I dataskyddsdirektivet finns krav på författningsreglering av vissa förhållanden som gäller utnämningen och avsättandet av tillsynsmyndighetens chef (se artikel 44.1 d). Den svenska ordningen innebär att motsvarande förhållanden inte är författningsreglerade i alla delar varför en ändring behövs. Detta bör ske på förordningsnivå. Till skillnad från *Datainspektionen* och *Arbetsgivarverket* bedömer regeringen att utredningens förslag om en anställningstid för myndighetschefen om minst fyra år, med obegränsade möjligheter till förlängning, är väl avvägd. Förslaget följer regleringen i såväl dataskyddsförordningen som dataskyddsdirektivet. Vidare instämmer regeringen i utredningens bedömning att svensk rätt innehåller bestämmelser som ger ett starkt anställningsskydd och som innebär ett förbud mot godtyckliga avskedanden, inte minst när det gäller chefer för förvaltningsmyndigheter. En chef för en förvaltningsmyndighet under regeringen som har en tidsbegränsad anställning får visserligen förflyttas enligt 33 § lagen (1994:260) om offentlig anställning (LOA) till en annan motsvarande statlig anställning. För detta förutsätts dock att en förflyttning krävs av organisatoriska skäl eller annars motiveras av hänsyn till myndighetens bästa. Enligt utredningen innebär även dessa krav ett tillräckligt skydd mot att regeringen, som dessutom fattar sina beslut under parlamentariskt ansvar, på godtyckliga grunder gör sig av med en myndighetschef. Regeringen delar utredningens bedömning och det saknas skäl för att tillsynsmyndighetens chef bör ha ett ännu starkare anställningsskydd och anställas med fullmakt, något som *Sveriges advokatsamfund* förordar, eller undantas från förflyttningsmöjligheten enligt LOA, något som Datainspektionen förordar. Det finns inte heller i övrigt anledning att ifrågasätta utredningens bedömning att svensk rätt dels uppfyller dataskyddsdirektivets krav på att tillsynsmyndigheten ska vara fullständigt oberoende (artikel 42), dels motsvarar dataskyddsdirektivets bestämmelser om tillsynsmyndighetens organisation och utnämning respektive avsättande av tillsynsmyndighetens chef (artiklarna 42.5, 43 och 44.1). Detta gäller bland annat kraven på ett öppet rekryteringsförfarande, skydd mot godtyckligt avskedande och förbud mot förtroendeskadliga bisysslor, där allmänna författningsregleringar redan finns. Uppgifter om vilka som har sökt en utannonserad tjänst som chef för en förvaltningsmyndighet under regeringen kan visserligen omfattas av sekretess. Sekretessen tar sikte på allmänhetens möjligheter att med stöd av den svenska offentlighetsprincipen begära ut uppgifterna. Den hindrar däremot inte att utnämningsprocessen kan vara föremål för annan insyn, exempelvis inom ramen för riksdagens granskning av regeringen.

Dataskyddsdirektivet förutsätter också en nationell reglering av de kvalifikationer som krävs för en anställning som myndighetschef. I likhet med utredningen menar regeringen att det krav på förtjänst och skicklighet som följer av regeringsformen och LOA samt saklighetskravet i 1 kap. 9 § regeringsformen sammantaget innebär ett krav på att den som anställs som chef för Datainspektionen ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området för dataskydd, som krävs för att ledamoten ska kunna fullgöra sitt uppdrag och utöva sina befogenheter.

Av dataskyddsförordningen framgår vilka uppgifter en tillsynsmyndighet enligt dataskyddsförordningen har. Med hänsyn till förordningens

krav på oberoende är utrymmet för regeringen att styra Datainspektionen genom regleringar i myndighetsinstruktionen begränsat. Regeringen delar därför Datainspektionens och *Stockholms universitets* bedömning att Datainspektionens instruktion inte längre bör ange att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud.

Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden har i dag tillsyn över personuppgiftsbehandling i Polismyndighetens brottsbekämpande verksamhet. Utredningen föreslår att tillsynen endast ska utföras av Datainspektionen.

Den renodling av tillsynen som utredningen föreslår har å ena sidan uppenbara fördelar. Å andra sidan har Säkerhets- och integritetsskyddsnämnden tillsyn över polisens användning av hemliga tvångsmedel och därmed sammanhängande verksamhet. Kunskapen om och erfarenheten av den granskade verksamheten ökar förutsättningarna för att tillsynen inriktas på områden som kan ge upphov till särskilda risker från integritetssynpunkt. Det parallella tillsynsuppdraget kan alltså bidra till att tillsynen blir förstärkt och mer allsidig. Vidare kan Säkerhets- och integritetsskyddsnämndens parlamentariska anknytning öka förutsättningarna för att allmänheten ska känna förtroende för verksamheten. Myndigheterna har också utarbetat en praxis för att hantera de eventuella problem som kan uppstå med ett parallellt tillsynsansvar. Enligt en granskningsrapport från Riksrevisionen, Tillsyn över brottsbekämpande myndigheter – En granskning av Säkerhets- och integritetsskyddsnämnden (RiR 2016:2), utför Säkerhets- och integritetsskyddsnämnden sina uppgifter på ett ändamålsenligt sätt och de brottsbekämpande myndigheter som Säkerhets- och integritetsskyddsnämnden utför tillsyn över tar nämndens uttalanden på allvar. I likhet med *Säkerhets- och integritetsskyddsnämnden* menar regeringen av ovan anförda skäl att utredningens förslag inte kan förväntas innebära en förstärkning av den enskildes personliga integritet. Vidare saknas det anledning att anta att myndigheternas samarbete för att hantera de eventuella problem som kan uppstå med ett parallellt tillsynsansvar inte skulle kunna fortsätta även efter genomförandet av EU:s dataskyddsreform. Regeringens bedömning är därför, till skillnad från bland andra *Polismyndighetens* och Datainspektionens bedömning, att den nuvarande ordningen och rollfördelningen bör behållas. Frågan om det bör föranleda någon ändring i lagen om tillsyn över viss brottsbekämpande verksamhet kommer att behandlas i samband med att myndigheternas registerförfattningar anpassas.

11.5 Tillsynsmyndighetens uppdrag

11.5.1 Tillsynsmyndighetens oberoende ska värnas

Regeringens bedömning: Tillsynsmyndighetens oberoende ställning värnas bäst om det inte införs några regler om när och hur tillsyn ska inledas respektive avslutas eller hur tillsynen närmare ska bedrivas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Sveriges advokatsamfund* anser att ramlagen uttryckligen bör slå fast att tillsynsmyndigheten ska vara oberoende.

Skälen för regeringens bedömning

Hur ska myndighetens oberoende säkerställas?

Tillsynsmyndigheten ska enligt artikel 42.1 vara fullständigt oberoende när den utför sitt uppdrag. Oberoendet ska enligt artiklarna 42.2–6, 43 och 44 framför allt värnas genom olika organisatoriska åtgärder och vissa rättsliga befogenheter enligt artikel 47.5. Som konstaterats i avsnitt 11.4 uppfyller svensk rätt, med de ändringar som nu föreslås i förordning, direktivets krav i dessa delar.

Tillsynsmyndigheten förutsätts göra en självständig granskning av hur personuppgiftsansvariga och personuppgiftsbiträden tillämpar lagar och andra bindande föreskrifter. Det är fråga om rättslig tillsyn, vilket har betydelse både för hur tillsynen utförs och vad den kan resultera i.

Tillsynsverksamhet är i dag till stor del oreglerad. Även om det finns regler om ramarna för tillsynen – exempelvis i vilka fall en myndighet har rätt att utöva tillsyn, vilka som står under tillsyn och vad tillsynen omfattar – saknas det närmare regler om hur tillsynen ska bedrivas. Skälet till det är bl.a. att tillsyn kan avse vitt skilda sektorer av samhället och ha olika fokus, från konkreta åtgärder på plats som inspektion av djur eller anläggningar till rättsligt inriktad tillsyn. Tillsynsuppgifterna, befogenheterna och resultatet av tillsynen kan därmed variera avsevärt. Därför är det inte lämpligt att i en särskild lag reglera tillsyn generellt (skr. 2009/10:79 s. 10 f.).

Regleringen i direktivet måste uppfattas på det sättet att tillsynsmyndighetens oberoende ska värnas dels genom organisatoriska åtgärder, dels genom att myndigheten ska vara fri när det gäller urvalet av tillsynsobjekt, arbetsformerna och redovisningen av resultaten av tillsynen. Vid genomförandet av direktivet finns det skäl att vara återhållsam med detaljregler som kan påverka hur tillsynsverksamheten bedrivs eller som kan göra att tillsynsmyndighetens oberoende ställning kan ifrågasättas. Det innebär att de regler som ändå krävs för att genomföra direktivet måste säkerställa att tillsynen kan bedrivas oberoende och effektivt. Regleringen måste nämligen ge tillsynsmyndigheten frihet att välja att utöva tillsynen på det sätt som den anser vara bäst inom de ramar som lagstiftningen ger.

Vad behöver regleras?

Enligt de principer som utvecklats i praxis avgör en tillsynsmyndighet själv när och hur den ska inleda tillsyn och vad tillsynen ska omfatta. Tillsynsmyndigheten kan utöva tillsyn på eget initiativ, t.ex. på grund av egna iakttagelser, efter information från allmänheten eller en annan myndighet eller med anledning av inkomna klagomål. Tillsyn kan också ha sin grund i att myndigheten vill se hur ny lagstiftning tillämpas eller få underlag för att bedöma behovet av nya råd eller föreskrifter. I framtiden bör – förutom tillsyn på begäran av en utländsk myndighet – även rapportering av personuppgiftsincidenter eller uppföljning av förhandssam-

råd kunna leda till att tillsynsmyndigheten inleder tillsyn i någon form (se avsnitt 9.4.2 och 9.2.5).

Att det inte är reglerat vad som kan initiera tillsyn verkar inte ha vållat några problem hittills. I direktivet förutsätts inte heller att det ska regleras. Det finns därför inte skäl att införa bestämmelser om i vilka situationer tillsyn bör initieras, särskilt som det skulle kunna uppfattas som en begränsning av myndighetens oberoende.

Regeringen instämmer i utredningens uppfattning att det framför allt är tillsynsområdet (avsnitt 11.3.1), vem som ska utöva tillsyn (avsnitt 11.4), tillsynsmyndighetens uppgifter (avsnitt 11.6) och vilka befogenheter tillsynsmyndigheten ska ha (avsnitt 11.7) som behöver regleras. Det behövs även vissa regler om handläggningen av ärenden (avsnitt 11.8). Någon ytterligare reglering av hur tillsynsmyndigheten ska arbeta bör däremot inte införas av hänsyn till myndighetens oberoende. Det ställningstagandet ligger i linje med hur Utredningen om tillsynen över den personliga integriteten ser på behovet att reglera tillsynsmyndighetens uppgifter vid tillsyn över regleringen i dataskyddsförordningen (SOU 2016:65 s. 154 f.). Ett förslag innebärande en begränsad reglering är enligt regeringens uppfattning det bästa sättet att värna tillsynsmyndighetens oberoende. Regeringen delar således inte *Sveriges advokatsamfunds* uppfattning att tillsynsmyndighetens oberoende uttryckligen ska framgå av ramlagen.

Att det saknas formella regler för hur tillsyn kan inledas innebär naturligtvis inte att den nya förvaltningslagen (2017:900) inte är tillämplig, om tillsynsmyndigheten väljer att lägga upp ett formellt ärende. Då gäller vanliga regler om dokumentation, inhämtande av yttranden och kommunikationsskyldighet. Regeringen återkommer i avsnitt 11.8 till vissa handläggningsfrågor.

11.5.2 Tillsynsmyndigheten ska ha dubbla perspektiv

Regeringens förslag: Tillsynsmyndigheten ska verka både för att fysiska personers grundläggande rättigheter och friheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom ramlagens tillämpningsområde.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* avstyrker utredningens förslag om att tillsynsmyndigheten, utöver att verka för att fysiska personers grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter, även ska verka för att underlätta det fria flödet av personuppgifter inom ramlagens tillämpningsområde.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Av artikel 41.1 framgår att tillsynsmyndighetens övergripande uppdrag ska vara att övervaka reglerna om behandling av personuppgifter i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen och underlätta det fria flödet av personuppgifter

inom EU. Enligt 1 § Datainspektionens instruktion ska inspektionen bl.a. verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.

Tillsynsmyndighetens övergripande uppdrag ska regleras

Regeringen avser, som tidigare nämnts, att utse Datainspektionen till tillsynsmyndighet enligt både direktivet och dataskyddsförordningen och myndighetens instruktion kommer att ändras i detta avseende.

Av artikel 41.1 framgår att tillsynsmyndigheten ska vara ansvarig för tillämpningen av direktivet, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen och att underlätta det fria flödet av personuppgifter inom unionen. Genom formuleringen tydliggörs att tillsynsmyndigheten inte enbart kan utgå från enskildas perspektiv utan även ska beakta att ett viktigt syfte med direktivet är att underlätta informationsutbyte mellan bl.a. brottsbekämpande myndigheter (skäl 7).

Datainspektionen anser att artikel 41.1 innebär att tillsynsmyndigheten ska övervaka tillämpningen av direktivet och inte att tillsynsmyndighetens uppdrag ska präglas av dubbla perspektiv. I skäl 75 som behandlar tillsynsmyndighetens uppdrag nämns endast skyddet av fysiska personer, vilket Datainspektionen anser ger stöd för inspektionens uppfattning. Regeringen delar inte Datainspektionens tolkning. Att skäl 75 enbart tar upp det ena perspektivet minskar enligt regeringens mening inte betydelsen av att båda perspektiven nämns i artikel 41.1. Samtidigt som tillsynsmyndigheten ska verka för en hög skyddsnivå för personuppgifter och bedriva ett kraftfullt tillsynsarbete, måste myndigheten därför även beakta de behöriga myndigheternas perspektiv.

Regeringen anser att tillsynsmyndighetens övergripande uppdrag att övervaka att fysiska personers grundläggande rättigheter och friheter skyddas vid behandling av personuppgifter är så viktigt att det bör få en framskjuten plats i ramlagen. Om det uppdraget lyfts fram bör det också framgå att myndigheten när den utför sina uppgifter och utövar sina befogenheter även ska beakta att det fria flödet av personuppgifter inom EU underlättas. Som framgår av avsnitt 14.2.2 gäller direktivet även för vissa andra stater än EU:s medlemsstater. Det är således det fria flödet av personuppgifter inom ramlagens tillämpningsområde som ska underlättas.

Frågan är då vad det innebär för tillsynsmyndigheten att direktivets dubbla syften lyfts fram i artikel 41.1. Det är uppenbart att dessa intressen kan strida mot varandra i vissa fall. Regeringen instämmer i utredningens uppfattning att det inte är självklart hur tillsynsmyndigheten kan underlätta det fria flödet av personuppgifter. Att direktivets båda syften även kommit till uttryck i den grundläggande bestämmelsen om tillsynsmyndigheten måste enligt regeringen uppfattas så att det ställs krav på myndigheten utifrån båda perspektiven. Vid sidan av enskildas intresse av en hög skyddsnivå ska tillsynsmyndigheten även beakta intresset av ett fritt flöde av personuppgifter. Direktivet ger ingen närmare vägledning kring hur avvägningen mellan dessa intressen ska göras. Det är följaktligen tillsynsmyndigheten som måste göra detta. Övergripande kan dock konstateras att om det finns utrymme att välja olika lösningar som kan betraktas som likvärdiga ur integritetssynpunkt, bör tillsynsmyndig-

heten välja den som bäst tillgodoser det fria flödet av personuppgifter. Ett annat exempel kan vara att myndigheten underlättar informationsutbytet genom att sprida sådan kunskap som den fått genom att följa utvecklingen av informations- och kommunikationsteknik eller goda exempel som kan förbättra skyddet för personuppgifter (jfr artikel 46.1 j).

11.6 Tillsynsmyndighetens uppgifter

11.6.1 Huvuduppgifterna bör regleras i ramlagen

Regeringens förslag: Tillsynsmyndigheten ska
1. utöva allmän tillsyn över personuppgiftsbehandling,
2. handlägga klagomål från registrerade,
3. utföra kontroll på begäran av fysiska personer, och
4. på begäran bistå en tillsynsmyndighet i en annan medlemsstat.

Tillsynsmyndigheten ska även ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd och när det i övrigt är påkallat.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens förslag

Innehållet i direktivet

I artikel 46.1 räknas tillsynsmyndighetens konkreta arbetsuppgifter upp. Enligt punkt a har tillsynsmyndigheten det generella uppdraget att övervaka och verkställa tillämpningen av de bestämmelser som antas i enlighet med direktivet. De närmare tillsynsuppgifterna regleras i punkterna f–i. Där anges att tillsynsmyndigheten ska behandla klagomål från registrerade, kontrollera om viss behandling är laglig, samarbeta med och ge bistånd till tillsynsmyndigheter i andra medlemsstater och utföra undersökningar om tillämpningen av direktivet.

Tillsynsmyndigheten har också en vidsträckt skyldighet att ge råd och lämna information till olika aktörer. Myndigheten ska enligt punkt b öka allmänhetens medvetenhet och kunskaper om risker, regler, skyddsåtgärder och rättigheter i samband med personuppgiftsbehandling. Personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter ska enligt punkt d också ökas. Enligt punkt c ska myndigheten i enlighet med nationell rätt ge råd åt nationella parlament, regeringen och andra institutioner och organ om lagstiftningsmässiga och administrativa åtgärder som rör skyddet för fysiska personer vid personuppgiftsbehandling. Myndigheten ska vidare enligt punkt e på begäran informera registrerade om hur de ska utöva sina rättigheter och för det ändamålet samarbeta med tillsynsmyndigheter i andra medlemsstater. Myndigheten ska också enligt punkt k ge råd till personuppgiftsansvariga och personuppgiftsbiträden om behandling av personuppgifter som innebär särskilda risker (se närmare om förhandssamråd i avsnitt 9.2.5).

Slutligen ska tillsynsmyndigheten enligt punkt j följa sådan utveckling som påverkar skyddet av personuppgifter, bl.a. inom informations- och kommunikationsteknik, och enligt punkt l bidra till verksamheten vid den styrelse som ska inrättas enligt artikel 51.

Nuvarande reglering

Enligt 1 § Datainspektionens instruktion ska myndigheten bl.a. följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Den ska särskilt inrikta sin verksamhet på att informera om gällande regler och ge råd och hjälp åt personuppgiftsombud.

De huvudsakliga tillsynsuppgifterna bör regleras

Eftersom direktivet ska genomföras i svensk rätt är det lämpligt att reglera uppgiften att bedriva tillsyn men frågan är hur det bör göras. Vissa av tillsynsmyndighetens uppgifter måste under alla förhållanden regleras. Med hänsyn till tillsynsmyndighetens oberoende är det inte lämpligt att bara reglera vissa uppgifter, eftersom det kan uppfattas som att de uppgifterna tillmäts större vikt. Mot den bakgrunden bör tillsynsmyndighetens huvuduppgifter framgå direkt av ramlagen. Som angetts i avsnitt 11.2 och 11.5 bör dock regleringen inte gå utöver vad som är nödvändigt för att genomföra direktivet, med hänsyn till tillsynsmyndighetens oberoende.

I ramlagen bör det tas in bestämmelser som återger tillsynsmyndighetens huvuduppgifter så som de anges i direktivet. De är att utöva allmän tillsyn över personuppgiftsbehandling (avsnitt 11.5), att handlägga klagomål från registrerade (avsnitt 11.6.2), att kontrollera om behandling är författningsenlig (avsnitt 11.6.3), att ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd och när det i övrigt är påkallat (avsnitt 11.6.4) och att på begäran lämna bistånd till en tillsynsmyndighet i en annan medlemsstat (avsnitt 11.10.1).

Under tillsynsmyndighetens uppdrag att bedriva allmän tillsyn ryms enligt regeringens mening de uppgifter som nämns i artikel 46.1 punkterna a och i. Under uppgiften att lämna bistånd till en utländsk tillsynsmyndighet ryms artikel 46.1 punkt h.

11.6.2 Klagomål från enskilda

Regeringens bedömning: Förutom att det ska framgå att handläggning av klagomål ingår i tillsynsuppgifterna bör det inte regleras hur tillsynsmyndigheten ska behandla klagomål.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans har något att invända i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

Enligt artikel 52.1 har alla registrerade rätt att lämna in klagomål till tillsynsmyndigheten. Enligt artikel 46.1 f ska tillsynsmyndigheten behandla klagomål från en registrerad eller dennes ombud och inleda en undersökning i sak där så är lämpligt. Tillsynsmyndigheten ska inom rimlig tid underrätta den klagande om hur undersökningen fortskrider och om resultatet, särskilt om det krävs ytterligare undersökningsåtgärder eller samordning med en tillsynsmyndighet i en annan medlemsstat.

Enligt artikel 52.2–4 ska tillsynsmyndigheten utan dröjsmål överlämna ett klagomål som lämnats till fel tillsynsmyndighet till behörig myndighet och informera den registrerade om det. Därutöver ska den registrerade på begäran få ytterligare hjälp. Han eller hon ska underrättas om klagomålets handläggning och resultat och om rätten till rättsmedel enligt artikel 53. Enligt artikel 46.2 ska tillsynsmyndigheten underlätta inlämningen av klagomål, exempelvis genom att tillhandahålla elektroniska formulär, vilket inte ska utesluta andra former av inlämning.

Nuvarande reglering och tillämpning

Att vem som helst kan göra en framställning till en myndighet, som då är skyldig att behandla den, följer av allmänna förvaltningsrättsliga principer. En myndighet är enligt förvaltningslagen skyldig att lämna enskilda råd och hjälp genom att bl.a. vidarebefordra felsända handlingar till rätt myndighet. Myndigheterna anses vidare vara skyldiga att informera om handläggningen och resultatet av en framställning som gjorts och vid behov samverka med andra myndigheter. En myndighet som får in en framställning från en enskild anses också vara skyldig att lämna någon form av svar som inte får dröja längre än nödvändigt (prop. 1985/86:80 s. 59 och prop. 2016/17:180 s. 66 f).

Den som ger in ett klagomål till en tillsynsmyndighet har enligt rättspraxis inte någon rätt att överklaga tillsynsmyndighetens beslut i tillsynsfrågan (jfr RÅ 2010 ref. 29).

I dag tar Datainspektionen emot klagomål över behandling av personuppgifter. Inspektionen avgör själv när det finns anledning att inleda ett tillsynsärende. Den klagande får alltid ett besked i någon form med anledning av klagomålet. Ibland underrättas den enskilde om att någon utredning inte kommer att göras i hans eller hennes fall, men att informationen i klagomålet kan komma att användas i tillsyn vid ett senare tillfälle (SOU 2016:65 s. 81).

Behöver klagomålshanteringen regleras?

Artikel 46.1 f förutsätter inte att alla klagomål som kommer in till tillsynsmyndigheten utreds, däremot att alla klagomål behandlas. Frågan är då vad som avses med det. Av skäl 81 framgår att tillsynsmyndigheten bör hantera klagomål från registrerade och att utredning bör göras i den utsträckning som det är lämpligt i det enskilda fallet. Regleringen i direktivet förefaller utgå från att klagomål alltid framförs skriftligen men det är inte ett krav. Ordet behandla bör här tolkas som ett krav på att klagomål måste leda till någon form av handläggning. Det minsta som kan

krävas är att tillsynsmyndigheten tar ställning till om klagomålet ska föranleda någon tillsynsåtgärd. Tillsynsmyndigheten får med andra ord inte helt negligera ett klagomål. Här räcker det dock att konstatera att en utredning i sak bara behöver göras om tillsynsmyndigheten anser att det är lämpligt i det enskilda fallet. Enligt artikel 53.2 ska tillsynsmyndigheten informera om resultatet av klagomålet. Vad det innebär diskuteras i avsnitt 13.6.

I likhet med utredningen anser regeringen att starka skäl talar för att tillsynsmyndigheten även fortsättningsvis ska ha stor frihet att bestämma om klagomål ska utredas. Bestämmelserna i direktivet om hur klagomål ska hanteras av tillsynsmyndigheten motsvarar vad som redan tillämpas enligt allmänna principer för tillsyn och reglerna i förvaltningslagen. Enligt regeringen krävs det därför, utöver att det ska framgå att handläggning av klagomål ingår i tillsynsuppgifterna, inga lagstiftningsåtgärder för att genomföra bestämmelserna i artiklarna 46.1 f, 52.3 och 52.4. Eftersom regeringen avser att utse endast Datainspektionen till svensk nationell tillsynsmyndighet enligt direktivet behöver inte heller artikel 52.2 genomföras. Regeringen återkommer i avsnitt 13 till frågor som rör klagomål och rättsmedel.

Den allmänna serviceskyldigheten rymmer att en myndighet ska tillhandahålla de formulär och blanketter som behövs för verksamheten. Det behövs därför inga lagstiftningsåtgärder för att genomföra artikel 46.2.

11.6.3 Kontroll av om behandling är författningsenlig

Regeringens förslag: Tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär en sådan kontroll ska visa att han eller hon har begärt information från eller en korrigeringsåtgärd av den personuppgiftsansvarige. Myndigheten ska få vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad.

Regeringens bedömning: Vilka formkrav som ska gälla för begäran och beslut om kontroll och hur sökanden ska underrättas om att kontrollen har utförts kan regleras i förordning.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* konstaterar att kontrollerna som behandlas i detta avsnitt är en ny uppgift för inspektionen och anser att regleringen inte ska gå utöver de krav som ställs i direktivet. *Säkerhets- och integritetsskyddsnämnden* anser att direktivet inte kräver att sökanden har rätt till kontroll när den personuppgiftsansvarige har lämnat begärd information eller vidtagit korrigeringsåtgärder. Nämnden påpekar vidare att tillsynsmyndighetens underrättelse till sökanden kan kräva att sekretessbrytande bestämmelser införs.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet och nuvarande reglering

Personuppgiftsansvariga får under vissa förutsättningar begränsa enskildas rätt till information eller underlåta att lämna information. I sådana fall ska den registrerades rättigheter enligt artikel 17.1 kunna utövas genom tillsynsmyndigheten. Tillsynsmyndigheten ska då enligt artikel 46.1 g kontrollera om behandlingen är laglig och enligt artikel 17.3 inom rimlig tid underrätta den registrerade om att kontrollen har genomförts. Den registrerade ska också informeras om rätten att begära rättslig prövning. Om en begäran om kontroll är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får tillsynsmyndigheten enligt artikel 46.4 ta ut en rimlig avgift för de administrativa kostnaderna eller vägra att tillmötesgå begäran. Tillsynsmyndigheten har bevisbördan för att begäran är uppenbart ogrundad eller orimlig. Enligt artikel 46.1 g ska tillsynsmyndigheten informera den registrerade om skälen för att någon kontroll inte genomförs.

I artikel 28.4 i 1995 års direktiv föreskrivs att var och en har rätt att hos tillsynsmyndigheten begära att en kontroll görs av om personuppgiftsbehandlingen är tillåten och att få besked om utfallet av begäran. Någon sådan rätt infördes dock inte när det direktivet genomfördes. I Säkerhets- och integritetsskyddsnämndens uppdrag ingår att göra sådana kontroller. Enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet är Säkerhets- och integritetsskyddsnämnden skyldig att på begäran av enskilda kontrollera om deras personuppgifter har behandlats enligt polisdatalagen och om behandlingen har utförts författningsenligt. Den enskilde ska underrättas om att kontrollen har utförts. Även juridiska personer kan begära sådan kontroll.

Datainspektionen är i dag inte skyldig att utföra sådana kontroller. Myndigheten kan inom ramen för sin tillsyn utföra liknande kontroller, men den enskilde har inte någon rätt att kräva det. Datainspektionen hänvisar därför enskilda till Säkerhets- och integritetsskyddsnämnden när inspektionen får en begäran om kontroll inom ett område där nämnden utövar tillsyn. Nämnden är bara skyldig att utföra sådana kontroller när det gäller Polismyndighetens och Säkerhetspolisens personuppgiftsbehandling.

Kontroll av om behandlingen är författningsenlig bör regleras

Att en enskild kan få information om och insyn i hur hans eller hennes personuppgifter behandlas är som tidigare nämnts en förutsättning för att han eller hon ska kunna kontrollera om behandlingen är författningsenlig och i övrigt ta till vara sina intressen och rättigheter. Det kan t.ex. gälla att få felaktiga personuppgifter rättade, kompletterade eller raderade eller att göra andra invändningar mot behandlingen. I avsnitt 10.3.1 redovisas på vilka grunder den personuppgiftsansvarige kan begränsa eller underlåta att lämna information. När den enskilde, till följd av att den personuppgiftsansvarige utnyttjat en sådan möjlighet, saknar möjlighet att ta till vara sin rätt ska det ändå vara möjligt att kontrollera personuppgiftsbehandlingen. Då ska tillsynsmyndigheten enligt direktivet kontrollera om behandlingen är författningsenlig.

Kontrollen ska utföras av en myndighet som har utsetts till tillsynsmyndighet enligt direktivet. Att tillsynsmyndigheten ska vara skyldig att på begäran kontrollera om behandlingen är författningsenlig bör regleras i ramlagen. Detta hindrar dock inte att även andra myndigheter kan ha motsvarande skyldigheter. Det finns därför inget hinder mot att Säkerhets- och integritetsskyddsnämnden behåller sina skyldigheter enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet.

Hur bör regleringen utformas?

Kontrollerna kan bli resurskrävande inom ramlagens tillämpningsområde eftersom sekretess inom vissa verksamheter i stor utsträckning medför att information om personuppgiftsbehandlingen inte kan lämnas. Det är därför inte lämpligt att införa en kontrollskyldighet som går utöver de krav som ställs i direktivet.

Utredningen har föreslagit att bara fysiska personer bör kunna kräva kontroll av om behandlingen är författningsenlig. Vidare bör enligt utredningen en förutsättning för kontroll vara att den som ger in begäran först har vänt sig till den personuppgiftsansvarige och begärt besked om vilka personuppgifter om honom eller henne som behandlas eller har begärt en korrigeringsåtgärd.

Säkerhets- och integritetsskyddsnämnden anser att rätten till kontroll inte bör föreligga om den personuppgiftsansvarige har lämnat den begärda informationen eller vidtagit den begärda korrigeringsåtgärden. Enligt nämnden uppfylls direktivets krav om kontrollskyldigheten inträder först när den personuppgiftsansvarige verkligen har begränsat informationen till den enskilde med stöd av den föreslagna bestämmelsen i 4 kap 5 § i ramlagen. Det är enligt nämnden i sådana fall som den enskilde själv saknar möjlighet att ta till vara sin rätt och kan antas ha ett befogat intresse av att tillsynsmyndigheten kontrollerar personuppgiftsbehandlingen.

Regeringen instämmer med Säkerhets- och integritetsskyddsnämnden i att det visserligen är i de fall då den enskilde själv saknar möjlighet att ta till vara sin rätt som det finns ett behov av kontroll. Regeringen kan emellertid inte se hur en reglering som begränsar kontrollskyldigheten till sådana situationer ska kunna hantera problematiken med hur det kan säkerställas att den enskilde får tillgång till tillräcklig information för att kunna ta till vara sin rätt. Även om besked lämnas till den enskilde från den personuppgiftsansvarige kan han eller hon inte med säkerhet veta om det föreligger en begränsning i den information som lämnas. Ytterligare behandling inom verksamheter som omfattas av sekretess kan förekomma och då föreligger hinder mot att lämna ut information. Sekretessen kan innebära att inte ens en uppgift om huruvida personuppgifter behandlas kan lämnas. Förutsättningen för kontroll bör därför som utredningen föreslagit vara att den som har begärt kontroll ska visa att han eller hon har begärt besked om vilka personuppgifter om honom eller henne som behandlas eller har begärt en korrigeringsåtgärd.

Syftet med kontrollen är inte att den enskilde genom tillsynsmyndigheten ska få kännedom om huruvida hans eller hennes uppgifter behandlas hos en behörig myndighet utan att en oberoende myndighet får insyn i sådan personuppgiftsbehandling som registrerade inte själva kan kontrol-

lera. Det bör därför regleras att tillsynsmyndigheten skriftligen ska underrätta den sökande om att kontrollen har genomförts. Underrättelsen bör som regel endast ge besked om att tillsynsmyndigheten har genomfört kontrollen (jfr prop. 2006/07:133 s. 66 f. och s. 81 och prop. 2009/10:85 s. 272 f.). Underrättelseskyldigheten kan enligt regeringens bedömning regleras i förordning. Enligt artikel 46.1 g ska underrättelsen lämnas inom rimlig tid. Enligt regeringens mening behöver detta inte regleras, eftersom kravet får anses följa av förvaltningslagen. *Säkerhets- och integritetsskyddsnämndens* synpunkter på förordningsregleringen om underrättelse kommer regeringen att ta ställning till i samband med framtagande av kompletterande föreskrifter.

Det bör ställas vissa krav på en begäran

För att regleringen inte ska kunna missbrukas bör det ställas vissa krav på en begäran om kontroll. Sådana krav kan enligt regeringens bedömning regleras i förordning.

Tillsynsmyndigheten ska kunna vägra att utföra kontroll

Tillsynsmyndigheten har enligt artikel 46.4 möjlighet att vägra att utföra kontroll om begäran är uppenbart ogrundad eller orimlig. Det bör framgå av ramlagen att kontroll kan vägras i sådana fall.

Frågan är när en begäran kan anses vara orimlig eller uppenbart ogrundad. Ett skäl som framhålls i direktivet är att förfrågan är repetitiv, dvs. att den återupprepas. Av skäl 43 framgår att fysiska personer bör ha rätt att med rimliga intervall utöva sin rätt att hålla sig underrättade om att behandling sker och kunna kontrollera om den är laglig. Någon ytterligare ledning för vad som är rimliga intervall ges inte i direktivet.

När personuppgiftslagen infördes ansåg regeringen, vid tolkningen av begreppet rimliga intervall i artikel 12 a i 1995 års dataskyddsdirektiv, att en enskild bör ha rätt att av den personuppgiftsansvarige en gång per kalenderår få besked om hans eller hennes personuppgifter behandlas (se 26 § personuppgiftslagen och prop. 1997/98:44 s. 82). Kontroller av om uppgifter om en person behandlas författningsenligt kan dock vara betydligt mer resurskrävande. Det beror bl.a. på att tillsynsmyndigheten – i motsats till den personuppgiftsansvarige – inte har tillgång till de personuppgifter som behandlas. Tillsynsmyndigheten måste därför alltid begära hjälp av den personuppgiftsansvarige med att klarlägga om några uppgifter om personen behandlas och kan först därefter ta ställning till vilken kontroll som i så fall krävs. Det är därför inte givet att de överväganden som gjordes beträffande registerutdrag enligt 26 § personuppgiftslagen har samma relevans för tillsynsmyndighetens kontroller.

Enligt regeringens mening är det inte lämpligt att i författning reglera hur lång tid som bör förflyta mellan framställningar om kontroll. Det bör i stället avgöras i praxis hur ofta en begäran får upprepas utan att den betraktas som orimlig.

En begäran om kontroll bör även kunna vägras om den är orimligt omfattande eller om den är så oprecis att det skulle krävas oproportionerligt mycket arbete för att kunna utföra kontrollen. Som exempel kan nämnas en opreciserad begäran om kontroll av om Polismyndighetens behandling av uppgifter om en person är författningsenlig. Det säger sig självt att en

sådan begäran, med hänsyn till Polismyndighetens knappt 30 000 anställda, hela landet som verksamhetsområde och mångskiftande arbetsuppgifter, skulle kräva orimliga insatser av både tillsynsmyndigheten och tillsynsobjektet. Det är tillsynsmyndigheten som har bevisbördan för att en begäran är orimlig eller uppenbart ogrundad.

Av skäl 40 – som hänför sig till artiklarna om enskildas rättigheter – framgår att en begäran bör anses som uppenbart ogrundad om den enskilde saknar skäl för sin begäran eller på annat sätt missbrukar sin rätt till information. I övrigt ger direktivet ingen ledning för i vilka fall en begäran kan anses vara uppenbart ogrundad. Enligt regeringens mening kan en begäran t.ex. vara uppenbart ogrundad om den som begär kontroll inte först begärt att den personuppgiftsansvarige lämnar information.

Ett beslut att vägra utföra kontroll bör kunna överklagas, om förutsättningarna i övrigt är uppfyllda (se avsnitt 13.7.1). Det bör därför krävas ett skriftligt beslut där skälen för vägran framgår. Det kan regleras i förordning.

Bör kontroll kunna utföras mot avgift?

Ett alternativ till att vägra utföra kontroll är enligt artikel 46.4 att tillsynsmyndigheten tar ut en rimlig avgift för de administrativa kostnaderna. Frågan är om den möjligheten bör utnyttjas vid genomförandet av direktivet. Å ena sidan talar ett av direktivets huvudsyften – att skydda den enskildes rättigheter – för att den enskilde i så stor utsträckning som möjligt ska få en kontroll utförd. Av artikel 46.4 följer å andra sidan att det är förenligt med direktivet att begränsa den enskildes rättigheter i vissa fall. En avgift kan inte läka bristen om en begäran är uppenbart ogrundad. Detsamma gäller en framställning som är orimlig av något annat skäl än att den upprepas alltför ofta. Det skulle kunna övervägas att ge enskilda möjlighet att mot avgift begära kontroll oftare än vad som är rimligt. Eftersom kontroll kan vara arbetskrävande anser regeringen att varken tillsynsmyndigheten eller tillsynsobjektet bör belastas med alltför täta kontroller. Möjligheten att ålägga tillsynsmyndigheten att mot avgift genomföra kontroller som är orimliga eller uppenbart ogrundade bör därför inte utnyttjas.

Information om rätt till rättslig prövning

Enligt artikel 17.3 och skäl 48 ska tillsynsmyndigheten även informera den registrerade om hans eller hennes rätt att begära rättslig prövning. Det är oklart vad som avses. Eftersom kontroll av om behandlingen är författningsenlig normalt inte utmynnar i något förvaltningsbeslut kan det inte annat än undantagsvis finnas något som en domstol kan pröva med anledning av kontrollen. Den enskilde har emellertid enligt artiklarna 53 och 54 rätt till effektiva rättsmedel om hans eller hennes rättigheter enligt direktivet kränks. Enligt utredningen bör det vara beslut om avslag på begäran om kontroll som avses. Regeringen delar denna bedömning. Regeringen återkommer till frågor om överklagande i avsnitt 13.7.1. Här räcker det att konstatera att det inte behövs någon lagstiftningsåtgärd för att tydliggöra att tillsynsmyndigheten, i de fall där ett beslut är överklagbart eller kan prövas på annat sätt, är skyldig att upplysa om det, eftersom den skyldigheten följer av andra regler.

11.6.4 Information och rådgivning

Regeringens förslag: Tillsynsmyndigheten ska vid förhandssamråd och när det i övrigt är påkallat ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

En central arbetsuppgift för tillsynsmyndigheten är att på eget initiativ eller på begäran ge information och råd till olika aktörer om regler som styr behandlingen av personuppgifter.

I artiklarna 46.1 c, 47.3 och 28.2 föreskrivs att tillsynsmyndigheten ska ha en rådgivande uppgift, genom att på eget initiativ eller på begäran avge yttranden om lagstiftning och administrativa åtgärder till riksdag, regering, andra myndigheter och organ och till allmänheten i frågor som rör skydd av personuppgifter. Enligt artikel 46.1 d ska tillsynsmyndigheten öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om deras skyldigheter enligt direktivet. Förhandssamråd, som regleras i artikel 28, innebär att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten bl.a. inför behandling av personuppgifter i nyinrättade register. Enligt artikel 46.1 k ska tillsynsmyndigheten då ge skriftliga råd.

Av artikel 46.1 b framgår att tillsynsmyndigheten självmant ska lämna allmän information om risker, regler, skyddsåtgärder och rättigheter till allmänheten. Vidare ska tillsynsmyndigheten enligt artikel 46.1 e på begäran tillhandahålla mer specifik information till registrerade om hur de ska utöva sina rättigheter och vid behov samarbeta med tillsynsmyndigheter i andra medlemsstater för det ändamålet. Av artiklarna 17.3, 52.3 och 52.4 framgår att den som har kontakt med tillsynsmyndigheten med anledning av en begäran om kontroll eller ett klagomål ska få mer specifik information om hur han eller hon ska ta till vara sin rätt i det aktuella fallet.

I 1 § Datainspektionens instruktion föreskrivs att inspektionen särskilt ska inrikta sin verksamhet på att informera om gällande regler och ge råd och hjälp åt personuppgiftsombud.

Förhandssamråd

I avsnitt 9.2.5 behandlas det förhandssamråd mellan personuppgiftsansvariga och tillsynsmyndigheten som krävs i vissa fall. Det som är av intresse här är tillsynsmyndighetens roll. Myndigheten ska ta emot sådana konsekvensbedömningar som ska upprättas enligt artikel 27, delta i samrådet och, om den planerade behandlingen riskerar att inte vara förenlig med regelverket, lämna skriftliga råd. Regeringen återkommer i avsnitt 11.7.5 till myndighetens befogenheter vid samrådet. Förhandssamråd är en viktig del i tillsynsmyndighetens förebyggande arbete och

bör därför uttryckligen anges i bestämmelsen om myndighetens rådgivande roll.

Information och rådgivning till personuppgiftsansvariga, personuppgiftsbiträden och dataskyddsombud

Genom direktivet ökar kraven på personuppgiftsansvariga och personuppgiftsbiträden i olika avseenden jämfört med i dag. Enligt artikel 46.1 d ska tillsynsmyndigheten öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om deras skyldigheter. Direktivet reglerar även dataskyddsombudens uppdrag mera i detalj. De ska bl.a. informera och ge råd till personuppgiftsansvariga om deras skyldigheter, övervaka efterlevnaden av regelverket och samarbeta och fungera som kontaktpunkt för tillsynsmyndigheten. Förändringarna bör enligt utredningens bedömning medföra att behovet av information och rådgivning från tillsynsmyndigheten till personuppgiftsansvariga, personuppgiftsbiträden och dataskyddsombud kommer att öka. Regeringen delar denna bedömning.

I avsnitt 11.4 gör regeringen bedömningen att det inte längre ska anges i Datainspektionens instruktion att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud. Det finns varken utrymme för eller behov av en sådan reglering på dataskyddsförordningens område (SOU 2016:65 s. 157 f.) Bedömningen ska ses mot bakgrund av att bestämmelsen innebär en anvisning från regeringen om hur tillsynsmyndigheten ska prioritera sina tillsynsuppgifter. En sådan regel anses enligt bedömningen inte vara förenlig med kraven på tillsynsmyndighetens oberoende.

Det väcker frågan om tillsynsmyndighetens informations- och rådgivningsskyldighet gentemot personuppgiftsansvariga och personuppgiftsbiträden enligt direktivet bör regleras. Regeringen delar utredningens bedömning att vissa krav på information och rådgivning, bl.a. artikel 46.1 d, går utöver det som ryms i den allmänna service- och samverkansskyldigheten enligt förvaltningslagen. Mot den bakgrunden bör även uppgiften att informera och ge råd till personuppgiftsansvariga och personuppgiftsbiträden pekas ut som en särskild uppgift för tillsynsmyndigheten. Det kan vara lämpligt att formulera uppgiften på liknande sätt som i den nu gällande 1 § Datainspektionens instruktion, att tillsynsmyndigheten ska ge råd och stöd. Skyldigheten bör omfatta råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden. Skyldigheten bör begränsas till information om deras författningsenliga skyldigheter.

Det finns enligt regeringens mening inget hinder mot att ange råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden som en uppgift bland flera, så länge regleringen inte innebär att den viktas högre eller lägre än någon av de övriga uppgifterna. Om tillsynsmyndighetens uppgifter regleras i ramlagen finns det inte heller någon risk för konflikt med vad som kommer att gälla på dataskyddsförordningens område. En reglering med denna innebörd i ramlagen står därmed inte i motsatsställning till bedömningen att uppgiften att särskilt inrikta verksamheten på att informera samt ge råd och hjälp inte längre bör anges i Datainspektionens instruktion i avsnitt 11.4. Av hänsyn till tillsynsmyndighetens oberoende bör bestämmelsen utformas så att det, förutom vid förhands-

samråd, tydligt framgår att myndigheten själv avgör när råd och stöd kan vara påkallat.

Även fortsättningsvis kommer dataskyddsombuden att behöva samråda med tillsynsmyndigheten i många frågor. De är i många fall den naturliga kontaktpunkten för tillsynsmyndigheten (avsnitt 9.5.3). I den utsträckning dataskyddsombud har behov av råd och stöd från tillsynsmyndigheten bör myndigheten naturligtvis på samma sätt som i dag tillgodose det behovet.

Information och rådgivning till riksdag, regering och andra myndigheter

I artikel 28.2 i 1995 års dataskyddsdirektiv finns motsvarande reglering om tillsynsmyndighetens rådgivande roll som i artiklarna 28.2, 46.1 c och 47.3 i det nya direktivet. När personuppgiftslagen infördes ansåg regeringen att svensk rätt uppfyllde de kraven utan någon lagstiftningsåtgärd (prop. 1997/98:44 s. 102).

Enligt 7 kap. 2 § regeringsformen ska vid beredningen av regeringsärenden behövliga upplysningar och yttranden begäras in från berörda myndigheter. Beredningskravet gäller för både riksstyrelseärenden, exempelvis beslut om propositioner och förordningar, och förvaltningsärenden (jfr prop. 2009/10:80 s. 215). Myndigheter under regeringen är skyldiga att svara på de remisser de får. I 10 kap. 8 § riksdagsordningen föreskrivs att en statlig myndighet är skyldig att lämna upplysningar och yttra sig när ett riksdagsutskott begär det.

Enligt förvaltningslagen är myndigheterna skyldiga att samverka med varandra i frågor som rör deras respektive verksamhetsområden. Skyldigheten enligt lagen att svara på remisser omfattar remisser från andra myndigheter.

Regleringen i artiklarna 28.2, 46.1 c och 47.3 skiljer sig inte från 1995 års dataskyddsdirektiv. Det finns inte anledning att göra en annan bedömning i fråga om behovet av reglering än när personuppgiftslagen infördes. Några lagstiftningsåtgärder för att genomföra dessa artiklar behövs alltså inte.

Information till allmänheten

Tillsynsmyndigheten är enligt direktivet skyldig att självmant informera allmänheten i frågor som rör personuppgiftsbehandling. Enligt förvaltningslagen har myndigheter serviceskyldighet i förhållande till enskilda och allmänheten. Principen är en del av det som är att anse som god förvaltning och innebär att förvaltningsmyndigheter ska lämna upplysningar, vägledning, råd och annan sådan hjälp till enskilda i frågor som rör myndighetens verksamhetsområde. Hjälpen ska lämnas i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov och myndighetens verksamhet. Eftersom uppgiften redan är reglerad krävs inte någon lagstiftningsåtgärd för att genomföra artikel 46.1 b och aktuell del av artikel 47.3. En stor del av Datainspektionens verksamhet ägnas redan i dag åt sådan information och vägledning.

Artikel 46.1 e tar enligt regeringens uppfattning sikte på två olika saker. Den ena är allmän informationsskyldighet i förhållande till enskilda om hur de kan ta till vara sina rättigheter. Sådan allmän information ska lämnas på tillsynsmyndighetens eget initiativ. Den andra är mer specifik information om den enskilde t.ex. har gett in ett klagomål till tillsynsmyndigheten. Specifik information ska lämnas bara om det behövs. Om det krävs ska tillsynsmyndigheten även samarbeta med tillsynsmyndigheter i andra medlemsstater för att kunna ge information till enskilda.

Den allmänna skyldigheten enligt förvaltningslagen att lämna hjälp gäller oavsett om det rör sig om en förfrågan från en part i ett ärende eller från någon som har ett allmänt intresse av att få upplysningar om tillsynsmyndighetens verksamhet. När det behövs och är lämpligt ska myndigheten vägleda den enskilde genom att ta initiativ till ytterligare utredning, verka för att utredningen begränsas till vad som är nödvändigt och fästa den enskildes uppmärksamhet på om det finns något annat, bättre sätt att nå det han eller hon eftersträvar. Serviceskyldigheten är vidsträckt men inte obegränsad. Myndigheten ska göra en bedömning från fall till fall av hur långt den ska sträcka sin service (prop. 1985/86:80 s. 59 och även prop. 2016/17:180 s. 65 f.).

I fråga om sådan information som nu diskuteras krävs inte mer än vad som redan följer av myndigheternas allmänna serviceskyldighet. Det behövs därför ingen lagstiftningsåtgärd för att genomföra artikel 46.1 e.

Det kan anmärkas att Datainspektionen har en särskild upplysningstjänst som via telefon och e-post besvarar frågor om personuppgiftsbehandling och att det finns omfattande informationsmaterial på myndighetens hemsida.

11.7 Tillsynsmyndighetens befogenheter

11.7.1 Hur bör tillsynen bedrivas?

I de flesta avseenden bör tillsynen över personuppgiftsbehandling kunna bedrivas på samma sätt som i dag. Tillsynen är av rättslig karaktär, dvs. den inriktas på om den granskade följer gällande regelverk för behandling av personuppgifter. Sådan tillsyn bedrivs framför allt genom granskning av dokumentation och upplysningar från tillsynsobjektet. Den kan dock även innefatta åtgärder som tillsyn över hur regelverket generellt tillämpas eller kontroll av att t.ex. en loggningsfunktion eller annan teknisk säkerhetsåtgärd fungerar som avsett. När det gäller personuppgiftsbehandling kan särskilt tillsynen över säkerhetsåtgärder behöva utföras på plats hos tillsynsobjektet.

Tillsyn kan påbörjas formlöst, t.ex. genom en faktisk åtgärd som en inspektion på plats, eller mer eller mindre formaliserat där ett formellt beslut som anger exakt vad tillsynen ska omfatta är den andra ytterligheten. Det förhållandet att tillsyn kan initieras i en mängd olika situationer och att det inte alltid finns något givet svar på vad tillsynen ska resultera i, innebär att tillsynsarbetet också kan ha olika skepnader. Tillsynen kan bedrivas förutsättningslöst, t.ex. vid ett rutinmässigt tillsynsbesök hos en myndighet. Den kan också vara målinriktad och exempelvis inriktas på

behandlingen i ett enskilt register eller att klarlägga om ett konkret klagomål har fog för sig.

Syftet med tillsynen avgör vad som krävs för att genomföra den. Om syftet är att undersöka klagomål i ett enskilt ärende kan det vara tillräckligt att tillsynsmyndigheten tar del av personuppgifterna och dokumentation om hur de har behandlats. Är det fråga om en kontroll där den som begär kontrollen ifrågasätter att uppgifter om honom eller henne behandlas kan det behövas ett bredare anslag. Om tillsynsmyndigheten behöver få underlag för ett föreläggande kan inledande åtgärder som inhämtande av handlingar behöva följas upp med tillsynsbesök och upprepade kontakter med den personuppgiftsansvarige.

Tillsyn kan också vara tematisk, vilket innebär att en viss fråga eller typ av behandling eller behandlingen i en viss typ av register undersöks oberoende av vilka som utför sådana behandlingar. Tillsynen kan då omfatta många olika tillsynsobjekt och t.ex. bestå i att myndigheten inhämtar skriftlig information.

På samma sätt som det oftast inte finns någon given början på tillsynen är det inte heller reglerat hur tillsynen ska avslutas och vad den ska utmynna i. Tillsynen kan avslutas formlöst, t.ex. genom att myndigheten bestämmer sig för att inte längre avsätta resurser för den. Tillsynen kan också avslutas genom ett protokoll över genomförd inspektion. En tematisk tillsyn kan utmynna i nya föreskrifter eller allmänna råd. Tillsyn behöver alltså inte utmynna i ett beslut.

Om fel upptäcks i samband med tillsyn kan tillsynsmyndigheten utöva sina befogenheter. När det gäller personuppgiftsbehandling kan det innebära att beslut om t.ex. rättelse, komplettering eller radering kan aktualiseras. Tillsyn kan när som helst övergå i ett vanligt förvaltningsärende hos tillsynsmyndigheten, även om den har påbörjats formlöst. Då ska de regler som gäller för det förfarandet tillämpas.

Tillsynsmyndigheten sätter alltså själv gränserna för vad som ska göras och hur och när det ska göras, så länge det inte kommer i konflikt med den reglering som genomför artiklarna 46.1 g (se avsnitt 11.6.3), 28.5 (se avsnitt 11.6.4), 53.2 (se avsnitt 13.6) och 50.4 (se avsnitt 11.10.1).

11.7.2 Utgångspunkterna för regleringen

Regeringens bedömning: Regleringen av tillsynsmyndighetens befogenheter bör utformas i nära anslutning till regleringen i dataskyddsförordningen.

Utredningens bedömning: överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* konstaterar att direktivet innehåller särskilt anpassade bestämmelser när det gäller arbetsuppgifter och befogenheter för tillsynsmyndighet och att det krävs starka skäl för att motivera att gå längre än direktivet kräver på detta område.

Skälen för regeringens bedömning: Enligt tillsynsskrivelsen bör ett tillsynsorgan, när en brist konstateras, ha möjlighet till någon form av ingripande, som ska vara effektivt och tydligt. Det är viktigt att ingripandemöjligheterna har en framåtsyftande funktion och säkerställer att regelverket följs i framtiden, samtidigt som tillsynsorganet också måste kunna

ingripa mot regelöverträdelser som inte kan göras ogjorda. Ingripandemöjligheterna bör utformas efter de särskilda förutsättningarna inom respektive tillsynsområde och så att de skapar större enhetlighet, särskilt inom närliggande tillsynsområden (skr. 2009/10:79 s. 41 f.).

För att genomföra direktivets bestämmelser och skapa förutsättningar för en effektiv tillsyn bör enligt regeringens uppfattning tillsynsmyndighetens befogenheter regleras i ramlagen. En så tydlig reglering som möjligt bör eftersträvas. De uttalanden som gjorts i tillsynsskrivelsen bör prägla hur befogenheterna regleras. Hänsyn bör således tas till om motsvarande reglering finns i dataskyddsförordningen när tillsynsmyndighetens befogenheter på direktivets område regleras.

I skäl 82 framhålls att när befogenheterna utövas ska varje åtgärd vara lämplig, nödvändig och proportionerlig för att säkerställa efterlevnaden av regelverket. Åtgärderna ska utformas så att onödiga kostnader och stora olägenheter undviks. Det väcker frågan om det bör införas en proportionalitetsregel som återspeglar innehållet i skäl 82. Regeringen delar emellertid utredningens bedömning att de befogenheter som tillsynsmyndigheten föreslås få inte är av den karaktären att en uttrycklig proportionalitetsregel är nödvändig.

11.7.3 Undersökningsbefogenheter

Regeringens förslag: Tillsynsmyndigheten ska ha rätt att av personuppgiftsansvariga och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. den hjälp och den information som behövs för tillsynen.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt artikel 47.1 ska tillsynsmyndigheten ha effektiva undersökningsbefogenheter som minst ska inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina tillsynsuppgifter.

Enligt 43 § personuppgiftslagen, som är tillämplig på de behöriga myndigheterna, har tillsynsmyndigheten rätt att för sin tillsyn på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid den och tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

Som tidigare nämnts består rättslig tillsyn till stor del av granskning av dokumentation. För att kunna utöva tillsynen effektivt kan tillsynsmyndigheten dock inte bara förlita sig på de handlingar som den får tillgång till. Den kan även i viss utsträckning behöva besöka lokaler där personuppgiftsbehandling pågår för att bl.a. kunna inspektera säkerhetsåtgärder. Tillsynsbesök kan också ge tillsynsmyndigheten bättre inblick i förutsättningarna för den verksamhet där personuppgiftsbehandlingen äger rum.

Tillsynsmyndigheten behöver alltså tillgång till de personuppgifter som behandlas. Tillsynsmyndigheten behöver även upplysningar och dokumentation om pågående behandlingar, t.ex. de register över behandlingar som den personuppgiftsansvarige ska föra (se avsnitt 9.2.7). Därutöver bör tillsynsmyndigheten ha rätt till annan information som behövs, bl.a. dokumentation av säkerhets- och skyddsåtgärder. Det kan också röra sig om dokumentation som inte är direkt kopplad till den behandling som granskas, men som tillsynsmyndigheten ändå behöver för att genomföra sin tillsyn. Det bör därför framgå av ramlagen att tillsynsmyndigheten ska ges tillgång till de personuppgifter som behandlas, tillgång till dokumentation om behandlingen av dem och övrig dokumentation som behövs för tillsynen.

Det normala förfarandet bör vara att tillsynsmyndigheten tar hjälp av personal vid den granskade myndigheten för att få tillgång till behandlade personuppgifter. Tillgång på det sättet ska enligt utredningens mening inte betraktas som en rätt till direktåtkomst, vilket regeringen instämmer i (jfr HFD 2015 ref. 61 och SOU 2015:39 s. 389 f). I vissa fall skulle det kunna underlätta om tillsynsmyndigheten själv i samband med en inspektion på plats får använda datorer och andra medel som tillsynsobjektet använder. En sådan möjlighet torde dock förutsätta att tillsynsmyndigheten ges direktåtkomst till de behöriga myndigheternas information (jfr Datainspektionens samrådsyttrande i dnr 126-2013). Tillsynsmyndigheten bör därför enligt regeringens mening ges tillgång till utrustning och andra medel som har anknytning till behandlingen av personuppgifter enbart med hjälp av tillsynsobjektets personal.

Frågan är om rätten att få tillgång till behandlade personuppgifter även ger rätt att beordra de körningar och andra åtgärder som behövs för att få fram de personuppgifter som behandlas. Enligt 4 § lagen om tillsyn över viss brottsbekämpande verksamhet har Säkerhets- och integritetsskyddsnämnden bl.a. rätt till det biträde som nämnden begär. Sådant biträde kan bestå i att den granskade myndigheten gör lokaler, arkiv och databaser tillgängliga för nämnden. En förutsättning för att få tillgång till de personuppgifter som behandlas är att personal från den granskade myndigheten bistår vid tillsynen genom att utföra de sökningar som behövs. Enligt regeringens uppfattning har tillsynsmyndigheten behov av den typen av biträde och en bestämmelse om det bör tas in i ramlagen. Vid sökningar som görs på direkt begäran av tillsynsmyndigheten anses tillsynsobjektet inte vara bunden av de begränsningar i fråga om behandlingen av personuppgifter som annars gäller i verksamheten. Det kan t.ex. gälla ändamålen för behandlingen eller hur känsliga personuppgifter får behandlas.

Tillsynsmyndigheten kan även behöva tillgång till lokaler, utrustning och andra medel som används för att behandla personuppgifter. Tillsynsmyndigheten bör inte ha rätt att med tvång skaffa sig tillgång till lokaler (jfr SOU 1997:39 s. 443 och prop. 1997/98:44 s. 102). Att göra lokaler tillgängliga ingår dock i den personuppgiftsansvariges samarbetsskyldighet i förhållande till tillsynsmyndigheten (se avsnitt 9.2.6). Vägran att ge tillträde kan också enligt förslaget i avsnitt 12.5.2 leda till sanktionsavgift.

Regeringen återkommer till frågan om vad tillsynsmyndigheten kan göra om den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller sina skyldigheter att bistå tillsynsmyndigheten (se avsnitt 11.7.6 och 12.5.2).

11.7.4 Skillnad mellan förebyggande och korrigerande befogenheter

Regeringens bedömning: Det bör göras tydlig skillnad mellan tillsynsmyndighetens förebyggande och korrigerande befogenheter.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* välkomnar förslagen avseende tillsynsmyndighetens befogenheter och betonar vikten av att tillsynsmyndigheten själv ska kunna välja vilken åtgärd som ska vidtas enligt ramlagen och att en skarpare åtgärd inte ska kräva att mindre ingripande åtgärd redan vidtagits. *Dataskydd.net* ifrågasätter behovet av ytterligare reglering rörande tillsynsmyndighetens befogenheter och befarar ett utdraget tillsynsförfarande mot bakgrund av antalet åtgärder i direktivet. Dataskydd.net anser vidare att tillsynsmyndighetens skyldighet att ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden vid förhandssamråd och när det i övrigt är påkallat täcker behovet av förebyggande åtgärder.

Skälen för regeringens bedömning

Innehållet i direktivet

I artikel 47.2 anges att tillsynsmyndigheten ska ha effektiva korrigerande befogenheter, t.ex. för att kunna

a) utfärda varningar till personuppgiftsansvariga och personuppgiftsbiträden om att planerade behandlingar sannolikt kommer att stå i strid med de bestämmelser som antas i enlighet med direktivet,

b) beordra personuppgiftsansvariga och personuppgiftsbiträden att se till att behandlingen av personuppgifter är förenlig med direktivet och, om lämpligt på visst sätt och inom viss tid, bl.a. beordra rättelse, radering eller begränsning av behandlingen enligt artikel 16, och

c) införa tillfälliga eller definitiva begränsningar av, inklusive förbud mot, behandlingen.

Nuvarande reglering

I artikel 28.3 i 1995 års dataskyddsdirektiv regleras tillsynsmyndighetens korrigerande befogenheter, som delvis har genomförts i 44–47 §§ personuppgiftslagen. Paragraferna är till stor del tillämpliga på de behöriga myndigheterna.

Enligt 45 § personuppgiftslagen ska tillsynsmyndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse, om myndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Går det inte att åstadkomma rättelse eller är saken brådskande får myndigheten förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem. Enligt 47 § personuppgiftslagen får tillsynsmyndigheten ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas. Enligt 44 § personuppgiftslagen får tillsynsmyndigheten förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, om myndigheten vid en begäran enligt 43 § inte kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig.

Tydligare reglering av tillsynsmyndighetens befogenheter

Datainspektionen vidtar i dag samma åtgärder både för att förebygga otillåten personuppgiftsbehandling och för att korrigera behandling som strider mot personuppgiftslagen. Regeringen ansåg när lagen infördes att det var viktigt att tillsynsmyndigheten i första hand kunde fungera som stöd för de personuppgiftsansvariga och ge dem råd. Datainspektionen ska genom påpekanden och andra åtgärder försöka förmå personuppgiftsansvariga att vidta åtgärder som medför att behandlingen blir laglig (prop. 1997/98:44 s. 103). Påpekanden och liknande förfaranden har i praxis ansetts rymma även åtgärder i form av förelägganden av tvingande karaktär. Tillsynsobjekten har emellertid ansett det oklart om ett föreläggande från Datainspektionen är tvingande och om det får överklagas (SOU 2015:39 s. 622 f.).

I artikel 47.2 görs tydlig skillnad mellan förebyggande och korrigerade befogenheter. För att regleringen i ramlagen ska bli så tydlig som möjligt bör tillsynsmyndighetens befogenheter i förebyggande respektive korrigerande syfte regleras i olika paragrafer. De bör också spegla i vilken ordning befogenheterna bör användas.

En särskild fråga är hur det bör uttryckas vad tillsynsmyndigheten ska ingripa mot. Enligt artikel 47.2 punkterna a och b ska tillsynsmyndigheten se till att uppgiftsbehandlingen är förenlig med de författningar som genomför direktivet. Vilka författningar som omfattas av tillsynsområdet behandlas i avsnitt 11.3.1. Enligt regeringens uppfattning bör de förebyggande befogenheterna användas om det finns risk för att viss personuppgiftsbehandling kan komma att stå i strid med lag eller annan författning, medan de korrigerande befogenheterna bör användas när det har konstaterats att behandlingen strider mot gällande bestämmelser.

Tillsynsmyndighetens befogenheter enligt ramlagen bör ses som en trappa som ger möjlighet att successivt använda kraftfullare medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig efter myndighetens anvisningar. Befogenheterna sträcker sig från rådgiv-

ning till möjligheten att besluta om sanktionsavgift. Det bör dock – i likhet med vad *Datainspektionen* påpekar – understrykas att de korrigerande åtgärderna inte är kopplade till varandra på det sättet att en strängare åtgärd förutsätter att alla mindre ingripande åtgärder redan har prövats. Den omständigheten bör enligt regeringens bedömning även motverka ett utdraget tillsynsförfarande med många steg, som *Dataskydd.net* befarar.

11.7.5 Förebyggande befogenheter

Regeringens förslag: Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser att varningar bör vara rättsligt bindande och överklagbara.

Skälen för regeringens förslag

Råd och stöd

En viktig uppgift för tillsynsmyndigheten är att lämna råd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter och att stödja deras strävanden att skapa författningsenliga och integritetssäkra lösningar. Inom ramen för det förebyggande arbetet bör tillsynsmyndigheten på olika sätt försöka förmå den som är ansvarig att vidta de åtgärder som behövs för att motverka risken för att behandling av personuppgifter kan komma att stå i strid med lag eller annan författning. Medlen för det bör främst vara muntliga eller skriftliga råd, rekommendationer och påpekanden som inte är tvingande.

På vilket sätt förändringen ska åstadkommas bör i första hand lämnas åt den personuppgiftsansvarige eller personuppgiftsbiträdet att avgöra. I många fall torde det vara tillräckligt att tillsynsmyndigheten upplyser om på vilket sätt personuppgiftsbehandlingen riskerar att strida mot regelverket. Tillsynsmyndigheten är skyldig att lämna skriftliga råd vid förhandssamråd (se avsnitt 11.6.4 och avsnitt 9.2.5).

Varning

Enligt artikel 47.2 a ska tillsynsmyndigheten t.ex. kunna utfärda varningar till personuppgiftsansvariga och personuppgiftsbiträden för att planerade behandlingar sannolikt kommer att strida mot regelverket för personuppgiftsbehandling. I likhet med utredningen tolkar regeringen direktivet så att varning bör vara en åtgärd i det förebyggande arbetet. Möjligheten att utfärda varning är ny och en varning kan vara ett lämp-

ligt komplement till de förebyggande åtgärder som finns i dag. Varning bör kunna användas av tillsynsmyndigheten för att i ett enskilt fall markera allvaret i en situation och försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att ändra sig i fråga om planerad behandling. Därigenom kan det förebyggas att behandling som inte är förenlig med regelverket påbörjas. Varning bör emellertid även kunna användas om pågående behandling riskerar att strida mot lag eller annan författning.

Att utfärda varning bör som regel bli aktuellt först om tillsynsmyndigheten bedömer att den inte på annat sätt kan förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att följa regelverket. Varningen ska tjäna som väckarklocka för den personuppgiftsansvarige eller personuppgiftsbiträdet. Varning bör nämligen – även om den inte är tvingande – ses som ett steg på vägen mot ett föreläggande.

En varning bör vara skriftlig och tydligt ange på vilket sätt behandlingen riskerar att strida mot regelverket. En varning bör kunna avse vilken form av förändring som helst i behandlingen, t.ex. vilka personuppgifter som får behandlas, hur ett behandlingssystem bör utformas, vilka säkerhetsåtgärder som krävs eller något annat som har betydelse för behandlingen. Till skillnad från *Datainspektionen* anser regeringen att en varning inte ska vara bindande. Därmed är det inte fråga om ett beslut av tillsynsmyndigheten som är överklagbart.

Det kan i och för sig diskuteras om ordet varning, som används i direktivet, är ett lämpligt uttryck. Det skulle kunna leda tankarna fel, eftersom ordet varning används i många olika betydelser. Mot bakgrund av att samma ord används både i annan tillsynsverksamhet och i dataskyddsförordningen för motsvarande befogenhet har utredningen ansett att den nya åtgärden bör benämnas varning. Regeringen delar denna uppfattning.

11.7.6 Korrigerande befogenheter

Regeringens förslag: Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom förebyggande åtgärder försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
3. förbjuda fortsatt behandling om bristen är allvarlig, eller
4. besluta om en sanktionsavgift.

Om tillsynsmyndigheten utfärdar ett föreläggande ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Dataskydd.net* anser att sanktionsavgifter inte bör hindra att tillsynsmyndigheten ska kunna förena förelägganden med vite.

Skälen för regeringens förslag

Vilka åtgärder kan komma i fråga?

Om tillsynsmyndigheten konstaterar att den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller kraven på författningsenlig personuppgiftsbehandling bör det finnas möjlighet för myndigheten att uppmana den ansvarige och biträdet att uppfylla sina skyldigheter. Det kan göras genom vissa av de åtgärder som normalt används i det förebyggande arbetet, nämligen råd, rekommendationer eller påpekanden. Om den personuppgiftsansvarige eller personuppgiftsbiträdet vidtar de åtgärder som krävs så snart tillsynsmyndigheten väcker en fråga torde det räcka med fortsatt dialog. Tillsynsmyndigheten behöver emellertid också kunna tvinga den personuppgiftsansvarige eller personuppgiftsbiträdet att fullgöra sina skyldigheter. Medlen för det bör vara bindande förelägganden, förbud mot fortsatt behandling och beslut om sanktionsavgift.

Bindande förelägganden

Enligt artikel 47.2 b ska tillsynsmyndigheten t.ex. kunna beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att en behandling ska bli förenlig med bestämmelserna som genomför direktivet. I artikel 58.2 d i förordningen används ordet förelägga i motsvarande bestämmelse. Regleringen tar sikte på att tillsynsmyndigheten ska kunna utfärda bindande beslut som uppmanar tillsynsobjektet att vidta vissa åtgärder för att göra personuppgiftsbehandlingen författningsenlig. Eftersom ordet förelägga används i förordningen är det lämpligt att använda det i ramlagen.

I direktivet anges rättelse, radering och begränsning av behandlingen som exempel på åtgärder som tillsynsmyndigheten ska kunna förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta. Vad som avses med korrigeringsalternativen behandlas i avsnitt 10.4. När det gäller sådana åtgärder kan det vara lämpligt att tillsynsmyndigheten i föreläggandet anger vilken åtgärd som ska vidtas. I många andra fall är dock tillsynsobjektet bättre lämpat att avgöra vad som bör göras för att behandlingen ska bli författningsenlig. Det kan t.ex. vara fråga om vilka tekniska åtgärder som bör vidtas eller vilka säkerhetslösningar som bör väljas. Tillsynsmyndigheten bör därför endast om det är lämpligt ange vilken åtgärd som ska vidtas. Däremot ska det alltid framgå när åtgärden ska vara genomförd.

En särskild fråga är om tillsynsmyndigheten bör kunna förelägga att uppgifter ska raderas. Datainspektionen får i dag inte själv besluta om radering av personuppgifter. Beslut om radering är en mycket ingripande åtgärd, särskilt för myndigheter. Som framgår av avsnitt 10.4.2 kan radering sällan komma i fråga med hänsyn till reglerna i 2 kap. tryckfrihetsförordningen. Med anledning av åtgärdens begränsade tillämpningsområde tillämpas 47 § personuppgiftslagen sällan mot myndigheter, men upplevs trots det inte som obsolet. I likhet med utredningen anser rege-

ringen att tillsynsmyndigheten bör kunna utfärda föreläggande om radering. Myndigheten måste givetvis beakta att åtgärden inte får stå i strid med annan lagstiftning.

Förelägganden bör inte bara kunna utfärdas för att säkerställa att personuppgiftsbehandling ska vara författningsenlig. För att tillsynsmyndigheten ska ha effektiva befogenheter behöver den även kunna utfärda bindande förelägganden som tar sikte på att personuppgiftsansvariga och personuppgiftsbiträden ska uppfylla andra skyldigheter. Det kan t.ex. vara att införa bättre säkerhetslösningar, fullgöra dokumentationsskyldighet eller att överlämna viss dokumentation eller ge tillträde till lokaler.

Förbud mot fortsatt behandling

Enligt artikel 47.2 c ska tillsynsmyndigheten kunna införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, fortsatt behandling. Med förbud mot fortsatt behandling avses att någon behandling inte längre får förekomma. Personuppgifter får dock alltid behandlas om det är nödvändigt med hänsyn till reglerna i 2 kap. tryckfrihetsförordningen.

För att genomföra direktivet bör en bestämmelse om förbud mot fortsatt behandling tas in i ramlagen. I flera lagstiftningsärenden har det ansetts naturligt att förbud mot fortsatt behandling även bör kunna riktas mot myndigheter (prop. 2009/10:85 s. 275 och prop. 2014/15:148 s. 89). Åtgärden bör dock på samma sätt som i dag användas restriktivt (jfr prop. 1997/98:44 s. 103). Förbud mot fortsatt behandling bör bara kunna meddelas om en myndighet på ett allvarligt sätt har åsidosatt sina skyldigheter och bristerna är sådana att de inte kan åtgärdas på annat sätt än att behandlingen upphör (jfr SOU 2015:39 s. 626 f.).

Att en personuppgift har behandlats på ett sådant sätt att förbud mot fortsatt behandling aktualiseras behöver inte innebära att all behandling av uppgiften måste upphöra. Förbudet måste kopplas till vad som föranledde det (jfr avsnitt 10.4.3). Hur omfattande förbudet blir beror på vilken typ av personuppgift det är och hur den har behandlats.

Ett förbud mot fortsatt behandling bör normalt vara permanent. I vissa fall kan dock ett tillfälligt förbud vara en lämplig åtgärd, t.ex. om den personuppgiftsansvarige trots påpekande eller varning från tillsynsmyndigheten har påbörjat otillåten personuppgiftsbehandling och myndigheten bedömer att bristerna kan rättas till.

Ska förelägganden kunna förenas med en sanktion?

Regeringen föreslår i avsnitt 12.7 att tillsynsmyndigheten ska få besluta om administrativa sanktionsavgifter. Sådana avgifter kan aktualiseras t.ex. om en personuppgiftsansvarig eller ett personuppgiftsbiträde underlåter att följa ett föreläggande eller beslut från tillsynsmyndigheten. Till skillnad från *Dataskydd.net* anser regeringen att det är det tillräckligt att tillsynsmyndigheten i ett föreläggande kan upplysa om att sanktionsavgift kan komma att tas ut om föreläggandet inte följs. Det finns därför inget behov av att även kunna förena ett föreläggande med vite.

11.8 Handläggningen av tillsynsfrågor

11.8.1 Förvaltningslagens tillämplighet

På samma sätt som i dag ska förvaltningslagen tillämpas i tillsynsmyndighetens verksamhet. Lagen innehåller grundläggande regler om handläggning av ärenden hos förvaltningsmyndigheterna men gäller bara i den utsträckning det inte finns avvikande regler i andra författningar. Som tidigare nämnts saknas generell författningsreglering av tillsynsverksamhet. Det är i huvudsak inte heller fråga om ärendehantering utan en arbetsuppgift som kan lösas på olika sätt. I vissa fall lägger tillsynsmyndigheten upp ett tillsynsärende för att kunna hantera inkommande handlingar. Det är t.ex. vanligt att klagomål som enskilda ger in hanteras som ärenden.

Direktivet innehåller vissa detaljbestämmelser som tar sikte på tillsynsmyndighetens handläggning av framställningar från enskilda, t.ex. regler om hur tillsynsmyndigheten ska hantera klagomål från enskilda och om kontroller av om behandlingen är författningsenlig. Utöver förvaltningslagen krävs vissa handläggningsregler för tillsyn enligt ramlagen. Regeringen anser att dessa bestämmelser i största möjliga utsträckning bör tas in i ramlagen och den tillhörande förordningen. Därigenom skapas en samlad reglering som kan anpassas till vad som krävs enligt direktivet.

11.8.2 Kommunikationsskyldighet

Regeringens bedömning: Det behöver inte regleras att tillsynsmyndigheten ska kommunicera före beslut som tillsynsmyndigheten avser att fatta med stöd av korrigerande tillsynsbefogenheter, eftersom förvaltningslagens allmänna bestämmelser om kommunikation gäller.

Utredningen föreslår att särskilda bestämmelser om kommunikation införs.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: I 46 § personuppgiftslagen finns bestämmelser som utgör ytterligare processuella skyddsåtgärder för den personuppgiftsansvarige när tillsynsmyndigheten utövar sin befogenhet att besluta om vitesföreläggande. Bland annat anges att den personuppgiftsansvarige, enligt huvudregeln, ska ha fått tillfälle att yttra sig innan tillsynsmyndigheten beslutar om vite.

Utredningen föreslår att det i ramlagen ska införas en liknande bestämmelse om kommunikation inför beslut som tillsynsmyndigheten avser att fatta med stöd av sina korrigerande tillsynsbefogenheter. Av 25 § i den nya förvaltningslagen framgår dock att innan en myndighet fattar ett beslut i ett ärende ska den, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Denna bestämmelse fyller samma funktion som utredningens förslag. Dessa överväganden gör sig även gällande på förordningens område (se prop. 2017/18:105 s. 156 f.). Mot denna bakgrund bedömer regeringen att det inte finns något behov av bestämmelser om kommunikation.

11.8.3 Beslut ska gälla när de fått laga kraft

Regeringens förslag: Tillsynsmyndighetens beslut ska inte få verkställas omedelbart.

Utredningens bedömning överensstämmer i sak med regeringens. Utredningen har dock inte ansett att det behövs några lagstiftningsåtgärder.

Remissinstanserna: *Polismyndigheten* tillstyrker att tillsynsmyndighetens beslut inte ska få verkställas omedelbart. *Datainspektionen* avstyrker att tillsynsmyndigheten inte ska få förordna att myndighetens beslut ska gälla omedelbart.

Skälen för regeringens förslag: Enligt 51 § andra stycket personuppgiftslagen får tillsynsmyndigheten besluta att ett av myndigheten meddelat beslut ska gälla även om det överklagas. I flertalet av de registerförfattningar som gäller för de myndigheter som kommer att tillämpa ramlagen finns dock ingen hänvisning till den bestämmelsen, varför tillsynsmyndigheten i dag inte har möjlighet att fatta sådana beslut i relation till de myndigheterna.

I förarbetena till åklagardatalagen konstateras att det finns både för- och nackdelar med att låta 51 § andra stycket personuppgiftslagen gälla för åklagarmyndigheterna. Systematiska skäl talar för att regleringen borde utformas på samma sätt, oavsett vem beslutet gäller. Verksamhetsskäl anses dock tala mot att införa en sådan möjlighet. På samma sätt som vid införandet av polisdatalagen konstateras att det inte finns skäl att ge Datainspektionen möjlighet att meddela interimistiska beslut (prop. 2014/15:63 s. 57 och prop. 2009/10:85 s. 91). I förarbetena till domstolsdatalagen görs bedömningen att det inte finns något praktiskt behov av en sådan möjlighet (prop. 2014/15:148 s. 95). Samma bedömning görs för Kustbevakningen (prop. 2011/12:45 s. 87).

Det som talar för att tillåta interimistiska beslut är att det ger möjlighet att hindra sådan behandling som tillsynsmyndigheten anser strider mot regelverket. Samtidigt ger beslut av det slaget förtursbehandling i domstol. Utan förtursbehandling kan domstolsprövningen dra ut på tiden. Detta är argument som, i likhet med vad *Datainspektionen* anför, talar för att tillsynsmyndigheten ska kunna förordna att myndighetens beslut ska gälla omedelbart.

Tillsynsmyndigheten och de granskade myndigheterna har emellertid inte alltid samma uppfattning om en behandling är författningsenlig, samtidigt som verksamheten hos behöriga myndigheter är central i en rättsstat. Det är inte heller givet att tillsynsmyndigheten har tillräcklig kunskap om den granskade verksamheten och dess villkor för att kunna ta nödvändiga hänsyn till verksamheten. Det finns därför anledning att vara försiktig med att låta tillsynsmyndigheten förbjuda en annan myndighet att bedriva den verksamhet som statsmakterna beslutat om.

Även om det alltså finns skäl som talar för att tillåta interimistiska beslut, anser regeringen i likhet med utredningen att de argument som tidigare anförts mot en sådan möjlighet inom ramlagens tillämpningsområde alltjämt väger tungt när det gäller tillsyn av personuppgiftsbehandling på direktivets område. Tillsynsmyndigheten bör därför inte kunna besluta att myndighetens beslut ska gälla utan hinder av att det inte fått laga kraft.

Direktivet innehåller inga bestämmelser om när ett beslut som fattats av tillsynsmyndigheten ska börja gälla. Däremot reglerar 35 § i den nya förvaltningslagen närmare när beslut får verkställas. Att ett beslut vunnit laga kraft är som huvudregel förutsättning för verkställighet. Bestämmelsen innehåller emellertid i andra och tredje styckena vissa undantagssituationer då beslut får verkställas omedelbart. Som konstaterats ovan ska tillsynsmyndigheten tillämpa förvaltningslagen i verksamheten. För att tillsynsmyndigheten inte ska kunna besluta att myndighetens beslut ska gälla utan hinder av det inte fått laga kraft, behöver detta regleras. Det finns därför enligt regeringens mening anledning att ta in en bestämmelse i ramlagen om att tillsynsmyndighetens beslut inte ska få verkställas omedelbart.

11.8.4 Befogenhet att göra rättsliga myndigheter uppmärksamma på felaktigheter

Regeringens bedömning: Det behövs inga lagstiftningsåtgärder för att genomföra direktivets bestämmelse om befogenhet för tillsynsmyndigheten att göra rättsliga myndigheter uppmärksamma på felaktigheter.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att det ska införas en skyldighet för tillsynsmyndigheten att anmäla förhållanden som skulle kunna utgöra brott till Åklagarmyndigheten och felaktigheter som skulle kunna medföra skadeståndsansvar för staten till Justitiekanslern.

Remissinstanserna: *Justitiekanslern* avstyrker utredningens förslag, bl.a. mot bakgrund av att direktivet inte ställer krav på anmälningsskyldighet. *Säkerhets- och integritetsskyddsnämnden* anser att den föreslagna anmälningsskyldigheten är för vidsträckt och att den bör inträda först efter att den enskilde vänt sig till tillsynsmyndigheten.

Skälen för regeringens bedömning: Tillsynsmyndighetens befogenheter tar sikte på förhållanden som myndigheten har rätt att ingripa mot. Ibland kan emellertid myndigheten vid sin tillsyn upptäcka förhållanden som det ankommer på andra myndigheter att ingripa mot. Enligt artikel 47.5 ska tillsynsmyndigheten ha befogenhet att göra rättsliga myndigheter uppmärksammade på överträdelser av de bestämmelser som genomför direktivet. En liknande reglering finns i 1995 års dataskyddsdirektiv, men några bestämmelser om detta infördes inte i personuppgiftslagen.

En tillsynsmyndighet kan redan i dag uppmärksamma utredande myndigheter på felaktigheter som upptäcks vid tillsynen. Om man skulle införa en skyldighet att anmäla felaktigheter skulle man enligt utredningen åstadkomma ett effektivt sanktionssystem. I likhet med *Justitiekanslern* konstaterar dock regeringen att direktivet inte ställer krav på att det ska finnas någon sådan skyldighet att anmäla överträdelser till rättsliga myndigheter. När det gäller skadestånd är det dessutom ett civilrättsligt institut där det normala är att den enskilde måste inkomma med en begäran för att en myndighet ska pröva frågan, till skillnad från om en anmälan från en tillsynsmyndighet skulle inleda ett ärende vilket skulle

bli fallet med utredningens förslag. Det finns därför enligt regeringens mening anledning att vara restriktiv med att införa en sådan skyldighet.

En anmälningsskyldighet liknande den utredningen föreslår finns för Säkerhets- och integritetsskyddsnämnden (20 § förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden). Säkerhets- och integritetsskyddsnämnden utövar emellertid tillsyn över bl.a. hemliga tvångsmedel och andra områden där sekretess ofta gäller även i förhållande till den enskilde själv. Inom ramlagens tillämpningsområde är möjligheten för den enskilde att själv ta del uppgifter som behandlats och information från tillsynsmyndigheten om hur hans eller hennes personuppgifter har behandlats betydligt större. Som *Säkerhets- och integritetsnämnden* påpekar skulle dessutom utredningens förslag om anmälningsskyldighet när felaktigheter uppmärksammas i tillsynsverksamhet på ramlagens område kunna innebära att den enskildes personuppgifter sprids trots att den enskilde inte vill detta. Mot denna bakgrund anser regeringen att en reglering om anmälningsskyldighet för tillsynsmyndigheten inte ska införas.

11.9 Möjlighet att ifrågasätta giltigheten av unionsrättsakter

Regeringens bedömning: Det saknas för närvarande skäl att ge tillsynsmyndigheten möjlighet att ansöka hos förvaltningsrätten om att en tillsynsåtgärd ska vidtas, i stället för att själv besluta om åtgärden.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att tillsynsmyndigheten ska få ansöka hos allmän förvaltningsdomstol om att en tillsynsåtgärd beslutas om tillsynsmyndigheten vid handläggningen av ett ärende bedömer att det finns särskilda skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av ramlagen.

Remissinstanserna: *Kammarrätten i Stockholm* anser att den föreslagna bestämmelsen utgör en helt ny företeelse i svensk rätt och att det behöver utvecklas hur förfarandet är tänkt att fungera. *Datainspektionen* påtalar vikten av att den föreslagna bestämmelsen utformas på motsvarande sätt som i dataskyddsförordningen och den följande dataskyddslagen.

Skälen för regeringens förslag: Varje medlemsstat ska enligt artikel 47.5 i direktivet i lag säkerställa att tillsynsmyndigheten har befogenhet att bl.a., när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med direktivet. En liknande bestämmelse finns i artikel 28.3 tredje strecksatsen i 1995 års dataskyddsdirektiv, men berördes inte vid genomförandet av det direktivet i svensk rätt.

EU-domstolen har, i det mål som gällde giltigheten av kommissionens beslut att de så kallade Safe Harbor-principerna säkerställde ett adekvat skydd för personuppgifter som överförs till USA, klargjort att bestämmelsen i dataskyddsdirektivet kan innebära ett krav på kompletterande processuella bestämmelser i nationell rätt (dom Schrems, C-362/14,

EU:C:2015:650). I domen konstateras att EU-domstolen är exklusivt behörig att förklara en EU-rättsakt ogiltig, t.ex. ett kommissionsbeslut om adekvat skyddsnivå i ett tredjeland. Nationella domstolar har således inte någon sådan befogenhet, och än mindre de nationella tillsynsmyndigheterna när de utreder om ett kommissionsbeslut är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter. EU-domstolen konstaterar mot den bakgrunden att om en nationell tillsynsmyndighet anser att det finns fog för en invändning mot behandling av personuppgifter som skett med stöd av ett kommissionsbeslut, måste tillsynsmyndigheten ha möjlighet att inleda ett rättsligt förfarande. Enligt EU-domstolen ankommer det på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för tillsynsmyndigheten att vid nationella domstolar göra gällande sådana invändningar. På så sätt kan den nationella domstolen, om den delar myndighetens tvivel angående en unionsrättsakts giltighet, hänskjuta en begäran om förhandsavgörande till EU-domstolen för att pröva rättsaktens giltighet.

I svensk rätt finns det ingen möjlighet för tillsynsmyndigheter att initiera en domstolsprövning i syfte att skapa förutsättningar för ett klargörande från EU-domstolen. Utredningen föreslår mot den bakgrunden att tillsynsmyndigheten vid handläggningen av ett ärende ska få ansöka hos allmän förvaltningsdomstol om att en korrigerande åtgärd ska vidtas, om myndigheten bedömer att det finns särskilda skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av ramlagen.

I lagrådsremissen Ny dataskyddslag (s. 157–159) föreslogs en liknande bestämmelse på dataskyddsförordningens tillämpningsområde. Lagrådet konstaterade i det ärendet att det inte framstår som klart att dataskyddsförordningen eller EU-rätten i övrigt ställer krav på att en domstolsprövning kan komma till stånd genom tillsynsmyndighetens försorg och avstyrkte förslaget (prop. 2017/18:105 s. 333 f.). Med beaktande av Lagrådets synpunkter uttalade regeringen i den propositionen att det för närvarande inte finns tillräckliga skäl att införa en sådan möjlighet i svensk rätt och lämnade därför inget sådant lagförslag. Mot denna bakgrund lämnar regeringen inte heller något sådant förslag till bestämmelse i denna proposition.

11.10 Internationellt samarbete

11.10.1 Skyldighet att bistå en tillsynsmyndighet i en annan medlemsstat

Regeringens förslag: Tillsynsmyndigheten ska på begäran bistå en tillsynsmyndighet i en annan medlemsstat. Bistånd ska endast få vägras om det skulle strida mot en lag eller en förordning att tillmötesgå begäran. Vid sådant bistånd får tillsynsmyndigheten använda sina befogenheter enligt ramlagen.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Innehållet i direktivet

Av artiklarna 46.1 h och 50.1 framgår att tillsynsmyndigheten ska samarbeta med tillsynsmyndigheter i andra medlemsstater. Myndigheterna ska utbyta information och ge varandra bistånd för att säkerställa att direktivet tillämpas på ett enhetligt sätt. Biståndet ska särskilt omfatta information och tillsynsåtgärder, t.ex. samråd, inspektioner och utredningar. Enligt artikel 50.2 ska tillsynsmyndigheten vidta alla lämpliga åtgärder för att kunna besvara en begäran om bistånd utan onödigt dröjsmål och inte senare än en månad efter det att begäran togs emot. Med lämpliga åtgärder avses t.ex. att översända information om en pågående utredning. Information som utbytts får enligt artikel 50.3 endast användas för det syfte för vilket den har begärts. En begäran får enligt artikel 50.4 vägras endast om tillsynsmyndigheten inte är behörig i sakfrågan eller att utföra de åtgärder som begärs eller om det skulle strida mot direktivet, unionsrätten eller nationell rätt att tillmötesgå begäran. Enligt artikel 50.5 ska den begärande myndigheten få information om resultatet av begäran och hur åtgärderna som vidtagits för att tillmötesgå den fortskrider. Även skälen för att vägra tillmötesgå en begäran ska anges.

Det internationella samarbetet bör regleras

För att genomföra direktivet behövs det vissa bestämmelser om internationellt bistånd, både när det gäller bistånd som den svenska tillsynsmyndigheten ska lämna och myndighetens möjligheter att själv begära bistånd från en annan medlemsstat. Av ramlagen bör det framgå att tillsynsmyndigheten på begäran ska bistå andra medlemsstater och vilka befogenheter myndigheten har vid sådant bistånd. Regeringen delar utredningens bedömning att den svenska tillsynsmyndigheten bör kunna vidta samma åtgärder på begäran av en tillsynsmyndighet i en annan medlemsstat som myndigheten själv kan vidta vid sin tillsyn.

En begäran om bistånd får bara vägras i de situationer som anges i artikel 50.4. En begäran om bistånd bör bara få vägras om det skulle strida mot en lag eller en förordning att tillmötesgå den. Det bör framgå av ramlagen. Begäran får således vägras t.ex. om den svenska lagstiftningen inte medger att tillsynsmyndigheten agerar på det sätt som begärs. Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU-rättsakter här i landet med den verkan som följer av EU-fördragen. Detta innebär bl.a. att EU-förordningar är att jämställa med svensk lag. Detaljerna beträffande samarbetet bör regleras i förordning.

Som nämns i avsnitt 11.4 avser regeringen att utse endast Datainspektionen till svensk nationell tillsynsmyndighet enligt dataskyddsdirektivet. Mot den bakgrunden finns det inget behov av en vägransgrund som tar sikte på tillsynsmyndighetens behörighet i sakfrågan.

Personuppgiftsbehandlingen inom ramlagens tillämpningsområde utförs huvudsakligen av ett begränsat antal statliga myndigheter och behandlingen utförs till största delen inom Sverige. På flera områden samarbetar behöriga myndigheter internationellt och utbyter personuppgifter. Det ingår i tillsynsmyndigheternas uppdrag att granska det internationella uppgiftsutbytet. En tillsynsmyndighet i en annan medlemsstat

kan därför vid sin tillsyn behöva bistånd med vissa kontrollåtgärder, t.ex. om personuppgifter har överförts till personuppgiftsansvariga eller personuppgiftsbiträden i Sverige. Av artikel 40 b framgår att det internationella samarbetet ska omfatta bl.a. hänskjutande av klagomål, bistånd med utredningar och informationsutbyte. Beroende på hur andra medlemsstater väljer att genomföra direktivet kan det även bli aktuellt med bistånd att på enskildas begäran kontrollera om viss personuppgiftsbehandling är författningsenlig.

Om bistånd lämnas ska tillsynsmyndigheten underrätta den utländska tillsynsmyndigheten om hur handläggningen fortskrider och resultatet av begäran. En begäran från en annan medlemsstat om bistånd bör besvaras snabbt, men enligt artikel 50.2 senast en månad efter att den togs emot. Det kan regleras i förordning.

Informationen ska enligt artikel 50.6 som regel tillhandahållas elektroniskt i ett standardiserat format. Kommissionen får enligt artikel 50.8 i genomförandeakter ange format och förfaranden för sådant bistånd. Även formerna för elektronisk överföring av information mellan tillsynsmyndigheterna och mellan dem och styrelsen får regleras på det sättet. Artiklarna 50.6 och 50.8 kräver inga lagstiftningsåtgärder.

Regeringen behandlar i avsnitt 11.10.2 frågan om tillsynsmyndigheten bör kunna ställa upp villkor för användningen av den information som lämnas till den utländska tillsynsmyndigheten vid en svensk begäran om bistånd. Behovet av sekretess och en sekretessbrytande bestämmelse i det internationella samarbetet behandlas i avsnitt 15.2.

11.10.2 Svensk begäran om bistånd av en annan medlemsstat

Regeringens förslag: Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat ska inte få användas för något annat ändamål än det för vilket informationen begärdes.

Regeringens bedömning: Att tillsynsmyndigheten får begära bistånd av en tillsynsmyndighet i en annan medlemsstat och förfarandet vid en sådan begäran kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag och bedömning: Den svenska tillsynsmyndigheten ska kunna begära bistånd av en tillsynsmyndighet i en annan medlemsstat med att utföra åtgärder som tillsynsmyndigheten själv kunnat vidta. Enligt artikel 50.3 ska en sådan begäran innehålla all nödvändig information, inklusive syftet med och skälen för den. Informationen som den svenska tillsynsmyndigheten tar emot får inte användas för andra syften än dem för vilka den har begärts.

En svensk begäran om bistånd kan bli aktuell t.ex. om tillsynsmyndigheten vill göra en allmän kontroll av att regelverket följs när personuppgifter sänds till andra medlemsstater. Ett annat exempel är att en svensk brottsbekämpande myndighet har överfört personuppgifter som borde ha

rättats till en annan medlemsstat vilket gör att den svenska tillsynsmyndigheten vill få information om hur uppgifterna har behandlats av mottagaren.

Det behövs en reglering av när och hur den svenska tillsynsmyndigheten ska kunna begära bistånd. Regeringen delar utredningens bedömning att reglerna om svensk begäran om bistånd av en tillsynsmyndighet i en annan medlemsstat kan tas in i förordning.

I artikel 50.3 föreskrivs att information som en tillsynsmyndighet får genom samarbete med en tillsynsmyndighet i en annan medlemsstat endast får användas för det syfte för vilket den begärdes. Det bör därför tas in en bestämmelse i ramlagen om att den information som den svenska tillsynsmyndigheten får från en annan medlemsstat med anledning av en begäran om bistånd inte får användas för andra syften än dem för vilka informationen begärdes. En sådan bestämmelse bör finnas i lag eftersom den ska ta över andra bestämmelser i både lag och förordning (jfr prop. 1990/91:131 s. 18).

Den föreslagna användningsbegränsningen väcker också frågan om tillsynsmyndigheten bör ges möjlighet att ställa upp villkor för användningen av den information som lämnas till den utländska tillsynsmyndigheten. Eftersom alla medlemsstater är skyldiga att genomföra direktivet, och den utländska tillsynsmyndigheten alltid får veta för vilket ändamål informationen begärs, bör det inte krävas någon begränsning av användningen av den. Det finns därför inget behov av en regel om användningsbegränsning som tar sikte på den information som den svenska tillsynsmyndigheten lämnar när den begär bistånd.

11.11 Tillsyn ska vara avgiftsfri

11.11.1 Tillsynsmyndigheten ska inte kunna ta ut avgifter

Regeringens bedömning: Att tillsynsmyndigheten som huvudregel ska utföra sina tillsynsuppgifter avgiftsfritt kan regleras i förordning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Dataskydd.net* anser att utredningen missförstått artikel 46.3 och att det ska finnas en möjlighet för tillsynsmyndigheten att ta ut administrativa avgifter av tillsynsobjekt.

Skälen för regeringens bedömning

Innehållet i direktivet och nuvarande reglering

Enligt artikel 46.3 ska tillsynsmyndigheten utföra sina uppgifter avgiftsfritt för både enskilda och dataskyddsombud.

Datainspektionens verksamhet finansieras genom statliga anslag. Enligt 3 och 4 §§ avgiftsförordningen (1992:191) får en myndighet ta ut avgifter för varor och tjänster som den tillhandahåller endast om det följer av lag eller förordning eller av ett särskilt beslut av regeringen. Därutöver får en myndighet ta ut avgift i vissa fall, bl.a. för att tillhandahålla information, rådgivning och annan service, om det är förenligt med myndighetens arbetsuppgifter enligt lag, instruktion eller annan förord-

ning och verksamheten är av tillfällig natur eller av mindre omfattning. Enligt regleringsbrevet för budgetåret 2017 får Datainspektionen ta ut avgift för varor och tjänster även om de inte är av tillfällig natur eller mindre omfattning. Det som avses är rätten för myndigheten att ta ut ersättning för den omfattande utbildningsverksamhet som den bedriver. Det har ansetts värdefullt att Datainspektionen kan genomföra utbildning för bl.a. personuppgiftsansvariga och personuppgiftsombud och att det får göras mot avgift. Inspektionen tar även ut avgift för vissa trycksaker.

Tillsynsverksamheten ska vara avgiftsfri

Till skillnad från *Dataskydd.net* anser regeringen att det framgår av artikel 46.3 att utförandet av tillsynsverksamheten ska vara avgiftsfritt. För att tydliggöra att tillsynsmyndigheten som huvudregel ska utföra sina tillsynsuppgifter utan kostnad bör en särskild bestämmelse tas in i förordning. Bestämmelsen bör omfatta all verksamhet som tillsynsmyndigheten utför enligt ramlagen. Därmed omfattar den även uppgifter som myndigheten utför på begäran av en annan medlemsstat (se avsnitt 11.10.1 och 11.11.2). Regleringen innebär att tillsynsmyndighetens arbete med att handlägga klagomål, utföra kontroller, genomföra inspektioner, ge råd och stöd till personuppgiftsansvariga, personuppgiftsbiträden och dataskyddsombud och utfärda föreskrifter och allmänna råd inte får avgiftsbeläggas.

Tillsynsmyndigheten bör dock, i den mån avgiftsförordningen och särskilda beslut medger det, även fortsättningsvis kunna ta ut avgift för sådant som ligger utanför ramlagen. Enligt regeringen bör på samma sätt som i dag t.ex. mer omfattande utbildningsinsatser inte ingå i uppgiften att lämna råd och stöd. Det är också rimligt att tillsynsmyndigheten får ta betalt för sådana trycksaker som går utöver vad som kan krävas enligt ramlagen eller förvaltningslagen. Någon ändring i sak i förhållande till nuvarande ordning är således inte avsedd. Frågor om avgift ska kunna tas ut i vissa fall behandlas även i avsnitt 11.6.3 och 11.11.2.

11.11.2 Ersättning för bistånd till en annan medlemsstat

Regeringens bedömning: Att åtgärder som vidtas på begäran av en tillsynsmyndighet i en annan medlemsstat som huvudregel ska utföras utan ersättning kan regleras i förordning. Tillsynsmyndighetens rätt att överenskomma med utländska tillsynsmyndigheter om ersättning för bistånd i vissa fall kan också regleras i förordning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens bedömning: Enligt artikel 50.7 får tillsynsmyndigheterna som huvudregel inte ta ut någon avgift av varandra för åtgärder som vidtagits med anledning av en begäran om bistånd. Tillsynsmyndigheterna får dock komma överens om regler för ersättning för vissa utgifter i samband med bistånd.

I avsnitt 11.11.1 föreslår regeringen att tillsynsmyndigheten som huvudregel inte får ta ut avgift för att utföra sina tillsynsuppgifter. Avgiftsfriheten föreslås gälla i förhållande till alla, dvs. både i förhållande

till svenska och utländska myndigheter och andra organ. Frågan är om möjligheten att göra undantag från huvudregeln när en annan medlemsstat begär bistånd med tillsynsåtgärder i Sverige bör utnyttjas. Sådana undantag förutsätter att det har träffats bindande överenskommelser mellan berörda stater om det.

Överenskommelser med annan stat ingås som huvudregel av regeringen. Regeringen kan även uppdra åt en förvaltningsmyndighet att ingå en internationell överenskommelse i en fråga där överenskommelsen inte kräver riksdagens eller Utrikesnämndens medverkan (10 kap. 1 och 2 §§ regeringsformen).

En myndighets behörighet att ingå offentligrättsliga avtal måste grundas på ett uttryckligt bemyndigande från regeringen. Bemyndigandet kan avse en viss fråga, men det kan också utformas generellt. Bestämmelsen i 10 kap. 2 § regeringsformen ställer inte upp några begränsningar i fråga om förvaltningsmyndighetens avtalspart i internationella överenskommelser. Det kan t.ex. vara en myndighet eller en annan regering. Med offentligrättsliga avtal avses sådana som endast kan ingås av stater och andra folkrättssubjekt och som får folkrättsliga verkningar. Sådana avtal är folkrättsligt förpliktande för Sverige när de ingåtts av en statlig eller kommunal förvaltningsmyndighet efter bemyndigande från regeringen. Något bemyndigande krävs däremot inte när förvaltningsmyndigheter ingår avtal av uteslutande privaträttslig natur. Om ett avtal ska anses vara privaträttsligt får avgöras utifrån omständigheterna i det enskilda fallet, t.ex. avtalets omfattning eller politiska innebörd (Riktlinjer för handläggningen av ärenden om internationella överenskommelser, Ds 2016:38, s. 17 f.).

Det är svårt att förutse i vilken omfattning andra medlemsstater kommer att begära bistånd av den svenska tillsynsmyndigheten. Det är likaså svårt att förutsäga om biståndet blir resurskrävande för myndigheten. Det ligger i svenskt intresse att kostnader som tillsynsmyndigheter i andra medlemsstater vållar den svenska tillsynsmyndigheten inte alltid ska belasta dess budget. Regeringen delar därför utredningens bedömning att det är rimligt att tillsynsmyndigheten får rättsliga möjligheter att ingå avtal med tillsynsmyndigheter i andra medlemsstater på det sätt som anges i artikel 50.7.

De överenskommelser som är aktuella här kommer att ingås mellan två eller flera myndigheter och rör offentligrättsliga åtgärder. Överenskommelserna kan därmed inte anses vara ett avtal av uteslutande privaträttslig karaktär. Därför krävs en regel som bemyndigar tillsynsmyndigheten att ingå avtal med behöriga tillsynsmyndigheter i andra medlemsstater om ersättning vid begäran om bistånd. Frågan kan regleras i förordning.

Enligt huvudregeln i artikel 46.3 ska tillsynsuppgifter vara avgiftsfria för den registrerade och dataskyddsombudet. Om en tillsynsmyndighet i en annan medlemsstat begär bistånd i en fråga som rör en enskild utgår regeringen därför från att de eventuella avgifter som medlemsstaterna kommer överens om inte kommer att drabba någon enskild.

11.12 Övriga frågor om tillsyn

Regeringens bedömning: Övriga bestämmelser om tillsyn kräver inga lagstiftningsåtgärder.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Enligt artikel 49 ska tillsynsmyndigheten upprätta en årlig rapport om sin verksamhet. Den ska lämnas in till det nationella parlamentet, regeringen eller andra myndigheter som utsetts enligt nationell rätt och offentliggöras. Rapporten kan t.ex. omfatta en förteckning över anmälda överträdelser och vilka sanktioner som har beslutats. Enligt artikel 28.5 i 1995 års direktiv ska tillsynsmyndigheten regelbundet upprätta en rapport om sin verksamhet, som ska offentliggöras.

Enligt 3 § myndighetsförordningen (2007:515) ska varje myndighet redovisa sin verksamhet till regeringen. Myndigheterna ska också enligt förordningen (2000:605) om årsredovisning och budgetunderlag årligen avge en årsredovisning till regeringen. Förutom redogörelser för myndighetens ekonomiska förhållanden ska årsredovisningen enligt 2 kap. 4 § innehålla information om andra förhållanden av väsentlig betydelse för regeringens uppföljning och prövning av verksamheten. Någon lagstiftningsåtgärd behöver därför inte vidtas för att säkerställa den årliga rapporteringen enligt artikel 49.

I artikel 51 föreskrivs att den styrelse som ska inrättas enligt dataskyddsförordningen ska fullgöra motsvarande arbetsuppgifter på direktivets område. Enligt artikel 46.1 l ankommer det på tillsynsmyndigheten att bidra till styrelsens arbete.

I artikel 29 i 1995 års dataskyddsdirektiv regleras vad som gäller för den arbetsgrupp i vilken Datainspektionen ingår som representant för Sverige. Arbetsgruppen kommer att avvecklas i och med att det direktivet upphör att gälla. Regeringens avsikt är att Datainspektionen ska representera Sverige i styrelsen och att det ska framgå av Datainspektionens instruktion (se avsnitt 11.4). Någon ytterligare åtgärd för att genomföra artikel 46.1 l behövs inte.

Enligt artikel 46.1 j ska tillsynsmyndigheten följa sådan utveckling som påverkar skyddet av personuppgifter, bl.a. inom informations- och kommunikationsteknik. I 1 § Datainspektionens instruktion föreskrivs att myndigheten ska följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Någon lagstiftningsåtgärd krävs därför inte för att Sverige ska leva upp till kraven i artikel 46.1 j.

12 Sanktioner

12.1 Utgångspunkter för valet av sanktionssystem

12.1.1 Olika typer av sanktioner

Det finns ingen rättslig definition av begreppet sanktion. En sanktion är i princip alltid handlingsdirigerande eller har ett bestraffande syfte. Med en vid definition skulle sanktion kunna sägas vara alla former av påföljder som kan följa på ett rättsstridigt handlande.

En sanktion kan vara repressiv eller icke repressiv. Med att en sanktion är repressiv menas att det är staten som kan ta initiativ till sanktionen. En icke repressiv sanktion är t.ex. möjligheten att begära skadestånd i en civilprocess (se avsnitt 13.3).

Det finns flera olika sorters repressiva sanktioner. Den mest ingripande formen är straff. En annan typ av repressiv sanktion är administrativa avgifter, t.ex. sanktionsavgifter. Sanktionsavgift kan i vissa fall vara ett komplement till andra åtgärder och användas för att i enskilda fall nyansera ingripandet. Sanktionsavgift ersätter i andra fall kriminalisering.

Även t.ex. åtgärdsföreläggganden (i förening med vite), skyldighet att vidta rättelse och möjlighet för en tillsynsmyndighet att meddela förbud räknas som repressiva administrativa sanktioner.

12.1.2 Innehållet i direktivet och nuvarande reglering

Innehållet i direktivet

I direktivet överlåts det till medlemsstaterna att välja sanktioner. Enligt artikel 57 ska medlemsstaterna föreskriva sanktioner för överträdelser av bestämmelser som antas enligt direktivet och vidta de åtgärder som krävs för att säkerställa att de genomförs. Sanktionerna ska vara effektiva, proportionerliga och avskräckande. Enligt skäl 89 ska både fysiska och juridiska personer, oavsett om de är privaträttsliga eller offentligrättsliga subjekt, kunna träffas av sanktioner om de överträder bestämmelserna om personuppgiftsbehandling.

Dagens sanktionssystem

I personuppgiftslagen finns dels regler om straffansvar i 49 §, dels regler som ger tillsynsmyndigheten rätt att vid vite förbjuda behandling på annat sätt än genom lagring i 44 och 45 §§. Vidare får tillsynsmyndigheten enligt 47 § hos domstol ansöka om att personuppgifter som behandlats på ett olagligt sätt ska utplånas. Dessa bestämmelser genomför artikel 24 i 1995 års dataskyddsdirektiv. Artikeln ålägger medlemsstaterna att säkerställa att direktivet genomförs och att särskilt besluta om sanktioner som ska användas vid överträdelser av de bestämmelser som genomför direktivet. Möjligheten att begära skadestånd brukar, förutom att ses som ett rättsmedel, också ses som en del av sanktionssystemet.

I förarbetena till personuppgiftslagen framhöll regeringen att de huvudsakliga sanktionerna mot personuppgiftsansvariga som inte följer lagen är skadestånd och vite. Dessa sanktioner ansågs effektiva och i stort sett

tillräckliga. Regeringen konstaterade att trenden gick mot avkriminalisering, men föreslog en straffbestämmelse som kriminaliserade vissa åtgärder (prop. 1997/98:44 s. 108.). Då kriminaliserades även oaktsamhet av normalgraden, men straffansvaret har senare begränsats till grov oaktsamhet (prop. 2005/06:173 s. 47 f.). Den som uppsåtligen eller av grov oaktsamhet lämnar osann uppgift i vissa fall, behandlar känsliga personuppgifter eller uppgifter om lagöverträdelser i strid med bestämmelserna i lagen, brister i anmälningsskyldighet eller överför personuppgifter i strid med reglerna om överföring till tredjeland döms till böter eller fängelse i högst sex månader. Om brottet är grovt är straffet fängelse i högst två år. Ringa fall är undantagna från straffansvar. Om någon inte har följt ett vitesföreläggande döms inte till ansvar för samma gärning. Straffansvar kan utkrävas av den som utfört handlingen eller är ansvarig för underlåtenheten. Han eller hon behöver inte vara personuppgiftsansvarig.

Eftersom 49 § personuppgiftslagen enbart straffbelägger brott mot den lagen och föreskrifter som har meddelats med stöd av den omfattar straffansvaret inte brott mot bestämmelser i myndigheternas registerförfattningar. Straffbestämmelsen gäller över huvud taget inte för Polismyndigheten, Tullverket, Kustbevakningen, åklagarväsendet och domstolarna. Skälet till det är enligt förarbetena till dessa myndigheters registerförfattningar att det i brottsbalken föreskrivs straffrättsligt ansvar för otillåten hantering av personuppgifter. Ansvar kan, beroende på omständigheterna, utkrävas för tjänstefel enligt 20 kap. 1 § brottsbalken, brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken eller dataintrång enligt 4 kap. 9 c § brottsbalken (se t.ex. prop. 2014/15:63 s. 56 f.).

Även bestämmelserna om disciplinansvar i lagen (1994:260) om offentlig anställning kan aktualiseras, om någon bryter mot bestämmelserna om personuppgiftsbehandling. En arbetstagare kan meddelas disciplinpåföljd för tjänsteförseelse. Disciplinpåföljderna är varning eller löneavdrag. Disciplinansvar förutsätter att den misstänkta gärningen inte ska anmälas till åtal eller, om den redan prövats straffrättsligt, att den inte har ansetts vara något brott av annat skäl än bristande bevisning. Arbetsdomstolen har bl.a. prövat frågan om disciplinansvar för en handläggare som gjort obehöriga slagningar i Försäkringskassans datasystem (AD 2005 nr 82).

12.1.3 Ett sammanhållet sanktionssystem

Ett av direktivets övergripande syften är att motverka otillåten behandling av personuppgifter i syfte att förhindra att enskildas integritet kränks. Utgångspunkten för överväganden om sanktioner är att de ska vara effektiva och bidra till god efterlevnad av bestämmelserna om personuppgiftsbehandling inom ramlagens tillämpningsområde. I avsnitt 11.7.6 behandlas tillsynsmyndighetens korrigerande befogenheter i form av förelägganden och beslut om förbud mot fortsatt behandling. Skadestånd behandlas i avsnitt 13.3. Det som återstår att behandla här är frågor om straffrättsliga, disciplinära och andra offentligrättsliga sanktioner.

Var och en av sanktionerna ska vara effektiv, proportionerlig och avskräckande. För att uppfylla kraven i direktivet ska sanktionerna också bilda en helhet som sammantaget utgör ett effektivt sanktionssystem.

Dataskyddsdirektivet och dataskyddsförordningen har stora likheter i fråga om enskildas rättigheter och personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter. De myndigheter och andra aktörer som ska tillämpa ramlagen ska också i varierande utsträckning tillämpa förordningen. Det är mot den bakgrunden svårt att motivera att helt olika sanktionssystem ska gälla beroende på om ramlagen eller förordningen är tillämplig för överträdelser som är likartade och som därför kan antas vara värda samma sanktion. Vid övervägandena om hur sanktionssystemet bör utformas finns det därför skäl att beakta vad som gäller enligt förordningen.

12.2 Vilket sanktionssystem bör väljas?

12.2.1 Ingen straffbestämmelse i ramlagen

Regeringens bedömning: Överträdelser av regler om personuppgiftsbehandling bör inte vara straffsanktionerade, utöver vad som gäller enligt brottsbalken.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Några remissinstanser, däribland *Uppsala universitet*, instämmer i utredningens bedömning att överträdelser av regler om personuppgiftsbehandling inte ska vara straffsanktionerade. *Umeå universitet* anser att ett eventuellt system med sanktionsavgifter borde kompletteras med en bestämmelse om straff- eller disciplinansvar för enskilda tjänstemän för att bli effektivt.

Skälen för regeringens bedömning

Är dagens bestämmelser om straff- och disciplinansvar effektiva?

Personuppgiftslagens straffbestämmelse är i dag inte tillämplig inom större delen av ramlagens tillämpningsområde. Det straffbara området har också begränsats genom att den numera bara gäller för grovt oaktsamma och uppsåtliga brott. När oaktsamhet av normalgraden avkriminaliserades år 2006 anfördes bl.a. att utvecklingen hade gått mot att straff inte är en nödvändig reaktion på överträdelser av personuppgiftslagen eller anslutande registerförfattningar (prop. 2005/06:173 s. 47 f.).

Frågan är om det finns bärande skäl att nu införa en straffbestämmelse som gäller för ramlagens tillämpningsområde. Det finns inget känt exempel på att en person har dömts för brott mot personuppgiftslagen för en överträdelse som han eller hon gjort sig skyldig till som anställd vid en myndighet (SOU 2015:39 s. 637). Av det förhållandet att 49 § personuppgiftslagen inte såvitt känt har lett till några fällande domar mot anställda vid myndigheter – vilket ibland anförs som skäl för att någon straffbestämmelse inte behövs – går det emellertid inte att dra någon slutsats om bestämmelsen fyllt sin funktion att avhålla från brott.

Det som talar för att ha en särskild straffbestämmelse är att bestämmelserna i brottsbalken inte motsvarar det som i dag kriminaliseras i 49 § personuppgiftslagen eller de överträdelser som det skulle kunna vara aktuellt att kriminalisera i ramlagen. Brottsbalksbrotten tar i stället primärt sikte på andra straffvärda förfaranden än felaktig behandling av personuppgifter och har helt andra rekvisit.

Den straffbestämmelse som det ligger närmast till hands att jämföra med är bestämmelsen om dataintrång (4 kap. 9 c § brottsbalken). Om t.ex. en arbetstagare behandlat personuppgifter felaktigt i eget intresse, exempelvis gjort registerslagningar som inte krävts för arbetsuppgifterna, fyller bestämmelsen om dataintrång en viktig funktion. Det kan t.ex. vara fråga om någon som av nyfikenhet kontrollerat uppgifter om en granne eller en närstående. Det är inte ovanligt att offentliganställda döms för dataintrång. Dataintrång omfattar dock inte oaktsamhetsbrott och täcker inte heller vissa andra typer av förfaranden som kriminaliseras i personuppgiftslagen.

Bestämmelsen om tjänstefel (20 kap. 1 § brottsbalken) torde sällan kunna tillämpas på överträdelser av regler om personuppgiftsbehandling. Det kan t.ex. vara svårt att med stöd av reglerna i brottsbalken fälla någon till ansvar för att ett olagligt register har inrättats.

Regler om disciplinansvar fyller en viktig funktion för att säkerställa att arbetstagare inte bryter mot arbetsgivarens föreskrifter, t.ex. om hur personuppgifter får behandlas, men bör inte ses som ett medel för att genomföra direktivets sanktionsbestämmelser. Det gäller även de straffbestämmelser som finns i brottsbalken, eftersom de primärt har ett annat syfte.

Överträdelser ska inte straffsanktioneras i ramlagen

Inom ramlagens tillämpningsområde hanteras i stor utsträckning känsliga personuppgifter eller annars särskilt integritetskänsliga uppgifter, vilket talar för att det behövs en särskild straffbestämmelse.

Det som talar mot en straffbestämmelse som den i personuppgiftslagen är både den restriktivitet med nya straffbestämmelser som förordas och att kriminalisering troligen inte skulle få avsedd effekt. Straffansvaret skulle i första hand träffa den som faktiskt felbehandlat personuppgifterna på visst sätt. Det torde i de flesta fall vara en person i underordnad ställning som kanske av oförstånd eller okunskap inte följt reglerna om personuppgiftsbehandling. Överträdelser kan dessutom vara resultatet av flera personers agerande och underlåtenhet. Det blir då svårt att visa var skulden ligger och vad som lett till överträdelsen. En straffbestämmelse med den straffskala som skulle vara aktuell i det här fallet kan också komma att behöva nedprioriteras till förmån för bekämpande av grövre brottslighet. Det kan alltså diskuteras hur stor avskräckande effekt en straffbestämmelse skulle ha för att förhindra felaktig personuppgiftsbehandling inom myndigheter.

Direktivet förutsätter vidare att sanktioner ska kunna träffa både fysiska och juridiska personer. De personuppgiftsansvariga som ska tillämpa ramlagen är emellertid nästan uteslutande juridiska personer, men straffansvar kan enligt svensk rätt inte träffa sådana.

Regeringen delar utredningens bedömning att en kriminalisering motsvarande 49 § personuppgiftslagen inte skulle vara en lämplig sanktion, eftersom den i huvudsak skulle träffa andra än personuppgiftsansvariga och personuppgiftsbiträden. En annan typ av sanktion riktad direkt mot framför allt personuppgiftsansvariga kan antas få mycket större effekt. Med hänsyn till att straffsanktion ska användas i sista hand och endast om det inte finns någon annan sanktion som är tillräckligt effektiv, anser regeringen – i likhet med utredningen – att en annan sanktionsform bör väljas. Någon straffbestämmelse bör alltså, till skillnad från vad *Umeå universitet* förordar, inte tas in i ramlagen.

12.2.2 En ny administrativ sanktion ska införas

Regeringens förslag: En ny administrativ sanktion, sanktionsavgift, ska införas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ett antal remissinstanser, däribland *Datainspektionen* och *Uppsala universitet*, tillstyrker att sanktionsavgifter ska införas som administrativ sanktion. Flera remissinstanser, däribland *Polismyndigheten*, *Försvarsmakten* och *Skatteverket*, avstyrker förslaget. Polismyndigheten framhåller att systematiska brister som berör en stor mängd personer regleras med skadestånd som då snabbt når höga nivåer. Bl.a. mot den bakgrunden menar myndigheten att skadestånd skulle kunna anses uppfylla kravet på effektiva och avskräckande sanktioner. I vart fall skulle skadestånd tillsammans med straffbestämmelser, disciplinansvar och tillsynsmyndighetens åtgärder enligt Polismyndigheten utgöra ett samlat sanktionssystem som bör kunna motsvara direktivets krav. *Sveriges advokatsamfund* ifrågasätter att en kombination av sanktionsavgifter och skadestånd är det mest effektiva sättet att se till att lagstiftningen följs. Vissa remissinstanser, däribland *Helsingborgs tingsrätt* och *Umeå universitet*, menar att en sanktionsavgift är en omfördelning av resurser inom statskassan och ifrågasätter om en sådan åtgärd kan anses vara en effektiv sanktion.

Skälen för regeringens förslag

Behovet av en ny typ av sanktion

Genomförandet av direktivet förutsätter att det finns sanktioner mot överträdelser och att de är tillräckligt effektiva och avskräckande. Samma krav ställs i artikel 24 i 1995 års dataskyddsdirektiv. I förarbetena till personuppgiftslagen ansågs även bestämmelsen om skadestånd till vissa delar genomföra den artikeln. Tanken bakom det synsättet torde vara att skadestånd ibland ses som en civilrättslig sanktion som kompletterar offentligrättsliga sanktioner som t.ex. straffbestämmelser och sanktionsavgifter. Skadestånd behandlas i avsnitt 13.3. Även om skadestånd vid systematiska eller allvarliga överträdelser kan uppgå till mycket höga belopp, som *Polismyndigheten* påpekar, är möjligheten att begära skadestånd enligt regeringens mening inte tillräcklig för att uppfylla kravet på effektiva sanktioner. Inte heller skadestånd tillsammans med straffbe-

stämmelser, disciplinansvar och tillsynsmyndighetens åtgärder kan enligt regeringens mening anses uppfylla de krav som ställs i direktivet. Som tidigare konstaterats träffar inte brottsbalksbestämmelserna primärt felaktig behandling av personuppgifter och en kriminalisering i ramlagen är inte aktuell. Disciplinansvarsreglerna ska inte heller ses som ett medel att genomföra sanktionsbestämmelserna i direktivet. Det krävs därför någon annan typ av sanktion för att uppfylla de krav som ställs i direktivet.

Dataskyddsförordningen har ett nytt sanktionssystem

I dataskyddsförordningen föreskrivs en ny form av sanktion, administrativa sanktionsavgifter, för överträdelser av reglerna om personuppgiftsbehandling. Syftet med sanktionsavgifterna är att stärka verkställigheten av förordningens bestämmelser (skäl 148). Det ligger nära till hands att överväga samma sanktionssystem som i förordningen.

Systemet med sanktionsavgifter regleras i artikel 83 och motiveras i skäl 148–150 i förordningen. Den nationella tillsynsmyndigheten ska enligt artikel 83.1 besluta om sådana avgifter. I artikel 83.2 räknas upp vilka omständigheter som allmänt ska beaktas när sanktionsavgifter beslutas och avgiftens storlek bestäms. I artikel 83.3 regleras hur avgiften ska beräknas vid flera överträdelser.

I princip ska sanktionsavgift beslutas för överträdelse av samtliga bestämmelser i förordningen som föreskriver rättigheter för registrerade eller skyldigheter för personuppgiftsansvariga eller personuppgiftsbiträden. Sanktionsavgift ska enligt artiklarna 83.5 e och 83.6 även tas ut när någon inte följer tillsynsmyndighetens förelägganden eller beslut eller inte ger myndigheten tillgång till uppgifter. Enligt artikel 83.8 ska det finnas effektiva rättsmedel och rättssäkerhetsgarantier vid beslut om sanktionsavgifter. Medlemsstaterna får avgöra om sanktionsavgifter ska kunna beslutas mot offentliga myndigheter och organ.

Fördelar och nackdelar med sanktionsavgift

Sanktionsavgifter finns inom en rad rättsområden. De har olika syfte och utformning. Tillämpningsområdet varierar också. I vissa fall är sanktionsavgift den enda sanktionen för en överträdelse, men i andra fall kan avgift tas ut vid sidan av eller i stället för straff. Användningen av sanktionsavgifter har ökat kraftigt. Övergången från straffbestämmelser till bestämmelser om sanktionsavgift syftade ursprungligen till att utnyttja rättsväsendets resurser bättre och att kunna beivra en del mindre allvarliga och ofta förekommande överträdelser effektivare. Ofta kan avgift tas ut oberoende av om reglerna överträtts uppsåtligen eller av oaktsamhet.

Ett annat syfte med sanktionsavgift var att skapa en kännbar ekonomisk sanktion mot juridiska personer, som inte kan bli föremål för straffrättsliga åtgärder. Sanktionsavgift kan riktas mot det subjekt som tjänar på överträdelsen eller har agerat mest klandervärt eller bär det största ansvaret för att överträdelsen begicks. Om sanktionsavgiften riskerar att innebära en kostnad eller förlust som är lika stor som eller större än den besparing som görs genom att regelverket inte följs, skapar avgiften incitament att undvika överträdelser. När sanktionsavgift tas ut av en myndighet har den ekonomiska aspekten dock inte lika stor betydelse. Vissa remissinstanser, däribland *Helsingborgs tingsrätt* och *Umeå uni-*

versitet, menar vidare att en sanktionsavgift är en omfördelning av resurser inom statskassan och ifrågasätter om en sådan åtgärd kan anses vara en effektiv sanktion.

Utredningen hänvisar till Krigsmaterielexportöversynskommittén som ingående belyser för- och nackdelarna med sanktionsavgifter (SOU 2014:83 s. 104 f.). Kommittén hämtade in information, förutom från länsstyrelserna, från 16 myndigheter med tillsyn över bl.a. områdena miljö, arbetsmiljö, fiskeri, transport, bank- och finansverksamhet samt konsument- och konkurrensfrågor, där det finns sanktionsavgifter. Kommittén ville veta hur tillsynsmyndigheterna ansåg att systemen med administrativa sanktionsavgifter fungerade.

Fördelarna med sanktionsavgifter ansågs vara många. En vanlig åsikt var att sanktionsavgifter har bättre förutsättningar att bidra till regelefterlevnad än straffsanktioner, eftersom brott mot den aktuella lagstiftningen inte prioriteras. Administrativa sanktionsavgifter ansågs också vara mer förutsägbara, vilket leder till en bättre preventiv effekt. Det uppgavs t.ex. att antalet beslutade avgifter hos vissa av myndigheterna minskat över tid. Myndigheterna bedömde att det berodde på ökad regelefterlevnad.

Sanktionsavgifter ledde enligt myndigheterna också till enklare och snabbare beivrande av överträdelser, jämfört med straffsanktioner. Sanktionsavgifter ansågs också vara resurseffektiva, eftersom den tillsynsmyndighet som beslutar om avgifterna fattar beslutet baserat på sin egen utredning. Andra myndigheter behöver inte kopplas in i processen, utom vid överklagande eller om avgiften ska beslutas av domstol på ansökan av tillsynsmyndigheten.

Det finns givetvis också nackdelar med sanktionsavgifter. Om sanktionsavgiftsbeloppet är lågt kan verksamhetsutövaren se avgiften som enbart en kostnad som det går att kalkylera med. I dessa fall bidrar avgiften inte till ökad regelefterlevnad. System med sanktionsavgifter kan kräva mer resurser hos tillsynsmyndigheten. Domstolsväsendet kan, i vart fall inledningsvis, få fler ärenden att hantera om sanktionsavgifter införs. Innan det finns vägledande praxis kan det t.ex. råda osäkerhet om när sanktionsavgift ska tas ut och med vilket belopp. Det behöver alltså inte bli en ekonomisk besparing för staten att införa sanktionsavgifter (SOU 2014:83 s. 106). Avsaknaden av en domstols bedömning av händelseförlopp kan inverka menligt på rättssäkerheten (prop. 2007/08:107 s. 17).

Är sanktionsavgift en lämplig reaktion mot myndigheter?

Vid överväganden om vilken sanktionsform som bör väljas måste hänsyn tas till att det i huvudsak är myndigheter som kommer att tillämpa ramlagen. Det har länge funnits en samsyn om att vitesföreläggande inte bör användas myndigheter emellan, om det inte finns särskilda skäl för det. Därför har bl.a. personuppgiftslagens regel om att tillsynsmyndigheten får förena förelägganden med vite i många fall inte gjorts tillämplig på myndigheter. När det gäller statens roll som arbetsgivare har det dock i olika sammanhang ansetts rimligt att inte särbehandla staten i fråga om ekonomiska sanktioner (se bl.a. 4 kap. 5 § diskrimineringslagen [2008:567] och 7 kap. 7 § arbetsmiljölagen [1977:1160]).

Sanktionsavgift kan tas ut av myndigheter på vissa områden. Hit hör bl.a. miljösanktionsavgift enligt miljöbalken och förordningen (2012:259) om miljösanktionsavgifter. Enligt praxis tas dock inte miljösanktionsavgift ut av myndigheter om överträdelsen skett vid myndighetsutövning.

Det finns också exempel på sanktionsavgifter som särskilt riktar sig mot myndigheter. Enligt 21 kap. 1 § 3 lagen (2016:1145) om offentlig upphandling får allmän förvaltningsdomstol vid otillåten direktupphandling besluta att en upphandlande myndighet ska betala upphandlingsskadeavgift. I förarbetena till den tidigare lagen om offentlig upphandling, som innehöll en motsvarande bestämmelse, betonades vikten av att sanktionsbestämmelserna är desamma för alla slag av upphandlande myndigheter och enheter och att något undantag för statliga myndigheter därför inte borde göras även om det innebär att staten betalar en avgift till staten (Nya rättsmedel på upphandlingsområdet, prop. 2009/10:180 s. 183).

Direktivet syftar till att förbättra skyddet för enskildas integritet. Enskildas intresse av skydd för sin personliga integritet väger lika tungt oavsett om uppgifter behandlas i det allmännas verksamhet eller i den privata sektorn. Såväl statliga som kommunala myndigheter hanterar mycket stora mängder personuppgifter, ofta känsliga sådana. De utbyts dessutom i allt större utsträckning över myndighets- och nationsgränser. Även om det allmännas verksamhet styrs av annan lagstiftning än personuppgiftsregleringen, exempelvis tryckfrihetsförordningen, offentlighets- och sekretesslagen och arkivlagstiftningen, behandlas personuppgifter på i stort sett samma villkor som i privat sektor. Till det kommer att dataskyddsförordningen kommer att tillämpas av alla myndigheter och att sanktionsavgifter således kan komma att drabba även dem, om regelverket görs tillämpligt på myndigheter.

Det är, som utredningen konstaterar, en principiell skillnad mellan att låta en myndighet använda ekonomiska påtryckningsmedel i syfte att förmå en annan myndighet att göra eller underlåta något och att använda ekonomiska sanktioner som reaktion på begångna överträdelser.

Regeringen delar utredningens bedömning att administrativa sanktionsavgifter är en lämplig åtgärd mot myndigheter vid överträdelser av regler om personuppgiftsbehandling.

Är sanktionsavgift i övrigt en lämplig reaktion?

Frågan är då om sanktionsavgift i övrigt är en lämplig reaktion på överträdelser av bestämmelser i ramlagen. Det finns, som utredningen påpekar, flera skäl som talar för en sådan lösning. De myndigheter som i dag tillämpar sanktionsavgifter inom andra områden ser många fördelar med den sanktionen. De argument som dessa lyft fram väger tungt även vid personuppgiftsbehandling.

Sanktionsavgift är en snabb och tydlig sanktion – som även kan vara kännbar ekonomiskt. Risken att som personuppgiftsansvarig drabbas av en sådan sanktion skulle verka avskräckande. Sanktionsavgifter skulle också leda till att ansvar för överträdelser utkrävs på rätt nivå. Det finns nämligen skäl att förmoda att överträdelser av reglerna om personuppgiftsbehandling ofta beror på att otillräckliga resurser avsatts för att ut-

forma it-system som stödjer en korrekt personuppgiftsbehandling, för att utarbeta handledningar och för att utbilda personalen. Risken att drabbas av sanktionsavgift skulle öka incitamenten för personuppgiftsansvariga att satsa på förebyggande åtgärder och att avsätta tillräckliga resurser för den interna kontrollen av personuppgiftsbehandlingen. Överträdelserna skulle därmed på sikt kunna minska på det sätt som beskrivits inom andra områden. Det finns också anledning att anta att ett system med sanktionsavgifter skulle vara effektivare än straffsanktioner. Mindre bevissvårigheter kan leda till att fler överträdelser beivras än om ansvaret är straffrättsligt. Dessa resonemang gör sig även gällande på förordningens och den föreslagna dataskyddslagens område (se prop. 2017/18:105 s. 139 f.). Mot denna bakgrund anser regeringen, till skillnad från bl.a. *Polismyndigheten*, *Försvarsmakten*, *Skatteverket* och *Sveriges advokatsamfund* att det i ramlagen bör tas in regler om sanktionsavgift.

12.3 Utformningen av sanktionsavgiftssystemet

Regeringens bedömning: Sanktionsavgiftssystemet bör utformas med beaktande av regeringens riktlinjer för sådana avgifter, regleringen i dataskyddsförordningen och Sveriges internationella åtaganden.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning

Regeringens riktlinjer för att använda sanktionsavgift

Sanktionsavgift har använts som sanktionsform under lång tid. Införandet av skattetillägg i början av 1970-talet brukar ses som inledningen på mer allmän användning av sanktionsavgift som sanktionsform (SOU 2013:38 del 2, s. 467). Inledningsvis fanns det inga riktlinjer för hur sanktionsavgifter skulle utformas och användas. I samband med lagstiftningsarbetet om ekonomiska sanktioner i näringsverksamhet togs dock ett samlat grepp om frågan (Ds Ju 1981:3, och prop. 1981/1982:142. Jfr även Wiweka Warling-Nerep, Sanktionsavgifter – särskilt i näringsverksamhet, 2010 s. 53, i fortsättningen Warling-Nerep). I nyssnämnda proposition lade regeringen fram allmänna riktlinjer för hur ett sanktionsavgiftssystem bör utformas (prop. 1981/82:142 s. 24 f.)

Riktlinjerna i propositionen har kommit att ligga till grund för förslagen i olika lagstiftningsärenden och tillämpas alltjämt (se t.ex. prop. 2015/16:118 och prop. 2016/17:22). Riktlinjerna kan sammanfattas enligt följande.

- Ett avgiftssystem kan erbjuda en ändamålsenlig lösning i fall där regelöverträdelser är särskilt frekventa eller speciella svårigheter föreligger att beräkna storleken av den vinst eller besparing som uppnås i det särskilda fallet.

- Avgifter bör få förekomma endast inom speciella och klart avgränsade rättsområden.
- Bestämmelserna om beräkning av avgiftsbeloppet bör konstrueras så att de utgår från ett mätbart moment i den aktuella överträdelsen – en parameter – som gör det möjligt att förutse och fastställa hur stor avgiften ska bli i det särskilda fallet.
- Beroende på det aktuella rättsområdets natur bör särskilt prövas om uppsåt eller oaktsamhet ska förutsättas för avgiftsskyldighet eller om skyldigheten ska bygga på strikt ansvar. För att en konstruktion med strikt ansvar ska vara försvarbar från rättssäkerhetssynpunkt bör det finnas starkt stöd för en presumtion om att överträdelser på området inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet. Bestämmelser som reglerar möjligheten till jämkning av avgiftsbelopp bör så långt möjligt vara så preciserade att det inte föreligger någon tvekan om deras räckvidd.
- Något hinder bör inte föreligga mot att låta avgiftsregler som i första hand riktas mot juridiska personer och straffrättsliga bestämmelser riktade mot fysiska personer vara tillämpliga vid sidan av varandra. De subjektiva rekvisiten kan vara annorlunda utformade i de olika systemen – strikt ansvar vid avgift och uppsåt eller oaktsamhet vid straffrättsligt ansvar.
- Att ta ut sanktionsavgifter kan i viss utsträckning överlämnas till de administrativa myndigheter som är verksamma på det aktuella området. I vissa fall är det emellertid lämpligt att överlämna denna prövning till domstol.

Riktlinjerna tar sikte på sanktioner med vinstbegränsande syfte. De brukar dock också läggas till grund för utformningen av sådana sanktionssystem som har ett bestraffande syfte.

Andra riktlinjer på området

Vid sidan om regeringens riktlinjer i nyssnämnda proposition finns det ytterligare riktlinjer som bör beaktas vid utformningen av ett sanktionsavgiftssystem. Europakonventionen kan vara av betydelse för sanktionsavgiftssystem, om de är jämställa med en straffrättslig påföljd (se avsnitt 12.8).

Europarådets rekommendation nr R (91) om administrativa sanktionsavgifter omfattar åtta principer. Många av frågeställningarna regleras också i Europakonventionen. Några behandlas dock inte i konventionen. Rekommendationen, som inte är rättsligt bindande, får därför anses komplettera den. Principerna kan sammanfattas enligt följande (se SOU 2014:83 s. 110 f.).

- Såväl sanktionens innehåll som de omständigheter som krävs för att sanktionen ska kunna åläggas någon ska framgå av lag.
- Förbud mot retroaktiv tillämpning.
- Förbud mot dubbelprövning (ne bis in idem).
- Krav på rimlig handläggningstid.

- Krav på ett slutligt beslut. Varje inlett förfarande som kan föranleda att en sanktion åläggs en person ska avslutas med ett slutligt avgörande.
- Krav på ett öppet, objektivt och rättvist förfarande. Varje person som riskerar att åläggas en sanktion ska informeras om anklagelsen och den bevisning som åberopas. Vidare ska han eller hon få tillfälle att yttra sig och få tillräcklig tid till det. Ett sanktionsbeslut ska innehålla skälen för beslutet.
- Bevisbördan åligger den som beslutar om sanktionen.
- Krav på domstolsprövning. En sanktion beslutad av en administrativ myndighet ska kunna överprövas av en domstol.

Utgångspunkter för utformningen av sanktionsavgiftssystemet

Vid utformningen av sanktionssystemet bör regeringens riktlinjer och Sveriges internationella åtaganden beaktas. Frågor som rör Europakonventionen behandlas i avsnitt 12.8.

Bestämmelserna om sanktionsavgift bör utformas i linje med hur sådana avgifter utformats inom andra rättsområden och de rättssäkerhetskrav som ställs på sanktionsavgift bör få genomslag. Det innebär att frågor om sanktionsavgift bör regleras i lag och att det av den bör framgå när, hur och av vem sanktionsavgift får tas ut. Systemet ska också vara förutsägbart och möta kraven på rimlig handläggningstid, domstolsprövning och en rättssäker process.

Dataskyddsförordningen har ett system med sanktionsavgifter. De behöriga myndigheterna kommer även att tillämpa förordningen, som är direkt tillämplig i svensk rätt. Överträdelser av bestämmelser om personuppgiftsbehandling bör, som utredningen anger, i princip föranleda samma sanktioner. Det är dock inte möjligt att skapa helt identiska system, eftersom tillämpningsområdena för förordningen och direktivet och regleringen i övrigt skiljer sig åt. Förordningens system med sanktionsavgifter föreslås även gälla för myndigheter inom förordningens tillämpningsområde (prop. 2017/18:105 s. 139 f.). Regeringen utgår därför i förslagen från hur sanktionsavgifter regleras i förordningen och den föreslagna dataskyddslagen.

12.4 Vem ska betala sanktionsavgift?

Regeringens förslag: Sanktionsavgift får tas ut av personuppgiftsansvariga och i vissa fall av personuppgiftsbiträden.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: En personuppgiftsansvarig ansvarar för all personuppgiftsbehandling som utförs under dennes ledning eller på dennes vägnar. Det gäller även den behandling personuppgiftsbiträden, anställda, personer som är att jämställa med anställda (t.ex. inhyrd personal) eller uppdragstagare utför. Sanktionsavgift bör därmed kunna tas ut av personuppgiftsansvariga. Vem som är personuppgiftsansvarig på ramlagens område framgår i dag oftast av författning.

Även om sanktionsavgift normalt kommer att tas ut av personuppgiftsansvariga, bör enligt utredningens mening sanktionsavgift även kunna tas ut av personuppgiftsbiträden. Regeringen delar denna uppfattning. Det bör dock bara gälla om ett personuppgiftsbiträde brutit mot uttryckliga skyldigheter enligt ramlagen. I avsnitt 12.5.2 utvecklas i vilka fall sanktionsavgift bör kunna tas ut av personuppgiftsbiträden. Om ett personuppgiftsbiträde bestämt ändamålen med och medlen för behandlingen i strid med ramlagen är biträdet att anse som personuppgiftsansvarig för den behandlingen (se avsnitt 9.6.3). För sådan behandling bör samma regler om sanktionsavgift gälla som för andra personuppgiftsansvariga.

12.5 Vad ska leda till en sanktionsavgift?

12.5.1 Utgångspunkter

Överträdelser som kan leda till sanktionsavgift enligt dataskyddsförordningen är något förenklat överträdelser av bestämmelser om personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter gentemot registrerade och överträdelser av bestämmelser om rättigheter för registrerade. Även vägran att ge tillsynsmyndigheten tillgång till uppgifter eller att följa beslut eller förelägganden som myndigheten meddelat kan leda till sanktionsavgift.

Många av de överträdelser som kan leda till sanktionsavgift enligt förordningen bör i motsvarande fall kunna göra det enligt ramlagen. Skälen för att vissa överträdelser bör leda till sanktionsavgift är nämligen i allt väsentligt desamma. Det rör sig om överträdelser av de bestämmelser i ramlagen som är viktigast för att värna registrerades integritet, som innehåller de grundläggande reglerna för hur personuppgifter får behandlas och som – om de inte efterlevs – riskerar att leda till allvarliga kränkningar av registrerades integritet. Mot den bakgrunden finns det inte skäl att för varje enskild bestämmelse i detalj redogöra för varför sanktionsavgift är motiverad. I det följande redovisas vilka resonemang som ligger bakom urvalet av överträdelser.

Vissa bestämmelser i ramlagen är dock av den arten att någon sanktionsavgift inte bör komma i fråga. Om den som berörs av ett beslut kan överklaga det beslutet bör sanktionsavgift inte komma i fråga, eftersom möjligheten till domstolsprövning är tillräcklig för att ta till vara registrerades intressen. Det är som regel inte heller lämpligt med sanktionsavgift vid överträdelse av bestämmelser som ger utrymme för olika bedömningar, t.ex. om det är nödvändigt att informera i ett specifikt fall. Bestämmelser om dokumentations- eller underrättelseskyldighet bör normalt inte heller föranleda sanktionsavgift.

12.5.2 Överträdelser som kan leda till en sanktionsavgift

Regeringens förslag: En sanktionsavgift får tas ut av en personuppgiftsansvarig eller ett personuppgiftsbiträde vid överträdelse av vissa bestämmelser om behandling av personuppgifter.

En sanktionsavgift får också tas ut av den som låter bli att bistå tillsynsmyndigheten eller inte rättar sig efter förelägganden eller beslut som myndigheten meddelat.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Södertörns tingsrätt* tillstyrker förslaget generellt men anser att det kan krävas ytterligare överväganden och förtydliganden eftersom det för vissa krav som föreslås sanktionsföreläggas, t.ex. rörande skyldigheter om tekniska och organisatoriska åtgärder, inte är tydligt när ansvar inträder. Tingsrätten anser att det kan ifrågasättas om det är lämpligt att regler av sådan karaktär omfattas av sanktionsavgifter. *Dataskydd.net* anser att brott mot bestämmelser om förpliktelser mot enskilda och rörande förhållandet mellan personuppgiftsansvarig och personuppgiftsombud bör vara sanktionsbelagda.

Skälen för regeringens förslag

Överträdelse av bestämmelser till skydd för registrerades integritet

Att överträda bestämmelser som syftar till att skydda registrerades integritet eller deras rättigheter bör som regel leda till sanktionsavgift. Med det som utgångspunkt bör överträdelser av följande skyldigheter föranleda sanktionsavgift.

Bestämmelserna om att personuppgiftsbehandlingen ska ha rättslig grund och utföras för ett särskilt angivet och berättigat ändamål är av så grundläggande natur att överträdelser av dem bör föranleda sanktionsavgift. Även överträdelse av bestämmelserna om behandling för nya ändamål bör kunna föranleda sanktionsavgift, oavsett om det nya ändamålet ligger innanför eller utanför ramlagens tillämpningsområde.

Bestämmelserna om personuppgifters kvalitet föreskriver konkreta skyldigheter i fråga om bl.a. uppgifternas korrekthet, aktualitet, adekvans och relevans. Även kraven på att göra skillnad mellan olika slag av uppgifter och att se till att alla rimliga åtgärder vidtas för att rätta och komplettera personuppgifter är viktiga för skyddet av enskildas integritet. Alla dessa skyldigheter, liksom den personuppgiftsansvariges skyldighet att radera personuppgifter eller begränsa behandlingen av dem om de behandlats på otillåtet sätt och att inte behandla fler personuppgifter än nödvändigt och inte längre än vad som behövs, bör därför kunna föranleda sanktionsavgift. Otillåten behandling av känsliga personuppgifter är i dag straffsanktionerad och bör redan av det skälet kunna föranleda sanktionsavgift.

Även skyldigheten att vidta tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter är författningsenlig och kunna visa det bör kunna leda till sanktionsavgift. *Södertörns tingsrätt* ifrågasätter om dessa krav är sådana att det föreligger tillräcklig säkerhet och tydlighet beträffande när ansvar inträder. Regeringen konstaterar emellertid att skyldigheten preciseras genom andra bestämmel-

ser, både om vilka personuppgifter som får behandlas och hur det får göras och genom konkreta krav på bl.a. inbyggt dataskydd, dataskydd som standard och loggning.

Skyldigheten att internt begränsa tillgången till personuppgifter är också en viktig del i skyddet för personuppgifter och bör vid överträdelser kunna leda till sanktionsavgift.

Överträdelser av kravet på att vidta åtgärder för att skydda personuppgifter mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada bör också kunna leda till sanktionsavgift. Vad kravet innebär preciseras bl.a. i regler om vad som är en lämplig säkerhetsnivå. Även underlåtenhet att anmäla eller dokumentera personuppgiftsincidenter till tillsynsmyndigheten bör kunna föranleda sanktionsavgift. Det bör också gälla skyldigheten att göra en konsekvensbedömning och att i vissa fall förhandssamråda med tillsynsmyndigheten.

Personuppgifter får bara överföras till tredjeland och internationella organisationer under vissa förutsättningar. I likhet med utredningen anser regeringen – mot bakgrund av att motsvarande överträdelser är straffsanktionerade i dag – att överträdelser av reglerna om överföring bör kunna föranleda sanktionsavgift.

Att inte bistå tillsynsmyndigheten eller att inte följa dess förelägganden eller beslut

I avsnitt 11.7.3 föreslås att tillsynsmyndigheten ska ges tillgång till uppgifter och dokumentation, tillträde till lokaler och annat nödvändigt bistånd för att kunna utöva sin tillsyn. Sanktionsavgift bör kunna tas ut vid underlåtenhet att bistå tillsynsmyndigheten vid tillsyn. I avsnitt 11.7.6 föreslås att tillsynsmyndigheten ska kunna meddela förelägganden om viss åtgärd. Tillsynsmyndigheten ska också kunna förbjuda viss behandling. Det är, som utredningen konstaterar, viktigt att sanktionsavgift kan tas ut av den som vägrar att rätta sig efter tillsynsmyndighetens beslut i sådana frågor. Tillsynsmyndighetens ställning kan annars undermineras.

Sanktionsavgift bör i vissa fall kunna tas ut av personuppgiftsbiträden

Eftersom den personuppgiftsansvarige ansvarar även för personuppgiftsbiträdens behandling bör sanktionsavgift tas ut av den personuppgiftsansvarige vid överträdelser som berott på biträdets agerande. Som framgår av avsnitt 12.4 bör dock sanktionsavgift kunna tas ut även av personuppgiftsbiträden i vissa fall när de har uttryckliga skyldigheter som framgår av författning.

Sanktionsavgift bör således kunna tas ut av personuppgiftsbiträden om tillgången till personuppgifter internt inte begränsas till vad varje tjänsteman behöver för att utföra sina arbetsuppgifter eller om tillräckliga åtgärder inte vidtas för att säkerställa att de personuppgiftsuppgifter som behandlas skyddas t.ex. mot obehörig eller otillåten behandling. Sanktionsavgift bör också kunna tas ut om skyldigheten att se till att behandling loggas inte fullgörs.

Skyldigheten att bistå tillsynsmyndigheten och att följa förelägganden och beslut som meddelats av tillsynsmyndigheten föreslås gälla även för personuppgiftsbiträden (se avsnitt 11.7.3 och 11.7.6). Det bör därför vara

möjligt att ålägga personuppgiftsbiträden sanktionsavgift om de inte fullgör sådana förpliktelser.

I övrigt bör personuppgiftsbiträden inte kunna åläggas sanktionsavgift.

Sanktionsavgift bör inte tas ut för vissa överträdelser

Som nyss nämnts bör inte sanktionsavgift tas ut för överträdelser av alla bestämmelser i ramlagen och de föreskrifter som meddelas i anslutning till den. Det finns inte skäl att ta ut sanktionsavgift för överträdelser av bestämmelser om personuppgiftsansvarigas skyldighet att på begäran av en registrerad rätta, komplettera eller radera personuppgifter eller begränsa behandlingen av dem eller ompröva vissa beslut. Om det finns sakskäl för att vidta åtgärden är den personuppgiftsansvarige skyldig att utföra den oberoende av begäran (se avsnitt 8.1.6). Sanktionsavgift kan då tas ut på grund av att de grundläggande bestämmelserna om åtgärder för att säkerställa personuppgifternas kvalitet har överträtts och regeringen anser därför till skillnad från *Dataskydd.net* inte att bestämmelserna om skyldigheter i förhållande till den registrerade i dessa avseenden bör sanktioneras.

Eftersom sanktionsavgift kan tas ut för överträdelser av de mer konkreta skyldigheterna i ramlagen anser regeringen vidare i likhet med utredningen att det inte finns skäl att ta ut sanktionsavgift för överträdelser av bestämmelsen om att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Sanktionsavgift bör inte heller tas ut om skyldigheten att utse dataskyddsombud inte fullgörs. Regeringen håller med utredningen om att det är tillräckligt att det finns en skyldighet att anmäla att ombud har utsetts och entledigats till tillsynsmyndigheten. Om en personuppgiftsansvarig inte skulle fullgöra den skyldigheten, kan tillsynsmyndigheten reagera och t.ex. utfärda ett föreläggande.

Till skillnad från Dataskydd.net anser regeringen inte heller att bestämmelser som reglerar förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden bör kunna föranleda sanktionsavgift. Inte heller personuppgiftsbiträdens underlåtenhet att anmäla personuppgiftsincidenter till den personuppgiftsansvarige bör kunna leda till sanktionsavgift.

Inte heller överträdelser av bestämmelser som reglerar skyldigheter mellan gemensamt personuppgiftsansvariga bör kunna föranleda sanktionsavgift. Om överträdelser förekommer i situationer där personuppgiftsansvaret är gemensamt får det avgöras i det enskilda fallet om avgift bör tas ut av en av parterna eller av flera.

En personuppgiftsansvarig ska tillhandahålla viss information till de registrerade. De bestämmelser som reglerar skyldigheten att tillhandahålla allmän information och information som ska lämnas i ett enskilt fall bör inte kunna föranleda sanktionsavgift. Den allmänna informationen är av sådan karaktär att det inte finns någon större risk att en registrerad lider en rättsförlust om den inte lämnas. Skyldigheten att lämna personrelaterad information i ett enskilt fall förutsätter en bedömning av när information ska lämnas, vilket gör att sanktionsavgift inte bör kunna tas ut. Skyldigheten att på begäran informera om eller ge tillgång till personuppgifter bör inte heller kunna leda till sanktionsavgift, eftersom beslut i sådana frågor får överklagas.

12.5.3 Ska sanktionsavgift alltid tas ut?

Regeringens förslag: Regleringen av sanktionsavgifter ska bygga på strikt ansvar.

Det ska inte vara obligatoriskt att ta ut sanktionsavgift när en bestämmelse i ramlagen som kan föranleda avgift har överträtts.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Sanktionsavgiftssystemet bör bygga på strikt ansvar

Huvudregeln är att sanktionsavgiftssystem bygger på strikt ansvar. I propositionen Ny dataskyddslag tolkas bestämmelserna i dataskyddsförordningen som att varken uppsåt eller oaktsamhet är ett krav för att ta ut sanktionsavgift. Det räcker att en bestämmelse faktiskt har överträtts. Däremot kan det påverka frågan om sanktionsavgift ska tas ut eller inte, och avgiftens storlek, om överträdelsen är uppsåtlig eller oaktsam (prop. 2017/18:105 s. 138).

Regeringen håller med utredningen om att det inte finns skäl att avvika från grundprincipen för sanktionsavgifter att ansvaret ska vara strikt. Det är framför allt den omständigheten att det inte behöver bevisas att handlandet varit avsiktligt eller att avgöra hur oaktsamt handlandet har varit som gör att system med sanktionsavgifter anses vara så effektiva. För att inte den fördelen ska gå förlorad bör den personuppgiftsansvarige och personuppgiftsbiträden ha strikt ansvar för sådan felaktig behandling av personuppgifter som kan föranleda att sanktionsavgift tas ut. Det är också svårt att se att överträdelser kan bero på annat än uppsåt eller oaktsamhet.

Lagrådet har uttalat att skrivningar om att avgiftsskyldigheten bygger på strikt ansvar inte bör tas med i författningstext. I motsats till vad som gäller för straffbestämmelser finns det nämligen inte något formellt krav på uppsåt eller oaktsamhet för att besluta om sanktionsavgift (Ny lag om kontroll av ekologisk produktion, prop. 2012/13:55 s. 142). Det finns därför inget skäl att uttryckligen föreskriva att ansvaret ska vara strikt.

Ska det vara obligatoriskt att ta ut sanktionsavgift?

Strikt ansvar innebär att det varken krävs uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut. Strikt ansvar medför emellertid inte att sanktionsavgift måste tas ut vid varje överträdelse. En viktig fråga är därför om det ska vara obligatoriskt att ta ut sanktionsavgift när en viss bestämmelse har överträtts.

Regeringen anser, i likhet med utredningen, att inte varje överträdelse av de bestämmelser i ramlagen som kan föranleda sanktionsavgift bör medföra att sådan avgift faktiskt tas ut. Reglerna om personuppgiftsbehandling är mycket komplexa och det nya regelverket kommer inte att förenkla tillämpningen. Det skulle ställa alltför höga krav på de personuppgiftsansvariga och lägga en orimlig börda på tillsynsmyndigheten om varje överträdelse av en viss bestämmelse skulle leda till att sanktionsavgift tas ut. Som exempel kan nämnas att det inte är rimligt att ålägga en myndighet sanktionsavgift för att någon i enstaka fall behandlat en per-

sonuppgift felaktigt, även om det kan vara djupt kränkande. Om det däremot har satts i system att göra sådana behandlingar eller om påpekanden om att det krävs utbildning för att undvika sådant felbeteende inte följs, bör sanktionsavgift kunna övervägas. Det bör således ligga hos den som har till uppgift att besluta om avgiften att avgöra om en överträdelse är så allvarlig eller systematisk att sanktionsavgift bör tas ut. Bestämmelsen bör därför utformas så att det inte är obligatoriskt att besluta om sanktionsavgift.

Det kan diskuteras om lagstiftningen med en sådan regel lever upp till direktivets krav på effektiva sanktioner. Liksom utredningen utgår emellertid regeringen från att de personuppgiftsansvariga – som i huvudsak är myndigheter – normalt kommer att rätta sig efter tillsynsmyndighetens påpekanden, förelägganden och beslut och att det bara i ett litet antal fall kommer att vara nödvändigt att ta ut sanktionsavgift. Sanktionssystemet som helhet uppfyller således enligt regeringen kraven i direktivet.

12.6 Hur sanktionsavgiften ska bestämmas

12.6.1 Sanktionsavgiftens storlek

Regeringens förslag: För mindre allvarliga överträdelser ska avgiften bestämmas till högst 5 000 000 kronor. För allvarliga överträdelser ska avgiften bestämmas till högst 10 000 000 kronor. Det ska av ramlagen framgå vilka överträdelser som kan leda till den lägre respektive högre sanktionsavgiften.

Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlingar, ska sanktionsavgiften bestämmas efter överträdelsernas allvar. Sanktionsavgiften får dock aldrig överstiga maximibeloppet för den allvarligaste överträdelsen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att högsta avgiften för mindre allvarliga överträdelser ska vara 10 000 000 kronor och för allvarliga överträdelser 20 000 000 kronor. Dessutom föreslår utredningen minimibelopp på respektive nivå.

Remissinstanserna: *Datainspektionen* påpekar att det är viktigt att ramlagen utformas på samma sätt som dataskyddsförordningen och den kompletterande dataskyddslagen och ifrågasätter införande av minimibelopp. Några remissinstanser, däribland *Malmö kommun* och *Norrköpings kommun*, anser att de föreslagna beloppen om högst 20 000 000 kronor är för höga. *Dataskydd.net* anser att sanktionerna ska bidra till att den tillsedda aktören får ekonomiska incitament att agera på tillsynens resultat och att dataskyddsförordningens nivåer borde gälla.

Skälen för regeringens förslag

Hur hög bör sanktionsavgiften vara?

I dataskyddsförordningen regleras vilken sanktionsavgift som maximalt kan tas ut vid olika överträdelser. I förordningen är de belopp som anges mycket höga och anges dessutom i euro. Några minimibelopp anges inte,

men maximibeloppen är 10 000 000 euro respektive 20 000 000 euro, alternativt en viss procentsats av den totala globala årsomsättningen.

När det gäller sanktionsavgifter är det inte ovanligt att det i författning eller genom myndighetsföreskrifter anges fasta belopp för olika typer av överträdelser. Regeringen instämmer med utredningen i att en sådan ordning inte är ändamålsenlig i detta fall. Ett flertal faktorer som inte går att standardisera måste beaktas i det enskilda fallet för att avgöra hur stor sanktionsavgiften bör vara. På samma sätt som i förordningen bör sanktionsavgiften inte baseras på i förväg fastställda belopp utan bestämmas med utgångspunkt i omständigheterna i det enskilda fallet.

Överträdelser av bestämmelserna i ramlagen kan typiskt sett inte förväntas generera stora besparingar eller vinster för den personuppgiftsansvarige eller personuppgiftsbiträdet. Det finns därmed inte förutsättningar att knyta avgiften till omsättningen av verksamheten, vinsten eller något liknande kriterium.

Varken på miljöområdet eller på arbetsmiljöområdet är de avgifter som kan tas ut tillnärmelsevis så höga som de som anges i dataskyddsförordningen. Det högsta beloppet som kan beslutas vid en överträdelse inom dessa områden är 1 000 000 kronor. Inte heller företagsbot eller upphandlingsskadeavgift kan uppgå till lika höga belopp som enligt förordningen. För företagsbot är maximibeloppet idag 10 000 000 kronor. För upphandlingsskadeavgift enligt lagen (2016:1145) om offentlig upphandling är det högsta beloppet 10 000 000 kronor. Avgiften får dock aldrig överstiga en viss procentsats av upphandlingens värde.

De överträdelser som enligt förordningen kan bli föremål för sanktionsavgift har till största delen sin motsvarighet i direktivet. Det skulle givetvis kunna hävdas att samma typ av överträdelse bör leda till samma sanktion. Utredningen anser dock att det är viktigare att sanktionerna i ramlagen utgör en rimlig reaktion på överträdelserna, särskilt mot bakgrund av att det framför allt är myndigheter som kan komma att träffas av sanktionsavgifterna. Regeringen delar denna bedömning. Avgifterna bör också beloppsmässigt ligga i paritet med andra sanktionsavgifter i svensk rätt. Skillnaden mellan sanktionsavgifternas storlek i förordningen och ramlagen kan också motiveras av att de personuppgiftsansvariga som ska tillämpa förordningen kan vara multinationella företag där det krävs synnerligen höga sanktionsbelopp för att det ska vara kännbart. Inom ramlagens tillämpningsområde kan även en lägre avgift förväntas påverka agerandet i önskad riktning. Till det kommer att ett felaktigt handlande av en myndighet sällan föranleds av en önskan att maximera vinst eller att göra en större besparing, även om det inte kan uteslutas att det finns ekonomiska motiv. Lägre men tillräckligt kännbara belopp torde därför påverka myndigheterna så länge budgetprincipen upprätthålls och de inte får ekonomiska tillskott för att kunna betala sina sanktionsavgifter.

Ett av huvudsyftena med sanktionsavgifter är att de ska vara avskräckande. För att regleringen ska få en tillräckligt avskräckande effekt krävs, trots det som sagts om myndigheters relativt sett högre känslighet även för låga sanktionsavgifter, enligt regeringens mening att maximibeloppet sätts relativt högt.

De överträdelser som kan leda till sanktionsavgift kan se olika ut och de ekonomiska förutsättningarna för dem som avgiften ska tas ut av kan

variera. Spannet inom vilket avgift kan bestämmas bör därför vara relativt stort.

Beträffande personuppgiftsbiträden väger argumenten ovan inte lika tungt eftersom de ofta, även inom ramlagens tillämpningsområde, är privaträttsliga aktörer som drivs av affärsmässiga överväganden och vinstintressen. Som framgår av avsnitt 9.6.2 agerar myndigheter ibland personuppgiftsbiträden åt varandra. Syftet med det torde vara att spara på statens resurser. Mot den bakgrunden bör samma sanktionsavgifter tillämpas på personuppgiftsbiträden som på personuppgiftsansvariga.

Sammanfattningsvis delar regeringen utredningens bedömning att sanktionsavgiftsbeloppen bör vara lägre än i dataskyddsförordningen och ligga mer i linje med de sanktionsavgifter som i dag finns på andra områden och med företagsbot. I avsnitt 12.6.2 återkommer regeringen till hur avgiften bör bestämmas i det enskilda fallet.

Sanktionsavgift ska enligt dataskyddsförordningen tas ut enligt två olika nivåer – en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser och underlåtenhet att följa förelägganden eller beslut av tillsynsmyndigheten eller att på annat sätt bistå den. Regeringen instämmer med utredningen i att det även inom ramlagens tillämpningsområde bör finnas två avgiftsnivåer. I propositionen Ny dataskyddslag föreslås att sanktionsavgifter införs för statliga och kommunala myndigheter på förordningens område (prop. 2017/18:105 s. 139 f.). Däremot föreslås inga minimibelopp på de olika avgiftsnivåerna. Utgångspunkten bör som nämnts i avsnitt 12.3 vara att sanktionssystemen i ramlagen och förordningen så långt möjligt ska stämma överens. Det är även ett argument som *Datainspektionen* anför emot införande av minimibelopp i ramlagen. Mot denna bakgrund anser regeringen till skillnad mot utredningen att endast maximibelopp för sanktionsavgifter ska anges i ramlagen.

Avgiftsnivåer vid överträdelser

Det är viktigt att avgiftsnivåerna sätts så pass högt att de har en avskräckande effekt. *Dataskydd.net* anser att förordningens nivåer bör gälla. De sanktionsavgifter som kan tas ut med stöd av dataskyddsförordningen är emellertid synnerligen höga. Utredningen föreslår ett maximibelopp om 10 000 000 kronor för mindre allvarliga överträdelser och att det ska kunna påföras maximibelopp om 20 000 000 kronor för allvarliga överträdelser. Regeringen anser emellertid, i likhet med bl.a. *Malmö kommun* och *Norrköpings kommun*, att även dessa belopp är höga. Som tidigare konstaterats är 10 000 000 kronor maximibelopp för både företagsbot och upphandlingsskadeavgift. Regeringen anser att högre belopp än så inte heller bör kunna påföras en myndighet vid överträdelser inom ramlagens tillämpningsområde. Enligt regeringens bedömning skulle en avgift om 10 000 000 kronor utgöra en effektiv, proportionell och avskräckande sanktion också mot allvarliga överträdelser, även för de största myndigheterna. Dessa resonemang gör sig även gällande för sanktionsavgifter för myndigheter på förordningens område (se prop. 2017/18:105 s 141).

Till allvarligare överträdelser bör räknas alla överträdelser av grundläggande krav på personuppgiftsbehandlingen. Bestämmelserna är cen-

trala för skyddet av registrerades integritet, oavsett om det är fråga om känsliga personuppgifter eller personuppgifter i allmänhet. En annan sak är att sanktionsavgiften normalt bör bestämmas till ett högre belopp om överträdelsen avser känsliga personuppgifter.

Eftersom åtgärder för att säkerställa författningsenlig behandling syftar till att avskräcka från behandling i strid med de grundläggande principerna för personuppgiftsbehandling bör överträdelser mot de bestämmelserna också ses som allvarliga, dock med undantag för tillgången till personuppgifter internt.

Även överträdelser av bestämmelser som avser skyldighet att vidta åtgärder för att säkerställa säkerhet vid behandling bör ses som allvarliga, eftersom sådana överträdelser kan få mycket långtgående konsekvenser för registrerade.

Överträdelser av vad som gäller vid överföring till tredjeland och internationella organisationer bör också leda till den högre sanktionsavgiften. Det är allvarligt att uppgifterna får spridning om inte skyddet för dem kan garanteras.

Den högre avgiften bör också tillämpas vid underlåtenhet att följa tillsynsmyndighetens förelägganden eller beslut eller att på annat sätt underlåta att bistå den. Genom det inskärps allvaret i att inte rätta sig efter tillsynsmyndighetens synpunkter.

Det finns utifrån den modell som föreslås i dataskyddslagen skäl att bestämma beloppen för mindre allvarliga överträdelser till hälften, dvs. 5 000 000 kronor (prop. 2017/18:105 s. 141). Till mindre allvarliga överträdelser bör räknas att den personuppgiftsansvarige eller ett personuppgiftsbiträde inte begränsat tillgången till personuppgifter internt. Även om det är en viktig bestämmelse är risken för kränkning av den enskildes integritet mindre än om uppgifterna sprids utanför verksamheten eller behandlas otillåtet på något annat sätt.

Till mindre allvarliga överträdelser bör också räknas underlåtenhet av personuppgiftsansvariga att dokumentera personuppgiftsincidenter. Även underlåtenhet att göra en konsekvensbedömning eller att inleda förhandssamråd med tillsynsmyndigheten bör anses som mindre allvarlig.

Flera samtidiga överträdelser

Felaktig eller otillåten personuppgiftsbehandling kan innebära att flera bestämmelser om behandling av personuppgifter överträds samtidigt. Det kan t.ex. vara fråga om behandling som inte bara saknar rättslig grund utan som också strider mot andra bestämmelser om hur personuppgifter får behandlas. På motsvarande sätt kan en överträdelse, oavsett om den strider mot en eller flera bestämmelser, upprepas genom personuppgiftsbehandlingar som är sammankopplade med varandra. Det kan få till följd att en felaktig behandling följer med till nästa behandling. Var och en av dessa överträdelser kan, om den är tillräckligt allvarlig, leda till att sanktionsavgift tas ut. Som utredningen konstaterar är det emellertid inte rimligt att tillsynsmyndigheten i dessa fall lägger samman beloppen som fastställts för var och en av överträdelserna till en gemensam sanktionsavgift. Sanktionsavgiften måste framstå som en rimlig reaktion på samtliga överträdelser som är föremål för bedömning. Om den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till flera över-

trädelser genom samma eller sammankopplade personuppgiftsbehandlingar bör det totala beloppet för sanktionsavgiften i stället bestämmas efter de samlade överträdelsernas allvar. Om det är fråga om felaktig behandling på samma sätt av många personers personuppgifter, t.ex. om ett otillåtet register omfattar många personer, får alltså en samlad bedömning göras och en gemensam sanktionsavgift bestämmas med utgångspunkt i hur klandervärd den totala felbehandlingen är.

Sanktionsavgiften vid flera samtidiga överträdelser bör emellertid aldrig få överstiga maximibeloppet för den sanktionsavgiftsnivå som är aktuell. Det bör framgå av ramlagen. Det innebär att om någon av överträdelserna är av allvarligare slag får maximibeloppet för allvarligare överträdelser inte överskridas. Om ingen av överträdelserna är av allvarligare slag ska maximibeloppet för mindre allvarliga överträdelser tillämpas.

12.6.2 Hur avgiften ska bestämmas i det enskilda fallet

Regeringens förslag: Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas, ska särskild hänsyn tas till om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit samt till överträdelsens karaktär, svårhetsgrad och varaktighet. Vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen ska också vägas in, liksom om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Omständigheter som bör påverka sanktionsavgiften

Det är inte obligatoriskt att ta ut sanktionsavgift. Det bör därför regleras vilka omständigheter som kan göra att sanktionsavgift inte tas ut och vad som kan påverka avgiftens storlek. Det sistnämnda är särskilt viktigt, eftersom sanktionsavgiftens storlek inte anges till ett fast belopp i lagen. En uppräkning av sådana omständigheter kan dock inte göras uttömmande utan bör ange de omständigheter som är särskilt viktiga. Bestämmelsen bör lämna utrymme för att också beakta andra förmildrande eller försvårande omständigheter.

Uppräkningen i dataskyddsförordningen av vilka omständigheter som bör beaktas kan tjäna som ledning för vad som är relevant. Regeringen håller med utredningen om att i princip samtliga omständigheter som räknas upp i artikel 83.2 i förordningen kan vara av större eller mindre betydelse för frågan om avgift ska tas ut och storleken på avgiften.

Enligt *Lagrådets* mening utesluter inte den omständigheten att tillämpningsområdet i olika avseenden skiljer sig åt att förordningens teknik för att bestämma vad som ska påverka avgiftsuttaget kan användas också i ramlagen. En sådan samordning skulle enligt Lagrådet göra sanktionssystemet mer överblickbart för berörda myndigheter och underlätta tillämpningen för tillsynsmyndigheten och domstolarna. Lagrådet, som inte tillstyrker avgiftsmodellen som föreslås i lagrådsremissen, anser att möjligheten att så långt det går samordna sättet att ta ut sanktionsavgifter bör undersökas. Detta kan enligt Lagrådet innebära att de föreslagna bestämmelserna om hur avgiften ska bestämmas i det enskilda fallet ersätts med en bestämmelse om att vederbörlig hänsyn ska tas till de omständigheter som anges i artikel 83.2 a–k i dataskyddsförordningen vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas.

Regeringen instämmer med Lagrådet i att det är av största vikt att sanktionssystemet blir överblickbart för berörda myndigheter och att förutsättningarna för att tillämpa systemet ska vara klara. Dataskyddsförordningen har också varit den viktigaste utgångspunkten för regeringen när det gäller bestämmelser om hur avgifterna ska bestämmas i det enskilda fallet i ramlagen. De omständigheter som enligt förslaget i lagrådsremissen ska beaktas vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas förekommer i uppräkningen i artikel 83.2 i EU:s dataskyddsförordning. Även om dessa omständigheter bedöms som särskilt viktiga är dock i princip samtliga omständigheter i artikel 83.2 relevanta och avsikten är inte att uppräkningen i förslaget ska vara uttömmande. Artikel 83.2 i dataskyddsförordningen innehåller emellertid även omständigheter som inte är relevanta på direktivets område. Regeringen anser därför att en uttrycklig hänvisning till förordningen inte bör göras. Dessutom kommer de myndigheter som ska tillämpa ramlagen och tillsynsmyndigheten vid sin tillsyn att behöva förhålla sig till olika regelverk som skiljer sig åt i vissa avseenden. De olika sanktionsavgiftsregleringarna i sig bör dock enligt regeringens bedömning inte leda till tillämpningsproblem. Förslaget i denna del har heller inte ifrågasatts eller kritiserats av någon av remissinstanserna. Mot denna bakgrund anser regeringen att den ordning som föreslås i lagrådsremissen bör behållas.

Både vid bedömningen av om avgift överhuvudtaget bör tas ut och vid bestämmandet av avgiftens storlek bör för det första särskild hänsyn tas till om överträdelsen varit avsiktlig. En avsiktlig överträdelse visar tydligt på nonchalans mot regleringen och utrymmet att underlåta att ta ut avgift eller att bestämma avgiften till ett lågt belopp bör vara mycket litet. Tvärtom talar avsiktliga överträdelser starkt för att sanktionsavgift ska tas ut och att den ska sättas högt. I många fall är dock överträdelser resultatet av mer eller mindre oaktsamma förfaranden, t.ex. missförstånd om hur regleringen ska tillämpas eller ursäktliga bedömningsfel. Även graden av oaktsamhet bör därför vägas in.

För det andra bör beaktas vilken skada, fara eller kränkning som överträdelsen medfört. Ju större skadan, faran eller kränkningen är, desto mindre blir utrymmet att avstå från att ta ut avgift eller att bestämma avgiften till ett lågt belopp.

För det tredje bör överträdelsens karaktär, svårhetsgrad och varaktighet beaktas. Här spelar det roll vilken typ av personuppgifter som har behandlats, hur många uppgifter som har behandlats, för vilka syften och hur länge uppgifterna har behandlats. Om känsliga personuppgifter eller andra särskilt integritetskänsliga uppgifter har behandlats felaktigt, bör utrymmet för att avstå från att ta ut sanktionsavgift vara mindre och beloppet generellt sett sättas högre. Ju allvarligare överträdelsen är och ju längre den pågått, ju fler registrerade som berörs och ju större skada de registrerade drabbats av, desto starkare skäl talar både för att sanktionsavgift ska tas ut och för att beloppet ska sättas högt. Att en överträdelse vid en samlad bedömning anses vara ringa talar för att någon sanktionsavgift inte bör tas ut eller att den i vart fall bör sättas lågt.

För det fjärde bör hänsyn tas till vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen. Om de har vidtagit kraftfulla åtgärder för att lindra verkningarna bör det, som utredningen påpekar, öka möjligheten att avstå från att ta ut sanktionsavgift eller i vart fall leda till att sanktionsavgiften blir lägre än den annars skulle ha blivit. Även tekniska och organisatoriska åtgärder som vidtagits i syfte att undvika överträdelser bör beaktas. Ju fler och effektivare åtgärder som vidtagits, desto mindre klandervärt framstår de ansvarigas agerande. Hur överträdelsen kom till tillsynsmyndighetens kännedom bör också kunna beaktas. Om den personuppgiftsansvarige eller personuppgiftsbiträdet själv anmält överträdelsen eller tvärtom försökt att dölja den, bör det – som utredningen konstaterar – kunna beaktas i mildrande respektive försvårande riktning.

En femte viktig faktor är om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare gjort sig skyldig till överträdelser. Regeringen delar utredningens bedömning att det är särskilt graverande om den personuppgiftsansvarige eller personuppgiftsbiträdet trots påpekanden fortsatt att handla i strid med regleringen. Om den personuppgiftsansvarige eller personuppgiftsbiträdet däremot samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelser och minska negativa effekter av dem talar det i mildrande riktning.

Sanktionsavgiften bör kunna sättas ned helt eller delvis

Som tidigare konstaterats bör den personuppgiftsansvarige och personuppgiftsbiträden ha strikt ansvar för överträdelser (se avsnitt 12.5.3). Det är därför nödvändigt att ge utrymme för att jämka eller helt sätta ned sanktionsavgiften i fall där det inte framstår som rimligt och proportionerligt att ta ut avgift.

Sanktionsavgiften bör kunna sättas ned helt eller delvis om exempelvis en personuppgiftsansvarig eller ett personuppgiftsbiträde också blir skadeståndsskyldig. Den samlade reaktionen skulle, beroende på överträdelsen, totalt sett kunna bli alltför betungande. Det bör då vara möjligt att jämka beloppet för att undvika att den samlade reaktionen på överträdelsen blir oproportionerlig. Eftersom ansvaret för överträdelser är strikt, bör det också vara möjligt att jämka sanktionsavgiften om det framkommer omständigheter som gör att överträdelsen är ursäktlig. Om regelverket överträtts på ett sådant sätt att det varit närmast omöjligt för den personuppgiftsansvarige att upptäcka överträdelsen, t.ex. om någon anställd

i hemlighet manipulerat ett datasystem, skulle det t.ex. kunna finnas grund för jämkning.

Möjligheten att helt sätta ned avgiften bör tillämpas restriktivt och användas endast i undantagsfall. Det bör enbart aktualiseras om det skulle te sig oskäligt att ta ut sanktionsavgift.

12.7 Beslut om sanktionsavgift

12.7.1 Vem ska besluta om sanktionsavgift?

Regeringens förslag: Tillsynsmyndigheten ska besluta om sanktionsavgift.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* tillstyrker förslaget. *Polismyndigheten* anser att tillsynsmyndigheten ska ansöka hos domstol om att sanktionsavgift ska tas ut.

Skälen för regeringens förslag: Beslut om sanktionsavgift fattas normalt av en tillsynsmyndighet eller en domstol. Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En domstol brukar anses mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva framför allt subjektiva rekvisit eller andra svårbedömda rekvisit.

Polismyndigheten menar att de bedömningar och avvägningar som måste göras vid beslut om sanktionsavgift ska tas ut av en myndighet typiskt sett är av det slag att ärendet bör avgöras av domstol. Regeringen håller med utredningen om att kraven på effektivitet och rättssäkerhet naturligtvis måste balanseras mot varandra vid utformningen av ett system med sanktionsavgifter. Det innebär dock inte med nödvändighet att beslut i fråga om sanktionsavgift måste fattas av domstol.

Enligt artikel 83.1 i dataskyddsförordningen ska tillsynsmyndigheten besluta om sanktionsavgift. *Datainspektionen* hänvisar till den artikeln och förespråkar att det bör vara samma ordning på direktivets område. Av artikel 83.7 i förordningen framgår att medlemsstaterna får avgöra om och i vilken utsträckning sanktionsavgift ska kunna tas ut av offentliga myndigheter. I artikel 83.9 i förordningen anges att en medlemsstat får föreskriva att domstol i stället för en tillsynsmyndighet får besluta om sanktionsavgift om ett nationellt sanktionsavgiftssystem saknas. Enligt skäl 151 verkar den artikeln ta sikte på två särskilt utpekade medlemsstater vilkas rättssystem inte tillåter den ordning förordningen föreskriver.

I prop. 2017/18:105 Ny dataskyddslag föreslås att tillsynsmyndigheten ska besluta om sanktionsavgifter på dataskyddsförordningens område även för statliga och kommunala myndigheter (a. prop. s. 139). Som anges i avsnitt 12.3 har regeringen som utgångspunkt att sanktionssystemen i ramlagen och förordningen så långt möjligt ska stämma överens. Mot den bakgrunden bör, i likhet med vad *Datainspektionen* förespråkar, tillsynsmyndigheten besluta om sanktionsavgift även enligt ramlagen.

En särskild fråga är vem hos tillsynsmyndigheten som bör pröva frågor om sanktionsavgift. Det finns enligt regeringen starka skäl – inte minst från rättssäkerhetssynpunkt – som talar mot att samma person som utrett en eventuell överträdelse får besluta om sanktionsavgift. Det är viktigt att verksamheten organiseras så att förtroendet för tillsynsmyndigheten inte riskerar att rubbas. Med tanke på sanktionsbeslutens betydelse bör det enligt regeringens mening ställas höga krav på den som får besluta om sanktionsavgift. Det kan därför vara lämpligt att sådana beslut bara får fattas av ett fåtal personer.

Tillsynsmyndighetens beslut om sanktionsavgift bör få överklagas till allmän förvaltningsdomstol (se avsnitt 13.7.1). På så sätt tillgodoses rättssäkerhetsaspekterna för den som åläggs sanktionsavgift. På sikt kommer det att kunna bildas domstolspraxis till vägledning för tillsynsmyndighetens beslut.

12.7.2 Förfarandet vid beslut om sanktionsavgift

Regeringens förslag: En sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

Regeringens bedömning: Det behövs ingen särskild regel om att den som en sanktionsavgift ska tas ut av ska få yttra sig innan tillsynsmyndigheten beslutar i fråga om sanktionsavgift.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: *Justitiekanslern* påpekar att en femårig preskriptionstid kan hindra möjligheten att sätta ned sanktionsavgiften. I övrigt yttrar sig ingen remissinstans särskilt över förslaget i denna del.

Skälen för regeringens förslag och bedömning: Enligt artikel 57 ska medlemsstaterna vidta de åtgärder som krävs för att säkerställa att de sanktioner som införs också genomförs. Det finns inga generella förfaranderegler för handläggningen av ärenden om sanktionsavgift. Det krävs därför särskilda förfaranderegler i ramlagen.

Innan tillsynsmyndigheten beslutar om sanktionsavgift bör den som sanktionsavgiften ska tas ut av ges tillfälle att yttra sig. Det ger den personuppgiftsansvarige eller personuppgiftsbiträdet möjlighet att anföra omständigheter som kan påverka både frågan om sanktionsavgift ska tas ut och frågan om sanktionsavgiftens storlek. Möjligheten att komma till tals innan beslut fattas är en förutsättning för materiellt riktiga avgöranden och är en viktig rättssäkerhetsfråga. Av avsnitt 11.8.2 framgår att tillsynsmyndigheten ska kommunicera underlaget inför beslut som riktar sig mot personuppgiftsansvariga och personuppgiftsbiträden. Det gäller även beslut om sanktionsavgift. Någon särskild regel om kommunikation i ärenden om sanktionsavgift behövs därför inte.

Trots att beslut om sanktionsavgift sannolikt i huvudsak kommer att riktas mot myndigheter bör, som utredningen föreslår, besluten delges, eftersom utgångspunkten är att avgiften ska betalas kort tid efter beslutet och rättssäkerhetsskäl talar för en sådan ordning. I lagrådsremissen gjor-

des bedömningen att det kan regleras i förordning. *Lagrådet* förordar emellertid att en sådan bestämmelse tas in i ramlagen. Det kan konstateras att en motsvarande bestämmelse finns i den föreslagna dataskyddslagen (prop. 2017/18:105 s. 12). Att ett beslut om sanktionsavgift ska delges bör därför även enligt regeringens mening framgå av ramlagen.

Det bör finnas en bortre gräns för när en sanktionsavgift får beslutas. En regel som anger när avgift senast får beslutas, som blir en form av preskriptionsregel, bör därför tas in i ramlagen. Förfarandet är avsett att leda till snabbt beivrande av överträdelser, vilket talar för att tiden bör sättas kort. Samtidigt kan vissa överträdelser vara både svårupptäckta och ta tid att utreda. Möjligheten att besluta om sanktionsavgift får därför inte vara för begränsad om systemet ska bli effektivt och avskräckande. Med hänsyn till överträdelsernas karaktär har utredningen ansett att en tid motsvarande den preskriptionstid som gäller för brott där det svåraste straffet är mer än ett års fängelse, men inte överstiger fängelse i två år, är rimlig. Preskriptionstiden skulle därmed bli fem år. Som *Justitiekanslern* påpekar innebär en femårig preskriptionstid att det finns en risk för att ett eventuellt skadeståndsärende angående samma överträdelse skulle avgöras senare än sanktionsavgiftsfrågan eftersom preskriptionstiden för skadestånd är tio år. Detta skulle i praktiken kunna hindra en nedsättning av sanktionsavgiftsbeloppet i vissa fall (jfr. avsnitt 12.6.2). Regeringen anser trots detta att utredningens förslag är väl avvägt och kan i likhet med utredningen konstatera att en femårig preskriptionstid motsvarar vad som i dag gäller för grova brott mot 49 § personuppgiftslagen. Mot denna bakgrund anser regeringen, i likhet med utredningen, att preskriptionstiden bör vara fem år.

12.7.3 Betalning och verkställighet

Regeringens förslag: Sanktionsavgifterna ska tillfalla staten. En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom denna tid ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Regeringen ska kunna meddela ytterligare föreskrifter om sanktionsavgifter enligt ramlagen.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag. Utredningen föreslår inte något bemyndigande för regeringen att meddela ytterligare föreskrifter. Vidare föreslår utredningen att betalning och indrivning ska regleras på förordningsnivå.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget i denna del.

Skälen för regeringens förslag: Tillsynsmyndighetens beslut om sanktionsavgift bör gälla som en dom och vara verkställbar. En sådan ordning är rimlig med tanke på att de personuppgiftsansvariga i de flesta fall är myndigheter. Genom den lösningen blir också sanktionsavgiftssystemet effektivare.

Sanktionsavgiften bör som brukligt tillfalla staten, vilket bör framgå av ramlagen. Utredningen anser att regeringen bör bestämma till vilken myndighet betalningen ska göras. Regeringen gör ingen annan bedömning.

Betalning bör normalt göras inom 30 dagar från det att beslutet fick laga kraft. Det bör dock finnas möjlighet för tillsynsmyndigheten att i det enskilda fallet bestämma en längre betalningsfrist. Det kan t.ex. bli aktuellt vid mycket höga belopp. Om en individuellt bestämd betalningsfrist inte kopplas till när beslutet får laga kraft kan betalningsskyldighet således inträda trots att beslutet har överklagats. Ett beslut om sanktionsavgift bör få lämnas till indrivning efter sista betalningsdagen. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning tillämpas utsökningsbalken. Utredningen har föreslagit att en bestämmelse om betalning och indrivning ska tas in i förordning. Enligt regeringens mening bör bestämmelsen tas in i ramlagen.

Utredningen bedömer att föreskrifter om bl.a. verkställighet och återbetalning av sanktionsavgifter kan meddelas av regeringen eller den myndighet regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen. Regeringen anser dock att det sannolikt kommer att behövas föreskrifter om sanktionsavgifter som går utöver vad som omfattas av denna normgivningskompetens. Det behövs därför ett bemyndigande i ramlagen som anger att regeringen får meddela ytterligare föreskrifter om sanktionsavgifter.

12.7.4 Överklagande

Regeringens bedömning: Det behövs ingen särskild regel om överklagande av beslut om sanktionsavgift.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Ett beslut om att ta ut sanktionsavgift bör kunna prövas av domstol. Den som har ålagts sanktionsavgift bör ha rätt att överklaga beslutet. Eftersom det är fråga om ett förvaltningsbeslut bör beslutet överklagas till allmän förvaltningsdomstol.

Någon särskild överklaganderegel behövs inte, eftersom tillsynsmyndighetens beslut får överklagas enligt den regel om överklagande som föreslås i avsnitt 13.7.1.

12.8 Sanktionsavgift och Europakonventionen

12.8.1 Konventionens krav på rättssäkerhetsgarantier

Regeringens bedömning: Systemet med sanktionsavgift uppfyller Europakonventionens krav på rättssäkerhetsgarantier.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Sanktionsavgift är en straffliknande ekonomisk sanktion med ett avskräckande och bestraffande syfte. Det har därför i doktrinen framförts åsikter om att sanktionsavgifter normalt ska presumeras utgöra brottsanklagelser i Europakonventionens mening. Om den föreslagna sanktionsavgiften skulle anses ha den karaktären medför det att de rättssäkerhetsgarantier som ställs upp i artikel 6 i konventionen måste vara uppfyllda (se Warling-Nerep s. 153 f. och SOU 2013:38 s. 455).

Den som avgiften ska tas ut av ska underrättas om överträdelsen och ges rätt att yttra sig innan beslut om sanktionsavgift fattas. Beslutsmyndigheten har bevisbördan för att det är fråga om en överträdelse och att den bör föranleda sanktionsavgift. Ansvaret är visserligen strikt, men det finns möjlighet att avstå från att ta ut sanktionsavgift eller att jämka den. Den som åläggs sanktionsavgift har rätt till domstolsprövning och rätt att överklaga domstolens beslut. Den föreslagna regleringen uppfyller därför, som utredningen konstaterar, konventionens krav på rättssäkerhetsgarantier.

12.8.2 Konventionens förbud mot dubbelprövning

Regeringens bedömning: Det behövs ingen bestämmelse i ramlagen om förbud mot dubbelprövning.

Utredningens bedömning överensstämmer med regeringens

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Bestämmelser om att ingen ska kunna lagföras eller straffas två gånger för samma brott finns dels i sjunde tilläggsprotokollet till Europakonventionen, dels i rättighetsstadgan.

Enligt artikel 4.1 i sjunde tilläggsprotokollet får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan blivit slutligt frikänd eller dömd (förbud mot dubbelprövning). Dubbelprövningsförbudet är begränsat till samma rättssubjekt. Huvudsyftet med artikeln är att förhindra en upprepning av en brottmålsrättegång som avslutats med ett slutligt avgörande och att förhindra att samma rättssubjekt prövas för samma brott två gånger. Det är följaktligen inte förbjudet att döma ut flera straff för samma brott, utan endast att pröva samma brott på nytt, dvs. vid två olika tillfällen. Konventionen gäller som lag i Sverige och enligt 2 kap. 19 § regeringsformen får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden enligt konventionen.

I artikel 50 i rättighetsstadgan föreskrivs att ingen får lagföras eller straffas på nytt för en lagöverträdelse för vilken han eller hon redan har blivit frikänd eller dömd i unionen genom en lagakraftvunnen brottmålsdom. Enligt artikel 52.3 har artikel 50 samma innebörd som sin motsvarighet i Europakonventionen.

Sanktionsavgift får enbart tas ut av personuppgiftsansvariga och personuppgiftsbiträden, som i princip alltid är juridiska personer. Ställföreträdare och faktiska företrädare för de juridiska personerna eller deras anställda kan däremot aldrig bli föremål för sanktionsavgift enligt lagen.

Rekvisiten för de överträdelser av bestämmelser som kan föranleda sanktionsavgift i ramlagen och rekvisiten för straffansvar enligt brottsbalken är olika och bestämmelserna kommer därmed i praktiken mycket sällan att kunna träffa samma handlande. Vidare krävs att den som avgiften ska tas ut av också är den som är straffrättsligt ansvarig (se avsnitt 12.2.1). Eftersom juridiska personer inte kan straffas enligt svensk rätt är det enbart när en fysisk person är behörig myndighet enligt ramlagen eller personuppgiftsbiträde som förbudet mot dubbelprövning kan aktualiseras. Enda gången som det skulle kunna komma i fråga att ta ut sanktionsavgift av en fysisk person är om han eller hon är enskild näringsidkare. Det rör sig förmodligen om enstaka fall. Därmed kommer förbudet mycket sällan, om ens någonsin, att behöva tillämpas. Om det mot förmodan skulle bli fallet gäller Europakonventionen som svensk lag. Det innebär att en domstol alltid måste ta hänsyn till förbudet. Mot den bakgrunden delar regeringen utredningens bedömning att det inte behövs någon bestämmelse om förbud mot dubbelprövning i ramlagen.

13 Skadestånd och överklagande

13.1 Krav på effektiva rättsmedel vid felaktig personuppgiftsbehandling

Direktivet innehåller flera artiklar om rättsmedel, där den gemensamma nämnaren är att rättsmedlen ska vara effektiva. Den som på rimliga grunder påstår sig ha blivit utsatt för en kränkning av sina rättigheter ska ha möjlighet att få sitt påstående prövat och kunna få rättelse eller gottgörelse för konstaterade kränkningar. Rättsmedlet ska också vara effektivt i den meningen att det ska medge en tillfredsställande prövning. Det måste även vara praktiskt möjligt för berörda personer att utnyttja rättsmedlen. Även om ett visst rättsmedel sett för sig inte uppfyller kraven för att vara effektivt kan flera rättsmedel tillsammans göra det (Hans Danelius, Mänskliga rättigheter i europeisk praxis, 5 uppl. 2015, s. 539).

Enligt artikel 54 ska en registrerad ha rätt till ett effektivt rättsmedel, om han eller hon anser att hans eller hennes rättigheter har kränkts genom att personuppgifter har behandlats på ett sätt som inte är förenligt med de bestämmelser som genomför direktivet. Var och en som lidit skada till följd av behandling av personuppgifter i strid med bestämmelserna ska enligt artikel 56 kunna få ersättning. En registrerad som anser att behandlingen av hans eller hennes personuppgifter står i strid med de bestämmelser som genomför direktivet ska enligt artikel 52.1 också ha rätt att lämna in klagomål till en tillsynsmyndighet. Om tillsynsmyndigheten inte handlägger klagomålet inom viss tid har den registrerade enligt artikel 53.2 rätt till prövning i domstol av om myndigheten onödigt dragit ut på handläggningen av ärendet. Den som berörs av ett rättsligt beslut, meddelat av tillsynsmyndigheten, ska enligt artikel 53.1 kunna överklaga det till domstol.

Flertalet av rättsmedlen i direktivet gäller i förhållande till personuppgiftsansvariga och i vissa fall personuppgiftsbiträden. Så är fallet med be-

stämmelserna om rättsmedel i artikel 52.1 (rätten att ge in klagomål till tillsynsmyndigheten), artikel 54 (rätten att föra talan) och artikel 56 (rätten till skadestånd). Artiklarna 53.1 och 53.2 gäller däremot i förhållande till tillsynsmyndigheten.

De flesta av rättsmedlen är främst eller uteslutande tänkta att användas av registrerade. Det gäller framför allt de rättsmedel som riktar sig mot personuppgiftsansvariga och personuppgiftsbiträden. Rätten till skadestånd gäller dock för den som lidit skada till följd av en olaglig behandling av personuppgifter eller någon annan åtgärd som står i strid med de bestämmelser som genomför direktivet, även om det främst är registrerade som kan drabbas av sådan skada.

Talan mot tillsynsmyndighetens beslut är i första hand tänkt att kunna användas av personuppgiftsansvariga och personuppgiftsbiträden, eftersom det i huvudsak är de som träffas av bindande beslut. Även andra, exempelvis registrerade, ska dock kunna utnyttja rättsmedlet om besluten avser dem, eftersom ett rättsmedel ska vara tillgängligt för varje fysisk och juridisk person som ett rättsligt bindande beslut av tillsynsmyndigheten avser. Registrerade ska också ha rätt till ett effektivt rättsmedel om tillsynsmyndigheten inte i tid behandlar ett klagomål.

Rätten att använda ett visst rättsmedel får enligt direktivet inte påverka rätten att använda ett annat av rättsmedlen. Det innebär att en registrerad t.ex. kan välja att både ge in ett klagomål till tillsynsmyndigheten och begära skadestånd av den personuppgiftsansvarige avseende samma personuppgiftsbehandling.

Förutom de rättsmedel som anges i direktivet finns i svensk rätt dessutom möjlighet att enligt 52 § personuppgiftslagen överklaga vissa beslut som en myndighet fattat i egenskap av personuppgiftsansvarig.

13.2 Talerätt för registrerade

Regeringens bedömning: Rätten att vid allmän domstol föra talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde om en registrerads rättigheter har kränkts genom personuppgiftsbehandling kräver inga lagstiftningsåtgärder.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt i denna del.

Skälen för regeringens bedömning: Enligt artikel 54 ska en registrerad ha rätt till ett effektivt rättsmedel, om han eller hon anser att hans eller hennes rättigheter har kränkts genom att personuppgifter har behandlats på ett sätt som inte är förenligt med de bestämmelser som genomför direktivet. Av rubriken till artikeln – rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde – framgår att det är mot deras agerande som det ska finnas ett rättsmedel. Av skäl 85 framgår att det är ett rättsmedel enligt artikel 47 i rättighetsstadgan som avses. Det innebär att den registrerade ska ha rätt att föra talan vid domstol.

Enligt artikel 22 i 1995 års dataskyddsdirektiv har var och en rätt att föra talan inför domstol vid kränkningar till följd av behandling av personuppgifter. I skäl 55 förtydligas att det som avses är en möjlighet till

rättslig prövning när en personuppgiftsansvarig inte respekterar en registrerads rättigheter. Artikel 22 ledde inte till någon lagstiftning när personuppgiftslagen infördes. Frågan behandlas inte heller i förarbetena förutom i relation till 28 § personuppgiftslagen, som reglerar rätten för en registrerad att begära att en personuppgift rättas. Av förarbetena framgår att om oenighet uppstår mellan den personuppgiftsansvarige och den registrerade om huruvida korrigering ska göras, kan den registrerade vända sig till tillsynsmyndigheten. Där konstateras också att det finns en möjlighet för den registrerade att själv väcka talan vid allmän domstol (prop. 1997/98:44 s. 133 f.). Rätten att väcka talan vid allmän domstol i den ordning som gäller för tvistemål ansågs uppfylla kraven i 1995 års dataskyddsdirektiv (jfr. SOU 2015:39 s. 656).

Artikel 54 i det nya direktivet har enligt utredningens bedömning i sak samma innebörd. Regeringen delar denna bedömning. Artikeln innebär en rätt att föra talan vid domstol för den som anser att hans eller hennes rättigheter har kränkts vid behandlingen av personuppgifter. Regeringen gör ingen annan bedömning nu än den som gjordes beträffande artikel 22 i 1995 års dataskyddsdirektiv. Det krävs därmed inte någon lagstiftningsåtgärd för att genomföra artikel 54. Den möjlighet enskilda har att väcka talan vid allmän domstol i den ordning som gäller för tvistemål får anses vara tillräcklig.

Talan kan föras mot en personuppgiftsansvarig. Det finns skäl att i detta sammanhang påpeka att ett personuppgiftsbiträde som själv fastställt ändamålen med eller medlen för behandling ska betraktas som personuppgiftsansvarig för den behandlingen (se avsnitt 9.6.3).

Direktivet förutsätter att talan även ska kunna föras mot personuppgiftsbiträden. Eftersom personuppgiftsbiträden inte, utom i det fall som nyss nämnts, självständigt behandlar personuppgifter kommer troligen talan mycket sällan att väckas mot personuppgiftsbiträden.

13.3 Skadestånd

13.3.1 Det allmännas skadeståndsansvar

Enligt 3 kap. 2 § skadeståndslagen (1972:207) ska staten eller en kommun ersätta personskada, sakskada eller ren förmögenhetsskada som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommunen svarar. Ersättningsskyldigheten omfattar även ideell skada på grund av att någon genom fel eller försummelse vid myndighetsutövning kränkts på det sätt som anges i 2 kap. 3 § samma lag.

I 2 kap. 3 § skadeståndslagen föreskrivs att den som allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära ska ersätta den skada som kränkningen innebär. Ideellt skadestånd för att den personliga integriteten har kränkts, dvs. en skada av icke-ekonomisk natur, förutsätter alltså att kränkningen har orsakats genom brott. Det krävs också att kränkningen är allvarlig.

Ersättning för kränkning med stöd av 3 kap. 2 § jämförd med 2 kap. 3 § skadeståndslagen förutsätter att kränkningen har orsakats vid myndighetsutövning. Om det inte är fråga om myndighetsutövning kan ska-

stånd ändå utgå enligt 3 kap. 1 § skadeståndslagen för skada som vållats av arbetstagare. Det förutsätter att kränkningen har orsakats av att den anställde har begått brott i tjänsteutövningen.

Genom Högsta domstolens praxis har det lagts fast en rätt till ideellt skadestånd vid kränkningar av Europakonventionen även i andra fall än de som regleras i skadeståndslagen. Det har bl.a. varit fråga om kränkningar av rätten till privat- och familjeliv enligt artikel 8 i konventionen. En ny bestämmelse i skadeståndslagen om rätten till skadestånd vid överträdelser enligt Europakonventionen träder dessutom i kraft den 1 april 2018 (prop. 2017/18:7, Skadestånd och Europakonventionen).

Den som anser att han eller hon har orsakats skada av det allmänna kan väcka talan mot staten eller en kommun vid allmän domstol. Saken prövas då som tvistemål.

Enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten kan en skadelidande dessutom få ett skadeståndskrav mot staten prövat inom ramen för statens frivilliga skadereglering. Med det avses skadereglering som företrädelsevis sker hos Justitiekanslern, men som även i viss omfattning kan förekomma hos andra myndigheter. Enligt förordningen kan den enskilde i ett formlöst och kostnadsfritt förfarande vända sig direkt till en myndighet och få ett besked i frågan om huruvida staten är skadeståndsskyldig. Det är ett särskilt snabbt och effektivt sätt att komma i åtnjutande av det rättsmedel som rätten till skadestånd innebär. Vid ett negativt besked har den enskilde kvar möjligheten att vända sig till domstol för att få saken prövad. Justitiekanslerns inställning är inte bindande för domstolarna eller för den enskilde. Enligt förordningen kan Justitiekanslern bl.a. handlägga anspråk som grundas på 3 kap. 1 eller 2 § skadeståndslagen eller skadeståndsregler i vissa särskilt angivna författningar, t.ex. 48 § personuppgiftslagen (se avsnitt 13.3.2).

På det kommunala området finns det ingen motsvarande frivillig skadereglering. En kommun eller ett landsting är emellertid oförhindrad att frivilligt reglera en skada som någon orsakats i kommunens eller landstingets verksamhet, exempelvis i samband med otillåten behandling av personuppgifter. Om den enskilde inte är nöjd, får den enskilde vända sig till allmän domstol. Även socialnämnder och landsting kan ha uppgifter som omfattas av ramlagens tillämpningsområde, exempelvis verkställighet av påföljder som innebär vård.

13.3.2 Skadeståndsskyldighet för personuppgiftsansvariga

Regeringens förslag: Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med ramlagen eller föreskrifter som meddelats i anslutning till den.

Regeringens bedömning: Det bör inte införas någon jämkningsregel i ramlagen.

Utredningens förslag och bedömning överensstämmer i sak med regeringens.

Remissinstanserna: *Justitiekanslern* påpekar att det finns ett behov av en ändring i förordningen om handläggning av skadeståndsanspråk mot staten om myndigheten ska pröva anspråk enligt ramlagen. Vidare ifrågasätter Justitiekanslern om det nya dataskyddsdirektivet utesluter möjligheten till jämkning av skadestånd, t.ex. när den skadelidande underlåtit att begränsa sin egen skada. *Sveriges advokatsamfund* och *Dataskydd.net* ifrågasätter om möjligheten att driva skadeståndstalan utgör ett sådant effektivt rättsmedel som är avsikten enligt direktivet.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet och nuvarande reglering

Enligt artikel 56 ska var och en som lidit materiell eller immateriell skada till följd av olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de bestämmelser som genomför direktivet ha rätt till ersättning från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Enligt 48 § första stycket personuppgiftslagen ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med lagen har orsakat. Alla åtgärder som är oförenliga med personuppgiftslagen kan leda till skadeståndsskyldighet, om de allmänna kraven för skadestånd är uppfyllda. Ersättningsskyldighet inträder så snart en bestämmelse överträtts, vilket gör att skadeståndsansvaret är strikt.

I registerförfattningarna för myndigheterna i rättskedjan hänvisas till 48 § personuppgiftslagen. Myndigheternas skadeståndsansvar omfattar därmed överträdelser som begås både mot reglerna i registerförfattningen och mot de regler i personuppgiftslagen som gäller för myndigheten.

Regleringen i det nya direktivet motsvarar artikel 19 i dataskyddsrambeslutet. Varken i artikel 56 i direktivet eller i artikel 19 i dataskyddsrambeslutet finns det någon exculperingsregel. Med det avses en bestämmelse som gör att den personuppgiftsansvarige under vissa förhållanden kan undgå skadeståndsansvar trots att behandlingen av personuppgifter varit felaktig. En sådan regel finns däremot i 48 § andra stycket personuppgiftslagen (se även artikel 23.2 i 1995 års dataskyddsdirektiv).

Justitiekanslerns skadereglering i personuppgiftsärenden

Justitiekanslern handlägger inom ramen för statens frivilliga skadereglering skadeståndsanspråk enligt 48 § personuppgiftslagen. Under åren 2011–2013 kom det in 196 sådana ärenden. Under samma period avgjorde Justitiekanslern 225 ärenden varav ersättning utgick i 131 fall, dvs. i ungefär 60 procent av ärendena. Det kan jämföras med att det i ärenden om skadeståndsanspråk mot staten som grundas på skadeståndslagen normalt utgår ersättning i 12–13 procent av fallen. Exempel på överträdelser av personuppgiftslagen som enligt Justitiekanslerns beslut medfört ersättningsskyldighet är bristande gallringsrutiner, felaktiga personuppgifter i olika register och felaktiga uppgifter på domstolars upp-

ropslistor. I betänkandet Myndighetsdatalag redovisas en genomgång av Justitiekanslerns praxis (SOU 2015:39 s. 643 f.).

När det gäller Justitiekanslerns synpunkt om ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten för att myndigheten ska kunna pröva anspråk enligt ramlagen kommer denna tas om hand i samband med framtagandet av förordningsändringar.

Vem ska vara skadeståndsskyldig?

Direktivet förutsätter att enskilda ska kunna begära skadestånd vid behandling av personuppgifter i strid med de bestämmelser som genomför direktivet. Det behövs därför en bestämmelse i ramlagen om skadeståndsansvar.

Enligt 48 § personuppgiftslagen är det enbart den personuppgiftsansvarige som är skadeståndsskyldig. Gentemot den registrerade är den personuppgiftsansvarige ansvarig för all behandling, dvs. även när ett personuppgiftsbiträde eller annan hjälp anlitas. Om fel har begåtts av t.ex. ett personuppgiftsbiträde anses det alltså bero på den personuppgiftsansvarige.

Enligt dataskyddsförordningen ska det även finnas möjlighet att rikta skadeståndstalan mot personuppgiftsbiträden (artikel 82.1), men i direktivet finns ingen motsvarande bestämmelse. Däremot framgår det av rubriken till artikel 54 att den registrerade ska ha rätt till ett effektivt rättsmedel inte bara mot den personuppgiftsansvarige utan även mot personuppgiftsbiträden, dvs. kunna väcka talan vid allmän domstol mot dessa för att få en domstolsprövning till stånd.

Regeringen anser i likhet med utredningen att det skulle föra för långt att enbart av rubriken till artikel 54 dra slutsatsen att det måste finnas möjlighet för enskilda att föra skadeståndstalan även mot personuppgiftsbiträden. Det finns inte heller något annat som talar för att ålägga personuppgiftsbiträden skadeståndsansvar. Bara den personuppgiftsansvarige bör således vara skadeståndsansvarig enligt ramlagen. För den registrerade tillgodoses rätten till ersättning för skada som ett personuppgiftsbiträde har orsakat genom att den personuppgiftsansvarige är ansvarig även för biträdets handlande.

Det finns dock skäl att erinra om att ett personuppgiftsbiträde ibland är att anse som personuppgiftsansvarig för viss behandling och då givetvis kan bli skadeståndsskyldig i den egenskapen. Enligt artikel 22.5 gäller det om biträdet själv fastställt ändamålen och medlen för behandlingen (se avsnitt 9.6.3).

Regeringen återkommer till frågan om och i så fall i vilken utsträckning skadeståndsskyldighet enligt registerförfattningarna behöver regleras särskilt i samband med att dessa anpassas till dataskyddsdirektivet.

Vad avses med ”varje annan myndighet”?

Enligt artikel 56 ska den som har lidit materiell eller immateriell skada ha rätt till ersättning för skadan från den personuppgiftsansvarige eller från varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt. I skäl 88 förklaras att den som lidit skada bör få ersättning av den personuppgiftsansvarige eller någon annan myndighet som är behörig enligt nationell rätt.

Frågan är vad som avses med varje annan myndighet. Formuleringen skulle enligt utredningen kunna tolkas på tre olika sätt. För det första kan den tolkas som att inte bara den personuppgiftsansvarige kan bli skadeståndsskyldig, utan även någon annan behörig myndighet som bidragit till den felaktiga personuppgiftsbehandlingen. För det andra kan formuleringen avse att det i nationell rätt kan vara en annan myndighet än den personuppgiftsansvarige som är skadeståndsansvarig. För det tredje skulle formuleringen kunna syfta på att den enskilde kan vända sig till en särskild myndighet som hanterar frågor om det allmännas skadeståndsansvar.

Att någon annan myndighet vid sidan av den personuppgiftsansvariga myndigheten skulle kunna bli skadeståndsskyldig anser regeringen i likhet med utredningen inte vara en rimlig tolkning, eftersom det skulle urholka den ansvarsfördelning som direktivet bygger på. Att det däremot i vissa av medlemsstaterna kan finnas regler som gör att särskilt utpekade myndigheter i stället kan vara skadeståndsskyldiga kan inte uteslutas. Någon sådan ordning finns inte i svensk rätt. Om bestämmelsen ska tolkas på det tredje sättet finns det redan en sådan myndighet med det mandat som krävs, nämligen Justitiekanslern.

Regeringen håller med utredningen om att de båda senare tolkningarna är möjliga. Direktivet förutsätter inte att det införs en ordning där en särskild myndighet är skadeståndsansvarig. Det finns inte heller skäl att ändra den ordning som gäller. Det innebär att Justitiekanslern företräder staten när det gäller skadeståndsfrågor i statlig verksamhet. Någon bestämmelse i ramlagen behövs därmed inte för att genomföra artikel 56 i denna del.

Skadeståndets omfattning

Enligt artikel 56 ska både materiell och immateriell skada till följd av olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med regelverket ersättas. Begreppet skada bör enligt skäl 88 tolkas brett baserat på EU-domstolens rättspraxis och på ett sätt som fullt ut återspeglar direktivets mål. Skadeståndsansvaret är enligt direktivet strikt och förutsätter att en registrerad ersätts för all den skada han eller hon lidit till följd av behandling i strid med regelverket. Det finns således ingen möjlighet att ha regler som innebär att viss personuppgiftsbehandling aldrig ska kunna medföra skadeståndsansvar.

Rätten till personlig integritet är en immateriell rättighet. Den personuppgiftsansvarige är därför ersättningsskyldig inte bara för ekonomisk skada utan även för ideell skada. Den enskilde har alltså, förutom rätt till ersättning för personskada, sakskada och ren förmögenhetsskada, rätt till ekonomisk kompensation för kränkningen. Det är bara skada eller kränkning som behandlingen har fört med sig som ska ersättas. Orsakssambandet ska vara adekvat.

Som utredningen konstaterar möter den nuvarande skadeståndsregeln i personuppgiftslagen både kravet på att all skada ska ersättas och att det ska finnas adekvat kausalitet. Bestämmelsen i ramlagen kan därför utformas med den som mönster och bör i huvudsak kunna tolkas i enlighet med den praxis som har utvecklats med anledning av den skadeståndsregeln. Genom en sådan bestämmelse anser regeringen – till skillnad från

Sveriges advokatsamfund och *Dataskydd.net* – att ett effektivt rättsmedel som uppfyller direktivets krav uppnås.

Som tidigare nämnts finns det ingen exculperingsregel i artikel 56. Även om det, som *Justitiekanslern* framhåller, skulle kunna finnas andra grunder för jämkning, innehåller inte direktivet någon regel som motsvarar 48 § andra stycket personuppgiftslagen. Regeringen delar därför utredningens bedömning att det inte är möjligt att ha någon sådan jämkningsregel i ramlagen. Som Justitiekanslern påpekar ger emellertid inte direktivet några besked om vad som gäller beträffande andra grunder för jämkning. Regeringen håller med Justitiekanslern om att det skulle kunna finnas utrymme för att sätta ned skadestånd med stöd av allmänna skadeståndsrättsliga principer om jämkning.

Hur ska ersättningen för kränkning beräknas?

Liksom i dag bör ersättningen för kränkning uppskattas efter skälighet, mot bakgrund av samtliga omständigheter. Det som kan ha betydelse är bl.a. att personuppgifter spridits eller att det funnits risk för otillbörlig spridning av integritetskänsliga eller felaktiga personuppgifter. En annan omständighet kan vara att den registrerade drabbats av beslut eller andra åtgärder som fått eller kunnat få negativa konsekvenser för honom eller henne. Om den registrerade själv har lämnat oriktig eller ofullständig information till den personuppgiftsansvarige, kan även detta ha betydelse vid beräkningen. En jämförelse kan göras med vad som gäller i fråga om betydelsen av den skadelidandes eget agerande när det gäller kränkningsersättning vid brott (prop. 2000/01:68 s. 52).

Förhållandet till skadeståndslagen

Ramlagens bestämmelse kommer i likhet med 48 § personuppgiftslagen att vara en sådan specialbestämmelse om skadestånd som enligt 1 kap. 1 § skadeståndslagen tar över de allmänna reglerna i den lagen. Om en ersättningsfråga inte regleras i ramlagen – t.ex. hur ersättningen för en personskada eller sakskada ska beräknas (5 kap. skadeståndslagen) eller hur ansvaret ska fördelas när flera är skadeståndsskyldiga (6 kap. 4 § skadeståndslagen) – tillämpas de allmänna reglerna i skadeståndslagen.

13.4 Överklagande av personuppgiftsansvariga myndigheters beslut

Regeringens förslag: Om den personuppgiftsansvarige är en myndighet ska beslut som meddelats på begäran av den registrerade angående rättelse, komplettering, radering eller begränsning av behandlingen, kunna överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna sådan information eller att inte medge prövning på nytt av ett automatiserat beslut. Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Sådana beslut som meddelas av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän ska inte kunna överklagas.

Några andra beslut än de som uttryckligen anges i ramlagen ska inte få överklagas.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska beslut att inte på begäran lämna närmare information om automatiserade beslut gå att överklaga.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt direktivet krävs endast att tillsynsmyndighetens beslut ska kunna överklagas (se avsnitt 13.7.1). I övrigt ställs inga krav på att beslut ska kunna överklagas. Inte heller 1995 års direktiv ställer några sådana krav.

Enligt 52 § första stycket personuppgiftslagen får dock även vissa beslut som fattas av en personuppgiftsansvarig som är en myndighet överklagas till allmän förvaltningsdomstol. Det gäller emellertid bara vissa i paragrafen uppräknade beslut, nämligen beslut om information enligt 26 §, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Överklaganderätten gäller inte beslut av riksdagen, regeringen eller Riksdagens ombudsmän.

Skälet till att bestämmelsen infördes var troligtvis att beslut som en myndighet fattar i egenskap av personuppgiftsansvarig ses som ett utflöde av myndighetsutövning och inte som ett ställningstagande av myndigheten i ett civilrättsligt förhållande. En enskild ska därför inte behöva väcka talan vid allmän domstol i den ordning som gäller för tvistemål, utan i stället kunna överklaga besluten till allmän förvaltningsdomstol. De beslut som får överklagas har bedömts vara sådana beslut som får återverkningar för enskilda (jfr SOU 2015:39 s. 663).

Även i de behöriga myndigheternas registerförfattningar finns det bestämmelser om överklagande av sådana beslut, men det varierar hur överklagandebestämmelserna är utformade. I t.ex. 2 kap. 2 § första stycket 13 polisdatalagen (2010:361), 2 kap. 2 § första stycket 13 åklagardatalagen (2015:433) och 2 kap. 2 § första stycket 13 kustbevakningsdatalagen (2012:145) hänvisas till 52 § första stycket personuppgiftslagen. Domstolsdatalagen (2015:728) har däremot egna överklagandebestämmelser som i sak i allt väsentligt motsvarar 52 § första stycket personuppgiftslagen, men har anpassats till följd av instansordningen (20–22 §§). I lagen (2001:617) om behandling av personuppgifter inom kriminalvården finns det också särskilda överklagandebestämmelser (12–16 §§).

Behovet av en överklagandebestämmelse i ramlagen

Det är naturligt att se en myndighets beslut i egenskap av personuppgiftsansvarig, exempelvis i fråga om en personuppgift ska rättas eller inte, som ett utflöde av dess myndighetsutövning. I allmänhet har myndigheten behandlat personuppgifterna i syfte att fullgöra myndighetsuppgifter.

Personuppgifterna har också normalt behandlats med stöd av olika författningsbestämmelser, oberoende av den registrerades samtycke. I likhet med utredningen anser därför regeringen att ramlagen bör innehålla en bestämmelse som motsvarar 52 § första stycket personuppgiftslagen, även om direktivet inte ställer krav på att andra beslut än tillsynsmyndighetens ska kunna överklagas.

Regeringen kommer att behandla frågan om det behövs särskilda överklagandebestämmelser i registerförfattningarna i samband med att dessa anpassas till direktivet.

Vilka beslut ska kunna överklagas?

När det gäller enskildas rätt att överklaga myndighetsbeslut bör, som utredningen konstaterar, samma utgångspunkt gälla som i fråga om rätten att överklaga beslut enligt personuppgiftslagen. Överklaganderätten bör alltså enbart ta sikte på sådana beslut av myndigheten som den fattat i egenskap av personuppgiftsansvarig och som direkt berör den enskilde och som gått honom eller henne emot. Sådana beslut bör på samma sätt som andra förvaltningsbeslut kunna överklagas till allmän förvaltningsdomstol.

Utredningen har med den utgångspunkten övervägt vilka beslut som bör vara överklagbara. Regeringen håller med utredningen om att beslut som fattas på begäran av en registrerad om att personuppgifter ska rättas, kompletteras eller raderas eller att behandlingen av personuppgifter ska begränsas bör kunna överklagas. Det bör gälla oavsett om myndigheten avslår begäran eller vidtar en annan åtgärd än den som begärts. Har myndigheten helt eller delvis underlåtit att lämna information som den enskilde har begärt, bör beslutet kunna överklagas. Även beslut att ta ut avgift för information eller att vägra omprövning av ett automatiserat beslut bör kunna överklagas. Som anges i avsnitt 10.2.9 bör rätten att få närmare information om automatiserade beslut inte gå att begränsa. Det kommer alltså inte att kunna fattas beslut om att begränsa sådan information. Därmed saknas anledning att införa en möjlighet att överklaga sådana beslut.

Enbart vissa beslut som en myndighet i egenskap av personuppgiftsansvarig fattar bör alltså få överklagas. Det bör framgå direkt av ramlagen vilka beslut det är. Uppräkningen motsvarar i allt väsentligt de beslut som i dag får överklagas enligt 52 § personuppgiftslagen.

Överklagandena bör, på samma sätt som i dag, prövas av allmän förvaltningsdomstol. Vid överklagande till kammarrätten bör det, på samma sätt som i dag, krävas prövningstillstånd.

Vad bör inte få överklagas?

Alla beslut som en myndighet fattar i egenskap av personuppgiftsansvarig bör, som tidigare angetts, inte få överklagas. Administrativa beslut av en personuppgiftsansvarig myndighet, t.ex. i fråga om tillgången till personuppgifter, berör inte den enskilde på ett sådant sätt att de bör få överklagas. Det bör av ramlagen framgå att andra beslut än de som räknas upp inte får överklagas.

Rätten att överklaga bör inte heller gälla beslut av myndigheter vilkas beslut normalt inte får överklagas. En uttrycklig bestämmelse om det bör

tas in i ramlagen. Det gäller för beslut av regeringen (jfr regleringen av utlämnande av allmänna handlingar i 6 kap. 7 § offentlighets- och sekretesslagen). För utlämnande av allmänna handlingar gäller samma ordning för Riksdagens ombudsmän som för riksdagen och regeringen (se 4 § andra stycket lagen [1989:186] om överklagande av administrativa beslut av Riksdagsförvaltningen och riksdagens myndigheter). Beslut som fattas av Riksdagens ombudsmän i egenskap av personuppgiftsansvarig myndighet bör därför inte kunna överklagas.

Högsta domstolens och Högsta förvaltningsdomstolens beslut får inte överklagas (jfr 11 kap. 1 § regeringsformen). Därför bör inte heller deras beslut enligt ramlagen få överklagas (jfr prop. 2014/15:148 s. 94).

13.5 Klagomål

Regeringens bedömning: En registrerads rätt att lämna in klagomål till en tillsynsmyndighet om han eller hon anser att hans eller hennes personuppgifter har behandlats felaktigt kräver inga lagstiftningsåtgärder.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

I direktivet finns bestämmelser om hur klagomål över behandling av personuppgifter ska hanteras. Med klagomål avses här missnöje som uttrycks av enskilda och som inte avser begäran om rättelse, omprövning, överklagande eller någon annan formellt reglerad åtgärd.

Enligt artikel 52.1 har alla registrerade som anser att behandling av personuppgifter som avser dem står i strid med de bestämmelser som genomför direktivet rätt att lämna in klagomål till en enda tillsynsmyndighet. Av artikel 46.1 f framgår att det ska ingå i tillsynsmyndighetens uppgifter att behandla klagomål från registrerade. Rätten att ge in klagomål får inte påverka andra administrativa prövningsförfaranden eller rättsmedel och rätten till andra rättsmedel får inte påverka rätten att ge in klagomål.

Artiklarna 46.1 f, 46.2 och 52.2–4 innehåller bestämmelser av processuell karaktär som anger hur tillsynsmyndigheten ska hantera ett klagomål i förhållande till den enskilde. Där regleras bl.a. vilken information som tillsynsmyndigheten ska ge den enskilde om handläggningen och resultatet. Av artikel 53.2 framgår att den registrerade i normalfallet inte ska behöva vänta mer än tre månader på ett besked. Enligt artiklarna 13.1 d och 14 f ska den personuppgiftsansvarige göra information om rätten att lämna in klagomål till tillsynsmyndigheten tillgänglig för den registrerade. Den frågan behandlas i avsnitt 10.2.6 och 10.2.8.

I artikel 28.4 och skäl 63 i 1995 års direktiv finns bestämmelser om klagomålshantering. I korthet innebär de att var och en kan vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter vid personuppgiftsbehandling och att den som framställt en sådan begäran har rätt att få besked om vad den lett till. Indirekt framgår också att tillsynsmyndigheten har till uppgift att hantera klagomål.

I dag finns det inte någon uttrycklig regel om att den som är missnöjd med behandlingen av personuppgifter har rätt att ge in klagomål. Av 6 § förvaltningslagen (2017:900) följer dock att en enskild alltid kan kontakta en myndighet och framföra synpunkter.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen och de behöriga myndigheternas registerförfattningar. Enligt inspektionens praxis kan en enskild ge in klagomål dit. Myndigheten brukar informera den enskilde om vilka åtgärder klagomålet lett till. Om myndigheten anser att det krävs, genomför den tillsyn med anledning av klagomålet. Av avsnitt 11.1.2 framgår att Säkerhets- och integritetsskyddsnämnden också har tillsyn över viss personuppgiftsbehandling.

Regleringen avseende klagomål har två perspektiv

Dataskyddsdirektivet innehåller betydligt fler och mer utförliga bestämmelser om klagomålshantering än 1995 års direktiv. Tidigare fanns bestämmelserna enbart i kapitlet om tillsynsmyndigheten. I det nya direktivet har artiklarna delvis annat innehåll och annan placering. De finns både i det kapitel som rör tillsynsmyndighetens uppgifter och i det kapitel som rör rättsmedel för enskilda. Klagomålshanteringen har därmed fått en tydlig koppling även till registrerades rättigheter.

Artikel 52.1 behandlar främst hanteringen av klagomål från registrerades perspektiv. I artiklarna 46.1 f, 46.2 och 52.2–52.4 regleras klagomålshanteringen huvudsakligen från tillsynsmyndighetens perspektiv. Även om de sistnämnda artiklarna främst riktar sig till tillsynsmyndigheten, genom att de definierar dess uppgifter och anger hur klagomål ska behandlas av myndigheten, får de indirekt betydelse även för registrerade. De ger uttryck för vad registrerade kan förvänta sig av tillsynsmyndigheten och tydliggör därmed innebörden av rätten i artikel 52.1.

Regleringen har alltså, som utredningen konstaterar, två tydliga perspektiv: tillsynsmyndighetens och de registrerades.

Reglernas syfte är att ge den registrerade ett rättsmedel

Att registrerade kan framföra klagomål till en tillsynsmyndighet är ägnat att öka förtroendet för och därmed legitimiteten i den verksamhet som tillsynen avser. Syftet med en klagomålsfunktion är dels att skapa tilltro, dels att säkerställa att det finns en fristående instans som den som anser sig vara utsatt för felaktig behandling kan vända sig till med klagomål. De registrerades behov av att få klagomål utredda står alltså i centrum.

I direktivet är utgångspunkten att ge den som anser sig vara felaktigt behandlad en uttrycklig möjlighet att framföra sitt klagomål och få det hanterat. Möjligheten för den registrerade att ge in klagomål till tillsynsmyndigheten uttrycks som en rättighet. Även om tillsynsmyndigheten väljer att inte genomföra tillsyn med anledning av klagomålet, ska den

alltid ge den registrerade besked om vad klagomålet lett till. Placeringen av artikel 52 i kapitlet som behandlar rättsmedel, ansvar och sanktioner understryker att rätten att ge in klagomål ska ses som ett rättsmedel.

Behövs det en tydligare reglering av rätten att ge in klagomål?

Kraven på tillsynsmyndighetens hantering av klagomål har skärpts i förhållande till vad som gäller i dag. Artikel 52.1 innebär emellertid endast en rätt för den registrerade att vända sig till myndigheten med synpunkter på hur hans eller hennes personuppgifter behandlats. Vad den registrerade kan uppnå genom att ge in ett klagomål skiljer sig från vad han eller hon kan uppnå genom en domstolsprövning och kan inte jämställas med rätten att överklaga ett beslut fattat av tillsynsmyndigheten (se avsnitt 13.7.1).

Regeringen delar mot denna bakgrund utredningens bedömning att artikel 52.1 inte bör ges någon annan innebörd än att en registrerad ska tillförsäkras rätt att framföra eventuella klagomål till en tillsynsmyndighet.

Frågan är då om den mer detaljerade regleringen av klagomål i direktivet innebär att det behövs en uttrycklig bestämmelse i ramlagen som ger en registrerad rätt att ge in klagomål till tillsynsmyndigheten.

Av flera skäl vore det inte lämpligt att ta in en sådan regel i ramlagen. I andra lagstiftningsärenden där motsvarande fråga har behandlats har lagstiftaren valt att reglera rätten att ge in klagomål indirekt genom att i stället reglera tillsynsmyndighetens uppgifter (prop. 2009/10:216 s. 77 f., jfr också SOU 2003:113 s. 122 f.). Inte ens i lagen (1986:765) med instruktion för Riksdagens ombudsmän – vars främsta uppgift är att behandla klagomål från allmänheten – har möjligheten att klaga på myndigheter konstruerats som en rättighet för enskilda. Att uttryckligen föreskriva rätt att ge in klagomål avseende personuppgiftsbehandling skulle alltså avvika från systematiken i den svenska lagstiftningen. En sådan bestämmelse bör därför inte införas.

En annan viktig aspekt är att regleringen inte bör ge enskilda fel förväntningar. Redan i dag finns det tyvärr ofta felaktiga förväntningar på vad klagomål kan leda till och vilka åtgärder en tillsynsmyndighet kan vidta med anledning av klagomål. Enskilda förväntar sig t.ex. många gånger att tillsyn alltid ska utövas när klagomål har getts in eller att tillsynsmyndigheten kan ändra eller på annat sätt påverka ett beslut i sak. Regeringen håller med utredningen om att en reglering av rätten att ge in klagomål skulle kunna skapa felaktiga förväntningar hos enskilda om vad som kan uppnås genom ett klagomål (jfr Skapa tilltro – Generell tillsyn, enskildas klagomål och det allmänna ombudet inom socialförsäkringen, SOU 2015:46, s. 109 f.). Risken för felaktiga förväntningar skulle öka med en särskild regel, eftersom en sådan regel skulle avvika från vad som gäller vid annan klagomålshantering. I förlängningen skulle det kunna leda till att allmänhetens förtroende för verksamheten snarare undergrävs än motsatsen, eftersom de flesta klagomål inte leder till det resultat som klaganden förväntar sig.

Mot den bakgrunden delar regeringen utredningens bedömning att rätten att ge in klagomål endast bör regleras indirekt som en av tillsynsmyndighetens uppgifter (se avsnitt 11.6.1 och 11.6.2).

Vad avses med en enda tillsynsmyndighet?

Enligt artikel 52.1 ska den registrerade ha rätt att lämna in klagomål till en enda tillsynsmyndighet. Det är oklart vad som avses med det. Artikeln skulle kunna förstås som att en registrerad ska ha rätt att lämna in ett klagomål till vilken behörig tillsynsmyndighet som helst i en stat som är bunden av direktivet. En registrerad som bor i Sverige, vars uppgifter behandlas av en personuppgiftsansvarig i Tyskland, skulle vid en sådan tolkning kunna lämna in sitt klagomål till en svensk tillsynsmyndighet. Omvänt skulle någon som bor i Tyskland, vars personuppgifter behandlas av en personuppgiftsansvarig i Sverige, kunna lämna in sitt klagomål i Tyskland.

Det finns exempel på unionsrättsakter där det föreskrivs att enskilda ska kunna vända sig med en begäran till en behörig myndighet i valfri medlemsstat. Myndigheten som tagit emot begäran är sedan skyldig att vidarebefordra den till rätt myndighet, se t.ex. artikel 37.1 Europolförordningen. Eftersom det inte finns någon bestämmelse av motsvarande slag i direktivet anser regeringen, i likhet med utredningen, att hänvisningen till en enda tillsynsmyndighet inte kan ha den innebörden.

Uttrycket bör i stället tolkas så att den registrerade ska kunna vända sig till valfri tillsynsmyndighet med sitt klagomål, om det finns flera sådana myndigheter i en medlemsstat. Frågan aktualiseras därmed bara om en medlemsstat väljer att utse flera tillsynsmyndigheter. I Sverige föreslås enbart Datainspektionen bli tillsynsmyndighet enligt direktivet. Någon lagstiftningsåtgärd krävs därmed inte.

13.6 En effektiv handläggning av klagomål

Regeringens bedömning: Det behövs inga särskilda författningsbestämmelser om tillsynsmyndighetens skyldigheter att handlägga klagomål inom rimlig tid.

Utredningen föreslår till skillnad från regeringen särskilda bestämmelser om en rätt för den registrerade att föra en dröjsmålstalan i allmän förvaltningsdomstol.

Remissinstanserna: *Förvaltningsrätten i Linköping* och *Justitiekanslern* anser att de föreslagna bestämmelserna framstår som komplicerade, tidsödande och kostnadskrävande i förhållande till vad som rimligen går att uppnå. Det bör därför enligt Justitiekanslerns uppfattning övervägas om inte tillgången till ett effektivt rättsmedel kan säkerställas på något annat sätt. *Dataskydd.net* tillstyrker en reglering av en särskild dröjsmålstalan.

Skälen för regeringens bedömning: Enligt artikel 53.2 ska varje registrerad person ha rätt till ett effektivt rättsmedel om tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller informerar den registrerade om handläggningen av klagomålet eller vilket beslut som har fattats med anledning av detta.

Ett uppenbart ogrundat klagomål bör kunna besvaras av tillsynsmyndigheten tämligen omgående, i vart fall inom tre månader. I andra fall kan tillsynsmyndigheten ha anledning att utnyttja sina undersök-

ningsbefogenheter, exempelvis begära in information eller genomföra ett tillsynsbesök. Besked om huruvida sådan tillsyn ska utövas eller inte bör enligt regeringens mening i princip alltid kunna lämnas till den registrerade inom tre månader. I de undantagsfall ett sådant besked inte kan ges bör tillsynsmyndigheten i vart fall kunna lämna besked om hur ärendet fortskrider. Tillsynsmyndighetens informationsplikt gentemot den registrerade är då uppfylld. Artikel 53.2 ger inte den registrerade rätt att inom tidsfristen få ett slutligt besked om vilka eventuella åtgärder gentemot den personuppgiftsansvarige som klagomålet i förlängningen leder till. Bestämmelsen syftar i stället till att stävja passivitet hos tillsynsmyndigheten och säkerställa att den registrerade hålls underrättad om handläggningen av ärendet.

Vid sidan av bestämmelserna om tillsynsmyndighetens skyldigheter att bl.a. handlägga klagomål gäller skyndsamhetskrav och informationsskyldighet enligt förvaltningslagens allmänna bestämmelser (se avsnitt 11.6). För det undantagsfall att den registrerade ändå inte skulle få något besked från tillsynsmyndigheten rörande klagomålet inom rimlig tid finns det krav på att myndigheter ska handlägga ärenden skyndsamt och åtgärder för den enskilde att vidta. Myndigheter är föremål för krav från statsmakterna att förkorta handläggningstiderna och att arbeta bort ärendebalanser. I myndigheternas regleringsbrev poängterar regeringen ofta att handläggningen av ärenden ska bedrivas effektivt. Chefen för en myndighet har till uppgift att bevaka att ärenden inte blir liggande utan att åtgärder vidtas.

Även Justitiekanslerns och JO:s tillsyn ska motverka långsam handläggning. Enligt 29 § myndighetsförordningen (2007:515) ska också myndigheterna senast den 1 mars varje år till Justitiekanslern skicka in förteckningar över ärenden som har kommit in före den 1 juli föregående år men som inte har avgjorts vid årets utgång.

Sammanfattningsvis gör regeringen bedömningen att det i svensk rätt redan finns effektiva rättsmedel som är tillgängliga för den registrerade om tillsynsmyndigheten inte skulle uppfylla sin informationsskyldighet enligt direktivet. Denna bedömning görs även på förordningens område (prop. 2017/18:105 s. 152 f.) Regeringen anser därför, i likhet med *Förvaltningsrätten i Linköping* och *Justitiekanslern* men i motsats till *Dataskydd.net*, att det inte behövs några särskilda författningsbestämmelser om tillsynsmyndighetens skyldigheter att handlägga klagomål inom rimlig tid.

13.7 Överklagande av tillsynsmyndighetens beslut

13.7.1 Tillsynsmyndighetens beslut ska kunna överklagas

Regeringens förslag: Tillsynsmyndighetens beslut enligt ramlagen ska få överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Utredningens förslag överensstämmer i huvudsak med regeringens. I utredningens förslag anges inte uttryckligen att tillsynsmyndigheten har ställning som motpart i domstolen. Enligt utredningens förslag ska även tillsynsmyndighetens beslut enligt föreskrifter som meddelats i anslutning till ramlagen få överklagas till allmän förvaltningsdomstol.

Remissinstanserna: *Justitiekanslern* anser att förslagen till regleringar är otydliga när det gäller vilka beslut som går att överklaga. *Kammarrätten i Stockholm* anser att det bör klargöras att tillsynsmyndigheten är motpart om dess beslut överklagas. *Dataskydd.net* önskar ett tydliggörande av att rätten att överklaga även gäller privatpersoner.

Skälen för regeringens förslag

Innehållet i direktivet

I artikel 53.1 och skäl 86 slås fast att en fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och som meddelats av tillsynsmyndigheten. Enligt skäl 86 avses med beslut som får rättsliga följder bl.a. tillsynsmyndighetens beslut när den utövar sina utrednings- och korrigeringsbefogenheter. Däremot tar rätten inte sikte på beslut om åtgärder som inte är rättsligt bindande, t.ex. yttranden eller rådgivning.

Nuvarande reglering

Enligt 42 § förvaltningslagen (2017:900) får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Enligt 51 § första stycket personuppgiftslagen får tillsynsmyndighetens beslut, med undantag av beslut om föreskrifter, överklagas till allmän förvaltningsdomstol. Paragrafen genomför artikel 28.3 i 1995 års direktiv som slår fast att sådana beslut av tillsynsmyndighetens som går en part emot ska kunna överklagas till domstol.

Överklagandebestämmelsen i personuppgiftslagen är även tillämplig när tillsynsmyndigheten fattat beslut enligt vissa av registerförfattningarna för de behöriga myndigheterna. Det beror på att registerförfattningen innehåller en uttrycklig hänvisning till överklagandebestämmelsen (se t.ex. 2 kap. 2 § 13 åklagardatalagen). Några registerförfattningar innehåller överklagandebestämmelser med samma innebörd som överklagandebestämmelsen i personuppgiftslagen (se t.ex. 19 § domstolsdatalagen).

En överklagandebestämmelse i ramlagen

Om en myndighets befogenheter regleras i en författning bör det som huvudregel av samma författning framgå om och i så fall hur myndighetens beslut kan överklagas. En sådan ordning ger en samlad bild både av vilka befogenheter en myndighet har och hur den som blir föremål för myndighetens beslut kan angripa dem. Regeringen föreslår nu att tillsynsmyndighetens befogenheter regleras i ramlagen (se avsnitt 11.7). Ramlagen bör därför även reglera rätten att överklaga tillsynsmyndighetens beslut.

Vilka beslut ska få överklagas?

Enligt artikel 53.1 får endast rättsligt bindande beslut överklagas. Det ligger i linje med vad som allmänt gäller för överklagbarhet och klagorätt. Även om motsvarande artikel i 1995 års dataskyddsdirektiv har en något annorlunda språklig utformning beträffande vilka beslut som får överklagas anser regeringen i likhet med utredningen att det inte är någon saklig skillnad.

Rätten att överklaga beslut regleras genom bestämmelser i specialförfattningar och myndighetsinstruktioner. Även om det i en författning anges att ett beslut enligt författningen eller ett beslut av en viss myndighet får överklagas, innebär det inte att alla sådana beslut är överklagbara. Överklagbarheten är nämligen begränsad till följd av allmänna principer som har utbildats i rättspraxis (jfr RÅ 2007 ref. 7 och där angivna rättsfall). En myndighets faktiska handlande eller underlåtenhet att handla kan exempelvis inte överklagas. En annan förutsättning för överklagande är att beslutet har en inte alltför obetydlig verkan för parter eller andra. Normalt saknas det också möjlighet att klaga över motiveringen till ett beslut (prop. 1997/98:101 s. 49 f.). Frågan om överklagbarhet har prövats när det gäller tillsynsmyndighetens beslut enligt personuppgiftslagen (för exempel se Öman m.fl. s. 549 f.).

Bestämmelsen i ramlagen bör med beaktande av det som nu har sagts och i likhet med dagens reglering ha som utgångspunkt att tillsynsmyndighetens beslut ska kunna överklagas. Av tydlighetsskäl bör det, som *Kammarrätten i Stockholm* anför, även framgå av bestämmelsen att tillsynsmyndigheten har ställning som motpart i ett sådant mål hos domstolen (jfr 22 kap. 5 § lagen om offentlig upphandling). Som *Justitiekanslern* påpekar kan det i vissa fall vara svårt att förutse vilka beslut som går att överklaga. En fullständig reglering är emellertid inte lämplig att göra. På samma sätt som i dag får det i stället avgöras i rättstillämpningen om ett beslut som tillsynsmyndigheten har fattat är överklagbart.

I avsnitt 11.6.3 och 11.7.6 föreslår regeringen att tillsynsmyndigheten ska kunna fatta vissa beslut som saknar motsvarighet i dagens reglering. Tillsynsmyndigheten får bl.a. i vissa fall vägra att kontrollera om behandlingen av personuppgifter är författningsenlig och kommer också att kunna meddela förelägganden om radering av personuppgifter. I vilken utsträckning de nya typerna av beslut kommer att kunna överklagas blir på motsvarande sätt en fråga för rättstillämpningen.

Överklagandena bör på samma sätt som i dag prövas av allmän förvaltningsdomstol. Av de skäl som angetts i avsnitt 13.4 bör instansordningen inte beskäras så att förvaltningsrättens avgörande inte får överklagas. Vid överklagande till kammarrätten bör det dock krävas prövningstillstånd för att klaganden ska få sitt överklagande prövat i sak.

Till skillnad från utredningen anser dock regeringen att överklagandemöjligheten för kommande föreskrifter inte bör regleras i ramlagen.

Vem får överklaga?

För att någon ska få överklaga ett beslut ska han eller hon ha klagorätt. Om en person har klagorätt måste bedömas i varje enskilt fall av den domstol som behandlar överklagandet.

I 51 § personuppgiftslagen ställs det inte något krav på att den som klagar ska vara part. I praxis har det inte heller krävts att den som överklagar tillsynsmyndighetens beslut har ställning som part. I stället har det bl.a. förts resonemang kring dels om beslutet angått den som överklagat det, dels om det gått honom eller henne emot. Tillämpningen stämmer väl överens med de krav på klagorätt som ställs upp i direktivet. Ramlagens bestämmelse kan därför utformas med 51 § första stycket personuppgiftslagen som mönster.

Att det är den som beslutet angår och som det gått emot som har klagorätt innebär i praktiken att det är den beslutet riktas mot som har rätt att överklaga tillsynsmyndighetens beslut. I ett tillsynsärende kommer det oftast att vara den personuppgiftsansvarige eller ett personuppgiftsbiträde. När det gäller avslag på begäran om kontroll av om viss behandling är författningsenlig berörs den registrerade som har begärt kontrollen. Det kan dock inte uteslutas att beslut av tillsynsmyndigheten i något annat fall skulle kunna få rättsliga följder även för någon annan än den som beslutet riktar sig mot. Vederbörande har då rätt att överklaga beslutet enligt förvaltningslagens regler om talerätt. Regeringen anser mot denna bakgrund att något ytterligare förtydligande i enlighet med vad *Dataskydd.net* efterfrågar inte behövs.

Särskilt om tillsynsmyndighetens beslut i anledning av klagomål

Enligt rättspraxis avseende personuppgiftslagen är Datainspektionens beslut att inte vidta någon åtgärd med anledning av en anmälan (klagomål) eller att skriva av ett ärende om tillsyn inte möjliga att överklaga (se RÅ 2010 ref. 29).

I skäl 85 i direktivet framhålls att en registrerad ska ha rätt till ett effektivt rättsmedel också om tillsynsmyndigheten helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när det är nödvändigt för att skydda den registrerades rättigheter. Av skäl 86 framgår bl.a. att den registrerade ska kunna vända sig till behörig nationell domstol. Vidare sägs i artikel 52.4 att tillsynsmyndigheten ska underrätta den enskilde om handläggningen och resultatet av ett klagomål som han eller hon gett in och om rätten till rättsmedel enligt artikel 53. Av artikel 53.1 följer emellertid att det enbart är den som ett rättsligt bindande beslut riktar sig mot som ska ha tillgång till ett effektivt rättsmedel.

Direktivet innehåller således som utredningen konstaterar skrivningar som kan tala både för och emot en klagorätt för enskilda när det gäller tillsynsmyndighetens beslut i anledning av klagomål. En generell rätt till domstolsprövning av tillsynsmyndighetens beslut av det slag som nu är aktuellt skulle äventyra tillsynsmyndighetens oberoende ställning. Att tillsynsmyndigheten ska vara oberoende framgår bl.a. av artikel 42.1. Enligt artikel 46.1 f ska tillsynsmyndigheten behandla klagomål och när så är lämpligt undersöka den sakfråga klagomålet gäller. Tillsynsmyndigheten har därmed inte någon skyldighet att vidta tillsynsåtgärder eller ens att alltid närmare undersöka sakfrågan. Tvärtom har tillsynsmyndigheten enligt direktivet, på samma sätt som i svensk tillsynstradition, ett uttalat utrymme att själv avgöra vilka tillsynsärenden som ska drivas och på vilket sätt det ska göras.

Regeringen delar mot denna bakgrund utredningens bedömning att det får överlämnas till rättstillämpningen att avgöra i vilken utsträckning enskilda ska anses ha klagorätt.

Det bör också understrykas att en registrerad alltid har möjlighet att väcka talan i civilrättslig ordning mot en personuppgiftsansvarig eller ett personuppgiftsbiträde och i vissa fall även att överklaga en myndighets beslut i egenskap av personuppgiftsansvarig (se avsnitt 13.2, 13.3 och 13.4). En registrerad kan välja att väcka en sådan talan eller överklaga ett sådant beslut oavsett vad tillsynsmyndigheten gjort för överväganden i sin tillsyn.

Särskilt om myndigheters rätt att överklaga

De allmänna förvaltningsrättsliga principerna om klagorätt anses bara vara tillämpliga på myndigheter när de uppträder i någon privaträttslig egenskap, exempelvis som arbetsgivare eller fastighetsägare. Då anses myndigheter ha samma rätt att överklaga som enskilda. När myndigheter däremot uppträder i sin offentligrättsliga roll, vilket de gör i egenskap av personuppgiftsansvariga, är förhållandena annorlunda. En myndighet får då överklaga en annan myndighets beslut bara under vissa förutsättningar. Utgångspunkten är att överklagande kräver författningsstöd.

Till skillnad från vad som anges i t.ex. artiklarna 53.2 och 54 omfattar rätten till rättsmedel enligt artikel 53.1 inte bara den registrerade. Av artikel 53.1 jämförd med skäl 86 framgår att även myndigheter i sin egenskap av personuppgiftsansvariga ska ha rätt att överklaga tillsynsmyndighetens beslut. Både statliga, kommunala (t.ex. socialnämnden vid ungdomspåföljder) och landstingskommunala (t.ex. rättspsykiatriska enheter) myndigheter kommer att vara personuppgiftsansvariga enligt ramlagen.

Myndigheter som är personuppgiftsansvariga anses redan i dag kunna överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol enligt 51 § personuppgiftslagen. Detsamma bör gälla enligt ramlagen. Att kretsen av taleberättigade är vidare när det gäller tillsynsmyndighetens beslut än vid övriga rättsmedel är, som utredningen konstaterar, naturligt. Det är främst myndigheter som kommer att vara personuppgiftsansvariga för den behandling som utförs enligt ramlagen. Tillsynsmyndighetens beslut kommer oftast att rikta sig direkt mot de personuppgiftsansvariga och de kommer därför att ha intresse av att kunna överklaga besluten. Regeringen håller därför med utredningen om att bestämmelsen om överklagande av tillsynsmyndighetens beslut innebär att statliga, kommunala och landstingskommunala myndigheter ges rätt att överklaga.

13.7.2 Det behövs ingen ny forumregel

Regeringens bedömning: Det behövs ingen ny forumregel för talan mot tillsynsmyndighetens beslut.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Enligt artikel 53.3 ska medlemsstaterna föreskriva att talan mot en tillsynsmyndighet ska väckas vid domstol i den medlemsstat där tillsynsmyndigheten har sitt säte. Med

väcka talan måste i detta sammanhang förstås att ett domstolsförfarande mot tillsynsmyndigheten initieras genom överklagande av myndighetens beslut.

Utredningen anser att artikel 53.3 bör tolkas som ett krav på att det ska finnas en forumregel avseende prövningen av tillsynsmyndighetens beslut. Regeringen anser att artikeln snarare bör förstås som ett krav på att ett beslut av en tillsynsmyndighet i en viss medlemsstat endast ska kunna prövas av domstol i den medlemsstaten. Den svenska tillsynsmyndighetens beslut ska alltså inte kunna prövas av domstol i en annan medlemsstat. Att den svenska tillsynsmyndighetens beslut överklagas till svensk domstol följer av den föreslagna överklagandebestämmelsen och 14 § lagen (1971:289) om allmänna förvaltningsdomstolar.

Det krävs därför ingen åtgärd för att genomföra artikel 53.3.

13.8 Rättsmedlen är oberoende av varandra

Regeringens bedömning: Den föreslagna regleringen lever upp till kravet på att användningen av ett rättsmedel inte ska få påverka rätten att använda andra rättsmedel eller administrativa förfaranden.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Rätten till rättsmedel får enligt artikel 53.1 och skäl 86 inte påverka något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol. Även om den registrerade har rätt att överklaga ett beslut av en personuppgiftsansvarig myndighet ska han eller hon när som helst kunna utnyttja andra rättsmedel som står till buds.

Den registrerade kan således under vissa förutsättningar föra talan parallellt i både allmän förvaltningsdomstol (om ändring av ett myndighetsbeslut genom överklagande) och allmän domstol (om t.ex. skadestånd) om vad som i realiteten är samma sak.

Den registrerade kan dessutom när som helst lämna in klagomål till tillsynsmyndigheten, som oberoende av domstolsprocesserna kan agera och utnyttja sina befogenheter. Möjligheten att lämna in klagomål även till andra organ än tillsynsmyndigheten står också öppen.

Regeringen delar mot denna bakgrund utredningens bedömning att regleringen lever upp till kravet på att användningen av ett rättsmedel inte får påverka rätten att använda andra rättsmedel eller administrativa förfaranden.

13.9 Rätt för ideella organisationer att företräda registrerade

Regeringens bedömning: Det krävs inga lagstiftningsåtgärder för att en registrerad ska kunna ge en ideell organisation i uppdrag att företräda honom eller henne hos tillsynsmyndigheten eller i domstol.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Dataskydd.net* är kritisk mot att utredningen inte gjort någon ansats att förenkla grupptalan. Ingen annan remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning

Innehållet i direktivet

Enligt artikel 55 ska en registrerad ha rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte i uppdrag att lämna in klagomål till tillsynsmyndigheten och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning. Förutom att ge in klagomål till tillsynsmyndigheten ska alltså den som fått ett sådant uppdrag kunna överklaga beslut, väcka dröjsmålstalan eller väcka talan vid allmän domstol. Organets, organisationens eller sammanslutningens stadgeenliga mål ska vara av allmänt intresse och den ska vara verksam för att skydda registrerades rättigheter och friheter vid behandling av personuppgifter.

Enligt skäl 87 bör en registrerad som anser att hans eller hennes rättigheter enligt direktivet har kränkts ha rätt att ge ett organ som syftar till att skydda registrerades rättigheter och intressen vad gäller skyddet av deras personuppgifter i uppdrag att lämna in klagomål och utöva hans eller hennes rätt till rättsmedel. Den registrerades rätt att bli företrädd bör inte påverka nationella processuella regler enligt vilka det kan vara obligatoriskt att registrerade inför domstol företräds av en advokat.

För enkelhetens skull benämns organet, organisationen eller sammanslutningen i det följande ideell organisation.

Nuvarande reglering

Processrätten medger som huvudregel inte att organisationer intar partsställning vid sidan av den egentliga parten i en process. Undantag gäller dock för arbetstvister, (4 kap. 5 § lagen [1974:371] om rättegången i arbetstvister), tvister mellan konsumenter och näringsidkare om varor, tjänster eller andra nyttigheter (5 § lagen [2002:599] om grupprättegång), mål om skadestånd för vissa miljöskador och andra enskilda anspråk (32 kap. 13 och 14 §§ miljöbalken) och mål om diskriminering (6 kap. 2 § diskrimineringslagen [2008:567]). I personuppgiftslagen och annan reglering om personuppgiftsbehandling finns inga regler om talerätt för organisationer.

En enskild får enligt 48 § förvaltningsprocesslagen i en rättegång i allmän förvaltningsdomstol anlita ett ombud eller ett biträde. Enligt 12 kap. 1 § rättegångsbalken får en enskild anlita ett ombud i en process vid allmän domstol. I såväl förvaltningsprocesslagen som rättegångsbalken ställs uttryckliga kompetenskrav på ombudet eller biträdet (48 § första stycket förvaltningsprocesslagen respektive 12 kap. 2 § rättegångsbalken), varför juridiska personer inte kan uppträda som ombud i en rättegång (se Fitger m.fl., Rättegångsbalken, del 1, supplement 81, oktober 2016, s. 12:5 och prop. 2012/13:45 s. 106 f.). I förvaltningsärenden har hittills även en juridisk person kunnat agera ombud eller biträde, eftersom motsvarande kompetenskrav saknas (9 § första stycket förvalt-

ningslagen (1986:223), prop. 1971:30, del 2 s. 362 och RÅ 1963 ref. 37). Om ett ombud eller ett biträde är oskickligt, visar oförstånd eller är olämpligt på något annat sätt får myndigheten eller domstolen avvisa ombudet (48 § andra stycket förvaltningsprocesslagen, 12 kap. 5 § rättegångsbalken och 9 § andra stycket förvaltningslagen).

Behövs det en särskild reglering av organisationers rätt att företräda enskilda?

Artikel 55, som saknar motsvarighet i 1995 års dataskyddsdirektiv kan, som utredningen konstaterar, tolkas på två sätt. Den kan antingen tolkas som att ideella organisationer ska medges talerätt vid sidan av registrerade eller att registrerade ska kunna anlita en sådan organisation som ombud i mål och ärenden som rör personuppgiftsbehandling.

Regeringen delar utredningens bedömning att bestämmelsen inte kan uppfattas på det sättet att ideella organisationer ska ges talerätt vid sidan av registrerade. Det framgår tydligt av att det i artikeln sägs att den registrerade ska kunna ge organisationen i uppdrag att för hans eller hennes räkning vidta vissa åtgärder. Med den formuleringen kan regleringen inte förstås på annat sätt än att registrerade ska kunna anlita en ideell organisation som ombud.

Som konstaterats ovan medger dagens regler att registrerade i förvaltningsärenden anlitar en juridisk person, t.ex. en ideell organisation. När den nya förvaltningslagen träder i kraft den 1 juli 2018 kommer emellertid en juridisk person inte längre att kunna agera ombud i förvaltningsärenden. Detta följer av 14 § i den nya lagen. Den registrerade kan därmed inte ge en ideell organisation i uppdrag att för hans eller hennes räkning lämna in klagomål till tillsynsmyndigheten.

När det gäller kravet på att registrerade ska ha rätt att anlita sådana organisationer som ombud i en rättegång i domstol är det därmed inte möjligt för organisationen som sådan att företräda dem. Däremot kan en företrädare för organisationen som har tillräcklig kompetens uppträda som ombud, eftersom det inte finns något krav på att ett ombud ska vara advokat eller jurist eller på något sätt ha en särskild relation till huvudmannen. Den registrerade kan utforma en fullmakt för den ideella organisationen på ett sådant sätt att företrädare för organisationen omfattas av den. Det kan tilläggas att även om det skulle skapas förutsättningar för att anlita en organisation som ombud i domstol, skulle det i praktiken ändå vara en fysisk person – en representant för organisationen – som för den registrerades talan. Mot den bakgrunden delar regeringen utredningens bedömning att det inte finns skäl att föreslå någon regel om att ideella organisationer ska kunna vara ombud. Registrerades rätt att ge en ideell organisation sådana uppdrag som avses i direktivet tillgodoses, som utredningen konstaterar, genom de möjligheter som befintlig lagstiftning ger.

Utredningen har inte berört den fråga som *Dataskydd.net* väcker. Regeringen ser inte skäl att i detta sammanhang ta upp frågan.

14 Överföring till tredjeland och internationella organisationer

14.1 Bakgrund

14.1.1 2013 års lag

Dataskyddsrambeslutet (se avsnitt 4.7.3) reglerar behandlingen av personuppgifter vid de flesta informationsöverföringar som i dag görs inom tillämpningsområdet för det nya dataskyddsdirektivet. I rambeslutet fastställs gemensamma regler för behandling av personuppgifter inom ramen för polisiärt och straffrättsligt samarbete när personuppgifter överförs eller görs tillgängliga mellan EU-medlemsstater, Island, Liechtenstein, Norge och Schweiz och EU-organ och EU:s informationssystem. Dataskyddsrambeslutet är genomfört i Sverige huvudsakligen genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag).

Lagen reglerar möjligheterna för en svensk myndighet att föra över personuppgifter till ett tredjeland eller ett internationellt organ. Enligt 7 § får personuppgifter överföras till ett tredjeland eller ett internationellt organ om den som har överfört eller gjort uppgifterna tillgängliga för den svenska myndigheten har medgett att de överförs, överföringen är nödvändig för något av de ändamål som omfattas av lagens tillämpningsområde och mottagaren har ansvar för ett sådant ändamål. Därtill ska staten där den mottagande myndigheten eller organet finns ha en adekvat skyddsnivå för den avsedda behandlingen. Undantag från kravet på adekvat skyddsnivå görs i vissa enskilda fall som framgår av paragrafen. På samma sätt föreskrivs undantag från kravet på medgivande i förväg.

Eftersom 2013 års lag enbart är tillämplig på personuppgifter som härrör från andra medlemsstater eller från de andra stater, organ och informationssystem som nyss nämnts, gäller personuppgiftslagen (1998:204) för andra överföringar, bl.a. genom hänvisningar dit i myndigheters registerförfattningar. Som exempel på när personuppgiftslagen är tillämplig kan nämnas överföringar till USA, Kanada eller Kina av personuppgifter som har sitt ursprung i Sverige. Polismyndigheten står för en stor del av överföringarna av personuppgifter till tredjeland. Sådana överföringar kan göras med stöd av, förutom nyss nämnda lagar, lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och polisdatalagen (2010:361).

14.1.2 Personuppgiftslagen

Syftet med 1995 års dataskyddsdirektiv (se avsnitt 4.7.2) har varit att skapa en gemensam, hög nivå på integritetsskyddet vid behandling av personuppgifter för att på så sätt möjliggöra ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Direktivet har också genomförts i övriga stater som är anslutna till EES. Ett fritt flöde av personuppgifter till tredjeland är däremot inte tillåtet. Det har genom direktivet lagts fast

en gemensam nivå till skydd för personuppgifter som överförs till tredjeland.

Artiklarna 25 och 26 i 1995 års dataskyddsdirektiv om överföring till tredjeland har genomförts i 33–35 §§ personuppgiftslagen och 12–14 §§ personuppgiftsförordningen (1998:1191). I förarbetena till lagen framhålls att direktivets bestämmelser om överföring till tredjeland är detaljerade och komplicerade. En mer komplicerad reglering än vad som är nödvändig borde därför inte införas i lagstiftningen (prop. 1997/98:44 s. 95). Det ansågs ofrånkomligt att i personuppgiftslagen föreskriva förbud mot att överföra personuppgifter till tredjeland och de konkreta undantag från förbudet som räknas upp i direktivet (prop. 1997/98:44 s. 96). Regeringen eller den myndighet som regeringen bestämmer har bemyndigats att meddela föreskrifter om ytterligare undantag från överföringsförbudet.

I januari 2000 modifierades överföringsförbudet till att bara gälla de fall där det saknas en adekvat skyddsnivå i tredjelandet (prop. 1999/2000:11 s. 14 f.). Ändringen syftade till att skapa ökat utrymme för användning av internet och andra elektroniska kommunikationssätt, t.ex. e-post.

Enligt 33 § personuppgiftslagen är det alltså förbjudet att till tredjeland föra över personuppgifter som är under behandling, om landet inte har en adekvat skyddsnivå för personuppgifter. Förbudet gäller även överföring av personuppgifter för behandling där. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. I paragrafen anges vilka omständigheter som ska tillmätas särskild vikt. Den personuppgiftsansvarige anses ha bevisbördan för att skyddsnivån i tredjelandet är adekvat (prop. 1999/2000:11 s. 20).

Trots avsaknad av adekvat skyddsnivå är enligt 34 § personuppgiftslagen överföring av personuppgifter till tredjeland tillåten om den enskilde har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig i vissa särskilt uppräknade fall. Paragrafen reglerar vissa undantag från överföringsförbudet i 33 §. Ett viktigt undantag är att personuppgifter får föras över för användning enbart i en stat som har anslutit sig till dataskyddskonventionen (se avsnitt 4.9).

14.1.3 Innehållet i direktivet

Även det nya dataskyddsdirektivet reglerar förutsättningarna för att överföra personuppgifter till tredjeland. Dessutom regleras överföringar till internationella organisationer. Bestämmelserna, som är förhållandevis detaljerade, finns i artiklarna 35–40.

Ett grundläggande krav för överföring av personuppgifter till ett tredjeland eller en internationell organisation är att tredjelandet eller den internationella organisationen säkerställer en adekvat skyddsnivå för uppgifterna. Kommissionen beslutar om ett tredjeland eller en internationell organisation uppfyller det kravet. Sådana beslut får direkt verkan i medlemsstaterna. Kommissionen ska i sin bedömning bl.a. ta hänsyn till rättsstatsprincipen, tillgången till rättslig prövning och om det finns oberoende tillsyn i mottagarlandet.

Har kommissionen inte fattat något beslut om adekvat skyddsnivå, finns det ändå möjlighet att föra över personuppgifter till ett tredjeland eller en internationell organisation om överföringen omfattas av lämpliga skyddsåtgärder. Om det inte finns ett beslut om adekvat skyddsnivå och överföringen inte heller omfattas av lämpliga skyddsåtgärder, får överföringen göras endast om den är nödvändig i en särskild undantagssituation.

Huvudregeln är att överföringen ska göras till en behörig myndighet i tredjelandet. Medlemsstaterna ges dock möjlighet att föreskriva att personuppgifter, i enskilda och särskilda fall, får överföras direkt till mottagare i tredjeland.

14.2 Några grundläggande begrepp

14.2.1 Överföring

Regeringens bedömning: Det behövs inte någon definition av vad som avses med överföring.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* anser att det inte kan anses vara en överföring om någon befinner sig i tredje land och har tillgång till data, dvs. en situation när inga data transfereras. *Dataskydd.net* anser att uttrycket överföring borde definieras i ramlagen.

Skälen för regeringens bedömning

Vad avses med överföring?

Vilka åtgärder som innebär överföring av personuppgifter har diskuterats bl.a. av Informationshanteringsutredningen och E-offentlighetskommittén (SOU 2015:39 s. 478 f. och SOU 2010:4 s. 338).

Enligt Informationshanteringsutredningen är det inte fråga om överföring av personuppgifter till tredjeland bara genom att en person befinner sig utanför unionen med personuppgifter i sin besittning. Det krävs en avsikt att personuppgifterna ska nå en mottagare i tredjeland. Om en myndighet skickar, vidarebefordrar eller förmedlar information i elektronisk form till en mottagare som befinner sig i ett tredjeland torde det däremot vara fråga om en överföring (SOU 2015:39 s. 479 f.).

Det krävs inte att överföringen till tredjelandet innebär att personuppgifter lämnas ut till tredje man. Det anses vara en överföring även om personuppgifterna lämnas till ett personuppgiftsbiträde i tredjeland för att faktiskt behandlas där, t.ex. om en myndighet använder sig av en utländsk leverantör av en it-tjänst (SOU 2015:39 s. 480).

Det saknas vägledande avgöranden i rättspraxis om vad som är att se som en överföring. I den juridiska litteraturen har det förts viss diskussion om vad som ska förstås med överföring (se bl.a. Öman m.fl. s. 447 f.). I vilken mån det ska ses som en överföring att befinna sig i ett tredjeland och där ha elektronisk tillgång till personuppgifter som ”finns” i hemlandet anses exempelvis oklart.

När det gäller publicering på internet antogs det tidigare att all öppen publicering på en webbplats innebar att personuppgifterna blev tillgängliga i hela världen och därmed kunde anses överförda till alla länder i 1995 års dataskyddsdirektivs mening. EU-domstolen slog emellertid i det s.k. konfirmandlärarmålet fast att det inte är fråga om överföring till tredjeland när en person i en medlemsstat lägger ut personuppgifter på en webbplats på internet som är lagrad hos en fysisk eller juridisk person som har den webbplats där man kan komma åt sidan och som är etablerad i samma medlemsstat eller i en annan medlemsstat (dom av den 6 november 2003, Lindqvist, C-101/01).

Det har diskuterats hur långt EU-domstolens uttalande sträcker sig (se t.ex. SOU 2004:6 s. 232 f.). E-offentlighetskommittén anser att EU-domstolens avgörande klarlagt att det i de flesta fall inte innebär en överföring till tredjeland när information läggs ut på internet. Om uppgifterna t.ex. publiceras på en webbplats på internet och webbplatsen lagras hos en internetleverantör som är etablerad inom EU är det i princip inte fråga om en överföring till tredjeland. Enligt kommittén bör det alltså inte ses som överföring om en myndighet lägger ut information från ett s.k. allmänt register på sin hemsida så länge den aktuella servern finns inom EU (SOU 2010:4 s. 338). Högsta domstolen ansåg i NJA 2005 s. 361 att en rektor på en enskilt bedriven skola inte hade överfört personuppgifter till tredjeland genom att publicera uppgifterna på skolans webbplats.

Utredningen gör bedömningen att det är fråga om en överföring när en behörig myndighet skickar, vidarebefordrar eller förmedlar information i elektronisk form till någon som befinner sig i ett tredjeland eller till en internationell organisation. Regeringen delar denna bedömning. Det bör också, som utredningen bedömer, ses som överföring att en behörig myndighet gör information tillgänglig för ett tredjeland eller en internationell organisation genom att informationen tillförs ett för de behöriga myndigheterna gemensamt datasystem, t.ex. en databas hos Interpol. I likhet med *Polismyndigheten* anser regeringen att det inte kan vara fråga om en överföring om inga personuppgifter transfereras, dvs. bara den omständigheten att någon befinner sig utanför medlemsstaterna och har tillgång till personuppgifter innebär inte att en överföring kan anses ha ägt rum. Överföring på papper av personuppgifter som inte har undergått automatiserad behandling eller har ingått i ett manuellt register bör inte heller betraktas som en överföring.

En överföring av personuppgifter från en svensk myndighet till ett tredjeland eller en internationell organisation kan samtidigt innebära utlämnande av allmänna handlingar. Då aktualiseras även bestämmelser om sekretess. Regeringen återkommer till det i avsnitt 14.12.4.

Bör det införas en definition av överföring?

Dataskyddsdirektivet innehåller inte någon definition av överföring. Det definieras inte heller i 2013 års lag eller i personuppgiftslagen. Till skillnad från *Dataskydd.net* anser regeringen att det inte heller nu finns något behov av att i lag slå fast en definition av uttrycket överföring. Regeringen delar därför utredningens bedömning att uttrycket överföring inte ska definieras i ramlagen.

14.2.2 Medlemsstat

Regeringens förslag: Medlemsstat ska definieras som en stat som är medlem i EU samt Island, Liechtenstein, Norge och Schweiz.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Vad är en medlemsstat?

Kapitel V i direktivet gäller vid all överföring av personuppgifter från en medlemsstat till ett tredjeland eller till en internationell organisation. Kapitlet reglerar också vidareöverföring till ett tredjeland eller en internationell organisation av personuppgifter som tredjelandet eller den internationella organisationen har fått från en medlemsstat. Ordet medlemsstat används i stor utsträckning i direktivet. Det finns därför anledning att titta närmare på vad som avses med en medlemsstat.

I vanligt språkbruk benämns en stat som är medlem i EU medlemsstat. Direktivet utgår från att det gäller för alla EU:s medlemsstater. Danmark är enligt skäl 100 inte automatiskt bundet av det men beslutade i oktober 2016 att ansluta sig. I skäl 99 påminns om att Storbritannien och Irland inte är bundna av de delar av det straffrättsliga och polisiära samarbetet som de tidigare valt att stå utanför.

Enligt skäl 101–103 är direktivet en vidareutveckling av bestämmelserna i Schengenregelverket i förhållande till Island, Liechtenstein, Norge och Schweiz. De tre förstnämnda är, tillsammans med övriga medlemsstater i EU, anslutna till EES. Schweiz, som inte ingår i EES, har ingått avtal med EU med liknande innehåll.

Liksom utredningen anser regeringen att de stater som är bundna av direktivet ska betraktas som medlemsstater, eftersom de är skyldiga att garantera det skydd för personuppgifter som direktivet föreskriver.

Det bör införas en definition av medlemsstat

På flera ställen i direktivet används ordet medlemsstat för att bl.a. beskriva varifrån personuppgifterna som hanteras kommer och vilka staters intressen som ska beaktas i olika sammanhang. Det är svårt att undvika att använda ordet medlemsstat i ramlagen. Eftersom vissa stater som inte är medlemsstater i EU omfattas av direktivet går det inte att använda ordet medlemsstat i ramlagen utan att definiera det. Ett alternativ skulle vara att räkna upp alla berörda stater, men det skulle bli onödigt omfattande och komplicerat att göra det i alla bestämmelser. Genom att definiera medlemsstat blir det tydligt vilka stater regleringen omfattar utan att ramlagen tyngs av långa uppräkningar. Medlemsstat bör därför definieras i ramlagen.

Direktivet gäller för alla EU:s medlemsstater. Island, Liechtenstein, Norge och Schweiz är också bundna av direktivet och bör därför likställas med medlemsstater i ramlagen. Medlemsstat bör följaktligen definieras som en stat som är medlem i EU och Island, Liechtenstein, Norge och Schweiz.

Förhållandet till äldre rättsakter som gäller för EU:s medlemsstater

Dataskyddsdirektivet ska enligt artikel 60 inte påverka tillämpningen av särskilda bestämmelser om dataskydd i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som antagits före dagen för antagandet av direktivet. De bestämmelser som avses reglerar behandling av personuppgifter som överförs mellan medlemsstaterna eller tillgång till EU-informationssystem. Eftersom skyddet för personuppgifter ska tillämpas enhetligt i hela unionen ska kommissionen enligt artikel 62.6 se över om äldre rättsakter behöver anpassas till direktivet.

Som exempel på äldre rättsakter nämns i skäl 94 Prümrådsbeslutet och konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (se avsnitt 6.3).

Äldre rättsakter på området ska således fortsätta att tillämpas i förhållande till EU:s medlemsstater.

Förhållandet till EU:s organ och informationssystem

En särskild fråga är hur direktivet förhåller sig till EU:s organ och informationssystem. Direktivet reglerar enbart överföringar av personuppgifter från medlemsstater till tredjeland (eller andra än behöriga myndigheter i tredjeland, se avsnitt 14.8) och internationella organisationer. EU:s institutioner och organ, t.ex. Europol och Eurojust, och EU-informationssystem, som Schengens informationssystem (SIS II) och tullinformationssystemet (TIS), faller inte in under någon av dessa kategorier.

Enligt 2 § 2013 års lag, som bl.a. genomför artikel 1.2 i dataskyddsrambeslutet, gäller den lagen för överföring av personuppgifter till stater som är medlemmar i EU, Island, Liechtenstein, Norge eller Schweiz och till EU-organ eller EU-informationssystem. Någon motsvarande reglering i förhållande till EU:s organ och informationssystem finns inte i direktivet. Det enda som sägs om dem är att det i artikel 2.3 b anges att direktivet inte tillämpas på personuppgiftsbehandling som utförs av unionens institutioner, organ och byråer. Personuppgiftsbehandlingen inom EU:s institutioner och organ styrs i stället av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

Flera rättsakter som har antagits inom EU när det gäller polisiärt och straffrättsligt samarbete innehåller särskilda bestämmelser om skydd av personuppgifter som överförs eller på något annat sätt behandlas i enlighet med rättsakterna. I några fall utgör dessa bestämmelser en komplett och enhetlig uppsättning regler som omfattar alla relevanta aspekter av dataskydd och som är mer detaljerade än direktivet. Som exempel kan nämnas rättsakter som reglerar funktionssättet för Europol, Eurojust, SIS II och TIS. Rättsakterna möjliggör informationsutbyte mellan medlemsstaterna och medför även i vissa fall uppgiftsskyldighet för de nationella myndigheterna, se t.ex. artikel 7.6 i Europolförordningen. Uppgiftsskyldighet gäller även exempelvis i förhållande till Europeiska byrån för bedrägeribekämpning (Olaf) enligt artikel 8 i Europaparlamentets och rådets förordning (EU, EURATOM) nr 883/2013 av den

11 september 2013. Informationsutbyte äger också rum inom ramen för den europeiska gräns- och kustbevakningen, Frontex, enligt Europaparlamentets och rådets förordning (EU) 2016/1624 av den 14 september 2016 om en europeisk gräns- och kustbevakning och om ändring av Europaparlamentets och rådets förordning (EU) 2016/399 och upphävande av Europaparlamentets och rådets förordning (EG) nr 863/2007, rådets förordning (EG) nr 2007/2004 och rådets beslut 2005/267/EG.

Regeringen delar utredningens uppfattning att reglerad uppgiftsskyldighet eller andra åtaganden och möjlighet att utbyta information med EU:s organ eller genom EU:s informationssystem som förekommer i andra rättsakter bör gälla framför direktivet (jämför artikel 60 och skäl 94). Det gör att personuppgifter även i fortsättningen kan överföras till t.ex. SIS II och TIS i samma utsträckning som hittills. Om det inte finns några rättsakter får det förutsättas att kommissionen på något annat sätt kommer att reglera informationsflödet och skyddet för personuppgifter till unionens institutioner, organ, byråer och informationssystem (se artikel 62.6).

14.2.3 Tredjeland

Regeringens förslag: Tredjeland ska definieras som en stat som inte är en medlemsstat.

Utredningens förslag: överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.
Skälen för regeringens förslag: Direktivet innehåller inte någon definition av tredjeland. Regeringen delar utredningens bedömning att de överväganden som gjordes när personuppgiftslagen infördes gör sig gällande även nu, nämligen att tredjeland bör definieras (SOU 1997:39 s. 343). Särskilt mot bakgrund av det som nyss har sagts om att direktivet även ska tillämpas av några stater utanför EU, är en sådan definition nödvändig. Tillämpningsområdet för ramlagens överföringsregler blir också tydligare på det sättet.

Definitionen av medlemsstat bör bilda utgångspunkt för hur tredjeland definieras i ramlagen. Som framgår av avsnitt 14.2.2 avses med medlemsstat en stat som är medlem i EU och Island, Liechtenstein, Norge och Schweiz. Stater som inte är medlemsstater enligt direktivet ska betraktas som tredjeland. Definitionen av tredjeland bör därför vara en stat som inte är en medlemsstat.

14.2.4 Internationell organisation

Regeringens förslag: Internationell organisation ska definieras som en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: Det är en nyhet i direktivet att reglerna om överföring av personuppgifter även omfattar överföringar till internationella organisationer. 1995 års dataskyddsdirektiv reglerar bara överföring till tredjeland. Dataskyddsrambeslutet innehåller däremot bestämmelser om överföring till internationella organ (”international bodies”). Reglerna om överföring i 2013 års lag omfattar därför även överföring till sådana organ.

Internationell organisation definieras i artikel 3.16. I likhet med utredningen anser regeringen att direktivets uttryck internationell organisation, som också används i dataskyddsförordningen, bör användas i ramlagen. För att tydliggöra vad som avses bör det tas in en definition i lagen. Internationell organisation bör definieras som en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.

Inom ramlagens tillämpningsområde är det främst till Interpol som personuppgifter brukar överföras, men det finns även andra internationella organisationer som kan komma i fråga.

14.2.5 Internationella avtal

Regeringens bedömning: Det behövs inte någon definition av internationella avtal.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: I artikel 39.2 förklaras vad som menas med ett internationellt avtal. Enligt artikeln avses varje gällande bilateralt eller multilateralt internationellt avtal mellan medlemsstater och tredjeländer inom området för straffrättsligt samarbete och polissamarbete. I artikel 61 slås fast att sådana internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer och som medlemsstaterna ingick före den 6 maj 2016 och som är förenliga med unionsrätten som den tillämpades före den dagen, ska fortsätta att gälla tills de ändras, ersätts eller återkallas. Det bör inte vara nödvändigt att avtalet i sin helhet gäller personuppgiftsbehandling, utan ett avtal om t.ex. internationellt samarbete som innehåller bestämmelser om dataskydd bör också kunna ses som ett internationellt avtal i direktivets mening.

Artikel 39.2 behöver inte genomföras i nationell rätt. Liksom utredningen ser regeringen inte heller något behov av att definiera internationellt avtal, eftersom uttrycket inte används i ramlagen.

14.3 Allmänna principer för överföring av personuppgifter

14.3.1 Förutsättningar för överföring

Regeringens förslag: En behörig myndighet får, om vissa villkor är uppfyllda, överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation.

En behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation ska särskilt beakta risken för att enskilda får ett försämrat skydd för sina personuppgifter.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Eskilstuna tingsrätt* anser att kraven i artikel 35.3 i dataskyddsdirektivet om att skyddsnivån för fysiska personer inte får undergrävas fullt ut måste motsvaras av ramlagens bestämmelser. Även *Datainspektionen* framhåller vikten av genomförandet av den artikeln och att det måste framgå att kraven är grundläggande förutsättningar för överföring till tredjeland. Inspektionen efterfrågar också vilka konsekvenserna blir för en behörig myndighet om det konstateras ett försämrat skydd vid den avsedda överföringen. Datainspektionen och *Sveriges advokatsamfund* efterfrågar vidare en analys av riskerna med att överföra personuppgifter och behöriga myndigheters möjligheter att vidta åtgärder när uppgifter som överförts behandlas på ett sätt som inte avsetts.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

I artikel 35 anges allmänna principer för överföring av personuppgifter till ett tredjeland eller en internationell organisation.

En grundläggande förutsättning för överföring av personuppgifter till ett tredjeland eller en internationell organisation är att nationella bestämmelser om behandling av personuppgifter respekteras och att de villkor som räknas upp i punkterna a–d i artikel 35.1 är uppfyllda (se avsnitt 14.3.2–14.3.4). Det gäller för all överföring av personuppgifter oavsett på vilken grund överföringen görs (med undantag för att kravet i 35.1 b inte behöver vara uppfyllt när personuppgifter får överföras till någon annan än en behörig myndighet, se avsnitt 14.8). Enligt artikel 35.1 får behöriga myndigheter överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation.

En liknande bestämmelse finns i 7 § första stycket 2013 års lag, som genomför artikel 13.1 i dataskyddsrambeslutet. Enligt 33 § personuppgiftslagen omfattar förbudet mot överföring till tredjeland dels personuppgifter som är under behandling, dels personuppgifter som överförs för behandling i tredjeland.

Regeringen instämmer i utredningens förslag att artikel 35.1 ska genomföras i ramlagen. Av paragrafen bör framgå att behöriga myndigheter får överföra personuppgifter till ett tredjeland eller en internationell organisation endast om vissa särskilt uppräknade villkor är uppfyllda. Vilka de särskilda villkoren är och hur de ska komma till uttryck i ramlagen diskuteras i det följande. Här räcker det att konstatera att paragrafen bör utformas så att det framgår att samtliga villkor ska vara uppfyllda för att en behörig myndighet ska få överföra personuppgifter till ett tredjeland eller en internationell organisation. Behörig myndighet definieras i ramlagen (se avsnitt 6.4.4).

Av paragrafen bör vidare framgå att det ska vara fråga om personuppgifter som håller på att behandlas, dvs. är föremål för sådan behandling som omfattas av ramlagens tillämpningsområde (se avsnitt 6.4). Kravet på att personuppgifterna ska vara föremål för behandling uttrycks annorlunda i 1995 års dataskyddsdirektiv. Där talas det i stället om personuppgifter som är under behandling. I 33 § personuppgiftslagen används samma formulering. Att uttrycket ”håller på att behandlas” används i det nya dataskyddsdirektivet innebär inte någon ändring i sak i förhållande till vad som gäller i dag. Regeringen håller emellertid med utredningen om att ordet behandlas bör användas i ramlagen eftersom det stämmer bättre överens med förslagen i övrigt.

Paragrafen bör också reglera överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation. Det är fråga om sådana personuppgifter som inte är föremål för automatiserad eller annan strukturerad behandling i Sverige, utan överförs till ett tredjeland eller en internationell organisation för att automatiseras där t.ex. genom att läggas in i en databas.

Det är inte ovanligt att personuppgifter överförs till tredjeland genom så kallade nationella kontaktpunkter inom ramen för internationellt samarbete. Syftet med nationella kontaktpunkter är att underlätta det internationella samarbetet genom att varje stat pekar ut en viss myndighet som är ständigt tillgänglig och genom vilken all information till staten kanaliseras, oberoende av vem den slutliga mottagaren är. Kontaktpunkten ser till att informationen omedelbart vidarebefordras till mottagaren. Som exempel kan nämnas att Polismyndigheten är nationell kontaktpunkt bl.a. när det gäller FN:s vapenprogram (Förenta nationernas resolution 55/255, antagen den 31 maj 2001 av generalförsamlingen, tilläggsprotokoll mot olaglig tillverkning av och handel med skjutvapen, deras delar och komponenter och ammunition till Förenta nationernas konvention mot gränsöverskridande organiserad brottslighet) och enligt FN:s konventioner om bekämpande av nukleär terrorism och brott mot sjöfartens säkerhet (Förenta nationernas konvention den 13 april 2005 för bekämpande av nukleär terrorism och Förenta nationernas konvention den 10 mars 1988 för bekämpande av brott mot sjöfartens säkerhet med dess protokoll den 14 oktober 2005). Regeringen delar utredningens uppfattning att ramlagens reglering av överföring inte bör hindra att sådant samarbete är möjligt även i fortsättningen. Det är dock endast behöriga myndigheter som kan fungera som kontaktpunkter för informationsutbyte inom ramlagens tillämpningsområde.

Det kan, som *Datainspektionen* och *Sveriges advokatsamfund* påpekar, vara förenat med viss osäkerhet att överföra personuppgifter till tredjeland eller en internationell organisation. Det kommer att vila ett stort ansvar på de behöriga myndigheter som gör bedömningarna i vilka fall personuppgifter kan överföras. Det är av stor vikt att det finns ett fullgott skydd för den enskildes personliga integritet och att regleringarna i ramlagen motsvarar de krav direktivet ställer i detta avseende. I sammanhanget bör emellertid nämnas att stora delar av direktivet i denna del ansluter nära till vad som gäller enligt befintlig lagstiftning.

Överföringen ska vara förenlig med övriga bestämmelser i ramlagen

Ett krav för att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation är enligt artikel 35.1 att de nationella bestämmelserna som antas i enlighet med andra bestämmelser i direktivet respekteras.

Redan i dag ska de grundläggande kraven på behandling av personuppgifter i 9 § personuppgiftslagen alltid vara uppfyllda för att uppgifterna ska få överföras till ett tredjeland. Överföringen ska också vara tillåten enligt 10 § personuppgiftslagen. Är det exempelvis känsliga personuppgifter, uppgifter om lagöverträdelser eller personnummer som ska överföras, krävs det också att behandlingen är tillåten enligt 13–22 §§ (prop. 1997/98:44 s. 137).

För att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation bör det krävas att alla allmänna förutsättningarna för att få behandla personuppgifter är uppfyllda. Det följer av att överföringen som sådan är en behandling av personuppgifter i ramlagens mening. Överföringen får naturligtvis inte heller stå i strid med andra bestämmelser i lagen.

Skyddsnivån får inte försämras genom överföringen

Av artikel 35.3 framgår att alla bestämmelser som gäller överföring ska tillämpas för att den skyddsnivå som säkerställs genom direktivet inte ska undergrävas. Enligt skäl 64 är det viktigt att den skyddsnivå som direktivet garanterar fysiska personer inom unionen inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra adressater i tredjeland eller till internationella organisationer.

Bestämmelsen, som är av mer upplysande karaktär, fyller en viktig funktion för att tydliggöra att enskildas intresse av skydd för personuppgifter ska värnas även när uppgifterna lämnar medlemssfären. En bestämmelse som motsvarar innehållet i artikeln bör därför tas in i ramlagen. Av den bör framgå att en behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation särskilt ska beakta risken för att enskilda får ett försämrat skydd för sina personuppgifter.

Till skillnad från vad *Eskilstuna tingsrätt* och *Datainspektionen* anför anser regeringen att bestämmelsen därigenom väl uppfyller kraven i artikel 35.3. Det ligger i sakens natur att det inte alltid är möjligt att fullt ut överblicka konsekvenserna av en överföring till tredje land. Om det däremot konstateras att en överföring lett till ett försämrat skydd bör givet-

vis detta föranleda att myndigheten vidtar åtgärder för att dels begränsa konsekvenserna, dels säkerställa att motsvarande situation inte uppstår igen. Det kan även bli aktuellt med åtgärder inom ramen för tillsyn om överträdelse kan konstateras (se närmare avsnitt 11 och 12).

14.3.2 Överföringen ska vara nödvändig för ett visst ändamål och riktas till en behörig myndighet

Regeringens förslag: Personuppgifter får överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Överföringen ska riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans invänder mot förslaget.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt artikel 35.1 a får personuppgifter överföras till ett tredjeland eller till en internationell organisation endast om överföringen är nödvändig för de ändamål som anges i artikel 1.1. Enligt den artikeln ska direktivet tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Ett ytterligare villkor för överföring av personuppgifter är enligt artikel 35.1 b att uppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är en behörig myndighet för något av de ändamål som anges i artikel 1.1. I skäl 64 framhålls att en överföring endast bör utföras av behöriga myndigheter som agerar som personuppgiftsansvariga, utom när personuppgiftsbiträden uttryckligen har getts i uppdrag att göra överföringar för personuppgiftsansvarigas räkning.

I 2013 års lag finns motsvarande bestämmelser i 7 § första stycket 2 och 3, som genomför artikel 13.1 a och b i dataskyddsrambeslutet. Enligt paragrafen får personuppgifter överföras endast om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder och endast till en mottagare som har ansvar för sådan verksamhet.

Överföring enbart till behöriga myndigheter för vissa ändamål

Artikel 35.1 a och b bör, som utredningen föreslår, genomföras i ramlagen. Paragrafen bör formuleras på samma sätt som regleringen av lagens tillämpningsområde, dvs. knytas till arbetsuppgifterna förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och

säkerhet. Det blir mer överskådligt än att hänvisa till paragrafen som reglerar ramlagens tillämpningsområde. Det är också så bestämmelsen i 2013 års lag har formulerats.

Regeringen delar utredningens bedömning att kravet på att överföringen ska vara nödvändig bör tolkas på samma sätt som i allmänt språkbruk, dvs. att det är fråga om något som behövs (se avsnitt 7.2). Den personuppgift som överförs kan behövas antingen för att den överförande eller för att den mottagande myndigheten ska kunna utföra en arbetsuppgift som den har ansvar för inom det angivna tillämpningsområdet. En svensk behörig myndighet kan t.ex. behöva överföra personuppgifter till ett tredjeland för att få hjälp med bevisupptagning i ett ärende som handläggs i Sverige. På motsvarande sätt kan ett tredjeland eller en internationell organisation behöva få tillgång till svenska personuppgifter för sin brottsbekämpning, lagföring eller straffverkställighet.

Av paragrafen bör vidare framgå att det bara är tillåtet att föra över personuppgifter om det görs till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet. Personuppgifterna ska följaktligen överföras till en myndighet eller en annan aktör som har i uppdrag att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Den behöriga myndigheten som personuppgifterna lämnas till behöver inte ha samma arbetsuppgifter som den svenska myndigheten som överför personuppgifterna. Det bör således inte finnas något hinder mot att exempelvis en svensk åklagare lämnar personuppgifter till en utländsk domstol. Det bör inte heller finnas något hinder mot att personuppgifter överförs mellan två nationella kontaktpunkter oavsett vilken typ av myndighet som har utsetts till kontaktpunkt.

14.3.3 Viss skyddsnivå ska vara säkerställd

Regeringens förslag: Personuppgifter får överföras till ett tredjeland eller en internationell organisation endast om kommissionen har antagit ett beslut om adekvat skyddsnivå, eller, om det inte finns ett sådant beslut, om personuppgifterna omfattas av tillräckliga skyddsåtgärder hos adressaten. Om det inte finns ett beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder får personuppgifter överföras endast när ett undantag för särskilda situationer är tillämpligt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Remissynpunkter angående adekvat skyddsnivå, tillräckliga skyddsåtgärder och undantag i särskilda situationer redovisas i avsnitt 14.4–6.

Skälen för regeringens förslag: Enligt artikel 35.1 d gäller som huvudregel att personuppgifter får överföras till ett tredjeland eller en internationell organisation endast om viss skyddsnivå är säkerställd för personuppgiftsbehandlingen. Tanken är att den skyddsnivå som säkerställs genom direktivet som utgångspunkt ska gälla även när personuppgifter överförs till ett tredjeland eller en internationell organisation. För att personuppgifter ska få lämnas ut från en medlemsstat krävs det därför

enligt artikel 36 i första hand att tredjelandet eller den internationella organisationen omfattas av ett beslut från kommissionen om att landet eller organisationen säkerställer en adekvat skyddsnivå. Om det inte finns ett sådant beslut får personuppgifter enligt artikel 37 ändå överföras i vissa fall om lämpliga skyddsåtgärder har vidtagits eller säkerställts. Är inte heller det kravet uppfyllt får personuppgifter endast överföras i de särskilda undantagssituationer som är uttömmande reglerade i artikel 38.

De tre överföringsgrunderna redovisas mer ingående i samband med att artiklarna 36–38 behandlas. Det räcker därför här att konstatera att villkoret ska genomföras i svensk rätt genom en bestämmelse i ramlagen som motsvarar innehållet i artikel 35.1 d.

14.3.4 Överföring av uppgifter från andra medlemsstater ska vara medgiven

Regeringens förslag: Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

Om ett medgivande på grund av tidsbrist inte kan inhämtas i förväg, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller någon annan medlemsstat.

Regeringens bedömning: Att den andra medlemsstaten utan dröjsmål ska informeras om överföringen kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning**.**

Remissinstanser: *Säkerhets- och integritetsskyddsnämnden* anser att det av bestämmelsen måste framgå att samtliga grundläggande förutsättningar krävs vid överföring även när medgivande lämnats från en medlemsstat.

Skälen för regeringens förslag och bedömning

Innehållet i direktivet

Enligt artikel 35.1 c ska den som vill överföra personuppgifter som kommer från en annan medlemsstat till ett tredjeland eller en internationell organisation ha den andra medlemsstatens tillstånd till överföringen. Tillståndet ska ges innan överföringen får äga rum.

I artikel 35.2 görs undantag från huvudregeln om förhandstillstånd. Där anges att det är tillåtet att överföra personuppgifter utan förhandstillstånd om överföringen är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och tillstånd inte kan inhämtas i tid. Den som skulle ha gett tillstånd ska då utan dröjsmål informeras om att överföringen har gjorts.

Nuvarande reglering

I 2013 års lag finns motsvarande bestämmelse i 7 § första stycket 1, som genomför artikel 13.1 c i dataskyddsrambeslutet. Enligt den bestämmelsen får personuppgifter överföras endast om den som överfört eller gjort uppgifterna tillgängliga har medgett att de överförs. Enligt 7 § tredje stycket, som genomför artikel 13.2 i rambeslutet, får, om medgivande på grund av tidsbrist inte kan utverkas i förväg, personuppgifterna ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller en annan medlemsstat i EU. Den myndighet som skulle ha medgett överföringen ska, enligt 1 § förordningen (2013:343) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen, utan dröjsmål informeras om att överföringen gjorts utan föregående medgivande.

Huvudregeln är att förhandstillstånd krävs

Artikel 35.1 c bör, som utredningen föreslagit, genomföras i ramlagen. Av paragrafen bör det framgå att personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat personuppgifterna till en svensk myndighet i förväg har tillåtit det. Regeringen håller med utredningen om att ordet medge bör användas, eftersom det på ett bättre sätt speglar vad som avses.

Som *Säkerhets- och integritetsskyddsnämnden* påpekar kompletterar kravet på medgivande övriga krav som direktivet ställer för att personuppgifter ska få överföras till tredjeland. Detta framgår enligt regeringens bedömning tydligt genom det nu aktuella förslaget.

Undantag vid allvarlig fara

Även artikel 35.2 om undantag från kravet på förhandsmedgivande bör genomföras i ramlagen. Motsvarande bestämmelse i 2013 års lag är väl anpassad till hur svensk lagstiftning brukar utformas. Regeringen delar därför utredningens bedömning att det finns det skäl att använda en liknande formulering i ramlagen. Det innebär att ordet fara bör användas i stället för ordet hot, som används i den svenska språkversionen av direktivet. En motsvarande bestämmelse, som också syftar till att tillgodose skyddet för allmän säkerhet, finns i artikel 38.1 c. Där används ordet fara i den svenska versionen. I den engelska versionen av direktivet används ordet ”threat” i både artikel 35.2 och 38.1 c. Någon saklig skillnad kan därför inte vara avsedd.

Det är vidare, som utredningen föreslår, tillräckligt att det på samma sätt som i 2013 års lag anges att det ska vara fara för allmän säkerhet. Tillägget i direktivet att det ska gälla säkerheten i en medlemsstat eller ett tredjeland innebär att tillämpningsområdet omfattar alla stater och saknar därmed egentligt innehåll. Att använda formuleringen ”den allmänna säkerheten i en stat” skulle inte heller bidra till någon ökad klarhet. De väsentliga intressena, som enligt direktivet gäller till förmån för en medlemsstat, bör däremot avse Sverige eller en annan medlemsstat.

Av artikel 35.2 framgår att den som har överfört personuppgifter till ett tredjeland eller en internationell organisation utan förhandsmedgivande, när sådant krävs, utan dröjsmål ska informera den medlemsstat som lämnat uppgifterna till Sverige om överföringen. Detta kan regleras i förordning.

14.4 Beslut om adekvat skyddsnivå

Regeringens förslag: Om kommissionen har beslutat att det finns adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Uppsala universitet* och *Dataskydd.net* anser att det tydligare bör framgå vad som gäller om det finns tveksamheter angående kommissionens beslut om adekvat skyddsnivå och den nationella tillsynsmyndighetens uppgifter i sådana situationer.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 36.1 får personuppgifter överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet eller den internationella organisationen säkerställer en adekvat skyddsnivå. Därutöver ska förutsättningarna för överföring i artikel 35 vara uppfyllda.

Kommissionen får enligt artikel 36.3 besluta med bindande verkan för medlemsstaterna att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå. Den territoriella och sektoriella tillämpningen ska anges i beslutet och det ska också, i förekommande fall, anges vilken eller vilka myndigheter som är tillsynsmyndigheter. En mekanism för regelbunden översyn, minst vart fjärde år, ska inrättas. Vilka omständigheter kommissionen ska beakta när den beslutar om adekvat skyddsnivå framgår av artikel 36.2. Enligt artikel 36.4 ska kommissionen fortlöpande bevaka om utvecklingen i ett tredjeland eller hos en internationell organisation påverkar ett beslut om adekvat skyddsnivå.

Kommissionen får enligt artikel 36.5, även det med bindande verkan för medlemsstaterna, besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå. Kommissionen kan alltså dra tillbaka, ändra eller upphäva ett beslut om adekvat skyddsnivå och även förordna att beslutet ska gälla omedelbart. Om kommissionen fattar ett sådant beslut är det inte längre tillåtet att överföra personuppgifter dit. Däremot kan en överföring vara tillåten om kraven på lämpliga skyddsåtgärder eller undantag i särskilda situationer är uppfyllda (se skäl 70). Enligt artikel 36.8 ska kommissionen på sin

webbplats och i EU:s officiella tidning offentliggöra beslut i fråga om adekvat skyddsnivå.

Nuvarande reglering

I 2013 års lag finns motsvarande bestämmelse i 7 § första stycket 4, som genomför artikel 13.1 d i dataskyddsrambeslutet. Där anges som krav för överföring att den stat där den mottagande myndigheten eller det mottagande internationella organet finns har en adekvat skyddsnivå för den avsedda personuppgiftsbehandlingen.

Kommissionen får enligt artikel 25.6 i 1995 års dataskyddsdirektiv konstatera att ett tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, har en skyddsnivå som är adekvat. Om kommissionen meddelar ett sådant beslut är medlemsstaterna skyldiga att vidta nödvändiga åtgärder för att följa beslutet. Medlemsstaterna och kommissionen ska informera varandra om de anser att ett visst tredjeland inte har en adekvat skyddsnivå. Om kommissionen kommer fram till att ett tredjeland inte har en adekvat skyddsnivå är medlemsstaterna skyldiga att vidta de åtgärder som är nödvändiga för att förhindra att personuppgifter överförs dit. Kommissionen ska i sådant fall vid lämpligt tillfälle inleda förhandlingar med tredjelandet för att avhjälpa den uppkomna situationen.

Möjligheten för kommissionen att besluta om adekvat skyddsnivå enligt artikel 25.6 har utnyttjats i förhållande till vissa länder och områden. Av 13 § personuppgiftsförordningen och bilaga 1 till förordningen framgår i vilken utsträckning personuppgifter får överföras till ett tredjeland, eller till vissa mottagare i ett tredjeland, som har en adekvat dataskyddsnivå.

Adekvat skyddsnivå innebär att överföring alltid är tillåten

Medlemsstaterna ska alltså, på samma sätt som i dag, vara bundna av kommissionens beslut att ett tredjeland eller en internationell organisation har en adekvat skyddsnivå. Detsamma gäller ett beslut att ett tredjeland eller en internationell organisation inte längre uppfyller kraven på adekvat skyddsnivå. Även om ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå, ska det enligt artikel 36.7 fortfarande vara möjligt att i vissa fall föra över personuppgifter dit om lämpliga skyddsåtgärder enligt artikel 37 säkerställs eller ett undantag för särskilda situationer i artikel 38 är tillämpligt.

Merparten av artikel 36 behandlar kommissionens arbetsuppgifter och kräver därmed inga lagstiftningsåtgärder. Artiklarna 36.1 och 36.3 bör däremot, som föreslås av utredningen, genomföras i ramlagen. Av paragrafen bör framgå att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att landet eller organisationen säkerställer en adekvat nivå för skyddet av personuppgifter. Detsamma bör gälla om kommissionen har beslutat att det finns en adekvat skyddsnivå i en viss geografisk eller på annat sätt angiven del av ett tredjeland, vilket motsvarar direktivets uttryck ett territorium eller en eller flera specificerade sektorer inom ett tredjeland. Ett sådant beslut skulle kunna avse t.ex. en region eller en viss myndighet i ett tredjeland. Förutsättningarna för överföring av personuppgifter till ett

tredjeland eller en internationell organisation ska också vara uppfyllda för att personuppgifter ska få överföras.

Att kommissionen har återkallat ett beslut om adekvat skyddsnivå bör likställas med att det saknas ett sådant beslut. Det förhållandet att det inte längre finns en adekvat skyddsnivå hindrar inte att personuppgifterna överförs med stöd av någon av de andra tillåtna grunderna för överföring (lämpliga skyddsåtgärder eller undantag i särskilda situationer). Det följer av övriga bestämmelser i ramlagen. Både *Uppsala universitet* och *Dataskydd.net* har lyft frågan om tillsynsmyndighetens roll vid tveksamheter om adekvat skyddsnivå kan anses föreligga trots ett föreliggande kommissionsbeslut. Regeringen behandlar denna fråga i avsnitt 11.9.

14.5 Tillräckliga skyddsåtgärder

Regeringens förslag: Om det inte finns något beslut om adekvat skyddsnivå, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade, eller om den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för uppgifterna.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Polismyndigheten* påpekar att individuell prövning av skyddsnivån i ett land kommer att vara mycket svår att genomföra utom kontorstid.

Skälen för regeringens förslag

Innehållet i direktivet

Även om det inte finns något beslut av kommissionen om adekvat skyddsnivå får personuppgifter överföras till ett tredjeland eller en internationell organisation om lämpliga skyddsåtgärder kan säkerställas i det enskilda fallet. Enligt artikel 37.1 får personuppgifter överföras till ett tredjeland eller en internationell organisation om lämpliga skyddsåtgärder för personuppgifter har fastställts i ett rättsligt bindande instrument, eller om den personuppgiftsansvarige har bedömt alla omständigheter kring överföringen och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna ändå föreligger. Dessutom ska förutsättningarna för överföring i artikel 35 vara uppfyllda.

Som exempel på rättsligt bindande instrument anges i skäl 71 rättsligt bindande bilaterala avtal som har ingåtts av medlemsstaterna och genomförts i staternas rättsordningar och som kan åberopas av registrerade. De bilaterala avtalen ska i sådana fall sörja för att kraven på dataskydd uppfylls och att registrerades rättigheter, däribland rätten till effektiv administrativ eller rättslig prövning, respekteras.

Vid bedömningen av om det finns lämpliga skyddsåtgärder för personuppgifter bör enligt skäl 71 den personuppgiftsansvarige kunna beakta sådana samarbetsavtal som ingåtts mellan Europol eller Eurojust och tredjeland och som medger utbyte av personuppgifter. Det bör också

kunna beaktas att överföringen kommer att omfattas av tystnadsplikt och att personuppgifterna inte kommer att behandlas i annat syfte än det för vilket de överfördes. Dessutom bör den personuppgiftsansvarige beakta att personuppgifterna inte kommer att användas för att göra framställningar om, meddela eller verkställa ett dödsstraff eller någon annan form av grym eller omänsklig behandling. Den personuppgiftsansvarige bör också kunna begära ytterligare skyddsåtgärder.

Nuvarande reglering

Enligt artikel 26.2 i 1995 års dataskyddsdirektiv får en medlemsstat tillåta att personuppgifter överförs till ett tredjeland som inte säkerställer en adekvat skyddsnivå om den personuppgiftsansvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas och för utövandet av motsvarande rättigheter. Sådana garantier kan framgå av lämpliga avtalsklausuler. Artikeln har genomförts i 35 § andra stycket personuppgiftslagen som ger regeringen, eller den myndighet som regeringen bestämmer, möjlighet att meddela föreskrifter om undantag från överföringsförbudet i personuppgiftslagen om det finns tillräckliga garantier till skydd för de registrerades rättigheter. I enskilda fall får regeringen också besluta om undantag på sådan grund eller överlåta till tillsynsmyndigheten att fatta sådana beslut. Regeringen får vidare enligt 35 § första stycket personuppgiftslagen meddela föreskrifter om generella undantag från förbudet mot överföring av personuppgifter, när överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Av 13 § personuppgiftsförordningen och bilaga 2 till förordningen framgår i vilken utsträckning personuppgifter får överföras till ett tredjeland med stöd av vissa standardavtalsklausuler. Ytterligare avtal som har ingåtts med tredjeland har genomförts i Sverige genom 13 a § personuppgiftsförordningen och bilaga 3 till förordningen.

Enligt 7 § andra stycket 2013 års lag, som genomför bl.a. artikel 13.3 a i dataskyddsrambeslutet, får personuppgifter överföras även om kravet på adekvat skyddsnivå inte är uppfyllt, om mottagaren i det enskilda fallet tillhandahåller tillräckliga skyddsåtgärder för personuppgifterna.

Överföring är tillåten om det finns tillräckliga skyddsåtgärder

Det bör, som utredningen föreslår, i ramlagen tas in en bestämmelse om att personuppgifter får överföras till ett tredjeland eller en internationell organisation, trots att det inte finns ett beslut om adekvat skyddsnivå, om lämpliga skyddsåtgärder säkerställs för personuppgiftsbehandlingen där. Paragrafen bör motsvara innehållet i artikel 37.1. Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation ska också vara uppfyllda för att personuppgifter ska få överföras.

I enlighet med artikel 37.1 a bör för det första lämpliga skyddsåtgärder kunna föreligga om ett avtal säkerställer skyddet för personuppgifter. Ett sådant avtal är dataskyddskonventionen (se avsnitt 4.9). Det har också träffats ett avtal mellan USA och EU om skydd av personuppgifter i samband med förebyggande, utredning, avslöjande och lagföring av brott (kallat Umbrella agreement). Avtalet bör betraktas som ett sådant avtal

som ger tillräckliga garantier till skydd för behandlingen av personuppgifter. Även andra avtal om internationellt samarbete som innehåller bestämmelser om dataskydd och som respekterar registrerades rättigheter kan garantera tillräckligt skydd för personuppgifter som överförs.

För det andra bör personuppgifter få överföras om den personuppgiftsansvarige har tagit hänsyn till alla omständigheter kring överföringen och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger. Innebörden är att överföringen är tillåten om den behöriga myndighet som personuppgifterna överförs till säkerställer lämpliga skyddsåtgärder för personuppgifterna.

Direktivet använder uttrycket ”lämpliga skyddsåtgärder”. Det kan ge intryck av att den som vill överföra personuppgifter kan göra en skönsmässig bedömning av vilka skyddsåtgärder som är lämpliga, vilket inte är avsikten. I 2013 års lag används uttrycket ”tillräckliga skyddsåtgärder”, vilket är en lämpligare formulering. Utredningen föreslår att formuleringen ”skyddsåtgärder för personuppgifter som ger tillräckliga garantier till skydd för registrerades rättigheter” används beträffande skydd som garanteras genom avtal. Mot den bakgrunden anser regeringen i likhet med utredningen att det i den bestämmelse som genomför artikel 37.1 b bör föreskrivas att den behöriga myndighet som personuppgifterna överförs till på annat sätt än genom avtal ska garantera tillräckligt skydd för uppgifterna. Tillräckliga skyddsåtgärder kan då användas som ett samlingsbegrepp både för garantier genom avtal och för andra garantier.

När tillräckliga skyddsåtgärder inte garanteras genom ett avtal ska den personuppgiftsansvarige, inför överföring av personuppgifter till ett tredjeland eller en internationell organisation, bedöma alla omständigheter kring överföringen. Vid bedömningen bör den personuppgiftsansvarige t.ex. kunna beakta att den som ska behandla uppgifterna i tredjelandet eller den internationella organisationen kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförts. Kommer personuppgifterna att omfattas av sekretess efter att de överförts till ett tredjeland eller en internationell organisation kan det också vägas in vid bedömningen av om det finns tillräckliga skyddsåtgärder. Den personuppgiftsansvarige bör även kunna beakta vilka regler som gäller för behandling av personuppgifter i tredjelandet eller vilka interna rutiner som tillämpas i den internationella organisation dit personuppgifterna ska föras.

Prövningen av ett lands skyddsnivå ska göras med utgångspunkt i omständigheterna i det enskilda fallet. Det är alltså inte tillräckligt att det t.ex. årligen görs en bedömning av förhållandena i ett visst tredjeland eller hos en viss organisation och att den bedömningen sedan generellt läggs till grund för beslut att överföra personuppgifter dit. En annan sak är att överföring av vissa personuppgifter kan vara standardbetonad och ske regelbundet till vissa mottagare. Är det fråga om sådana rutinöverföringar kan det enligt regeringens mening vara tillräckligt att kontrollera skyddsnivån t.ex. någon gång per år eller när det i övrigt bedöms påkallat.

För att tillsynsmyndigheten ska kunna säkerställa att prövningen av skyddsnivån varit fullgod är det lämpligt att en hänvisning görs i det enskilda fallet till vilka dokument och eventuella upplysningar som har

legat till grund för bedömningen. Den omständigheten att det, som *Polismyndigheten* påpekar, ibland kan vara svårt att göra en prövning fråntar inte en myndighet ansvaret att göra erforderliga kontroller.

14.6 Undantag i särskilda situationer

14.6.1 Överföringen ska vara nödvändig i en särskild situation

Regeringens förslag: Om det inte finns något beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder får en överföring eller en samling av överföringar av personuppgifter göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig i vissa särskilda undantagssituationer.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Polismyndigheten* ser positivt på de möjligheter till undantag i särskilda situationer som tas upp i förslaget. *Datainspektionen* konstaterar att förslaget i denna del innebär en utvidgning i förhållande till nuvarande reglering avseende möjligheten att överföra personuppgifter till tredjeland i särskilda undantagssituationer och efterfrågar analys av eventuella negativa effekter för den personliga integriteteten.

Skälen för regeringens förslag

Innehållet i direktivet

Finns det inte något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder får en överföring, eller en kategori av överföringar, av personuppgifter endast äga rum i särskilda undantagssituationer som räknas upp i artikel 38.1. Förutsättningarna för att överföra personuppgifter till ett tredjeland eller en internationell organisation enligt artikel 35 ska dock alltid vara uppfyllda.

De situationer som anges i artikel 38.1 är att överföringen ska vara nödvändig för att

a) skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person,

b) skydda den registrerades berättigade intressen om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver det,

c) avvärja en omedelbar eller allvarlig fara för den allmänna säkerheten i en medlemsstat eller i ett tredjeland,

d) i ett enskilt fall förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot, förebygga och förhindra hot mot den allmänna säkerheten, och

e) i ett enskilt fall fastslå, göra gällande eller försvara rättsliga anspråk.

Nuvarande reglering

Enligt 7 § andra stycket 2013 års lag, som genomför artikel 13.3 a i dataskyddsrambeslutet, får, om kravet på adekvat skyddsnivå inte är uppfyllt, personuppgifter överföras i ett enskilt fall om överföringen är motiverad av ett berättigat intresse hos den som uppgifterna avser eller av ett särskilt viktigt allmänt intresse eller om mottagaren i det enskilda fallet tillhandahåller tillräckliga skyddsåtgärder för personuppgifterna.

Överföring är tillåten bara för att tillgodose viktiga intressen

Eftersom direktivet reglerar all personuppgiftsbehandling inom tillämpningsområdet kommer överföringsreglerna i ramlagen att tillämpas i fler situationer än motsvarande reglering i 2013 års lag. Den lagen är bara tillämplig beträffande sådana personuppgifter som Sverige har fått från en annan EU-medlemsstat, Island, Norge, Schweiz, Liechtenstein eller ett EU-organ eller EU-informationssystem. Det är därför av stor vikt att det i ramlagen tydligt regleras vad som bör gälla i de fall där ett visst tredjeland eller en viss organisation inte omfattas av ett beslut om adekvat skyddsnivå och där inte heller tillräckliga skyddsåtgärder garanteras. I enskilda fall kan det nämligen, trots bristen på skydd för personuppgifter, vara angeläget att kunna föra över vissa personuppgifter till ett sådant land eller en sådan organisation.

Ett exempel på när personuppgifter kan behöva överföras, trots att kraven på adekvat skyddsnivå och tillräckliga skyddsåtgärder inte är uppfyllda, kan vara att en misstänkt har överlämnats till Sverige enligt den europeiska arresteringsordern men har lyckats fly från lagföring eller verkställighet av straff och antas befinna sig i ett land utanför EU från vilket svenska myndigheter begär honom eller henne utlämnad. Ett annat exempel kan vara att svenska myndigheter har information om att en misstänkt terrorist befinner sig här i landet men personen identifieras först när han eller hon har rest till ett tredjeland och kan antas komma att begå brott där.

Det bör därför tas in en bestämmelse i ramlagen om att personuppgifter får överföras till ett tredjeland eller en internationell organisation, trots att det inte finns ett beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder, om överföringen är nödvändig i vissa särskilda undantagssituationer. Paragrafen bör motsvara innehållet i artikel 38.1. De särskilda situationerna behandlas i det följande.

Som *Datainspektionen* konstaterar innebär direktivets bestämmelser och förslaget till ramlag i denna del att ytterligare undantagssituationer då det är möjligt att överföra personuppgifter till tredjeland tillkommer utöver vad som gäller i dag. Den omständigheten ska emellertid inte innebära att ett fullgott skydd för den personliga integriteten äventyras. Direktivet ställer också krav på att skyddsnivån i detta avseende inte undergrävs (se ovan avsnitt 14.3.1) Det bör även i sammanhanget understrykas att samtliga allmänna förutsättningar för överföring alltid ska vara uppfyllda för att personuppgifter ska få överföras. Detta gäller alltså även i de särskilda undantagsfallen.

En nyhet i direktivet är uttrycket ”en kategori av överföringar av personuppgifter”. I den engelska språkversionen av direktivet talas det om ”a category of transfers” och i den tyska används uttrycket ”eine Katagorie von Übermittlungen”. Någon förklaring till vad som avses kan inte utläsas av direktivet. I dataskyddsförordningens bestämmelse om överföring av personuppgifter till tredjeland i särskilda situationer, artikel 49, talas det om ”uppsättning av överföringar”. Det engelska uttrycket som används där är ”set of transfers” och det tyska är ”Reihe von Übermittlungen”, vilka motsvarar den svenska språkversionen.

Ordet kategori används i andra artiklar, t.ex. kategorier av registrerade i artikel 6 och särskilda kategorier av personuppgifter i artikel 10. I dessa fall handlar det om olika grupper av personer, t.ex. personer som dömts för brott eller brottsoffer, respektive typer av personuppgifter, t.ex. genetiska uppgifter och uppgifter om hälsa och sexualliv. I artikel 14 b och c talas det om kategorier av personuppgifter respektive kategorier av mottagare. Kategorier av mottagare kan avse vilken typ av myndighet som får personuppgifterna, t.ex. domstolar.

Det är svårt att avgöra vad som avses med kategorier av överföringar bara genom att jämföra med hur ordet kategori används i andra artiklar. Regeringen delar utredningens bedömning att det ligger närmare till hands att anta att det rör sig om överföringar som på något sätt är samlade, antingen för att det rör sig om flera överföringar av samma typ av personuppgifter till olika mottagare, flera överföringar i ett ärende eller överföringar av samma personuppgifter till flera mottagare samtidigt. Som exempel kan nämnas att det i ett tredjeland utreds brott av en större liga som har anknytning till Sverige och myndigheter i tredjelandet begär att få utdrag ur belastningsregistret på samtliga misstänkta. Ett annat exempel kan vara om det till ett tredjeland lämnas ut en digital upptagning från en kameraövervakning och det på upptagningen finns flera personuppgifter i form av personer, fordon och andra indirekta personuppgifter. En utskrift från hemlig avlyssning av elektronisk kommunikation som skickas till ett tredjeland eller en internationell organisation kan t.ex. innehålla uppgifter om olika personer som förekommer i en förundersökning.

Regeringen delar utredningens uppfattning att uttrycket samling av överföringar bör användas i stället för kategori av överföringar.

14.6.2 Enskildas vitala intressen

Regeringens förslag: I undantagsfall får personuppgifter överföras om det är nödvändigt för att värna den registrerades eller någon annan fysisk persons vitala intressen.

Utredningens förslag överensstämmer i sak med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

Enligt artikel 38.1 a får en överföring, eller en kategori av överföringar, av personuppgifter göras till ett tredjeland eller en internationell organisation om det är nödvändigt för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person.

I 34 § första stycket d personuppgiftslagen, som genomför artikel 26.1 e i 1995 års dataskyddsdirektiv, föreskrivs att personuppgifter, trots det generella förbudet, får överföras till ett tredjeland om överföringen är nödvändig för att vitala intressen för den registrerade ska kunna skyddas.

Överföring för att värna enskildas vitala intressen

Den första undantagssituationen avser enligt artikel 38.1 a fall där överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person. Det bör tas in en regel i ramlagen som motsvarar innehållet i artikeln.

I den svenska språkversionen av 1995 års dataskyddsdirektiv anges i artikel 7 d, som en allmän princip för behandling av personuppgifter, att behandlingen ska vara nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade. I andra språkversioner av det direktivet används i stället uttryck som vitala eller livsviktiga intressen. I skäl 31 till det direktivet används uttrycket ”intressen som är av avgörande betydelse för den registrerades liv”. I artikel 26.1 e i 1995 års dataskyddsdirektiv, som föreskriver undantag från kravet på adekvat skyddsnivå vid överföring till tredjeland, används uttrycket ”intressen som är av avgörande betydelse för den registrerade”. På grund av den osäkerhet som har rått om bestämmelsen i 1995 års direktiv enbart syftar på sådant som är livsviktigt (gäller liv eller död) eller om även sådant som ”bara” är av grundläggande betydelse avses, valde lagstiftaren att i personuppgiftslagen använda uttrycket ”vitala intressen”. Vitala intressen ansågs i svenskan ha såväl en snävare som en bredare innebörd (SOU 1997:39 s. 361).

Det talas i den svenska språkversionen av det nya direktivet och dataskyddsförordningen om intressen som är av grundläggande betydelse eller om grundläggande intressen. I skäl 112 till dataskyddsförordningen används uttrycket ett intresse som är väsentligt för den registrerades eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv. I den tyska språkversionen av direktivet används uttrycket ”lebenswichtiger Intressen”, dvs. livsviktiga intressen, medan det i den engelska versionen talas om ”vital interests”. I övriga språkversioner används uttryck som till svenska kan översättas med vitala intressen, t.ex. ”des intérêts vitaux” på franska och ”los intereses vitales” på spanska. Det är oklart varför formuleringen ”intressen som är av grundläggande betydelse” – som kan tolkas som mer vittomfattande än vitala intressen – har använts i den svenska versionen.

Att ”vitala intressen” används i personuppgiftslagen och därmed är ett inarbetat uttryck talar för att välja den formuleringen även i ramlagen. Vitala intressen är också det uttryck som används i andra språkversioner av direktivet. Regeringen håller därför med utredningen om att ”vitala

intressen” är det uttryck som bör användas. Med det bör förstås att det ska vara fråga om ett väsentligt intresse för den enskilde. Det kan röra liv, hälsa eller något annat som är av avgörande betydelse för den enskilde.

Åtgärden ska vara nödvändig för att skydda vitala intressen för den registrerade eller en annan person. Vilken annan person det kan vara fråga om kan inte utläsas av direktivet. Någon annan än en fysisk person kan det inte vara fråga om, eftersom målsättningen med direktivet är ett ökat skydd för fysiska personer. Utöver det bör den personkrets som ska omfattas av undantaget inte begränsas ytterligare i ramlagen. Det bör således framgå att överföringen ska vara nödvändig för att skydda vitala intressen för den registrerade eller för en annan fysisk person.

14.6.3 Registrerades berättigade intressen

Regeringens förslag: I undantagsfall får personuppgifter överföras om det är nödvändigt för att värna den registrerades berättigade intressen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget i denna del.

Skälen för regeringens förslag: I artikel 38.1 b regleras den situationen att överföringen av personuppgifter är nödvändig för att skydda den registrerades berättigade intressen, om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver det.

Enligt 7 § andra stycket 2013 års lag, som genomför bl.a. dataskyddsrambeslutets artikel 13.3 a i, får personuppgifter överföras trots att kravet på adekvat skyddsnivå inte är uppfyllt, om överföringen är motiverad av ett berättigat intresse hos den som uppgiften avser.

Medlemsstaterna får välja om det ska föreskrivas undantag till skydd för den registrerades berättigade intressen. Liksom utredningen anser regeringen att den möjligheten bör utnyttjas. Ett särskilt skydd för registrerades berättigade intressen finns redan i dag i 2013 års lag och motsvarande skydd bör finnas även fortsättningsvis. Behovet tillgodoses inte genom de övriga undantagen för särskilda situationer. Rent språkligt innefattas t.ex. inte alla intressen som kan vara berättigade i vitala intressen. I Svenska Akademiens Ordbok förklaras ordet berättigad som någon som fått något tilldelat sig eller förvärvat något, eller som är i sin fulla rätt att göra något. Berättigad kan också innebära att något är rättmätigt, välgrundat eller grundat på fullgiltiga skäl. Det behöver alltså inte vara fråga om något som är livsviktigt eller annars av avgörande betydelse för den registrerade. En bestämmelse som motsvarar artikel 38.1 b bör tas in i ramlagen. Uttrycket berättigat intresse bör användas eftersom det är inarbetat.

I ärenden om utlämning för brott eller övertagande av lagföring kan personuppgifter om den misstänkte behöva överföras t.ex. för att ge den andra staten underlag för att bedöma om det finns tillräcklig grund för att utlämna personen eller att överta lagföringen. Det kan vara ett berättigat intresse för den misstänkte att lagföring kommer till stånd antingen i

Sverige eller i den andra staten. Ett annat exempel på berättigat intresse kan vara att en misstänkt begär att ett vittne som befinner sig i ett tredjeland ska förhöras där.

14.6.4 Myndigheters intresse i enskilda fall

Regeringens förslag: I undantagsfall får personuppgifter överföras om det är nödvändigt för att en behörig myndighet i ett enskilt fall ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 38.1 d får en överföring, eller en kategori av överföringar, av personuppgifter – trots avsaknad av beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder – göras till ett tredjeland eller en internationell organisation om överföringen är nödvändig i det enskilda fallet för de ändamål som omfattas av direktivets tillämpningsområde. Bestämmelsen är till för att tillgodose behöriga myndigheters intresse av att personuppgifter i ett specifikt fall ska kunna överföras till ett tredjeland eller en internationell organisation, trots att landet eller organisationen dit uppgifterna ska överföras inte omfattas av ett beslut om adekvat skyddsnivå och det inte heller finns tillräckliga skyddsåtgärder för personuppgifterna.

Överföring för myndighetsintressen

En bestämmelse som motsvarar artikel 38.1 d bör, som utredningen föreslår, tas in i ramlagen. Det är viktigt att behöriga myndigheter har möjlighet att i enskilda fall överföra personuppgifter till tredjeland eller internationella organisationer. Utan en sådan möjlighet försvåras brottsbekämpning och lagföring. Om polisen t.ex. får tillförlitliga uppgifter om ett nära förestående attentat från personer kopplade till ett visst tredjeland måste information kunna utbytas med behöriga myndigheter där, även om det inte finns ett beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder garanteras. Överföringen ska vara nödvändig för något syfte som omfattas av ramlagens tillämpningsområde. Att i regeln uttryckligen ange vilka ändamål som avses blir tydligare än att hänvisa till den paragraf där tillämpningsområdet regleras.

Situationer som skulle kunna göra det nu aktuella undantaget tillämpligt är om personuppgifter behöver överföras från Sverige till ett tredjeland för delgivning, bevisupptagning eller straffverkställighet där, eller för att få en person utlämnad därifrån för att tillgodose svenska behov. Undantaget kan även bli tillämpligt om ett tredjeland eller en internationell organisation på motsvarande sätt behöver få tillgång till svenska personuppgifter för brottsbekämpning, lagföring eller straffverkställighet.

Överföringen ska vara nödvändig i det enskilda fallet t.ex. för att få fram upplysningar om en person som är misstänkt för ett mord i Sverige och som polisen tror uppehåller sig i ett tredjeland. Ett annat exempel kan vara att överföringen är nödvändig för att kunna delge en i USA bosatt målsägande kallelse till en brottmålsrättegång vid svensk domstol.

I direktivet görs klart att undantaget bara får utnyttjas i enskilda fall. Man skulle kunna hävda att varje överföring av personuppgifter avser enskilda fall, men det kan noteras att ingen sådan begränsning görs när det gäller undantagen till skydd för enskildas intressen. Regeringen instämmer i utredningens tolkning att inskränkningen till enskilda fall i denna punkt får ses som ett uttryck för att undantaget för myndighetsintressen inte får utnyttjas för bl.a. storskaliga överföringar (se skäl 72). Mot den bakgrunden bör det av lagtexten framgå att det ska vara fråga om enskilda fall.

14.6.5 Rättsliga anspråk i enskilda fall

Regeringens förslag: I undantagsfall får personuppgifter överföras om det i ett enskilt fall är nödvändigt för att kunna fastställa, göra gällande eller försvara ett sådant rättsligt anspråk som hänför sig till ett sådant syfte som omfattas av ramlagens tillämpningsområde.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Innehållet i direktivet och nuvarande reglering

I artikel 38.1 e regleras den situationen att överföring av personuppgifter är nödvändig i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk som hänför sig till de syften som omfattas av direktivets tillämpningsområde. Även här pekar direktivet ut att det ska vara fråga om en överföring som är nödvändig i ett enskilt fall.

I 34 § första stycket c personuppgiftslagen, som genomför bl.a. artikel 26.1 d i 1995 års dataskyddsdirektiv, föreskrivs att personuppgifter, trots överföringsförbudet, får överföras till ett tredjeland om överföringen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. Det krävs inte att det rättsliga anspråket är knutet till något särskilt ändamål.

Överföring för att skydda rättsliga anspråk

En bestämmelse som motsvarar artikel 38.1 e bör tas in i ramlagen. Rättsligt anspråk används i dag förutom i 34 § första stycket c också i 16 § första stycket c personuppgiftslagen, där det anges som en grund för att få behandla känsliga personuppgifter. I kommentaren till sistnämnda bestämmelse sägs att det inte är helt klart vad som avses med rättsliga anspråk. Förmodligen avses sådana anspråk om vilka man kan föra talan i domstol eller ett domstolsliknande organ och som kan utkrävas av eller med hjälp av statsmakterna, t.ex. Kronofogdemyndigheten (Öman m.fl.

s. 301). I den tyska versionen av 1995 års dataskyddsdirektiv (artikel 8.2 e) talas det om ”vor Gericht”, alltså inför domstol.

Det råder viss oklarhet om vad som avses med ett rättsligt anspråk i personuppgiftslagen. Regeringen delar ändå utredningens bedömning att det uttrycket bör användas i ramlagen, eftersom uttrycket är inarbetat. Dessutom är det betydligt enklare att identifiera vad som kan vara ett rättsligt anspråk inom ramlagens tillämpningsområde. Det kan t.ex. vara ett enskilt anspråk i anledning av brott. Även uttrycken fastställa, göra gällande och försvara är inarbetade och bör användas i ramlagen.

Av paragrafen bör det framgå att det rättsliga anspråket ska hänföra sig till att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. I stället för att upprepa det i paragrafen kan en hänvisning kan göras till bestämmelsen om överföring för att tillgodose myndighetsintressen (se avsnitt 14.6.4). I likhet med vad som gäller för myndighetsintressena bör det framgå att undantaget till skydd för rättsliga anspråk bara får utnyttjas i enskilda fall.

14.6.6 Allvarlig fara för allmän säkerhet

Regeringens förslag: I undantagsfall får personuppgifter överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: Enligt artikel 38.1 c får personuppgifter överföras, trots avsaknaden av beslut om adekvat skyddsnivå och tillräckliga skyddsåtgärder, om överföringen är nödvändig för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland.

Det finns ett liknande krav på fara för allmän säkerhet i 7 § tredje stycket 2013 års lag, som genomför artikel 13.2 i dataskyddsrambeslutet, för att få överföra personuppgifter till ett tredjeland eller ett internationellt organ när det på grund av tidsbrist inte har gått att utverka ett förhandsmedgivande till överföringen.

Det nu aktuella undantaget bör återspeglas i ramlagen. Av paragrafen bör det framgå att personuppgifter i undantagsfall får överföras till ett tredjeland eller en internationell organisation, om överföringen är nödvändig för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Det är som utredningen föreslår tillräckligt att det, på samma sätt som i 2013 års lag, anges att det ska vara fara för allmän säkerhet. Tillägget i artikeln att det gäller säkerheten i en medlemsstat eller ett tredjeland gör att tillämpningsområdet omfattar alla stater. Det saknar därför materiellt innehåll. Formuleringen ”den allmänna säkerheten i en stat” skulle inte heller bidra till någon ökad klarhet.

Bestämmelsen skulle t.ex. kunna tillämpas om överföringen är nödvändig för att avvärja ett terroristattentat eller en flygplanskapning. Eftersom det typiskt sett är fråga om en överhängande fara för att något ska hända får prövningen i dessa fall göras med utgångspunkt i att åtgärden kan

antas vara nödvändig för att avvärja faran. Att faran inte förverkligas behöver inte innebära att överföringen har varit otillåten. Bedömningen måste självfallet göras med hänsyn till vad som är känt när prövningen görs.

14.6.7 En intresseavvägning ska göras i vissa fall

Regeringens förslag: Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs i det enskilda fallet för ett myndighetsintresse eller för att kunna fastslå, göra gällande eller försvara ett rättsligt anspråk.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* anser att den föreslagna intresseavvägningen fyller en mycket viktig funktion för integritetsskyddet, men att det tydligare bör framgå att integritetsskyddet är ett intresse som ska beaktas vid avvägningen. Inspektionen ifrågasätter vidare om utredningens förslag till reglering av intresseavvägningen inte ger ett sämre skydd än vad direktivet medger.

Skälen för regeringens förslag: I artikel 38.2 föreskrivs att personuppgifter inte får överföras till ett tredjeland eller en internationell organisation om den överförande behöriga myndigheten fastställer att den registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset av en sådan överföring som avses i punkt 1 d och e, dvs. myndigheters intresse av brottsbekämpning, lagföring, straffverkställighet och ordningshållning och rättsliga anspråk som hänför sig till sådana ändamål. Det ska alltså göras en intresseavvägning mellan skyddet för den enskildes rättigheter och friheter och det allmännas intresse av att överföringen görs för dessa ändamål. Väger den enskildes intresse av skydd mot kränkning av rättigheter och friheter tyngre än det allmännas intresse av att personuppgifterna överförs, får uppgifterna inte överföras. Sådana rättigheter och friheter kan t.ex. vara yttrandefrihet och religionsfrihet.

Artikeln bör genomföras i ramlagen. Lagtexten bör ansluta nära till direktivets text. Det bör framgå att personuppgifter inte får överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs i det enskilda fallet för något av de två nu aktuella ändamålen.

Regeringen anser, till skillnad från *Datainspektionen*, att den föreslagna utformningen av bestämmelsen är lämplig och på ett fullgott sätt beskriver den intresseavvägning som ska göras enligt direktivet.

14.7 Vidareöverföring

Regeringens förslag: En svensk behörig myndighet får inte tillåta att sådana personuppgifter som en svensk myndighet har fått från en annan medlemsstat, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation om inte någon behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras.

Frågan om en svensk behörig myndighet ska medge vidareöverföring till ett tredjeland eller en internationell organisation av personuppgifter som en svensk myndighet har lämnat till en annan medlemsstat som överfört uppgifterna till ett tredjeland eller en internationell organisation, ska bedömas med hänsyn till alla kända omständigheter som har samband med överföringen. Särskild vikt ska läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten och nivån på skyddet av personuppgifter i tredjelandet eller hos den internationella organisationen som uppgifterna ska vidareöverföras till.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt över förslaget i denna del.

Skälen för regeringens förslag

Innehållet i direktivet

Regleringen av överföring av personuppgifter till ett tredjeland eller en internationell organisation omfattar även vidareöverföring av personuppgifter från ett tredjeland eller en internationell organisation till ett annat tredjeland eller en annan internationell organisation. Det följer bl.a. av en bisats i artikel 35.1, i vilken det sägs att de behöriga myndigheterna endast får överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation, inklusive för vidareöverföring till ett annat tredjeland eller en annan internationell organisation […].

Av artikel 35.1 e framgår att det är den behöriga myndigheten som gjorde den ursprungliga överföringen eller en annan behörig myndighet i samma medlemsstat, som ska godkänna vidareöverföringen till ett annat tredjeland eller en annan internationell organisation. Myndigheten ska beakta alla relevanta faktorer, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter hos den som ska motta uppgifterna om de vidareöverförs.

Med vidareöverföring avses att personuppgifter överförs från ett tredjeland antingen till ett annat tredjeland eller till en internationell organisation. Det kan också vara fråga om att personuppgifter överförs från en internationell organisation till en annan internationell organisation eller till ett tredjeland. Det är fråga om en överföring i tre led. Personuppgifterna som ska vidareöverföras kommer då från en medlemsstat som lämnat dem vidare till en annan medlemsstat som i sin tur har överfört dem

till ett tredjeland eller en internationell organisation som vidareöverför dem.

Direktivet utgår från att det är den medlemsstat som först lämnade personuppgifterna till en annan medlemsstat som ska godkänna vidareöverföringen från ett tredjeland till ett annat. Även om det är den medlemsstat som överförde personuppgifterna till ett tredjeland som förfogat över uppgifterna senast, och därför har lättast att överblicka om vidareöverföringen bör tillåtas, är det alltså den medlemsstat som uppgifterna ursprungligen kom från som ska godkänna att de vidareöverförs. Om ett tredjeland vänder sig till den medlemsstat som tredjelandet fick personuppgifterna från bör direktivet tolkas så att den medlemsstaten ska inhämta tillstånd till vidareöverföring från den medlemsstat som ursprungligen lämnade uppgifterna.

Medgivande till vidareöverföring

Bestämmelsen om vidareöverföring bör genomföras i ramlagen. Som artikeln är utformad förefaller det närmast som att det i nationell rätt ska föreskrivas vad ett tredjeland (eller en internationell organisation) ska beakta vid överföring av personuppgifter som kommer från en medlemsstat till ett annat tredjeland eller till en internationell organisation. Som utredningen konstaterar ligger det i sakens natur att det inte är möjligt att reglera det i svensk rätt, annat än genom möjligheten att ställa upp villkor för tredjelandets eller den internationella organisationens användning av personuppgifterna (se avsnitt 14.9). Regleringen i ramlagen bör i stället utgå från vad en svensk myndighet ska göra när den får en förfrågan från ett tredjeland eller en internationell organisation om att vidareöverföra personuppgifter som en svensk myndighet har fått från en annan medlemsstat.

Med vidareöverföring avses här den överföring av personuppgifter som görs efter att personuppgifterna har lämnat medlemssfären, dvs. mellan tredjeländer och internationella organisationer. Rent språkligt är det fråga om vidareöverföring även när en svensk myndighet lämnar vidare personuppgifter som kommer från en annan medlemsstat till ett tredjeland eller till en internationell organisation. Det är sådana situationer som regleras i 2013 års lag. I dessa fall, som behandlas i avsnitt 14.3.4, bör man även i fortsättningen tala om överföring till tredjeland eller internationella organisationer.

Av lagtexten bör följaktligen framgå att personuppgifter, som en svensk myndighet har fått från en annan medlemsstat och överfört till ett tredjeland eller en internationell organisation, inte får vidareöverföras till ett tredjeland eller en internationell organisation, om inte den svenska myndigheten inhämtat godkännande till vidareöverföringen från behörig myndighet i den andra medlemsstaten. Medgivande till vidareöverföring kan inhämtas antingen från den myndighet som gjorde den ursprungliga överföringen eller från en annan behörig myndighet i samma medlemsstat. Ett exempel kan vara att en tysk polismyndighet ursprungligen lämnade personuppgifterna till Polismyndigheten men att ärendet, när frågan om vidareöverföring väcks, handläggs av tysk åklagare. Det är då naturligt att medgivande inhämtas från den tyska åklagaren.

En begäran om medgivande till vidareöverföring kan givetvis även omfatta personuppgifter som har sitt ursprung i den svenska myndigheten, eftersom handläggningen i Sverige kan ha genererat information som innehåller fler personuppgifter än vad Sverige fick. Den svenska myndigheten får då ta ställning till hur de personuppgifterna ska hanteras. Det kan vara naturligt att ta upp den frågan i dialogen med den behöriga myndigheten i den medlemsstat som lämnade personuppgifterna till Sverige, eftersom det eventuellt kan påverka dess syn på om medgivande ska lämnas.

I artikeln talas det om vidareöverföring till ett annat tredjeland eller en annan internationell organisation. Regeringen delar utredningens bedömning att tanken inte kan vara att personuppgifter inte kan vidareöverföras från ett tredjeland till en internationell organisation och vice versa. Paragrafen bör därför inte formuleras så att överföringen ska göras till ett annat tredjeland eller en annan internationell organisation.

Exempel på vidareöverföring kan vara att Sverige har fått personuppgifter från Tyskland och överfört dessa till USA som i sin tur vill vidareöverföra uppgifterna till Kanada. Då måste ett medgivande inhämtas från Tyskland för att USA ska få lämna personuppgifterna vidare till Kanada. Om USA inte känner till att Sverige har fått uppgifterna från Tyskland kommer USA att vända sig till Sverige med frågan om personuppgifterna får vidareöverföras. I ett sådant läge kan inte Sverige medge vidareöverföringen utan att inhämta ett medgivande från Tyskland. Den situationen kan också uppkomma att USA i det nyss nämnda exemplet i stället vill vidareöverföra personuppgifterna till en internationell organisation, t.ex. FN. Även i det fallet måste Sverige inhämta ett medgivande till vidareöverföring från Tyskland.

Bedömningen av om svensk myndighet ska medge vidareöverföring

Av ramlagen bör det framgå vad en svensk myndighet ska ta hänsyn till när den tillfrågas om den kan medge vidareöverföring av personuppgifter som Sverige har lämnat till en annan medlemsstat som i sin tur har överfört uppgifterna till ett tredjeland eller en internationell organisation som vill vidareöverföra dem. Det bör framgå att det ska vara en svensk behörig myndighet som ska lämna medgivandet. Det bör antingen kunna vara den behöriga myndigheten som ursprungligen lämnade de svenska personuppgifterna till en annan medlemsstat eller en annan behörig myndighet i Sverige. Myndigheten bör beakta alla omständigheter som har samband med vidareöverföringen. Regeringen delar utredningens uppfattning att alla omständigheter är ett bättre ordval än alla relevanta faktorer. Av naturliga skäl kan bara sådana omständigheter som är kända beaktas. Sådana omständigheter som inte är relevanta bör den tillfrågade myndigheten kunna bortse från utan att det direkt framgår av lagtexten.

Vid bedömningen av om ett medgivande till vidareöverföring ska lämnas, bör särskild vikt läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten och skyddsnivån för personuppgifter i tredjelandet eller den internationella organisationen som uppgifterna ska vidareöverföras till.

I sammanhanget bör nämnas att bestämmelsen om förhandsmedgivanden i artikel 35.1 e tar sikte på medgivande i det enskilda fallet. Medgivandet ska alltså avse en viss vidareöverföring av personuppgifter till ett tredjeland eller en internationell organisation. Artikeln hindrar emellertid inte att medgivande ges generellt i förväg för vidareöverföringar mellan tredjeländer och internationella organisationer som kan komma att bli nödvändiga. Bestämmelsen i ramlagen bör därför utformas så att det blir möjligt.

14.8 Överföring till andra än behöriga myndigheter

14.8.1 Förutsättningarna för överföring till andra än behöriga myndigheter

Regeringens förslag: En myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet får i ett enskilt fall överföra personuppgifter till någon som inte är behörig myndighet i ett tredjeland.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionens* synpunkter gällande överföring till andra än behöriga myndigheter finns i avsnitt 14.8.4.

Skälen för regeringens förslag

Innehållet i direktivet

Enligt artikel 39 får behöriga myndigheter överföra personuppgifter, i enskilda och särskilda fall, direkt till mottagare som är etablerade i tredjeland under förutsättning att direktivets övriga bestämmelser efterlevs och att samtliga i artikeln uppräknade villkor är uppfyllda. Artikeln reglerar ett undantag från den allmänna principen i artikel 35.1 b att personuppgifter som ska överföras till ett tredjeland eller en internationell organisation ska lämnas till en behörig myndighet. Bestämmelser som meddelas med stöd av artikel 39.1 ska dock inte hindra tillämpningen av internationella avtal och ska alltså inte betraktas som undantag från befintliga bilaterala eller multilaterala internationella avtal på området för straffrättsligt och polisiärt samarbete.

En förutsättning för att personuppgifter ska få överföras till andra än behöriga myndigheter i ett tredjeland är att den överförande myndigheten är en sådan behörig myndighet som avses i artikel 3.7 a. Med det avses en offentlig myndighet som har till arbetsuppgift att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla den allmänna säkerheten. Någon hänvisning till artikel 3.7 b görs inte, vilket innebär att ett annat organ eller någon annan som har anförtrotts myndighetsutövning inom direktivets tillämpningsområde inte har rätt att överföra personuppgifter till andra än behöriga myndigheter.

Bakgrunden framgår av skäl 73 där följande uttalas. Myndigheter i medlemsstaterna som är verksamma inom direktivets tillämpningsom-

råde tillämpar bilaterala eller multilaterala internationella avtal, som har ingåtts med tredjeländer på området för straffrättsligt samarbete och polissamarbete, för att utbyta information. Informationsutbytet sker i princip genom eller i samarbete med de tredjeländernas behöriga myndigheter. Ibland kan dock de ordinarie förfaranden som kräver kontakt med en myndighet i ett tredjeland vara ineffektiva och olämpliga, framför allt för att överföringen inte kan utföras i tid, eller för att myndigheten i tredjelandet inte respekterar rättsstatsprincipen eller internationella människorättsliga normer och standarder. I sådana fall underlättar det om behöriga myndigheter kan överföra personuppgifter direkt till andra än behöriga myndigheter i dessa tredjeländer.

Övriga bestämmelser i direktivet måste också efterlevas. Det innebär bl.a. att förutsättningarna i artikel 35 – med undantag för kravet på att överföringen ska göras till en behörig myndighet – ska vara uppfyllda. Vidare ska de i artikel 39.1 särskilt uppräknade villkoren vara uppfyllda för att överföringen ska vara tillåten. Villkoren kommer att beskrivas mer ingående i det följande.

Överföring till någon annan än en behörig myndighet

Det finns tillfällen då det underlättar om en svensk myndighet kan överföra personuppgifter till ett tredjeland utan att behöva kanalisera dem via en behörig myndighet i det landet. Så kan vara fallet när det rör sig om en särskilt brådskande åtgärd och en kontakt med den behöriga myndigheten riskerar att försena åtgärden eller göra den meningslös. Ett exempel är att det finns misstankar om penningtvätt eller annan ekonomisk brottslighet, där möjligheten att snabbt spåra ekonomiska transaktioner kan vara avgörande för att ingripa mot pågående brott och det krävs kontakt med ett organ som inte är en behörig myndighet. Ett annat exempel kan vara att en svensk myndighet snabbt vill kunna stoppa en utbetalning på grund av misstankar om bedrägeri och då behöver kontakta en bank eller ett finansinstitut i ett tredjeland. Det kan också finnas ett akut behov av att direkt kontakta en person som riskerar att utsättas för ett allvarligt våldsbrott.

I dag är det också vanligt att Polismyndigheten i sin brottsutredande verksamhet överför personuppgifter till t.ex. Google och Facebook, för att få uppgift om vilken fysisk person som ligger bakom ett användarkonto eller alias. Arbetet skulle väsentligt fördröjas om varje enskild förfrågan skulle behöva gå via en behörig myndighet i tredjelandet.

Mot den bakgrunden delar regeringen utredningens bedömning att möjligheten att införa undantag från kravet på att överföringen ska göras till en behörig myndighet bör utnyttjas. Artikel 39.1 bör därför genomföras i ramlagen. Av paragrafen bör framgå att det under vissa förutsättningar är möjligt att i ett enskilt fall föra över personuppgifter till någon som inte är en behörig myndighet i ett tredjeland. Det kan exempelvis vara fråga om överföringar till företag eller privatpersoner i ett tredjeland.

Den som personuppgifterna överförs till ska vara etablerad i tredjelandet. Regeringen anser i likhet med utredningen att det bör vara tillräckligt att en fysisk person är stadigvarande bosatt och att en juridisk person har sitt säte eller ett fast driftsställe i tredjelandet för att anses vara

etablerad där. Kravet på etablering behöver inte framgå av lagtexten. Det är enligt regeringens mening tillräckligt att det anges att personuppgifter får överföras till andra än behöriga myndigheter i tredjeland.

Det behöver inte föreskrivas att det ska vara fråga om särskilda fall. Att det rör sig om konkreta fall där det finns ett särskilt behov av att överföra personuppgifter till någon som inte är en behörig myndighet i ett tredjeland ligger redan i uttrycket enskilda fall.

Endast en myndighet som har som arbetsuppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda och lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet bör ges möjlighet att utnyttja undantaget. Andra aktörer som är behöriga myndigheter i ramlagens mening bör alltså inte få göra sådana överföringar.

14.8.2 Överföringen ska vara absolut nödvändig

Regeringens förslag: För att personuppgifter ska få överföras till andra än behöriga myndigheter i ett tredjeland ska överföringen vara absolut nödvändig för att den svenska myndigheten ska kunna utföra en arbetsuppgift som den har ansvar för och som ligger inom ramlagens tillämpningsområde. Den som ska ta emot personuppgifterna ska informeras om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag: Det första villkoret för att personuppgifter ska få överföras till annan än en behörig myndighet i ett tredjeland är enligt artikel 39.1 a att överföringen är absolut nödvändig för att den överförande myndigheten ska kunna utföra en arbetsuppgift som den ansvarar för enligt unionsrätten eller nationell rätt för de ändamål som omfattas av direktivets tillämpningsområde. Enligt artikel 39.1 e ska den överförande myndigheten informera mottagaren om de specifika ändamål för vilket eller vilka mottagaren får behandla personuppgifterna, förutsatt att den behandlingen är nödvändig. Artiklarna 39.1 a och e bör genomföras i ramlagen. Det görs lämpligen genom att innehållet i dem anges som villkor för att personuppgifter ska få överföras till andra än behöriga myndigheter i ett tredjeland.

Överföringen ska alltså vara absolut nödvändig för att t.ex. en domstol ska kunna utföra en arbetsuppgift. För att markera att undantaget ska tillämpas restriktivt och att det kan bli fråga om överföring endast i undantagsfall bör uttrycket ”absolut nödvändigt” användas. Personuppgifter får således överföras endast om det är absolut nödvändigt för att den överförande myndigheten ska kunna utföra en arbetsuppgift som den ansvarar för inom ramlagens tillämpningsområde.

Vidare bör det föreskrivas att den svenska myndighet som överför personuppgifterna ska lämna information om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas av mottagaren. Det ligger i sakens natur att det inte går att i svensk rätt föreskriva att behandlingen i tredjelandet ska vara nödvändig.

14.8.3 Om överföring till behörig myndighet blir ineffektiv eller är olämplig

Regeringens förslag: Personuppgifter får överföras till någon som inte är behörig myndighet i ett tredjeland om det skulle vara ineffektivt eller olämpligt att överföra uppgifterna till en behörig myndighet där.

Regeringens bedömning: Skyldigheten att informera den behöriga myndigheten i tredjelandet om överföringen och undantag från skyldigheten kan regleras i förordning.

Utredningens förslag överensstämmer med regeringens förslag och bedömning.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag och bedömning

Överföring till behörig myndighet bör undvikas

Enligt artikel 39.1 c får personuppgifter överföras direkt till en mottagare som är etablerad i ett tredjeland om den överförande myndigheten anser att en överföring till en behörig myndighet i tredjelandet skulle bli ineffektiv eller vara olämplig. Det gäller i synnerhet om överföringen inte kan göras inom rimlig tid. Enligt artikel 39.1 d ska behörig myndighet i tredjelandet utan dröjsmål informeras, såvida det inte blir ineffektivt eller det är olämpligt att lämna informationen.

Villkoret i artikel 39.1 c bör framgå av ramlagen. I likhet med utredningen anser regeringen att det är tillräckligt att det av paragrafen framgår att det skulle vara ineffektivt eller olämpligt att överföra personuppgifterna till en behörig myndighet i mottagarlandet. I kravet på att det skulle vara ineffektivt att föra över personuppgifterna till en behörig myndighet ligger att handläggningen riskerar att fördröjas. Exempel på när det kan vara ineffektivt att gå via en behörig myndighet i ett tredjeland kan vara överföringar till företag som Google eller Facebook, där det kan röra sig om stora mängder personuppgifter som behöver överföras på kort tid och det kan vara av avgörande betydelse med ett snabbt svar.

I undantagsfall kan det vara olämpligt att överföra en personuppgift via den behöriga myndigheten. Om tidigare kontakter i ärendet med den behöriga myndigheten fått negativa konsekvenser för den svenska myndighetens handläggning bör det kunna vara ett sådant fall. Ett annat exempel är kontakter med ett krigshärjat tredjeland där det kanske inte finns någon behörig myndighet att kommunicera med eller där det är oklart vem som är behörig företrädare för staten. Då är det nödvändigt att kunna överföra personuppgifter till andra än behöriga myndigheter.

Det är den överförande myndigheten som ska bedöma om det skulle vara ineffektivt eller på annat sätt olämpligt att överföra personuppgifterna till en behörig myndighet.

Av artikel 39.1.d framgår att den behöriga myndigheten i tredjelandet utan dröjsmål ska informeras om överföringen om det inte är ineffektivt eller olämpligt.

Bestämmelser om informationsskyldigheten och undantag från den kan, som utredningen föreslår, regleras i förordning.

14.8.4 En intresseavvägning ska göras

Regeringens förslag: Personuppgifter får inte överföras till någon som inte är en behörig myndighet i ett tredjeland om den registrerades intresse av skydd mot kränkning av rättigheter och friheter väger tyngre än det allmännas intresse av att överföringen görs.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* efterfrågar djupare analys av risker som kan uppstå vid överföring till andra än behöriga myndigheter och efterfrågar ett tydliggörande av att de grundläggande förutsättningarna för överföring ska gälla även vid överföring till andra än behöriga myndigheter. Inspektionen anser vidare att den föreslagna intresseavvägningen fyller en mycket viktig funktion för integritetsskyddet men att det tydligare bör framgå att integritetsskyddet är ett intresse som ska beaktas vid avvägningen. Inspektionen ifrågasätter vidare om utredningens förslag till reglering av intresseavvägningen inte ger ett sämre skydd än vad direktivet medger.

Skälen för regeringens förslag: Utöver de redan nämnda villkoren för att personuppgifter ska få överföras till andra än behöriga myndigheter, ska enligt artikel 39.1 b den överförande myndigheten ha fastställt att ingen av den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset som gör överföringen nödvändig i det aktuella fallet. En intresseavvägning ska alltså göras.

En bestämmelse som motsvarar innehållet i artikeln bör, som utredningen föreslår, tas in i ramlagen. Intresseavvägningen påminner till viss del om den intresseavvägning som föreslås i avsnitt 14.6.7. Bestämmelsen bör därför utformas på liknande sätt. De intressen som ska vägas mot varandra är å ena sidan den registrerades intresse av skydd mot att hans eller hennes rättigheter och friheter kränks genom överföringen och å andra sidan det allmännas intresse av att personuppgifterna överförs. Väger den registrerades intresse av skydd tyngre får överföringen inte göras.

Till skillnad från *Datainspektionen* anser regeringen att de föreslagna bestämmelserna om överföring till andra än behöriga myndigheter väl uppfyller direktivets krav. Det ligger i sakens natur att det inte går att överblicka alla eventuella risker som kan uppstå. Regleringen kommer dock innebära att det ska röra sig om absolut nödvändiga överföringar i enskilda fall när överföring till behörig myndighet i tredjeland skulle vara ineffektiv eller olämplig. Därtill kommer kravet på information om ändamål till den som ska ta emot uppgifterna och dessutom en intresseavvägning. Mot den bakgrunden anser regeringen att den föreslagna regleringen ger ett godtagbart skydd för den enskilde. Regeringen delar

emellertid Datainspektionens uppfattning att en upplysning om att de grundläggande förutsättningarna för överföring till tredjeland och internationella organisationer måste vara uppfyllda även vid överföring till andra än behöriga myndigheter bör föras in i förslaget till bestämmelse.

14.9 Villkor för användningen av personuppgifter

14.9.1 Villkor som ställs upp av utländska myndigheter eller organ

Regeringens förslag: Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och gäller på grund av en överenskommelse med tredjelandet eller den internationella organisationen villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* ser positivt på förslagen i denna del och pekar på att det ur ett internationellt samarbetsperspektiv är av yttersta vikt att respektera en s.k. handling code och inte vidarebefordra uppgifter till tredje land om inte medgivande har inhämtats. *Dataskydd.net* avstyrker förslaget.

Skälen för regeringens förslag: När en utländsk myndighet eller internationell organisation överför personuppgifter till en svensk myndighet är det inte ovanligt att den ställer upp villkor för hur uppgifterna får användas. Det kan handla om för vilka ändamål de får användas eller hur länge uppgifterna får behandlas.

Det finns flera författningar som innehåller regler om vad som gäller när en svensk myndighet får personuppgifter från en utländsk myndighet och det ställs villkor för hur uppgifterna får användas. Sådana regler finns bl.a. i 6 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete, 5 kap. 1 § lagen (2000:562) om internationell rättslig hjälp i brottmål, 4 kap. 2 § lagen (2000:1219) om internationellt tullsamarbete och 5 § lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar. I 8 § första stycket 2013 års lag, som bl.a. genomför artikel 12 i rambeslutet, finns en regel om att svenska myndigheter ska följa villkor som begränsar möjligheten att använda personuppgifter som den fått från medlemsstater i EU, Island, Norge, Schweiz eller Liechtenstein, ett EU-organ eller ett EU-informationssystem. Sådana regler innebär att svenska myndigheter är skyldiga att följa de villkor som ställs i fråga om hur lämnad information får användas. Det gäller oavsett om villkoren skulle stå i strid med svensk lagstiftning (se bl.a. JO 2007/08 s. 57 angående tillämpningen).

Direktivet föreskriver inte någon skyldighet för medlemsstaternas myndigheter att följa sådana villkor som ett tredjeland eller en internationell organisation har ställt upp för användningen av personuppgifter som överförs av tredjelandet eller den internationella organisationen. Regeringen delar utredningens uppfattning att det ändå behövs en sådan reglering i ramlagen, bl.a. mot bakgrund av att den nuvarande regleringen inte

täcker ramlagens hela tillämpningsområde. Av paragrafen bör framgå att svenska myndigheter ska följa villkor som ställts upp av ett tredjeland eller en internationell organisation. Sådana användningsbegränsningar bör följas oavsett vad som annars är föreskrivet i lag eller annan författning. Paragrafen bör utformas efter mönster av andra liknande bestämmelser.

14.9.2 Villkor när personuppgifter överförs av svenska myndigheter

Regeringens förslag: En svensk behörig myndighet får, vid överföring av personuppgifter till ett tredjeland eller en internationell organisation, i ett enskilt fall ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till den enskildes rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens förslag till reglering innehåller inte något krav på att villkoren inte får strida mot en bindande internationell överenskommelse.

Remissinstanserna: *Skatteverket* anser att det av regleringen även bör framgå av att det krävs stöd i en bindande internationell överenskommelse.

Skälen för regeringens förslag: När en svensk behörig myndighet överför personuppgifter till ett tredjeland eller en internationell organisation finns det ibland skäl att ställa villkor som begränsar användningen av uppgifterna, t.ex. för vilket ändamål och hur länge de får behandlas. Behovet av sådana användningsbegränsningar visar sig normalt redan i samband med att en utländsk myndighet begär att få ut personuppgifter som finns tillgängliga hos en svensk myndighet eller att den svenska myndigheten behöver överföra sådana uppgifter. Att personuppgifterna förses med villkor för användningen kan ibland vara en förutsättning för att det ska anses vara lämpligt att överföra uppgifterna.

I dag finns det inom ramlagens tillämpningsområde bestämmelser i flera lagar om att svenska myndigheter under vissa förutsättningar får ställa upp villkor som begränsar möjligheten att använda uppgifter som lämnas till en annan stat. Det gäller 6 kap. 4 § lagen om internationellt polisiärt samarbete, 5 kap. 2 § lagen om internationell rättslig hjälp i brottmål, 2 kap. 7 § lagen om internationellt tullsamarbete och 6 § lagen om vissa former av internationellt samarbete i brottsutredningar. Lagarna i fråga reglerar samarbete över gränserna och utbyte av information i det samarbetet. Regleringen gäller generellt och alltså inte bara i förhållande till tredjeland utan även i samarbetet mellan medlemsstater. Flertalet av dem gäller dock inte i förhållande till internationella organisationer. Lagarna gäller vidare bara för vissa svenska myndigheter.

I 9 § 2013 års lag, som bl.a. genomför artikel 12 i dataskyddsrambeslutet, föreskrivs att om en svensk myndighet överför personuppgifter, ska myndigheten underrätta mottagaren om de villkor som gäller för användningen av uppgifterna. Paragrafen gäller endast när personuppgifter över-

förs till medlemsstater i EU, till Island, Norge, Schweiz eller Liechtenstein eller till ett EU-organ eller ett EU-informationssystem.

Direktivet reglerar inte möjligheten för en behörig myndighet i en medlemsstat att ställa upp villkor för hur personuppgifter som överförs till ett tredjeland eller en internationell organisation får användas. Mot bakgrund av de skäl som nyss nämnts delar regeringen utredningens bedömning att det behövs en reglering i ramlagen. En bestämmelse om villkor för användningen av personuppgifter som överförs till tredjeland och internationella organisationer kan inte anses stå i strid med direktivet, eftersom det syftar till att stärka skyddet för enskilda.

Ett exempel på när det kan finnas behov av att ställa upp villkor för behandlingen av personuppgifter är när en svensk behörig myndighet vill kunna kontrollera att personuppgifterna inte utan myndighetens vetskap vidareöverförs till ett annat tredjeland (se avsnitt 14.7). Förses personuppgifterna med ett sådant villkor när de överförs begränsas risken för att uppgifterna sprids vidare.

Det bör därför föreskrivas att svenska behöriga myndigheter i ett enskilt fall får ange villkor för hur personuppgifter som överförs till ett tredjeland eller en internationell organisation får användas, om det krävs med hänsyn till enskildas rätt eller från allmän synpunkt. *Skatteverket* anser att en ytterligare förutsättning bör vara att det krävs stöd i en bindande internationell överenskommelse. Regeringen anser emellertid att bestämmelsen bör utformas i likhet med motsvarande bestämmelser i exempelvis lagen om internationellt polisiärt samarbete och lagen om internationell rättslig hjälp i brottmål, dvs. att villkoren inte får strida mot en bindande internationell överenskommelse.

14.10 Dokumentationskrav och informationsskyldighet

Regeringens bedömning: Skyldigheten att i vissa fall dokumentera överföringar som görs till tredjeland eller internationella organisationer kan regleras i förordning. Detsamma gäller den personuppgiftsansvariges skyldighet att informera tillsynsmyndigheten om vissa överföringar till tredjeland och internationella organisationer.

Utredningens förslag överensstämmer med regeringens bedömning.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* och *Datainspektionen* anser att det ska framgå vilka uppgifter som ska dokumenteras vid överföring till andra än behöriga myndigheter.

Skälen för regeringens bedömning

Innehållet i direktivet

En nyhet i direktivet är att det införs dokumentationskrav och skyldighet att informera tillsynsmyndigheten om vissa typer av överföringar till tredjeland och internationella organisationer.

Enligt artikel 37.2 ska den personuppgiftsansvarige informera tillsynsmyndigheten om kategorier av överföringar som görs enligt arti-

kel 37.1 b, dvs. på den grunden att den personuppgiftsansvarige har bedömt att det finns lämpliga skyddsåtgärder för personuppgifterna. Sådana överföringar ska enligt artikel 37.3 dokumenteras och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten. Även när en överföring görs enligt artikel 38.1, dvs. i särskilda situationer, ska överföringen dokumenteras och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten. Det framgår av artikel 38.3. I båda fallen ska dokumentationen innehålla upplysning om datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

En myndighet, som med stöd av artikel 39.1 har överfört personuppgifter direkt till en mottagare som är etablerad i ett tredjeland, ska enligt artikel 39.3 informera tillsynsmyndigheten om överföringen. Även sådana överföringar ska dokumenteras.

Informationsskyldighet och krav på dokumentation

Regeringen delar utredningens bedömning att det bör finnas bestämmelser som genomför direktivets krav på information och dokumentation när personuppgifter överförs till ett tredjeland eller en internationell organisation. Detta kan regleras i förordning.

Säkerhets- och integritetsskyddsnämndens och *Datainspektionens* synpunkter på förordningsregleringen kommer regeringen att ta ställning till vid utformningen av sådana bestämmelser.

14.11 Internationellt samarbete

Regeringens bedömning: Några lagstiftningsåtgärder krävs inte för att stärka Sveriges delaktighet i det internationella samarbetet till skydd för personuppgifter.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Av artikel 40 framgår att kommissionen och medlemsstaterna ska vidta lämpliga åtgärder för att utveckla rutiner för internationellt samarbete och på internationell nivå erbjuda ömsesidigt bistånd. Syftet är att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter. Det ömsesidiga biståndet kan avse bl.a. underrättelser, klagomål, hjälp vid utredningar och informationsutbyte. Lämpliga åtgärder ska också vidtas för att öka det internationella samarbetet när det gäller tillämpningen av aktuell lagstiftning. Vidare ska medlemsstaterna främja utbyte och dokumentation om lagstiftning och praxis. Några lagstiftningsåtgärder behövs inte för att genomföra reglerna om internationellt samarbete till skydd för personuppgifter.

Mot bakgrund av att Sverige redan deltar i internationellt samarbete när det gäller bl.a. polisiära och straffrättsliga frågor, i vilket personuppgiftsbehandling är en viktig del, och att det redan finns lagstiftning för det samarbetet (se bl.a. avsnitt 4.2.6 och 4.2.7), ser regeringen i likhet med utredningen inget behov av någon ytterligare lagstiftning.

Det internationella samarbetet mellan tillsynsmyndigheterna behandlas i avsnitt 11.10.

14.12 Sekretess vid överföring till tredjeland

14.12.1 Överföring innebär utlämnande

En överföring av personuppgifter från en svensk myndighet till ett tredjeland eller en internationell organisation är ett utlämnande i offentlighets- och sekretesslagens mening (se t.ex. 6 kap. 1 § om utlämnande av allmän handling och 6 kap. 4 § om utlämnande av uppgift). Frågan är då hur förutsättningarna för att överföra personuppgifter till tredjeland förhåller sig till reglerna om offentlighet och sekretess. Bestämmelserna i direktivet om överföring av personuppgifter till tredjeland är, liksom bestämmelserna i 2013 års lag och personuppgiftslagen, formellt neutrala i den meningen att det i princip inte påverkar tillämpningen om de personuppgifter som överförs omfattas av sekretess eller inte hos den utlämnande myndigheten. Det är en annan sak att eventuell sekretess för överförda personuppgifter kan påverka vilken skyddsnivå i mottagarlandet som krävs i det enskilda fallet. Är det fråga om sekretessbelagda uppgifter som ska överföras kan det exempelvis finnas skäl att ställa högre krav på tillräckliga skyddsåtgärder för att överföra personuppgifter på den grunden.

14.12.2 Utlämnande av offentliga allmänna handlingar till tredjeland

Om personuppgifter och andra uppgifter i en allmän handling är offentliga – dvs. inte omfattas av sekretess eller träffas av en sekretessbestämmelse och vid en prövning inte bedöms vara sekretessbelagda – ska handlingen lämnas ut till en enskild som begär att få ta del av den med stöd av 2 kap. tryckfrihetsförordningen. Det gäller oavsett om han eller hon befinner sig i ett tredjeland och oavsett medborgarskap. En utlänning i tredjeland har alltså samma rätt som en svensk medborgare att enligt 2 kap. 13 § tryckfrihetsförordningen mot avgift få en kopia av handlingen. I praktiken betyder det att en myndighet inte kan neka att lämna ut handlingen med hänvisning till att skyddsnivån för personuppgifter i mottagarlandet inte är tillräcklig. Myndigheterna är dock enligt 2 kap. 13 § första stycket andra meningen tryckfrihetsförordningen inte skyldiga att lämna ut allmänna handlingar i elektronisk form. Behandling av personuppgifter vid utlämnande av allmänna handlingar omfattas som anges i avsnitt 6.6 inte av ramlagens tillämpningsområde.

14.12.3 Uppgifter som inte är sekretessbelagda

Vid utlämnande av personuppgifter till ett tredjeland i andra situationer än med stöd av 2 kap. tryckfrihetsförordningen, är regelverket inte lika tydligt. Handlar det om utlämnande enligt bestämmelser om ärendehand-

läggning eller liknande, t.ex. bestämmelser om kommunikation eller partsinsyn, görs ingen skillnad på parter i Sverige, EU eller tredjeland.

Det finns inga generellt tillämpliga bestämmelser som vare sig förpliktar eller begränsar myndigheter vid utlämnande av offentliga personuppgifter till tredjeland, t.ex. en myndighet i ett sådant land (jfr SOU 2015:39 s. 484). Att en myndighet enligt 6 kap. 5 § offentlighets- och sekretesslagen på begäran av en annan myndighet är skyldig att lämna ut en uppgift som den förfogar över om uppgiften inte är sekretessbelagd, ses i allmänhet som en precisering av myndigheternas allmänna samverkansskyldighet som tar sikte på svenska förvaltningsmyndigheter och domstolar. Den medför inte någon skyldighet att lämna ut personuppgifter, vare sig de är sekretessbelagda eller inte, till utländska myndigheter (jfr bet. 1982/83:KU12 s. 36). En utländsk myndighet anses inte heller ha rätt att överklaga en myndighets beslut att inte lämna ut en allmän handling eller att avslå en begäran om att få del av en personuppgift.

14.12.4 Uppgifter som är sekretessbelagda

Utgångspunkten är att en sekretessbelagd uppgift inte får röjas för en utländsk myndighet eller en mellanfolklig organisation. Enligt 8 kap. 3 § offentlighets- och sekretesslagen får dock sekretessbelagda uppgifter lämnas ut till en utländsk myndighet eller en mellanfolklig organisation om utlämnandet görs med stöd av särskild föreskrift i lag eller förordning. Med det avses uttryckliga uppgiftsskyldigheter eller andra sekretessbrytande regler.

Sekretessbelagda uppgifter får enligt 8 kap. 3 § offentlighets- och sekretesslagen även lämnas till en utländsk myndighet eller en mellanfolklig organisation om uppgiften i motsvarande fall får lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas ut. Om en svensk myndighet i motsvarande läge inte skulle ha fått uppgifterna på grund av sekretess får de alltså inte lämnas ut. Vid bedömningen av om uppgiftslämnandet är förenligt med svenska intressen får bl.a. Sveriges intresse av internationellt samarbete med den utländska myndigheten eller det mellanfolkliga organet beaktas.

Det kan inom ramen för det internationella samarbetet finnas bestämmelser som hindrar att personuppgifter överförs till tredjeland. Enligt t.ex. 10 § lagen (2000:344) om Schengens informationssystem får en uppgift som behandlas i registret inte överföras eller göras tillgänglig för ett tredjeland (med vilket här bör förstås stater som inte är anslutna till Schengensamarbetet) eller en internationell organisation.

15 Sekretessfrågor

15.1 Inledande om offentlighet och sekretess

15.1.1 Rätten att ta del av allmänna handlingar

Enligt 2 kap. 1 § tryckfrihetsförordningen har var och en rätt att ta del av allmänna handlingar. Den rätten får enligt 2 kap. 2 § första stycket tryckfrihetsförordningen begränsas bara om det är nödvändigt med hänsyn till vissa intressen. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den förstnämnda lagen hänvisar till. Den särskilda lag som avses är offentlighets- och sekretesslagen (2009:400).

Sekretess innebär inte bara begränsningar av rätten att ta del av allmänna handlingar utan även förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretess innebär således både handlingssekretess och tystnadsplikt. Till den del sekretessbestämmelserna innebär tystnadsplikt, medför de en begränsning av yttrandefriheten enligt regeringsformen.

15.1.2 Huvuddragen i sekretessregleringen

En sekretessbestämmelse består som regel av tre huvudsakliga rekvisit som anger sekretessens föremål, räckvidd och styrka.

Sekretessens föremål är den information som kan hemlighållas och anges i lagen genom ordet ”uppgift” tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, t.ex. uppgift om enskilds personliga förhållanden.

Sekretessbestämmelsens räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Ett fåtal sekretessbestämmelser gäller utan någon begränsning av räckvidden. Uppgiften kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den finns.

Sekretessens styrka bestäms som regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att viss skada uppstår om de lämnas ut. Vid omvända skaderekvisit är utgångspunkten den motsatta. Då är presumtionen att uppgifterna omfattas av sekretess. Uppgifterna får då lämnas ut endast om det står klart att uppgifterna kan röjas utan att viss skada uppstår. Sekretessen kan även vara absolut, vilket innebär att de uppgifter som sekretessen omfattar ska hemlighållas utan någon skadeprövning om uppgifterna begärs ut.

Som huvudregel följer sekretess inte med en uppgift när den lämnas till en annan myndighet. Det beror bl.a. på att behovet av sekretess och styrkan i sekretessen inte kan bestämmas enbart med hänsyn till sekretessintresset utan varierar mellan myndigheter. Offentlighetsintresset kan kräva att de uppgifter som behandlas som hemliga hos en myndighet är

offentliga hos en annan (prop. 1979/80:2 Del A, s. 75 f.). Det finns dock vissa bestämmelser om överföring av sekretess.

Vid överföring av sekretess skiljer man mellan primära och sekundära sekretessbestämmelser. En primär sekretessbestämmelse gäller hos en myndighet eller för en viss typ av verksamhet eller en viss ärendetyp. En sekundär sekretessbestämmelse är en bestämmelse om sekretess som en myndighet ska tillämpa på grund av en särskild bestämmelse om överföring av sekretess. Överföring av sekretess innebär enligt 3 kap. 1 § offentlighets- och sekretesslagen att en primär sekretessbestämmelse som är tillämplig på en uppgift hos en myndighet, ska tillämpas på uppgiften även av en myndighet som uppgiften lämnas till. Om det finns en bestämmelse om överföring av sekretess kan således en och samma sekretessbestämmelse vara både en primär och en sekundär sekretessbestämmelse. Den är en primär sekretessbestämmelse hos den utlämnande myndigheten och en sekundär sekretessbestämmelse hos den mottagande myndigheten.

En primär sekretessbestämmelse kan normalt tillämpas på en uppgift oavsett om myndigheten har fått uppgiften från en annan myndighet eller från en enskild. När samma sekretessbestämmelse tillämpas som en sekundär sekretessbestämmelse kan den däremot bara tillämpas på uppgifter som den mottagande myndigheten har fått från den utlämnande myndigheten. En sekundär sekretessbestämmelse kan alltså inte tillämpas på uppgifter som den mottagande myndigheten har fått direkt från en enskild (prop. 1997/98:9 s. 38 f., prop. 2005/06:161 s. 30 och JO 2000/01 s. 44 och 50).

Sekretesstiden i olika sekretessbestämmelser varierar beroende på vilken typ av uppgift det är fråga om. Endast i ett fåtal bestämmelser saknas tidsgränser.

15.2 Sekretess i tillsynsverksamheten

15.2.1 Nuvarande reglering

Sekretess till skydd för tillsynsverksamheten

Tillsynsverksamhet skyddas av olika sekretessregler, både primära och sekundära. Enligt 17 kap. 1 § offentlighets- och sekretesslagen gäller sekretess för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjs.

Får en myndighet i verksamhet som rör tillsyn en sekretessreglerad uppgift från en annan myndighet, blir enligt 11 kap. 1 § offentlighets- och sekretesslagen sekretessbestämmelsen tillämplig även hos tillsynsmyndigheten. Därmed gäller i princip samma sekretess hos tillsynsmyndigheten som hos den myndighet som är föremål för tillsyn. Sekretessen gäller även för uppgifter som tillsynsmyndigheten hämtar in från andra myndigheter än den som granskningen avser, om uppgifterna behövs för tillsynen. Enligt 11 kap. 8 § gäller en primär sekretessbestämmelse som ska tillämpas av tillsynsmyndigheten framför överförd sekretess enligt 11 kap. 1 §.

Sekretess gäller enligt 42 kap. 5 § offentlighets- och sekretesslagen hos Säkerhets- och integritetsskyddsnämnden i dess tillsynsverksamhet. Sekretessen hos nämnden regleras uttömmande i 42 kap. 6–8 §§. Om nämnden har fått uppgifter från en enskild gäller enligt 42 kap 6 § sekretess enligt 15 kap. endast om det kan antas att riket lider betydande skada om uppgiften röjs och enligt 18 kap. endast om det kan antas att verksamheten för att förebygga eller beivra brott allvarligt motverkas om uppgiften röjs. Överföring av sekretess regleras i 42 kap. 8 §. Sekretess följer alltid med en uppgift som lämnats av en annan myndighet till nämnden. Enligt förarbetena är det viktigt att uppgifter i dessa fall inte får ett svagare skydd hos nämnden än hos den utlämnande myndigheten (prop. 2006/07:133 s. 74). Sekretess överförs både från myndigheter som omfattas av nämndens tillsyn och från andra myndigheter.

Sekretess till skydd för enskild i tillsynsverksamhet

Enligt 32 kap. 1 § offentlighets- och sekretesslagen gäller sekretess hos Datainspektionen i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen och i ärende om sådant bistånd som avses i dataskyddskonventionen, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Enligt 42 kap. 6 § andra stycket gäller sekretess hos Säkerhets- och integritetsskyddsnämnden till skydd för uppgift om enskildas personliga förhållanden som lämnas av enskilda själva, om uppgiften skulle ha varit sekretessreglerad om den funnits hos den myndighet som det aktuella tillsynsärendet får anses avse. Om uppgifterna inte kan hänföras till någon sådan myndighet, är de således offentliga.

Primär sekretess som kan gälla i tillsynsverksamhet

Den primära sekretessen för brottsbekämpande verksamhet enligt 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen gäller i princip hos alla myndigheter. Är det fråga om sådan sekretess gäller därmed sekretessen till skydd för uppgifter i förundersökningar, ärenden om användning av tvångsmedel och underrättelseverksamhet även hos tillsynsmyndigheten. Detsamma gäller sekretess enligt andra bestämmelser i 18 kap. som är konstruerade så att sekretessen följer med uppgiften. Särskilda sekretessbestämmelser gäller som nyss nämnts för Säkerhets- och integritetsskyddsnämnden.

Sekretess med hänsyn till förhållandet till andra stater

Enligt 15 kap. 1 § offentlighets- och sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. För att sekretess ska gälla krävs att den svenska myndigheten företräder Sverige på sådant sätt att kontakten anses röra Sveriges förbindelser med den andra staten. Paragrafen kan även vara tillämplig på en utländsk myndighets kontakter med en svensk myndighet, men utrymmet för sekretess är starkt begränsat (Eva Lenberg, Ulrika Geijer

och Anna Tansjö, i fortsättningen Lenberg m.fl., supplement 9, januari 2014, s. 15:1.1).

Sekretessen i 15 kap. 1 a § offentlighets- och sekretesslagen infördes för att möta ökade krav på sekretess i internationellt samarbete. Sekretess gäller för uppgift som en svensk myndighet har fått från ett utländskt organ på grund av bl.a. en bindande EU-rättsakt eller ett av EU ingånget avtal eller av riksdagen godkänt avtal med en annan stat eller mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbetet försämras om uppgiften röjs. Sekretess gäller också för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal. Bestämmelsen gäller hos alla som tillämpar offentlighets- och sekretesslagen.

Sekretess gäller enligt 42 kap. 7 § offentlighets- och sekretesslagen hos Säkerhets- och integritetsskyddsnämnden för uppgift som nämnden har fått direkt från en utländsk myndighet eller en mellanfolklig organisation. Förutsättningen för sekretess är att det skulle ha gällt sekretess för uppgiften om den hade funnits hos den myndighet som det aktuella tillsynsärendet får anses avse. Kan uppgifterna inte hänföras till någon sådan myndighet är de alltså offentliga. Datainspektionen har däremot inte någon motsvarande sekretessbestämmelse som skyddar allmänna utländska intressen i myndighetens tillsynsverksamhet.

15.2.2 Behovet av en ny sekretessbestämmelse

Regeringens bedömning: Det behövs en ny sekretessbestämmelse för att värna tillsynsmyndighetens internationella samarbete enligt ramlagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: De enda remissinstanser som uttalar sig i denna del är *Journalistförbundet* och *Tidningsutgivarna* som anser att utformningen av den sekretessbestämmelse som föreslås är problematisk och i praktiken kan komma att leda till en presumtion för sekretess. Eftersom en sådan sträng sekretess inte är motiverad enligt dem avstyrker de förslaget om en ny sekretessbestämmelse.

Skälen för regeringens bedömning

Ökat informationsutbyte mellan tillsynsmyndigheter

Brottsligheten är i allt större utsträckning gränsöverskridande. Det ställer krav på ökat samarbete mellan behöriga myndigheter inom olika delar av ramlagens tillämpningsområde. Ett av direktivets syften är att underlätta det fria flödet av uppgifter mellan behöriga myndigheter, nationellt och internationellt. Det får i sin tur betydelse för tillsynen över personuppgiftsbehandling. Ökat sådant informationsutbyte ställer högre krav på samarbete mellan tillsynsmyndigheterna, eftersom fler skyddsvärda och integritetskänsliga uppgifter kan komma att utbytas. Betydelsen av ett kraftfullt tillsynsarbete framhålls i skäl 4. Enligt artikel 50.1 ska medlemsstaterna införa åtgärder som bidrar till ett verkningsfullt samarbete

när det gäller tillsynen. Tillsynsmyndigheterna ska utbyta relevant information och bistå varandra med tillsynsåtgärder. Samarbetet behandlas i avsnitt 11.10.

I det internationella straffrättsliga samarbetet har det länge varit en självklar utgångspunkt att uppgifter skyddas av sekretess i alla medlemsstater, för att inte samarbetet ska äventyras. När det gäller uppgifter som utbyts inom ramen för internationellt polisiärt samarbete har regeringen nyligen föreslagit ett ökat sekretesskydd för utländska intressen (prop. 2016/17:208 s. 38 f.). Riksdagen har ställt sig bakom förslaget (bet. 2017/18:KU3, rskr. 2017/18:37).

Enligt artikel 44.2 i direktivet ska tystnadsplikt gälla för personal vid tillsynsmyndigheten för konfidentiell information som de får kännedom om vid utförandet av sina uppgifter eller utövandet av sina befogenheter.

Det behövs en ny sekretessbestämmelse

För att kunna fullgöra sina skyldigheter enligt ramlagen måste tillsynsmyndigheten både kunna hämta in och ta emot nödvändig information från tillsynsmyndigheter i andra medlemsstater. Informationen kan röra t.ex. personuppgiftsbehandling vid pågående förundersökningar, underrättelsearbete, samarbete i spaningsverksamhet eller andra uppgifter som kan vara sekretessreglerade. Av en svensk begäran om bistånd ska det framgå vilken hjälp den svenska tillsynsmyndigheten begär och skälen för begäran. En begäran om bistånd bör givetvis formuleras så att den inte i onödan avslöjar sekretessbelagd information. Regeringen anser i likhet med utredningen att de sekretessregler som finns är tillräckliga för att tillsynsmyndigheten ska kunna fullgöra sina skyldigheter när det gäller svenska framställningar om bistånd. Behovet av en sekretessbrytande bestämmelse behandlas i avsnitt 15.2.4.

Regleringen i offentlighets- och sekretesslagen utgår från att det är svenska myndigheter som åsyftas, om inte annat sägs (Lenberg m.fl., s. 8:1.1). Det får betydelse framför allt vid internationellt samarbete. Om uppgifter lämnas direkt från en utländsk myndighet eller mellanfolklig organisation till en svensk myndighet blir bestämmelserna om överföring av sekretess inte tillämpliga (prop. 2008/09:201 s. 102). Det väcker frågan om den nuvarande sekretessregleringen i tillräcklig utsträckning skyddar den information som den svenska tillsynsmyndigheten kan komma att motta från en utländsk tillsynsmyndighet.

Tillsynen över de behöriga myndigheterna kommer att ge tillsynsmyndigheten insyn i bl.a. brottsbekämpande verksamhet där intresset av sekretess till skydd för det allmännas verksamhet är starkt. Det gäller i lika hög grad utländska myndigheters brottsbekämpande verksamhet som svenska myndigheters. Det var mot den bakgrunden som sekretessen i 18 kap. 17 § offentlighets- och sekretesslagen infördes. Som nyss nämnts pågår lagstiftningsarbete i syfte att förbättra sekretesskyddet i det internationella polisiära samarbetet. Även om det inte är ett uttryckligt krav i direktivet är det enligt regeringen nödvändigt att uppgifter som härrör från internationellt samarbete på det brottsbekämpande och straffrättsliga området har ett fullgott sekretesskydd hos tillsynsmyndigheten vid tillsyn över sådant samarbete.

Regeringen gör bedömningen att de sekretessregler som finns är tillräckliga för att skydda den information som utländska tillsynsmyndigheter lämnar när de besvarar en svensk framställan om bistånd. I de fallen är det svenska myndigheter som är föremål för tillsyn vilket gör att bl.a. 18 kap. 1–2 §§ offentlighets- och sekretesslagen kan aktualiseras. Däremot kan det förhålla sig annorlunda vid utländska framställningar om bistånd. Om de uppgifter som utländska tillsynsmyndigheter lämnar när de begär svenskt bistånd inte skyddas genom sekretess hos den svenska tillsynsmyndigheten, kan det leda till att utländska tillsynsmyndigheter både kan komma att avhålla sig från att begära bistånd från Sverige och vara mindre villiga att bistå den svenska myndigheten när den begär att få uppgifter. Det skulle kunna hämma den svenska tillsynsmyndighetens möjlighet att bedriva ett effektivt tillsynsarbete och göra det svårt för Sverige att leva upp till direktivets skyldigheter om internationellt samarbete vid tillsyn. Samarbetet på ramlagens område kräver därför enligt regeringen att utländska allmänna intressen kan skyddas. Eftersom frågan om sekretess i det gränsöverskridande tillsynsarbetet över huvud taget inte berörs i direktivet, kan bestämmelsen om sekretess i 15 kap. 1 a § offentlighets- och sekretesslagen inte anses tillämplig. Den sekretessbestämmelsen aktualiseras normalt bara om det finns en tydlig sekretessbestämmelse i den aktuella EU-rättsakten (prop. 2012/13:192 s. 35 och 44).

Sverige har skyldighet att se till att regleringen i direktivet blir effektiv. I motsats till *Journalistförbundet* och *Tidningsutgivarna* håller regeringen med utredningen om att det därför finns skäl att införa en ny sekretessbestämmelse som skyddar uppgifter som tillsynsmyndigheten får när den på begäran bistår en utländsk tillsynsmyndighet vid tillsyn inom direktivets tillämpningsområde. Bestämmelsens närmare utformning behandlas i avsnitt 15.2.3.

Tillåtet intresse enligt tryckfrihetsförordningen

Enligt 2 kap. 2 § första stycket tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas bara för vissa där särskilt angivna intressen. Ett sådant intresse är rikets förhållande till annan stat eller mellanfolklig organisation (2 kap. 2 § 1 tryckfrihetsförordningen) och ett annat är myndighetsverksamhet för inspektion, kontroll eller annan tillsyn (2 kap. 2 § 3).

När bestämmelsen i 18 kap. 17 § offentlighets- och sekretesslagen infördes bedömde regeringen att ordalydelsen i fyra av de sju intressen som räknas upp i 2 kap. 2 § tryckfrihetsförordningen uttryckligen är begränsade till svenska förhållanden. Det gällde bl.a. intresset i punkten 3 (prop. 1999/2000:61 s. 164). Därefter har emellertid flera bestämmelser om sekretess i internationellt samarbete med skyddsintressen som liknar det nu aktuella införts. Som exempel kan nämnas 17 kap. 7 a § (administrativt samarbete avseende beskattning), 17 kap. 7 b § (tillsyn över marknaderna för el och naturgas) och 42 kap. 7 och 8 c §§ offentlighets- och sekretesslagen (Säkerhets- och integritetskyddsnämndens tillsyn över bl.a. behandling av personuppgifter).

Mot bakgrund av att det under senare år har införts flera sekretessregler, som lutar sig mot 2 kap. 2 § 3 tryckfrihetsförordningen och som syf-

tar till att skydda utländska allmänna intressen på tillsynsområdet, håller regeringen med utredningen om att det inte finns något som hindrar att det införs en ny sekretessbestämmelse som syftar till att värna utländska intressen på tillsynsområdet. Till det kommer att en sekretessregel i detta fall även är motiverad med hänsyn till rikets förhållande till annan stat.

15.2.3 Utformningen av sekretessbestämmelsen

Regeringens förslag: Sekretess ska gälla i tillsynsmyndighetens verksamhet enligt ramlagen för uppgift som, utan samband med en svensk begäran, har lämnats av en tillsynsmyndighet i en stat inom Europeiska ekonomiska samarbetsområdet (EES) eller i Schweiz, om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs. Sekretessen ska gälla i högst 40 år.

Utredningens förslag överensstämmer i sak med regeringens. Den bestämmelse utredningen föreslår har dock en annorlunda lydelse.

Remissinstanserna: *Journalistförbundet* och *Tidningsutgivarna* befarar att den föreslagna bestämmelsens utformning kommer att leda till en presumtion för sekretess, eftersom det är svårt att på förhand avgöra om möjligheterna att bedriva tillsyn kan komma att motverkas. De avstyrker därför förslaget. För det fall att en sekretessbestämmelse för att skydda uppgifter från utländska tillsynsmyndigheter ändå införs, anser Journalistförbundet att ett skaderekvisit liknande det som finns i 42 kap. 7 § offentlighets- och sekretesslagen bör väljas. Övriga remissinstanser yttrar sig inte om förslaget.

Skälen för regeringens förslag

Sekretessens föremål, räckvidd och styrka

Sekretessen bör skydda uppgifter som lämnas till den svenska tillsynsmyndigheten av en tillsynsmyndighet i en medlemsstat när den begär svenskt bistånd. Det som behöver kunna sekretessbeläggas är framför allt uppgifter som kan ge inblick i enskilda ärenden hos tillsynsobjekten eller avslöja hur arbetet bedrivs där, t.ex. vilken spanings- eller utredningsverksamhet som bedrivs eller vilka arbetsmetoder som används av t.ex. kriminalvårdsmyndigheter eller polisen. Den svenska tillsynsmyndigheten skulle också kunna få inblick i utländska tillsynsmyndigheters ställningstaganden och diskussioner kring gränsöverskridande samarbeten som inte berör Sverige.

Frågan är då hur sekretessregeln närmare bör utformas. En lösning kan vara att med 18 kap. 17 § offentlighets- och sekretesslagen som förebild föreskriva att sekretess gäller om det kan antas att viss åtgärd begärs under förutsättning att överlämnade uppgifter inte röjs. En sådan bestämmelse skulle fungera när en utländsk tillsynsmyndighet begär hjälp men inte skydda utländska intressen när uppgifter lämnas av den utländska tillsynsmyndigheten utan att denna begär något bistånd av den svenska tillsynsmyndigheten. En annan lösning kan vara att med 42 kap. 7 § som förebild föreskriva att sekretess gäller i den utsträckning uppgiften skulle

ha varit sekretessreglerad om den funnits hos den myndighet som det aktuella tillsynsärendet får anses avse. Nackdelen med den lösningen är att om uppgifterna inte kan hänföras till någon sådan myndighet blir de offentliga. En tredje lösning kan vara att utforma bestämmelsen på samma sätt som 17 kap. 7 b § offentlighets- och sekretesslagen. Den paragrafen tar sikte på om ett röjande skulle motverka den svenska myndighetens möjlighet att bedriva tillsyn. Bestämmelsen infördes med anledning av samarbetet inom EU vid tillsyn över marknaderna för el och naturgas (prop. 2012/13:7 s. 20).

När en ny sekretessbestämmelse övervägs ska det alltid göras en intresseavvägning mellan sekretessintresset och insynsintresset (prop. 1979/80:2 Del A, s. 78). När skälen för att införa en sekretessbestämmelse väger tyngre än insynsintresset kommer avvägningen mellan skyddsintresset och allmänhetens intresse av insyn normalt till uttryck genom att sekretessbestämmelsen förses med ett skaderekvisit. Det kan antingen vara ett rakt skaderekvisit, som innebär en presumtion för offentlighet, eller ett omvänt skaderekvisit, som innebär en presumtion för sekretess (se avsnitt 15.1.2). I vissa fall förses dock sekretessbestämmelsen med andra rekvisit som anger under vilka förutsättningar sekretessen gäller. Gemensamt för de bestämmelser som saknar ett traditionellt skaderekvisit är att de är tydligt avgränsade i fråga om föremål och räckvidd. Regeringen håller med utredningen om att det finns betydande svårigheter att tillämpa skaderekvisit i bestämmelser som avser att skydda utländska intressen. Möjligheterna att rätt bedöma skadan är begränsade i de fallen och därför bör en annan typ av rekvisit väljas. Regeln bör därför, till skillnad från vad *Journalistförbundet* anser men i likhet med vad utredningen föreslår, utformas så att sekretess gäller om det kan antas att tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs. Det är samma rekvisit som finns i sekretessregeln till skydd för det internationella samarbetet vid tillsyn över marknaderna för el och naturgas. De tillämpningsproblem som *Journalistförbundet* och *Tidningsutgivarna* pekar på att det skulle vara svårt att på förhand veta vilka konsekvenser ett utlämnande av en viss uppgift kan komma att få för möjligheten att bedriva tillsyn ska enligt regeringen inte överdrivas. Vid sekretessprövningen bör bl.a. vägas in vilken effekt ett offentliggörande av uppgiften skulle få på det framtida samarbetet och på den svenska tillsynsmyndighetens möjligheter att få bistånd i sin tillsyn från andra medlemsstater. Det bör också beaktas vilket sekretesskydd eller motsvarande skydd uppgiften har hos den medlemsstat som har lämnat uppgiften.

Av paragrafen bör det alltså framgå att sekretess gäller i tillsynsmyndighetens verksamhet enligt ramlagen för uppgift som, utan samband med en svensk begäran, har lämnats av en tillsynsmyndighet i en annan medlemsstat, om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs. I stället för att som utredningen föreslår använda formuleringen ”tillsynsmyndighet i en medlemsstat” i bestämmelsen och samtidigt hänvisa till brottsdatalagens definition av medlemsstat, bör den av *Lagrådet* föreslagna formuleringen ”tillsynsmyndighet i en stat inom Europeiska ekonomiska samarbetsområdet (EES) eller i Schweiz” användas.

Sekretesstiden och sekretessbestämmelsens placering

Vid utrikessekretess, internationellt rättsligt samarbete och annat tillsynssamarbete är sekretesstiden högst fyrtio år. Samma sekretesstid bör gälla för nu aktuella uppgifter.

Den nya sekretessbestämmelsen skulle kunna placeras antingen i kapitel 17, som reglerar sekretess till skydd för bl.a. myndigheters verksamhet för tillsyn, eller i kapitel 15, som reglerar sekretess till skydd för rikets förhållande till andra stater. Regeringen anser att den bör placeras i kapitel 17, där det redan finns bestämmelser med liknande skyddsintressen.

Rätten att meddela och offentliggöra uppgifter

Enligt 3 kap. 1 § offentlighets- och sekretesslagen innebär sekretess ett förbud att röja uppgift, vare sig det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt. När en ny sekretessbestämmelse införs måste därför ställning tas till om den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen bör ges företräde framför meddelarfriheten enligt 1 kap. 1 § tredje stycket tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen.

Enligt förarbetena till sekretesslagen bör som grundprincip alltid gälla stor återhållsamhet vid prövningen av om undantag ska göras från rätten att meddela och offentliggöra uppgifter. Den enskilda sekretessbestämmelsens konstruktion kan ge viss vägledning. När det är fråga om bestämmelser om absolut sekretess kan det finnas större anledning att överväga undantag från rätten att meddela och offentliggöra uppgifter än i andra fall (prop. 1979/80:2 Del A, s. 110 f.). Undantag från huvudregeln är framför allt aktuellt ifråga om sekretessregler utan skaderekvisit eller med omvänt skaderekvisit. Att undantag görs med hänsyn till allmänna intressen är ovanligt. De undantag som finns i dag rör särskilt viktiga skyddsintressen (prop. 2012/13:7 s. 18 f. och prop. 2012/13:192 s. 38). Enligt regeringen bör något undantag från huvudregeln inte göras i detta fall.

15.2.4 En sekretessbrytande regel för tillsynsverksamheten

Regeringens förslag: Tillsynsmyndigheten får, om det är förenligt med svenska intressen, lämna ut en uppgift till en behörig tillsynsmyndighet i annan medlemsstat, även om uppgiften är sekretessbelagd.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen av remissinstanserna yttrar sig särskilt om förslaget.

Skälen för regeringens förslag

Nuvarande reglering

Enligt 10 kap. 17 § offentlighets- och sekretesslagen hindrar sekretess inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för

tillsyn över eller revision hos den myndighet där uppgiften förekommer. Ordet myndighet syftar som tidigare nämnts på svenska myndigheter. Bestämmelsen möjliggör utlämnande till bl.a. Riksdagens ombudsmän, Justitiekanslern och Datainspektionen.

Sekretess hindrar enligt 10 kap. 2 § offentlighets- och sekretesslagen inte heller att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Syftet med paragrafen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet att sköta de uppgifter som den är skyldig att utföra.

Enligt 8 kap. 3 § offentlighets- och sekretesslagen får en uppgift för vilken sekretess gäller inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande görs med stöd av en särskild föreskrift i lag eller förordning, eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller till den mellanfolkliga organisationen. Lagen (1978:801) om internationellt samarbete rörande kriminalvård i frihet och lagen (2000:1219) om internationellt tullsamarbete är exempel på författningar med sådana särskilda föreskrifter.

Det behövs en ny sekretessbrytande bestämmelse

För att kunna utöva tillsyn behöver tillsynsmyndigheten få tillgång till all information som rör viss behandling av personuppgifter. För det ändamålet måste tillsynsmyndigheten inte sällan själv lämna ut sekretessbelagda uppgifter för att kunna få svar på förfrågningar. Regleringen i 10 kap. 2 § offentlighets- och sekretesslagen möjliggör för tillsynsmyndigheten att lämna ut information till andra myndigheter, för att kunna få den information som behövs för tillsynen. När det gäller utlämnande till en utländsk tillsynsmyndighet ska 8 kap. 3 § offentlighets- och sekretesslagen beaktas.

I avsnitt 11.10.1 föreslås att tillsynsmyndigheten på begäran ska bistå tillsynsmyndigheter i andra medlemsstater. På motsvarande sätt ska tillsynsmyndigheten, som framgår av avsnitt 11.10.2, kunna begära bistånd av en annan medlemsstat. Internationellt bistånd kan innefatta utbyte av information som omfattas av sekretess. Det är tveksamt om tillsynsuppgiften i sig innebär en sådan uppgiftsskyldighet som avses i 8 kap. 3 § offentlighets- och sekretesslagen. Om myndigheten bedömer att den måste lämna ut sekretessbelagda uppgifter för att få internationellt bistånd kan det finnas grund för att bryta sekretessen med stöd av 8 kap. 3 § och 10 kap. 2 § offentlighets- och sekretesslagen. Enligt förarbetena ska dock den senare paragrafen tillämpas restriktivt. Sekretessen får efterges bara när ett utlämnande av sekretessbelagda uppgifter är en nödvändig förutsättning för att en myndighet ska kunna fullgöra ett visst åliggande (prop. 1979/80:2 Del A, s. 465 och 494). För att genomföra direktivet och för att tillsynsmyndighetens internationella arbete ska underlättas bör det i ramlagen tas in en särskild bestämmelse som bryter sekretessen vid samarbete med en utländsk tillsynsmyndighet.

Av bestämmelsen bör framgå att en sekretessbelagd uppgift får lämnas ut till en behörig tillsynsmyndighet i en annan medlemsstat om det är förenligt med svenska intressen. Den prövningen bör endast få göras av den som enligt myndighetens arbetsordning eller motsvarande har rätt att fatta sådana beslut på myndighetens vägnar (jfr Lenberg m.fl., s. 8:3.1). Skulle det vid en sådan prövning bedömas vara oförenligt med svenska intressen att lämna ut uppgifterna, bör begäran om bistånd vägras med hänvisning till att det skulle strida mot lag att tillmötesgå den.

15.2.5 Sekretess för rapporter om personuppgiftsincidenter

Regeringens bedömning: Det finns inte skäl att ändra sekretessregleringen för personuppgiftsincidenter.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Tidningsutgivarna* instämmer i bedömningen. *Datainspektionen* anser att absolut sekretess alternativt sekretess med omvänt skaderekvisit ska gälla i tillsynsmyndighetens verksamhet för begäran om förhandssamråd och anmälningar av personuppgiftsincidenter.

Skälen för regeringens bedömning: En nyhet i direktivet är kravet på rapportering av personuppgiftsincidenter till tillsynsmyndigheten. Det väcker frågan om det kräver någon justering i sekretessregleringen.

Redan i dag gäller viss sekretess för rapporter om it-incidenter. Enligt 18 kap. 3 § offentlighets- och sekretesslagen gäller sekretessen för bl.a. brottsanmälningar och förundersökningar i 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen inte bara hos de brottsbekämpande myndigheterna utan även hos andra myndigheter när de biträder en brottsbekämpande myndighet. Myndigheter som står i begrepp att göra en anmälan till en brottsbekämpande myndighet förfogar över det underlag som utgör grunden för anmälan. Sekretessen i 18 kap. 3 § kompletterar den sekretess som gäller enligt 18 kap. 1 och 2 §§. Sekretessen gäller såväl hos myndigheter som har anmälningsskyldighet som hos andra. Om en personuppgiftsincident leder till en brottsanmälan skyddas alltså det underlag som en behörig myndighet eller tillsynsmyndigheten tar fram genom regleringen i 18 kap. 3 §. Regeringen håller med utredningen om att den sekretessen är tillräcklig för att tillgodose behovet av att skydda uppgifter om sådana personuppgiftsincidenter som kan utgöra brott.

Enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen gäller vidare sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information. Sekretess gäller oavsett var uppgiften finns. Uppgifter om de tekniska system som en personuppgiftsincident berör skyddas genom den sekretessbestämmelsen, som har ett rakt skaderekvisit.

Datainspektionen har i en skrivelse till regeringen begärt att vissa sekretessfrågor ska utredas (Ju2017/06035/L6). I skrivelsen och i remissyttrandet över utredningens förslag anger Datainspektionen att sekretessen

för uppgifter i bl.a. incidentrapporter inte är tillräcklig och att det krävs ett starkare sekretesskydd. Att bestämmelsen i 18 kap. 8 § 3 offentlighets- och sekretesslagen har ett rakt skaderekvisit innebär inte, som Datainspektionen anför, att sekretesskyddet är svagt. Ett rakt skaderekvisit innebär visserligen en presumtion för offentlighet, vilket också är utgångspunkten för den svenska offentlighetsprincipen, men presumtionen bryts om det kan antas att en sådan skada som anges i sekretessbestämmelsen uppstår om uppgiften röjs.

Bestämmelsen i 18 kap. 8 § 3 offentlighets- och sekretesslagen har i ett tidigare lagstiftningsärende ansetts innebära att uppgifter om ingivare av incidentrapportering avseende säkerhetsbrister i it-system till Post- och telestyrelsen, liksom uppgifter om innehållet i rapporterna, omfattas av sekretess (prop. 2003/04:93 s. 82). Utredningen om genomförande av NIS-direktivet har nyligen utrett om bestämmelsen behöver ändras för att känslig information i incidentrapporter som lämnas till Myndigheten för samhällsskydd och beredskap ska kunna skyddas. Den utredningen konstaterar i sitt betänkande att 18 kap. 8 § offentlighets- och sekretesslagen ger ett tillräckligt skydd för uppgifter som kan komma att rapporteras vid en incident (SOU 2017:36 s. 247–257). Regeringen gör ingen annan bedömning i propositionen Informationssäkerhet för samhällsviktiga och digitala tjänster (prop. 2017/18:205 s. 81 f.). Regeringen gör dessutom i samband med förslaget om en ny dataskyddslag bedömningen att den befintliga sekretessregleringen ger ett väl avvägt skydd i nu aktuellt avseende. I det ärendet uttalar regeringen både att incidentrapporter kan innehålla sådan skyddsvärd information rörande säkerhetsåtgärder som avses i 18 kap. 8 § 3 offentlighets- och sekretesslagen och att uppgift om vem som har lämnat in en sådan rapport i sig kan omfattas av sekretess enligt bestämmelsen (prop. 2017/18:105 s. 126 f.).

Mot denna bakgrund instämmer regeringen i utredningens bedömning att det inte finns skäl att ändra regleringen avseende sekretess för sådan personuppgiftsincidentrapportering som förutsätts ske enligt den nya ramlagen. Det finns inte heller behov av att införa ytterligare sekretessbestämmelser för den typen av information som kan lämnas till tillsynsmyndigheten i samband med en begäran om förhandssamråd. Den sekretessreglering som finns i dag, bl.a. i 18 kap. offentlighets- och sekretesslagen, är tillräcklig också i det avseendet.

15.2.6 En hänvisningsbestämmelse bör införas

Regeringens förslag: Det ska göras en hänvisning i offentlighets- och sekretesslagen till regeln om användningsbegränsning i ramlagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans har något att erinra mot förslaget.

Skälen för regeringens förslag: I avsnitt 11.10.2 föreslås en särskild regel om hur den information som tillsynsmyndigheten hämtar in från en tillsynsmyndighet i en annan medlemsstat får användas. En sådan användningsbegränsning har företräde framför andra författningsregler. I 9 kap. 2 § offentlighets- och sekretesslagen räknas det upp ett antal

sådana bestämmelser. En hänvisning till regeln i ramlagen bör införas i den paragrafen.

15.3 Tystnadsplikt för dataskyddsombud

Regeringens förslag: Den som fullgör uppgift som dataskyddsombud ska inte obehörigen få röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

I det allmännas verksamhet tillämpas i stället offentlighets- och sekretesslagen.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska den som fullgör uppgift som dataskyddsombud inte obehörigen få röja eller utnyttja det som han eller hon har fått veta om enskilds personliga eller ekonomiska förhållanden.

Remissinstanserna: *Datainspektionen* tillstyrker förslaget och påpekar att tystnadsplikten bör regleras på samma sätt som på dataskyddsförordningens område. Även *Sala kommun* uttrycker sig positivt om förslaget. *Umeå universitet* anser att rekvisitet obehörigt röjande inte uppfyller kraven på förutsägbarhet och att bestämmelsen därför bör förtydligas genom en uppräkning eller en exemplifiering av vad som inte anses utgöra ett obehörigt röjande. Övriga remissinstanser lämnar inga synpunkter på förslaget.

Skälen för regeringens förslag

Behovet av en bestämmelse om tystnadsplikt

Det är inte bara myndigheterna i rättskedjan som ska tillämpa brottsdatalagen utan även andra myndigheter. I vissa fall ska även andra aktörer tillämpa lagen. I avsnitt 9.5.2 föreslås att alla som ska tillämpa ramlagen ska utse dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas. Det gäller således även andra aktörer än myndigheter.

Eftersom det kommer att finnas dataskyddsombud hos behöriga myndigheter som inte tillämpar offentlighets- och sekretesslagen behövs det en regel om tystnadsplikt för sådana ombud. För dataskyddsombud hos myndigheter får däremot den sekretessreglering som gäller för myndigheterna anses tillräcklig. Förbud för myndigheter att röja en sekretessbelagd uppgift gäller enligt 2 kap. 1 § offentlighets- och sekretesslagen också för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, tjänsteplikt eller på annan liknande grund. Enligt regeringen måste ett dataskyddsombud anses delta i myndighetens verksamhet på det sätt som avses i bestämmelsen (prop. 2017/18:105 s. 132).

Dataskyddsombud som utses av myndigheter ska alltså tillämpa bestämmelserna i offentlighets- och sekretesslagen. Regeringen instämmer i utredningens uppfattning att det inte behövs någon ytterligare reglering av deras tystnadsplikt. Samma bedömning görs när det gäller dataskyddsförordningens tillämpningsområde (prop. 2017/18:105 s. 130 f.).

De dataskyddsombud som kommer att vara verksamma inom ramlagens tillämpningsområde och som inte träffas av regleringen i offentlighets- och sekretesslagen kommer sannolikt att ha uppgifter enligt både ramlagen och dataskyddsförordningen. Det är då lämpligt att, som *Datainspektionen* framhåller, reglerna om tystnadsplikt är utformade på samma sätt. Utredningen föreslår därför en bestämmelse om tystnadsplikt för dataskyddsombud som är utformad efter mönster av den bestämmelse som Dataskyddsutredningen föreslår. Utredningens förslag innebär att den som fullgör uppgift som dataskyddsombud inte obehörigen får röja eller utnyttja det som han eller hon har fått veta om enskilds personliga eller ekonomiska förhållanden. När det gäller förslaget till en ny dataskyddslag med kompletterande bestämmelser till EU:s dataskyddsförordning gör regeringen dock bedömningen att tystnadspliktens omfattning inte bör avgränsas till enskilds personliga eller ekonomiska förhållanden. Regeringen anser att tystnadsplikten enligt den lagen bör gälla för alla slags uppgifter som dataskyddsombudet vid fullgörandet av sin uppgift har fått kännedom om (prop. 2017/18:105 s. 133 f.). Det saknas skäl att göra en annan bedömning i fråga om tystnadsplikten enligt ramlagen.

Umeå universitet anser att bestämmelsen bör konstrueras på ett mer förutsägbart sätt genom att det direkt av lagtexten framgår i vilka fall det inte är fråga om ett obehörigt röjande. Som regeringen uttalar i propositionen Ny dataskyddslag är det dock inte lämpligt att uttömmande reglera i vilka fall utlämnande får ske. Detta måste bedömas utifrån omständigheterna i det enskilda fallet. Uppgifter kan dock normalt lämnas ut med samtycke från den uppgiften avser, till tillsynsmyndigheten eller annars som en följd av en skyldighet i lag eller författning. Det finns i svensk rätt flera bestämmelser om tystnadsplikt där obehörighetsrekvisitet används. Den praxis som finns rörande dessa bestämmelser bör i fråga om rekvisitets innebörd kunna tjäna som ledning även vid tolkningen och tillämpningen av den nu föreslagna bestämmelsen (prop. 2017/18:105 s. 134).

Enligt regeringen bör alltså den bestämmelse som nu föreslås ange att den som fullgör uppgift som dataskyddsombud inte obehörigen får röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om. Av bestämmelsen bör också framgå att offentlighets- och sekretesslagen gäller i det allmännas verksamhet. Bestämmelsen bör placeras i 3 kap. brottsdatalagen.

15.4 Sekretess för sammanställningar av känsliga personuppgifter

Regeringens bedömning: Någon förändring av den sekretessreglering som är tillämplig i behöriga myndigheters verksamhet behövs inte när det gäller uppgifter i sammanställningar av känsliga personuppgifter.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att det införs en regel om absolut sekretess till skydd för enskilda i offentlighets- och sekretesslagen. Den absoluta sekretessen föreslås gälla hos en behörig myndighet för uppgift i en sammanställning av känsliga personuppgifter. Enligt förslaget ska sekretessen gälla i högst 70 år och någon meddelarfrihet ska inte gälla för sådana uppgifter.

Remissinstanserna: *Eskilstuna tingsrätt* anser att skälen till att någon motsvarande sekretessbestämmelse inte införts i domstolsdatalagen (2015:728) fortfarande torde vara aktuella för domstolarnas del. *Umeå tingsrätt* är positiv till en bestämmelse om absolut sekretess, men är inte övertygad om att meddelarfriheten bör begränsas utan anser att den frågan bör övervägas ytterligare. *Journalistförbundet* avstyrker utredningens förslag om absolut sekretess och föreslår i stället att bestämmelsen förses med ett omvänt skaderekvisit. Journalistförbundet avstyrker även förslaget att meddelarfrihet inte ska gälla. *Tidningsutgivarna* förordar att bestämmelsen utformas med ett omvänt skaderekvisit och avstyrker utredningens förslag om att begränsa meddelarfriheten. *Skatteverket* anser att föremålet för sekretessen är otydligt formulerat i bestämmelsen och efterfrågar därför ett klargörande. Övriga instanser yttrar sig inte i den här delen.

Skälen för regeringens bedömning: I avsnitt 8.1.4 föreslår regeringen att det i ramlagen införs ett generellt förbud mot vissa sökningar. Det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Enligt utredningen bör det införas en sekretessregel som knyts till regeln om sökförbud i ramlagen. Utredningens skäl för att införa en sådan sekretessregel är att allmänheten inte med stöd av offentlighetsprincipen ska kunna få ut uppgifter i sammanställningar som utgör resultatet av sådana sökningar som sökförbudet är avsett att förhindra. Enligt utredningens förslag ska sekretessen vara absolut så att en behörig myndighet inte ska behöva göra en otillåten sökning för att kunna bedöma sekretessfrågan om uppgifter begärs ut (jfr prop. 2011/12:157 s. 17).

I likhet med utredningen anser regeringen att det är av stor vikt att enskildas integritet skyddas. Som utredningen påpekar rör det sig här om personuppgifter som omgärdas av starka dataskyddsregler. Redan i dag finns sekretessreglering som skulle aktualiseras om allmänheten begär ut känsliga personuppgifter sammanställda av behöriga myndigheter genom sökning. Som exempel kan nämnas att det i 18 kap. 1–2 §§ offentlighets- och sekretesslagen finns sekretessregler till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. I 35 kap. 1 § samma lag finns också en regel om sekretess till skydd för enskildas intressen i

förundersökning och annan brottsbekämpande verksamhet. Enligt 21 kap. 7 § offentlighets- och sekretesslagen gäller vidare sekretess för personuppgifter om det kan antas att uppgifterna efter ett utlämnande kommer att behandlas i strid med regleringen om hur personuppgifter får behandlas.

Några av remissinstanserna har haft synpunkter på utformningen av den av utredningen föreslagna sekretessbestämmelsen. Enligt regeringens bedömning ger den befintliga sekretessregleringen ett väl avvägt skydd för både enskilda och allmänna intressen i nu aktuellt avseende. Till skillnad från utredningen anser regeringen därför ett en regel om absolut sekretess för uppgifter i sammanställningar av känsliga personuppgifter hos behöriga myndigheter inte behöver införas. Som anges i avsnitt 8.1.4 ska tryckfrihetsförordningen tillämpas vid utlämnande av en allmän handling som sker på begäran av en enskild. Om en enskild begär att en behörig myndighet ska ta fram vissa uppgifter för ett utlämnande har myndigheten att ta ställning till om de uppgifter som efterfrågas utgör en allmän handling hos myndigheten. Utgör uppgifterna en allmän handling ska de lämnas ut såvida de inte omfattas av sekretess. Det gäller även om det är fråga om känsliga personuppgifter som har sammanställts genom sökning. Som nyss nämnts finns det befintliga sekretessregler som kommer att aktualiseras när det gäller sammanställningar av känsliga personuppgifter. Mot den bakgrunden anser regeringen att det inte behövs någon ändring av den sekretessreglering som är tillämplig i behöriga myndigheters verksamhet när gäller uppgifter i sådana sammanställningar.

16 Konsekvenser

16.1 Ett fåtal helt nya krav eller arbetsuppgifter men skärpta krav i vissa fall

Förslaget till brottsdatalag genomför dataskyddsdirektivet. En allmän utgångspunkt har varit att sträva efter lösningar som ansluter till nuvarande systematik för reglering av personuppgiftsbehandling. En strävan har också varit att ligga så nära dataskyddsförordningen som möjligt, när samma fråga behandlas i båda instrumenten och det inte finns sakliga skäl att välja en annan lösning för brottsdatalagens tillämpningsområde.

Direktivet innebär framför allt en harmonisering inom EU. De flesta bestämmelserna i brottsdatalagen motsvarar i större eller mindre utsträckning regler i personuppgiftslagen eller i myndigheternas registerförfattningar. Regeringens förslag ansluter nära till direktivet, men på ett fåtal punkter föreslås regler som ger ett starkare skydd för enskilda än vad som krävs enligt direktivet. I de flesta fall hör det samman med att den svenska lagstiftningen redan ger ett motsvarande skydd.

Förslagen i kapitlen 6, 7 och 8 har till stor del motsvarigheter i dagens lagstiftning. Kraven blir dock i vissa fall tydligare, vilket bör bidra till att lagstiftningen blir mer lättillämpad. I vissa avseenden ställs dock något högre krav på de personuppgiftsansvariga. Det gäller bl.a. att ytterligare

kategorier av personuppgifter ska betraktas som känsliga personuppgifter. Kraven på hur personuppgifternas kvalitet ska säkerställas blir också tydligare.

Även om många av kraven i kapitel 9 följer redan av dagens lagstiftning ställs det också vissa nya krav på de personuppgiftsansvariga. Det införs t.ex. skyldighet att dokumentera och rapportera personuppgiftsincidenter och kraven på organisatoriska och tekniska åtgärder blir tydligare och mera detaljerade än i dag. Det ställs också nya krav på att de personuppgiftsansvariga ska genomföra och dokumentera konsekvensbedömningar och ha förhandssamråd med tillsynsmyndigheten. Den skyldighet som flertalet av myndigheterna i rättskedjan har att utse personuppgiftsombud (i brottsdatalagen dataskyddsombud) blir generell. Kraven på personuppgiftsbiträden skärps och blir tydligare.

De skyldigheter för personuppgiftsansvariga som föreslås i kapitel 10 motsvaras till största delen av dagens krav, men enskildas rättigheter stärks genom att informationsskyldigheten utvidgas och förtydligas i viss utsträckning.

I kapitel 12 föreslås ett system med sanktionsavgifter för överträdelser av bestämmelser i brottsdatalagen. Det motsvarar det sanktionssystem som kommer att gälla för överträdelser av bestämmelser i dataskyddsförordningen. Det blir en ny arbetsuppgift för tillsynsmyndigheten att besluta om sanktionsavgifter, men antalet ärenden förväntas inte bli särskilt stort inom brottsdatalagens tillämpningsområde. Det beror bl.a. på att de som ska tillämpa brottsdatalagen till största delen är myndigheter, som i regel kan förväntas följa tillsynsmyndighetens synpunkter utan att det krävs repressiva åtgärder.

Förslagen beträffande rättsmedel och skadestånd i kapitel 13 motsvarar i allt väsentligt det som gäller i dag.

Reglerna om överföring till tredjeland och internationella organisationer i kapitel 14 motsvarar till stor del dem som finns i 2013 års lag. Grunderna för överföring har dock blivit fler och reglerna mer detaljerade. I några avseenden skärps också reglerna, bl.a. införs det krav på dokumentation och underrättelser till tillsynsmyndigheten. Reglerna kommer också att vara tillämpliga i många fler fall än i dag eftersom brottsdatalagen har ett vidare tillämpningsområde än 2013 års lag.

När det gäller kapitel 11, som behandlar tillsyn, innebär som nyss nämnts systemet med sanktionsavgifter en ny arbetsuppgift för tillsynsmyndigheten, men antalet ärenden inom brottsdatalagens tillämpningsområde förväntas inte bli särskilt stort. En annan nyhet är att tillsynsmyndigheten blir skyldig att utföra laglighetskontroller på begäran av enskilda inom hela brottsdatalagens tillämpningsområde, något som i dag endast utförs av Säkerhets- och integritetsskyddsnämnden i fråga om Polismyndighetens och Säkerhetspolisens personuppgiftsbehandling.

I kapitel 15 föreslås vissa ändringar i sekretessregleringen. De kan inte förväntas öka arbetsbördan för berörda myndigheter.

Den största förändringen som följer av EU:s dataskyddsreform är inte regeringens nu aktuella förslag utan det faktum att de som ska tillämpa brottsdatalagen med kompletterande lagstiftning även i varierande utsträckning ska tillämpa dataskyddsförordningen med kompletterande lagstiftning. Båda regelverken kommer att tillämpas parallellt, t.ex. när en personuppgift vid ett visst tillfälle ska behandlas både för ändamål inom

och utanför brottsdatalagens tillämpningsområde. Tillämparna måste således behärska dubbla regelverk.

16.2 Ekonomiska konsekvenser

16.2.1 Konsekvenser för staten

Regeringens bedömning: För de behöriga myndigheterna kommer förslaget till brottsdatalag att kräva utbildning. Kostnaderna för det bör rymmas inom befintliga anslag. Förslaget kommer också att innebära att de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter, men kostnadsökningarna kommer inte att bli större än att de ryms inom de befintliga ekonomiska ramarna.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Enligt *Justitiekanslern* har utredningen möjligen underskattat både behovet av och kostnaderna för utbildning. Justitiekanslern anser att det finns anledning att tro att relativt omfattande, både grundläggande och mera kvalificerade, utbildningsinsatser kommer att krävas inom alla berörda myndigheter. Även *Sveriges advokatsamfund* menar att behovet av utbildning, råd och stöd är omfattande för att personuppgiftsansvariga ska kunna leva upp till de krav som ställs och ser det som tveksamt om kostnadsökningarna kommer att rymmas inom befintliga anslag. Enligt *Kriminalvården* kommer inte bara utbildningsinsatser utan även utveckling och förvaltning av befintliga och nya it-system samt ambitionshöjningen vad gäller dataskyddsombudets uppgifter att leda till ökade kostnader. *Polismyndigheten* anser också att förslaget, utöver utbildning, kan väntas medföra behov av nya strukturer, ny mjukvara och eventuellt ny hårdvara. De ökade kostnader som skulle bli följden kommer enligt Polismyndigheten inte att rymmas inom befintligt anslag. Slutligen pekar ett antal domstolar på ekonomiska konsekvenser med anledning av utbildningsinsatser och anpassningar av it-system. *Domstolsverket* framhåller det problematiska i att det inte i något sammanhang görs en samlad bedömning av de konsekvenser som hela EU:s dataskyddsreform får för Sveriges Domstolar. Enligt Domstolsverket är det rimligt att anta att domstolarnas kostnader för bl.a. utbildningsinsatser, anpassningar av it-system, föreskrifter och rutiner inte kommer att rymmas inom befintliga anslag.

Skälen för regeringens bedömning: De förslag regeringen lägger fram kan som ett antal remissinstanser påpekar komma att kräva anpassningar och förändringar av it-system. När det gäller de ökade kraven på loggning föreslår regeringen att Sverige ska utnyttja möjligheten att skjuta upp tidpunkten när de förändringar som kan krävas ska vara genomförda till år 2023. Anledningen till det är som utvecklas i avsnitt 17.2.3 att myndigheterna behöver ha tid för att analysera vad de nya kraven innebär. Även om införandet av brottsdatalagen kan komma att medföra vissa kostnader för ändringar i system, bör dessa emellertid rymmas inom befintliga anslagsramar.

När ny lagstiftning införs krävs det normalt utbildningsinsatser. Det är inte unikt för de förslag som regeringen presenterar utan uppkommer

regelmässigt i olika lagstiftningsärenden. Att det krävs utbildning i detta fall beror inte heller enbart på den lagstiftning som regeringen nu föreslår utan på den samlade reformen. Kostnader för utbildning täcks normalt av myndigheternas anslag. Flera remissinstanser anser att utbildningsbehovet med anledning av den nu aktuella reformen är mycket omfattande. Som utredningen konstaterar har det vid genomförandet av andra stora reformer, t.ex. när offentlighets- och sekretesslagen infördes, inte ansetts nödvändigt att tillföra särskilda medel för utbildning. Kostnaderna för utbildning bör därför rymmas inom befintliga ramar även nu.

Ny lagstiftning kräver normalt också nya interna föreskrifter och styrande dokument. Det får anses ingå i de normala uppgifterna för myndigheterna.

Antalet beslut om sanktionsavgift bedöms av de skäl som nämns i avsnitt 16.1 bli få. Det bör därför inte påverka tillsynsmyndighetens arbetsbörda i någon större utsträckning. Eftersom sanktionsavgifterna kan vara kännbara ekonomiskt är det rimligt att utgå från att tillsynsmyndighetens beslut kommer att överklagas till allmän förvaltningsdomstol i relativt stor utsträckning. Det faktum att sådana beslut förväntas bli ovanliga innebär att även överklagandena bör stanna vid ett litet antal varje år. Kostnaderna för de allmänna förvaltningsdomstolarna bör därför rymmas inom befintliga anslagsramar.

16.2.2 Konsekvenser för kommuner och landsting

Regeringens bedömning: Eventuella kostnadsökningar som förslaget till brottsdatalag kan komma att medföra för kommuner eller landsting får anses vara marginella.

Utredningens bedömning överensstämmer delvis med regeringens. Att brottsdatalagen i vissa fall ska tillämpas i verksamhet som bedrivs av kommuner eller landsting innebär enligt utredningen inga ökade kostnader för dem.

Remissinstanserna: *Malmö kommun* påpekar att anpassningar av it-system och förändringar av arbetssätt kan medföra kostnader som är svåra att uppskatta i dagsläget.

Skälen för regeringens bedömning: Brottsdatalagens tillämpningsområde omfattar bl.a. myndigheter och andra aktörer som verkställer straffrättsliga påföljder. Viss vård, t.ex. ungdomsvård och vård för missbrukare, kan utdömas som en straffrättslig påföljd. Det innebär att brottsdatalagen blir tillämplig i viss verksamhet där man i dag tillämpar personuppgiftslagen eller lagen (2001:454) om behandling av personuppgifter inom socialtjänsten. Att brottsdatalagen ska tillämpas i stället för dataskyddsförordningen innebär i sig inga ökade kostnader.

Det som har sagts i avsnitt 16.2.1 om konsekvenserna för staten i fråga om it-system, utbildning och interna styrdokument har giltighet även för kommuner eller landsting. Regeringen bedömer dock att de kostnader som kan uppstå får anses vara marginella. De förändringar av it-system och styrdokument som kan komma att krävas med anledning av förslaget får, särskilt med beaktande av dagens reglering, anses utgöra ett mycket begränsat ingrepp i självstyrelsen. Regeringen bedömer att detta begrän-

sade ingrepp är nödvändigt mot bakgrund av intresset att skydda fysiska personers grundläggande fri- och rättigheter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

16.2.3 Konsekvenser för enskilda

Regeringens bedömning: Förslagen förbättrar skyddet för enskildas integritet och ger dem bättre förutsättningar att kunna ta till vara sina rättigheter. De medför inga ökade kostnader för enskilda.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig om bedömningen.

Skälen för regeringens bedömning: Förslagen syftar till att stärka integritetsskyddet för enskilda och att ge dem bättre möjligheter att kunna kontrollera hur deras personuppgifter behandlas. Förslagen får inte några konsekvenser för jämställdheten.

Förslagen förväntas inte leda till några kostnadsökningar för enskilda. Visserligen föreslås att de personuppgiftsansvariga i vissa fall ska kunna ta ut avgift för information som begärs, men det är i situationer där den enskilde alltför ofta återkommer med begäran om information. Den personuppgiftsansvarige kan då ge den enskilde informationen mot avgift i stället för att avslå begäran.

Det kan finnas fall där enskilda i egenskap av personuppgiftsansvariga ska tillämpa brottsdatalagen i stället för dataskyddsförordningen. Det torde röra sig om få fall och av de skäl som angetts tidigare finns det inte anledning att räkna med att de kommer att drabbas av några ökade kostnader.

16.3 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Regeringens bedömning: Förbättrat dataskydd ger möjlighet till ökat informationsutbyte mellan brottsbekämpande myndigheter, vilket är positivt för det brottsbekämpande arbetet. Förslagen förväntas inte få några direkta effekter på brottsligheten.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten* framhåller att en reform av den här omfattningen oundvikligen får konsekvenser för polisens kärnverksamhet. Enligt myndigheten finns det risk för hämmande effekter på brottsbekämpande myndigheters förmåga att fullgöra sina uppdrag, då ökade krav på administration och dokumentation innebär att resurser måste omfördelas från den brottsbekämpande verksamheten.

Skälen för regeringens bedömning: Förslagen kan inte förväntas få några direkta effekter på brottsligheten, eftersom det handlar om en administrativ reform.

När det gäller det brottsbekämpande arbetet kan däremot ett ökat informationsflöde både inom Sverige och mellan medlemsstaterna förväntas

få positiv inverkan. Särskilt för Polismyndigheten har olika initiativ till utökat utbyte av information inom EU och med de andra nordiska länderna visat sig ha en positiv effekt för brottsbekämpningen. Det gäller exempelvis det utökade utbytet av dna-uppgifter, fingeravtrycksuppgifter och kriminalregisterutdrag. Informationsutbytet bör enligt regeringens mening kunna förbättras ytterligare genom de nya dataskyddsreglerna. Harmoniserade regler om dataskydd underlättar också på annat sätt utbytet av information mellan brottsbekämpande myndigheter både inom och utom landet.

Polismyndigheten framför att ökade krav på administration och dokumentation riskerar att hämma den brottsbekämpande verksamheten. Även om en administrativ reform av det slag som det nu är fråga om kommer att kräva vissa resurser, särskilt i ett inledande skede, gör regeringen som nyss nämnts bedömningen att reformen i förlängningen kan förväntas ge positiva effekter för det brottsbekämpande arbetet.

16.4 Konsekvenser i övrigt

Regeringens bedömning: Förslagen förväntas inte få några andra konsekvenser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens bedömning: Förslagen får inte några samhällsekonomiska konsekvenser. Förslagen får inte heller några konsekvenser för jämställdheten eller andra konsekvenser som avses i 7 § förordningen (2007:1244) om konsekvensutredning vid regelgivning.

17 Ikraftträdande- och övergångsbestämmelser

17.1 Ikraftträdande

Regeringens förslag: Brottsdatalagen och övriga författningsförslag ska träda i kraft den 1 augusti 2018.

Ändringarna i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och brottsdatalagen som innebär att hänvisningen till 1996 års säkerhetsskyddslag ersätts med en hänvisning till den nya säkerhetsskyddslagen ska dock träda i kraft den 1 april 2019.

Utredningens förslag överensstämmer inte med regeringens. Utredningen föreslår endast att brottsdatalagen och övriga författningsförslag ska träda i kraft den 1 maj 2018.

Remissinstanserna: Ingen remissinstans invänder mot utredningens förslag.

Skälen för regeringens förslag: Enligt artikel 63 ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra direktivet. Bestämmelserna ska tillämpas av medlemsstaterna från och med samma dag. Den lagstiftning som regeringen nu föreslår bör därför träda i kraft så snart som möjligt. Mot den bakgrunden och med hänsyn till den tid som de olika leden i lagstiftningsprocessen kan förväntas ta anser regeringen att den 1 augusti 2018 framstår som den tidigaste möjliga tidpunkten för ikraftträdande av brottsdatalagen och de övriga författningsförslagen. För att all personuppgiftsbehandling på direktivets område, även sådan som inte omfattas av någon registerförfattning, ska ha rättsligt stöd under den tid som lagstiftningsarbetet med brottsdatalagen pågår har regeringen i propositionen Ny dataskyddslag föreslagit en övergångsreglering som ska tillämpas när personuppgiftslagen upphör att gälla (prop. 2017/18:105 s. 172 f.). Övergångsbestämmelsen som föreslås i propositionen bör upphävas i samband med att brottsdatalagen träder i kraft. Samtidigt bör, som föreslås i avsnitt 6.1.4, även 2013 års lag upphöra att gälla.

Regeringen har lämnat förslag om en ny säkerhetsskyddslag som ska träda i kraft den 1 april 2019 (prop. 2017/18:89). Hänvisningarna till den nu gällande säkerhetsskyddslagen (1996:627) i dels brottsdatalagen, dels den föreslagna lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning (se prop. 2017/18:105) bör samma dag ersättas av hänvisningar till den nya säkerhetsskyddslagen.

17.2 Övergångsbestämmelser

17.2.1 Ärendehandläggning m.m.

Regeringens förslag: Äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som har meddelats före brottsdatalagens ikraftträdande.

Regeringens bedömning: Det behövs ingen övergångsbestämmelse för ärenden om tillsyn som inte har avgjorts när brottsdatalagen träder i kraft och som rör personuppgiftsbehandling för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet.

Det behövs ingen övergångsbestämmelse för ärenden om skadestånd för felaktig personuppgiftsbehandling inom nyss nämnda områden.

Det behövs inga övergångsbestämmelser för de behöriga myndigheternas behandling av personuppgifter.

Utredningens förslag och bedömning överensstämmer till viss del med regeringens. För ärenden om tillsyn över personuppgiftsbehandling för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet som inte avgjorts när brottsdatalagen träder i kraft ska, enligt utredningens förslag, äldre bestämmelser om handläggningen fortsätta att gälla. Utredningen föreslår även att äldre bestämmelser ska fortsätta att gälla för ärenden om skadestånd för felaktig

personuppgiftsbehandling inom nyss nämnda områden, om skadan har orsakats före brottsdatalagens ikraftträdande.

Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag och bedömning: Det som kan behöva regleras i övergångsbestämmelser till brottsdatalagen – förutom bestämmelser som rör det nya sanktionssystemet (se avsnitt 17.2.2) och bestämmelser som rör loggning (se avsnitt 17.2.3) – är framför allt hur pågående ärenden hos de behöriga myndigheterna och hos de nuvarande tillsynsmyndigheterna bör hanteras.

I frågor som rör behandling av personuppgifter hos de behöriga myndigheterna bör den nya lagstiftningen tillämpas från det att den träder i kraft. Det innebär exempelvis att framställningar om att få del av information, ärenden om rättelse och andra oavslutade ärenden ska hanteras enligt brottsdatalagen. Några övergångsbestämmelser för de behöriga myndigheternas handläggning behövs därmed inte.

Beträffande tillsynsåtgärder följer det av allmänna principer att förelägganden och förbud som har meddelats med stöd av personuppgiftslagen och som rör brottsdatalagens tillämpningsområde fortsätter att gälla efter det att personuppgiftslagen upphävts. Det behövs därför inte någon särskild övergångsbestämmelse för det.

När det gäller andra frågor om tillsyn över behandling av personuppgifter inom brottsdatalagens tillämpningsområde föreslår utredningen att äldre bestämmelser ska fortsätta att gälla för de ärenden som har påbörjats före ikraftträdandet men inte hunnit avgöras när den nya ramlagen träder i kraft. I förslaget om en ny dataskyddslag (prop. 2017/18:105) föreslår regeringen inte någon motsvarande övergångsbestämmelse. Regeringen gör i det ärendet bedömningen att det saknas skäl för en sådan övergångsbestämmelse eftersom Datainspektionen påpekat att pågående behandling ska bedömas enligt regleringen i dataskyddsförordningen när den börjar tillämpas, dvs. från och med den 25 maj 2018 (se a. prop. s. 175 f.). Mot denna bakgrund anser regeringen att det inte heller bör införas någon sådan övergångsbestämmelse till brottsdatalagen.

Utredningen föreslår även en övergångsbestämmelse som anger att äldre föreskrifter om skadestånd fortfarande ska gälla för skada som har orsakats före brottsdatalagens ikraftträdande p.g.a. felaktig personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Det följer emellertid redan av allmänna rättsgrundsatser att ny lagstiftning ska gälla i fråga om skadestånd med anledning av skadefall som inträffar efter ikraftträdandet, medan äldre lag ska tillämpas på skadefall som har inträffat dessförinnan (prop. 1972:5 s. 593 och prop. 2017/18:105 s. 176). Någon särskild övergångsbestämmelse om detta behövs därför inte. Utredningens förslag bör alltså inte genomföras i den delen heller.

Utredningen föreslår vidare en övergångsbestämmelse om att äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som har meddelats före brottsdatalagens ikraftträdande och som rör behandling av personuppgifter för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Regeringen instämmer i utredningens uppfattning att en sådan övergångsbestämmelse behövs. Det innebär bl.a. att domstolen vid sin prövning ska tillämpa den äldre lagstiftningen.

17.2.2 Övergångsbestämmelser till det nya sanktionssystemet

Regeringens förslag: Någon sanktionsavgift får inte tas ut för sådana överträdelser av bestämmelser om personuppgiftsbehandling för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet som har skett före brottsdatalagens ikraftträdande.

Äldre föreskrifter ska fortsätta att gälla för överträdelser som har skett före ikraftträdandet.

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna: Ingen remissinstans yttrar sig i denna del.

Skälen för regeringens förslag

Ett nytt sanktionssystem införs

Enligt allmänna principer får en ny lag inte retroaktiv verkan. Frågan kompliceras emellertid i de fall där den nya lagen innehåller sanktionsbestämmelser, vilket är fallet med brottsdatalagen.

I avsnitt 12 föreslår regeringen ett nytt sanktionssystem för överträdelser av bestämmelserna om behandling av personuppgifter i ramlagen. Förslaget innebär att överträdelser ska beivras genom sanktionsavgift, som är en administrativ sanktion. Sanktionsavgift föreslås kunna tas ut både för överträdelser som inte varit straffsanktionerade tidigare och för överträdelser som i dag omfattas av straffansvaret i 49 § personuppgiftslagen. Sanktionsavgift ska tas ut av personuppgiftsansvariga och i vissa fall av personuppgiftsbiträden. Det gäller oavsett om de är juridiska eller fysiska personer. I huvudsak kommer sanktionsavgift att tas ut av andra rättssubjekt än de som i dag kan åläggas straffansvar. Det nya sanktionssystemet aktualiserar emellertid frågan hur överträdelser som begåtts före brottsdatalagens ikraftträdande bör hanteras.

Som framgår av avsnitt 12.2.1 föreslår regeringen ingen ny straffbestämmelse. Eftersom någon motsvarighet till 49 § personuppgiftslagen inte tas in i ramlagen bortfaller straffansvaret för de gärningar som regleras där, om inte frågan regleras genom särskilda övergångsbestämmelser.

Förbudet mot retroaktivitet och lindrigaste lagens princip

Vid bedömningen av om det behövs övergångsbestämmelser för de överträdelser som har begåtts tidigare men inte hunnit beivras när brottsdatalagen träder i kraft, ska artikel 7 i Europakonventionen, 2 kap. 10 § regeringsformen och 5 § andra stycket lagen (1964:163) om införande av brottsbalken beaktas.

Enligt artikel 7 i Europakonventionen får ingen fällas till ansvar för någon gärning eller underlåtenhet som vid den tidpunkt då den begicks inte utgjorde ett brott enligt nationell eller internationell rätt. Inte heller får ett strängare straff utmätas än som var tillämpligt vid den tidpunkt då brottet begicks.

I 2 kap. 10 § regeringsformen förbjuds retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses vara analogt tillämpligt på straffliknande administrativa påföljder (prop. 1975/76:209 s. 125). Av

5 § andra stycket lagen om införande av brottsbalken framgår att straff ska bestämmas enligt den lag som gällde när gärningen företogs, utom i fall där annan lag gäller när dom meddelas och den nya lagen leder till frihet från straff eller lindrigare straff. Bestämmelsen har enligt förarbetena generell räckvidd, dvs. den gäller även utanför brottsbalken (prop. 1964:10 s. 99). Den ger uttryck för det som brukar kallas den lindrigaste lagens princip.

Det behövs särskilda övergångsbestämmelser

Regeringen föreslår att vissa handlingar som i dag inte är straffbara ska kunna föranleda sanktionsavgift (se avsnitt 12.5.2). Det gäller exempelvis skyldigheten att anmäla personuppgiftsincidenter. Handlingar som i dag är straffbara föreslås inte längre kunna bestraffas men däremot kunna föranleda sanktionsavgift. Det gäller t.ex. otillåten överföring av personuppgifter till tredjeland.

Om en sådan överträdelse som kan leda till sanktionsavgift men som inte är straffbelagd i dag har inträffat före ikraftträdandet skulle det strida mot retroaktivitetsförbudet att besluta om sanktionsavgift. Detsamma gäller om en skyldighet blir mer omfattande än vad den är i dag. I vissa fall har brottsdatalagen liknande bestämmelser som de som finns i personuppgiftslagen, men det kan skilja sig i fråga om detaljer. Det kan då vara svårt att avgöra om det är fråga om ett förfarande som tidigare kunnat föranleda straff. Eftersom tillämpningsområdet för sanktionsavgift inte är detsamma som för straffansvar är det inte rimligt att låta systemet med sanktionsavgift gälla retroaktivt. Det är inte heller självklart hur bedömningen av vilken sanktion som är lindrigast – straffpåföljd eller sanktionsavgift – skulle utfalla i ett enskilt fall.

För att undvika de tolknings- och tillämpningsproblem som kan uppstå om den lindrigaste lagens princip skulle tillämpas på sanktionsavgift enligt brottsdatalagen är det enligt utredningens mening lämpligare att låta äldre bestämmelser fortsätta att gälla för de överträdelser som har begåtts innan brottsdatalagen trätt i kraft. Regeringen gör ingen annan bedömning. Det kan tilläggas att syftet med brottsdatalagens system med sanktionsavgifter är att effektivisera sanktionssystemet. Att överträdelser mot dataskyddsregleringen föreslås avkriminaliseras ska inte ses som ett uttryck för att överträdelserna ska bedömas lindrigare än tidigare. Sanktionsavgift bör därför bara kunna tas ut för överträdelser som ägt rum efter brottsdatalagens ikraftträdande, vilket bör tydliggöras genom en övergångsbestämmelse. För ett liknande resonemang rörande sanktionsväxling, se prop. 2012/13:143 s. 82 f. och prop. 2017/18:105 s. 176 f.

I likhet med utredningen anser regeringen att det är viktigt att de överträdelser som är straffsanktionerade kan beivras även efter ikraftträdandet av brottsdatalagen. Därför bör det även införas en övergångsbestämmelse som innebär att äldre föreskrifter ska fortsätta att gälla för överträdelser som har skett före ikraftträdandet.

17.2.3 Övergångsbestämmelser i övrigt

Regeringens förslag: Bestämmelsen om loggning behöver inte tillämpas på automatiserade behandlingssystem som har inrättats före den 6 maj 2016 förrän den 6 maj 2023.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag behöver bestämmelsen om loggning inte tillämpas på automatiserade behandlingssystem som har inrättats före den 6 maj 2018 förrän den 1 maj 2023.

Remissinstanserna: *Domstolsverket* påpekar att det är ett mycket omfattande arbete att se över existerande loggar och tillstyrker därför förslaget. *Datainspektionen* anser att förslaget riskerar att kraftigt försvaga nuvarande krav på loggning enligt 31 § personuppgiftslagen. Enligt inspektionen finns det en uppenbar risk för att tillsynsmyndigheten hamnar i tillämpningssvårigheter och gränsdragningsproblem vid tillämpning av bestämmelsen. Under alla omständigheter bör det, enligt Datainspektionen, vara tillräckligt med en tvåårsperiod för att implementera förändringar i automatiserade behandlingssystem. Övriga remissinstanser yttrar sig inte om förslaget.

Skälen för regeringens förslag

Särskilda övergångsbestämmelser för existerande behandlingssystem

Som tidigare nämnts ska de författningar som genomför direktivet vara i kraft senast den 6 maj 2018. Enligt artikel 63.2 får dock medlemsstaterna, om det skulle innebära oproportionerliga ansträngningar att anpassa ett automatiserat system som inrättats innan den 6 maj 2016, föreskriva att systemet ska anpassas till artikel 25.1 (kravet på loggning) senast den 6 maj 2023. Under exceptionella omständigheter får enligt artikel 63.3 en medlemsstat medge ytterligare anstånd med anpassningen, dock längst till den 6 maj 2026. Kommissionen ska, om det undantaget utnyttjas, underrättas om skälen till problemen och motiveringen för tidsperioden för anpassning.

Myndigheterna i rättskedjan använder automatiserade behandlingssystem som inrättats före den 6 maj 2016. I direktivet ställs mer detaljerade krav än tidigare på loggning i sådana system. Samtliga myndigheter har till utredningen uppgett att de behöver tid för att närmare analysera behovet av anpassningar och för att utforma systemen efter de krav på loggning som föreslås i avsnitt 9.2.2. Det kommer att krävas noggranna verksamhets- och systemanalyser för att klarlägga i vilken utsträckning dagens system för loggning uppfyller kraven och vilka eventuella förändringar som kan behövas. Arbetet med att analysera vilka anpassningar som krävs skulle möjligen hinna genomföras till dess att brottsdatalagen börjar gälla, men det anses inte vara möjligt att inom den korta tiden till ikraftträdandet också hinna anpassa systemen. Det kan vidare krävas viss samordning mellan myndigheterna, eftersom de utbyter många uppgifter elektroniskt och i vissa fall använder samma datasystem. Vad myndigheterna framfört visar att det skulle innebära oproportionerliga ansträngningar för dem att redan vid lagens ikraftträdande anpassa sina nuvarande system till loggningskraven. Till skillnad från *Datainspektionen* gör

regeringen bedömningen att en tvåårig tidsperiod för anpassning inte är tillräcklig. Regeringen håller i stället med utredningen om att det finns behov av en sådan övergångsbestämmelse som direktivet medger. Regeringen föreslår följaktligen att det införs en övergångsbestämmelse i brottsdatalagen som innebär att den nya bestämmelsen om loggning inte behöver tillämpas före den 6 maj 2023. Enligt utredningens förslag behöver loggningsbestämmelsen inte tillämpas före den tidpunkten på system som har inrättats före den 6 maj 2018. Den möjlighet direktivet ger att skjuta upp anpassningen gäller dock bara i fråga om system som har inrättats före den 6 maj 2016.

Datainspektionen uttrycker oro för att den föreslagna övergångsbestämmelsen ska försvaga det krav på loggning som följer av det övergripande kravet att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter. Som utredningen understryker sker i dag loggning i automatiserade behandlingssystem. Den föreslagna övergångsbestämmelsen träffar endast de mer preciserade kraven på loggning som uppställs i direktivet och påverkar inte de generella krav på loggning som redan gäller.

Övriga lagändringar

När det gäller övriga lagändringar ska de enligt huvudprincipen gälla från och med att de träder i kraft. Några övergångsbestämmelser behövs inte.

18 Författningskommentar

18.1 Förslaget till brottsdatalag

1 kap. Allmänna bestämmelser

Syftet med lagen

1 §

Paragrafen tydliggör att lagen genomför dataskyddsdirektivet och reglerar syftet med lagen. Den behandlas i avsnitt 6.1.3.

I *första stycket* anges att lagen genomför Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

I *andra stycket*, som genomför artikel 1, anges det övergripande syftet med lagen. Syftet är dubbelt. Det ena syftet är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter. Genom formuleringen tydliggörs att lagens skyddsobjekt är fysiska personer. Lagen innehåller inga bestämmelser till skydd för juridiska personer. Det andra syftet är att säkerställa att de myndigheter som är behöriga myndigheter enligt lagen kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt vid brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet. Det gäller både nationellt och internationellt informationsutbyte.

Paragrafen har utformats i enlighet med *Lagrådets* förslag.

Lagens tillämpningsområde

2 §

I paragrafen, som tillsammans med 3 och 4 §§ genomför artikel 2, anges lagens tillämpningsområde. Den behandlas i avsnitt 6.4.1–6.4.4. Gränsdragningsfrågor behandlas i avsnitt 6.7.

Lagen gäller vid behandling av personuppgifter. Vad som är en personuppgift och behandling av personuppgifter definieras i 6 §.

Lagen gäller bara när en behörig myndighet behandlar personuppgifter för vissa syften. Behörig myndighet definieras i 6 §.

Det framgår inte direkt av lagen vilka som är behöriga myndigheter. Det avgörande är om myndigheten har sådana uppgifter att den behandlar personuppgifter för syftena brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Ekobrottsmyndigheten, Åklagarmyndigheten, de allmänna domstolarna och Kriminalvården är behöriga myndigheter, men enbart när de behandlar personuppgifter för sådana syften. När t.ex. Skatteverket behandlar personuppgifter i beskattningsverksamheten eller Polismyndigheten utfärdar pass är myndigheten inte en behörig myndighet. Lagen gäller således inte generellt i de behöriga myndigheternas verksamhet. Även andra myndigheter än de

nyss nämnda har vissa arbetsuppgifter som gör lagen tillämplig, t.ex. Rättsmedicinalverket vid rättsmedicinska obduktioner och utfärdande av rättsintyg, Justitiekanslern i egenskap av åklagare i mål om tryckfrihetsbrott och yttrandefrihetsbrott och allmänna förvaltningsdomstolar när de prövar frågor som rör verkställighet av straff.

Exempel på arbetsuppgifter som inte gör en myndighet till behörig myndighet i lagens mening är skyldighet att anmäla brott eller annan uppgiftsskyldighet till brottsbekämpande myndigheter. Det förhållandet att en brottmålsdom expedieras till någon eller att en viss myndighet får tillgång till uppgifter om lagöverträdelser i belastningsregistret eller misstankeregistret gör inte heller att mottagaren av personuppgifterna blir en behörig myndighet i lagens mening.

Även andra aktörer än myndigheter kan vara behöriga myndigheter i lagens mening, om de har anförtrotts myndighetsutövning för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Det gäller t.ex. när naturvårdsvakter och jakttillsynsmän tar egendom i beslag och när ordningsvakter upprätthåller allmän ordning och säkerhet exempelvis vid domstolsförhandlingar.

Lagen ska däremot inte tillämpas av offentliga försvarare, målsägandebiträden och särskilda företrädare för barn. Eftersom någon myndighetsutövning inte har överlåtits till dem är de inte behöriga myndigheter i lagens mening.

Lagen gäller bara när behöriga myndigheter behandlar personuppgifter för vissa syften, nämligen att förebygga, förhindra eller upptäcka brottslig verksamhet, att utreda eller lagföra brott, att verkställa straffrättsliga påföljder eller att upprätthålla allmän ordning och säkerhet. När en behörig myndighet behandlar personuppgifter för något annat syfte gäller inte lagen.

Det är bl.a. Polismyndighetens och andra myndigheters underrättelseverksamhet som avses när formuleringen förebygga, förhindra eller upptäcka brottslig verksamhet används. Med underrättelseverksamhet avses arbete med insamling, bearbetning och analys av information i syfte att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att ett visst konkret brott har begåtts (prop. 2009/10:85 s. 318). Om det finns misstankar om ett konkret brott kan personuppgifter behandlas för att utreda brottet. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet med behandlingen är att förhindra brott. Annan brottsförebyggande verksamhet kan också omfattas av tillämpningsområdet, vilket utvecklas i avsnitt 6.4.2.

Lagen ska däremot inte tillämpas vid sådan kontrollverksamhet som vissa myndigheter som också har ett brottsbekämpande uppdrag utför med stöd av sina kontrollbefogenheter, t.ex. vid skattekontroll eller tullkontroll.

Med att utreda brott avses framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses ett konkret brott. Det kan vara fråga om såväl brott som bevisligen har begåtts som brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Om misstankarna enbart avser icke-preciserad brottslighet, är det i stället fråga om underrättelseverksamhet. Även den form av förenklat utredningsförfarande som regleras i 23 kap. 22 §

rättegångsbalken och åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken innan förundersökning har hunnit inledas omfattas av tillämpningsområdet. Brottsbekämpande myndigheters handläggning av brottsanmälningar hör också hit, även om de leder till beslut om att inte inleda förundersökning.

Reglerna om förundersökning i brottmål tillämpas även vid vissa andra typer av undersökningar. I den mån sådana undersökningar görs i syfte att utreda brott, t.ex. vid utredning om utlämning för brott, är lagen tillämplig. Görs de däremot i annat syfte, t.ex. för att ge underlag för bedömningar inom socialtjänsten, är lagen inte tillämplig.

Med uttrycket lagföra brott avses framför allt åklagares beslut i åtalsfrågor och om åtalsunderlåtelser samt brottmålsförfarandet i allmän domstol. Till brottmålsförfarandet räknas inte bara den rättegång och dom som följer på allmänt åtal utan även handläggningen av förprocessuella frågor som exempelvis förordnande av målsägandebiträde och offentlig försvarare och beslut om häktning och andra straffprocessuella tvångsmedel. Även expediering av domar och beslut hör till brottmålsförfarandet. Vid behandling av personuppgifter för sådana syften ska lagen tillämpas. Detsamma gäller vid personutredning inom ramen för brottmålet och i sådan stödverksamhet som avser att tillföra åklagare eller domstolar forensisk, medicinsk eller psykiatrisk kompetens.

I uttrycket lagföra brott ingår också de förenklade straffrättsliga förfaranden som i huvudsak används vid bötesbrott, föreläggande av ordningsbot och strafföreläggande.

Behandling av personuppgifter i syfte att verkställa straffrättsliga påföljder förekommer hos ett flertal myndigheter. Kriminalvården verkställer fängelsestraff, skyddstillsyn och samhällstjänst och ska då tillämpa lagen. Det är dock inte vid all behandling av personuppgifter i Kriminalvården som lagen ska tillämpas. När Kriminalvården exempelvis bedriver hälso- och sjukvård i fängelser och häkten ligger det utanför lagens tillämpningsområde. Kriminalvårdens hantering av administrativa frihetsberövanden ligger också utanför tillämpningsområdet.

När påföljden bestämts till böter behandlas personuppgifter av Polismyndigheten i egenskap av uppbördsmyndighet. Vid sådan behandling av personuppgifter är lagen tillämplig.

Statens institutionsstyrelse verkställer sluten ungdomsvård. Även socialnämnder verkställer i viss utsträckning straffrättsliga påföljder när påföljden är ungdomsvård, ungdomstjänst eller vård av missbrukare. På motsvarande sätt verkställer rättspsykiatriska enheter rättspsykiatrisk vård. Vid behandling av personuppgifter för sådana syften ska lagen tillämpas.

Lagen ska också tillämpas vid behöriga myndigheters behandling av personuppgifter när frågor som rör verkställigheten eller ändring av en straffrättslig påföljd prövas. Den är också tillämplig vid internationellt samarbete för de syften som anges i paragrafen. Det innebär att den ska tillämpas exempelvis vid informationsutbyte för brottsbekämpning och i ärenden om utlämning, överförande av lagföring och överförande av straffverkställighet.

Det är framför allt Polismyndigheten som har till uppgift att upprätthålla allmän ordning och säkerhet. Lagen ska bl.a. tillämpas på behandling av personuppgifter vid ingripanden enligt 13–13 c §§ polislagen

(1984:387), men inte vid förvaltningsbeslut enligt ordningslagen (1993:1617). Även Kustbevakningen har vissa ordningshållande uppgifter och ska då tillämpa lagen i samma utsträckning som Polismyndigheten. Polismyndighetens, åklagares och domstolars handläggning av frågor som rör tillträdesförbud vid idrottsarrangemang och det register över sådana förbud som Polismyndigheten för omfattas också av ramlagens tillämpningsområde. Däremot ska lagen inte tillämpas vid idrottsorganisationers behandling av uppgifter om sådana förbud, eftersom de inte är behöriga myndigheter.

Lagen ska även – under förutsättning att inte undantagsbestämmelsen i 1 kap. 4 § är tillämplig – tillämpas av militärpolisen, ordningsvakter och skyddsvakter när de ingriper i syfte att upprätthålla allmän ordning och säkerhet. Detsamma gäller sådana väktare som genom särskilt förordnande anförtrotts myndighetsutövning för något av de syften som gör lagen tillämplig. Avser förordnandet något annat syfte, t.ex. kontroll av flygpassagerare, är lagen inte tillämplig.

Behandling av personuppgifter vid omhändertagande enligt lagen (1976:511) om omhändertagande av berusade personer m.m. är ett annat exempel på när lagen inte ska tillämpas. Informationssäkerhet ligger också utanför lagens tillämpningsområde.

Om det ursprungliga syftet med att behandla personuppgifterna upphör, är lagen inte längre tillämplig. Ett exempel är att ett enskilt anspråk, som har behandlats tillsammans med ett brottmål, avskiljs för att i stället handläggas enligt den ordning som är föreskriven för tvistemål. Ett annat exempel är att det under en förundersökning klarläggs att det inte föreligat något brott, t.ex. att ett misstänkt dödsfall var naturligt. Någon grund för att behandla personuppgifterna med stöd av lagen finns då inte längre, annat än för att avskriva saken.

För att lagen ska vara tillämplig krävs både att myndigheten är behörig och att behandlingen i det enskilda fallet utförs för något av de tillåtna syftena. Det innebär att om t.ex. Polismyndigheten samtidigt skickar samma personuppgift rörande en ung lagöverträdare till två olika mottagare (åklagaren respektive socialnämnden) är lagen tillämplig i det ena fallet men inte i det andra beroende på att behandlingen har olika syften (att redovisa underlag för åklagarens beslut i fråga om förundersökning respektive att fästa socialnämndens uppmärksamhet på att nämndens sociala insatser kan behövas).

När det gäller tillämpningsområdet görs ingen skillnad mellan att uppgifter behandlas för en behörig myndighets egen verksamhet eller för att bistå en annan svensk eller utländsk behörig myndighet, så länge syftet med behandlingen är något av de som anges i lagen. Om t.ex. Åklagarmyndigheten bistår en utländsk myndighet med någon utredningsåtgärd inom ramen för internationell rättslig hjälp i brottmål eller i samband med att en arresteringsorder från en annan medlemsstat behandlas, ska lagen tillämpas.

Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Den gäller inte heller i verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Undantagen framgår av 4 §.

3 §

Paragrafen begränsar lagens tillämpningsområde huvudsakligen till helt eller delvis automatiserad behandling av personuppgifter, men även viss manuell behandling omfattas. Paragrafen genomför artikel 2.2 och behandlas i avsnitt 6.4.5.

För att lagen ska vara tillämplig krävs att behandlingen är helt eller delvis automatiserad eller att personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. När det gäller automatiserad behandling krävs det inte att de hanterade personuppgifterna finns i något som kan karaktäriseras som ett register eller att de annars är ordnade på visst sätt. Även behandling av enstaka personuppgifter, t.ex. namn, i löpande text omfattas således av lagens tillämpningsområde. Helt manuell behandling av personuppgifter som inte ingår i någon samling och inte heller är avsedda att ingå i en sådan, exempelvis handskrivna minnesanteckningar, ligger däremot utanför tillämpningsområdet.

4 §

Paragrafen reglerar i enlighet med artikel 2.3 och skäl 14 undantag från lagens tillämpningsområde. Paragrafen behandlas i avsnitt 6.5.1.

I paragrafen undantas Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet från tillämpningsområdet. Däremot undantas inte Säkerhetspolisens personuppgiftsbehandling i övrigt, exempelvis när myndigheten handlägger en förundersökning som den övertagit från Polismyndigheten med stöd av 30 § förordningen (2014:1102) med instruktion för Polismyndigheten.

I paragrafen anges även att lagen inte gäller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen eller i verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Något motsvarande generellt undantag för personuppgiftsbehandling som rör nationell säkerhet gäller inte för andra myndigheter som tillämpar lagen. Det innebär exempelvis att Åklagarmyndigheten och allmänna domstolar ska tillämpa lagen även vid handläggning av mål om brott mot Sveriges säkerhet.

Avvikande bestämmelser i annan författning

5 §

Paragrafen reglerar lagens förhållande till avvikande bestämmelser i en annan lag eller en förordning. Paragrafen behandlas i avsnitt 6.1.2 och 6.3.

Lagen är subsidiär till annan lagstiftning. Det innebär att om det finns avvikande bestämmelser i t.ex. en viss myndighets registerförfattning, som polisdatalagen (2010:361) eller åklagardatalagen (2015:433), eller i en författning som reglerar ett visst register, som lagen (1998:620) om belastningsregister, eller visst samarbete inom direktivets tillämpningsområde, gäller de i stället för bestämmelserna i lagen. Detsamma

gäller avvikande bestämmelser i rättegångsbalken och offentlighets- och sekretesslagen (2009:400).

Avvikande bestämmelser kan också finnas i författningar som genomför dataskyddsbestämmelser som har sin grund i rättsakter och avtal som enligt artiklarna 60 och 61 i direktivet ska ha företräde därför att de har tillkommit före direktivet, t.ex. samarbete enligt Prümrådsbeslutet som regleras i 4 kap. lagen (2017:496) om internationellt polisiärt samarbete.

Definitioner

6 §

I paragrafen, som genomför artikel 3, definieras vissa uttryck som används i lagen.

Behandling av personuppgifter

Definitionen motsvarar direktivets definition av behandling i artikel 3.2. Uttrycket behandlas i avsnitt 6.2.

Uttrycket behandling av personuppgifter omfattar alla åtgärder som vidtas med sådana uppgifter. Så snart personuppgifter hanteras på något sätt är det fråga om behandling som omfattas av lagens bestämmelser, om den är helt eller delvis automatiserad eller avser manuell behandling i en strukturerad samling av personuppgifter. Uppräkningen i definitionen av olika sätt att hantera personuppgifter är således inte uttömmande.

Behörig myndighet

Definitionen, som har utformats i enlighet med *Lagrådets* förslag, motsvarar direktivets definition av behörig myndighet i artikel 3.7. Uttrycket behandlas i avsnitt 6.4.4. Gränsdragningsfrågor behandlas i avsnitt 6.7.

Det framgår inte direkt av lagen vilka myndigheter som är behöriga myndigheter. Det avgörande är om myndigheten har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Myndigheterna är behöriga myndigheter bara när de utför sådana uppgifter. Vad som ryms i de uppgifterna och i vilka fall någon kan vara behörig myndighet utvecklas i kommentaren till 2 §. En myndighet kan således vara både behörig och icke behörig i lagens mening beroende på vilka uppgifter som utförs. En myndighet är vidare endast behörig när den behandlar personuppgifter för syftena brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet.

Även andra aktörer än myndigheter kan vara behöriga myndigheter i lagens mening om de har anförtrotts myndighetsutövning för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Det utvecklas i kommentaren till 2 §.

Biometriska uppgifter

Definitionen utgår från hur biometriska uppgifter definieras i artikel 3.13. Uttrycket behandlas i avsnitt 6.2.

Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är

riktig. Den baseras på fysiska karaktärsdrag hos den som ska identifieras. Mönster av fingeravtryck, ansiktsgeometri, ögats iris, regnbågshinna och näthinna, röst, hand, blodkärl, dna eller gång är exempel på områden där sådan teknik kan användas. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Uppgifterna kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. Fingeravtryck är en vanlig form av biometrisk uppgift. Personuppgifter, t.ex. fingeravtryck, som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska uppgifter utgör däremot inte biometriska uppgifter.

Biometriska uppgifter i form av fingeravtryck kan framgå av ett spår som påträffas vid utredning av ett brott. Även analys av spåren omfattas av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Dna-spår behandlas i kommentaren till uttrycket genetiska uppgifter.

Av 2 kap. 12 § framgår att biometriska uppgifter som används i syfte att identifiera en person är känsliga personuppgifter som bara får behandlas om det är särskilt föreskrivet och absolut nödvändigt.

Fotografier och filmer som inte bearbetas tekniskt i syfte att åstadkomma unik identifiering faller utanför definitionen. Bearbetning av bilder av personer för att förbättra bildkvaliteten, förstärka detaljer och liknande omfattas alltså inte. Om bilder däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram i syfte att identifiera personer omfattas de av definitionen. Att fotografier kan omfattas av regleringen av känsliga personuppgifter på andra grunder behandlas i kommentaren till 2 kap. 11 §.

Dataskyddsombud

Dataskyddsombud definieras inte i direktivet. Uttrycket behandlas i avsnitt 9.5.1.

Ett dataskyddsombud är en fysisk eller juridisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen. Ett dataskyddsombud kan antingen vara anställd hos den personuppgiftsansvarige eller en utomstående. Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden förutsätts framför allt ha goda kunskaper om reglerna om personuppgiftsbehandling. Ombuden bör också ha sådan ställning i organisationen att deras synpunkter och råd tas på allvar.

Dataskyddsombudens uppgifter regleras i 3 kap. 14 §.

Genetiska uppgifter

Definitionen utgår från hur genetiska uppgifter definieras i artikel 3.12. Uttrycket behandlas i avsnitt 6.2.

All information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från t.ex. en brottsplats eller ett prov från människokroppen omfattas av definitionen. Det innebär att den är något vidare än direktivets definition, som enbart omfattar

information om en persons fysiologi eller hälsa som härrör från en analys av ett prov från personen i fråga.

Genetiska uppgifter behandlas vid dna-analyser i forensisk verksamhet för att ta fram dna-profiler eller forensiska uppslag. Behandlingen kan avse genetiska uppgifter från såväl identifierade som oidentifierade personer. Eftersom nedärvda eller förvärvade genetiska kännetecken för en person kan framgå av ett spår som påträffas vid utredning av ett brott, omfattas även analys av spåren av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Själva dna-profilen, som behandlas i exempelvis Polismyndighetens dna-register, utgör däremot inte en genetisk uppgift, eftersom inga nedärvda eller förvärvade genetiska kännetecken kan utläsas ur den.

I 28 kap. 12–12 b §§ rättegångsbalken finns bestämmelser om provtagning för dna-analys.

Av 2 kap. 12 § framgår att genetiska uppgifter är känsliga personuppgifter som bara får behandlas om det är särskilt föreskrivet och absolut nödvändigt.

Internationell organisation

Definitionen utgår från hur internationell organisation definieras i artikel 3.16. Uttrycket behandlas i avsnitt 14.2.4.

Med internationell organisation avses dels organisationer och deras underställda organ som lyder under folkrätten, dels andra organ som inrättats genom eller på grundval av överenskommelser mellan två eller flera stater. Interpol och Världstullorganisationen (World Customs Organization) är exempel på internationella organisationer som omfattas av definitionen. Internationella domstolar och tribunaler som t.ex. Internationella brottmålsdomstolen, Internationella krigsförbrytartribunalen för det forna Jugoslavien och Tribunalen för Libanon ska också betraktas som internationella organisationer.

Medlemsstat

Definitionen har ingen motsvarighet i direktivet. Uttrycket behandlas i avsnitt 14.2.2.

Med medlemsstat avses sådana stater som är bundna av direktivet, vilket gäller EU:s medlemsstater. Dessutom ska några stater utanför EU – Island, Liechtenstein, Norge och Schweiz – tillämpa direktivet. Även de senare är medlemsstater i lagens mening.

Mottagare

Definitionen utgår från hur mottagare definieras i artikel 3.10. Uttrycket behandlas i avsnitt 6.2.

Mottagare definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Undantaget omfattar bl.a. myndigheter som tar del av personuppgifter i sin tillsyn över viss verksamhet, t.ex. Datainspektionen och Säkerhets- och integritetsskyddsnämnden som båda utövar tillsyn över personuppgiftsbehandling. Även andra myndigheter som utövar tillsyn, t.ex. JO och Justitiekanslern, omfattas av undantaget.

Personuppgift

Definitionen utgår från hur personuppgift definieras i artikel 3.1. Med personuppgift avses varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Uttrycket behandlas i avsnitt 6.2.

Varje upplysning som kan hänföras till en fysisk person är en personuppgift. Det gäller även upplysningar som kan hänföras till en individ om en fysisk person kan identifieras med hjälp av informationen. Det krävs inte att den personuppgiftsansvarige ska förfoga över samtliga uppgifter som gör identifieringen möjlig. Det innebär att t.ex. oidentifierade fingeravtryck och dna-profiler är personuppgifter, eftersom det är möjligt att identifiera en person med hjälp av dem. Även bild- eller ljudupptagningar kan utgöra personuppgifter, om man direkt eller indirekt kan avgöra vilken individ som upptagningen avser.

Definitionen omfattar bara uppgifter om personer som är i livet. Det innebär att behandling av uppgifter om avlidna eller ännu inte födda personer inte omfattas av lagen. Av lagen (1987:269) om kriterier för bestämmande av människans död och lagen (2005:130) om dödförklaring framgår när någon ska betraktas som avliden. Däremot omfattar definitionen uppgifter om vem som är släkt med den avlidne.

Uppgifter om juridiska personer omfattas inte av definitionen.

Personuppgiftsansvarig

Definitionen utgår från hur personuppgiftsansvarig definieras i artikel 3.8. Uttrycket behandlas i avsnitt 9.1.1.

Personuppgiftsansvarig är enligt definitionen den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Att bestämma ändamålen med behandlingen innebär i princip att bestämma att en behandling ska utföras och varför. Att bestämma medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen, dvs. hur behandlingen ska gå till. Det kan handla om vilka personuppgifter som ska behandlas, vilka som ska få ta del av dem och hur länge personuppgifterna får behandlas. Den personuppgiftsansvarige styr dock inte alltid själv över alla medel för behandlingen. Vid direktåtkomst bestämmer den som medger åtkomsten hur tillgången tekniskt ska lösas och vilka personuppgifter som ska tillgängliggöras. Den som ges direktåtkomst är personuppgiftsansvarig för behandlingen av de personuppgifter som direktåtkomsten avser. Som framgår av definitionen kan endast behöriga myndigheter vara personuppgiftsansvariga.

Det kan framgå av lag eller förordning vem som är personuppgiftsansvarig. I annat fall avgör de faktiska omständigheterna vem som är personuppgiftsansvarig.

Personuppgiftsbiträde

Definitionen utgår från hur personuppgiftsbiträde definieras i artikel 3.9. Uttrycket behandlas i avsnitt 9.6.1.

Ett personuppgiftsbiträde är en fysisk eller juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde behandlar personuppgifter endast enligt instruktioner från den personuppgiftsansvarige och har inte rätt att själv

bestämma över personuppgiftsbehandlingen. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen, t.ex. en servicebyrå eller en konsult. En myndighet kan också behandla personuppgifter som personuppgiftsbiträde åt en annan myndighet, t.ex. vid utkontraktering av it-drift. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

Personuppgiftsincident

Definitionen utgår från hur personuppgiftsincident definieras i artikel 3.11. Uttrycket behandlas i avsnitt 9.4.1.

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter. Det är som regel fråga om en oplanerad händelse som påverkar säkerheten för personuppgifterna på ett negativt sätt och som medför allvarliga konsekvenser för skyddet av uppgifterna. En personuppgiftsincident kan exempelvis uppstå vid fel eller störningar i system, komponenter eller programvara eller vid haveri i ett tekniskt system eller en komponent i infrastrukturen. En personuppgiftsincident kan också orsakas av en säkerhetsbrist i tekniska hjälpmedel. Det kan även vara fråga om handhavandefel, dvs. internt felaktigt bruk eller felaktig implementering av tekniska system eller komponenter. En informationsförlust eller ett informationsläckage kan också bedömas som en personuppgiftsincident. Det kan orsakas av exempelvis brand eller annan yttre påverkan, men kan också bero på felaktig avyttring av teknisk utrustning som innehåller information som inte ska vara allmänt tillgänglig, eller otillåtet eller oavsiktligt offentliggörande av sådan information. Personuppgiftsincidenter kan också vara olika typer av angrepp på och intrång i systemen, t.ex. överbelastningsattacker, införande av skadliga koder, hackning, olovligt nyttjande eller annat missbruk av lösenord, olovlig åtkomst till information genom skadliga program och obehörig användning av informationssystem. Även angrepp som möjliggjorts eller utförts av den personuppgiftsansvariges personal eller andra som har anknytning till myndigheten, exempelvis inhyrd personal, kan utgöra personuppgiftsincidenter.

Det saknar betydelse för definitionen av en personuppgiftsincident hur händelsen började och vem som ansvarade för att den uppkom. Det avgörande är i stället effekten av incidenten.

Registrerad

Definitionen har ingen direkt motsvarighet i direktivet, men ordet registrerad ingår i definitionen av personuppgifter i artikel 3.1. Uttrycket behandlas i avsnitt 6.2.

Med registrerad avses den fysiska person som en personuppgift rör. Av definitionen av personuppgift framgår bl.a. att personen ska vara i livet.

Tillsynsmyndigheten

Definitionen utgår från hur en tillsynsmyndighet definieras i artikel 3.15 och har i allt väsentligt utformats i enlighet med *Lagrådets* förslag. Uttrycket behandlas i avsnitt 11.3.1.

Tillsynsmyndigheten är enligt definitionen en myndighet som utses av regeringen enligt direktivet för att utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Genom att tillsynsområdet knutits till de grundläggande syftena med lagen omfattar tillsynen inte bara behandling enligt lagen utan även enligt den förordning som kompletterar lagen. Dessutom omfattar tillsynsområdet personuppgiftsbehandling med stöd av de registerförfattningar som gäller för behöriga myndigheter eller för ett särskilt register som förs för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Tillsyn över bestämmelser om personuppgiftsbehandling i andra författningar omfattas också, om bestämmelserna reglerar personuppgiftsbehandling som utförs av en behörig myndighet för något av de syften som ligger inom lagens tillämpningsområde. Exempel på bestämmelser av sådant slag är 26 och 27 §§ lagen (1988:688) om kontaktförbud.

Tredjeland

Tredjeland definieras inte i direktivet. Definitionen täcker alla stater som inte är medlemsstater i lagens mening och utgår alltså från hur medlemsstat definieras. Uttrycket behandlas i avsnitt 14.2.3.

Tredje man

Definitionen har ingen motsvarighet i direktivet. Tredje man definieras som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvarige eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Uttrycket behandlas i avsnitt 10.3.3.

Uppgift som rör hälsa

Definitionen motsvarar direktivets definition i artikel 3.14. Uttrycket behandlas i avsnitt 6.2. Med uppgift som rör hälsa avses en personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus. Av 2 kap. 11 § framgår att uppgifter som rör hälsa är känsliga personuppgifter som bara får behandlas under vissa förutsättningar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Rättsliga grunder

1 §

Paragrafen reglerar, tillsammans med 2 §, de tillåtna rättsliga grunderna för behandling av personuppgifter enligt lagen. Paragrafen, som i allt

väsentligt har utformats i enlighet med *Lagrådets* förslag, genomför artikel 8.1 och delar av artikel 8.2. Den behandlas i avsnitt 7.2.

Enligt *första stycket* får en behörig myndighet behandla personuppgifter om det är nödvändigt för att den ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten enligt lagen. Personuppgifter får behandlas bara om det är nödvändigt för att fullgöra en sådan uppgift. Nödvändighetsrekvisitet innebär att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt. Behandling av personuppgifter och behörig myndighet definieras i 1 kap. 6 §. Vad som avses med förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet och behörig myndighet redovisas i kommentaren till 1 kap. 2 §.

Av *andra stycket* framgår att personuppgiftsbehandling alltid måste gå att härleda till den behöriga myndighetens uppgifter så som de kommer till uttryck i unionsrätten eller i svensk lagstiftning och andra för verksamheten bindande beslut om uppgifter som regeringen meddelat. Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU-rättsakter här i landet med den verkan som följer av EU-fördragen. EU-förordningar är att jämställa med svensk lag.

2 §

Paragrafen reglerar, tillsammans med 1 §, de tillåtna rättsliga grunderna för behandling av personuppgifter enligt lagen. I paragrafen regleras två särskilt angivna fall där det är tillåtet att behandla personuppgifter oberoende av om förutsättningarna för behandling enligt 1 § är för handen. Tillämpningsområdet för paragrafen är begränsat, eftersom det enbart är personuppgifter som lämnats till en behörig myndighet som får behandlas. Frågan behandlas i avsnitt 7.3.

Enligt *punkt 1* får personuppgifter alltid behandlas om behandlingen är nödvändig för diarieföring. Normalt finns det en rättslig grund enligt 1 § för de behöriga myndigheternas diarieföring, t.ex. att det är fråga om en handling som hänför sig till en förundersökning, ett mål eller ett ärende. Den nu aktuella punkten täcker behovet av att kunna diarieföra handlingar i andra fall. Det kan även röra sig om muntliga uppgifter som nedtecknas i en tjänsteanteckning eller liknande. Vilka uppgifter som måste noteras i samband med diarieföring av en handling framgår av 5 kap. 2 § offentlighets- och sekretesslagen (2009:400). Vid diarieföring av inkomna handlingar får det således alltid anges vem en handling har kommit från och i korthet vad handlingen rör. Någon annan behandling än sådan som är nödvändig för diarieföringen får emellertid inte utföras med stöd av denna punkt. Den fortsatta behandlingen ska således – utom i fall där andra punkten i denna paragraf blir tillämplig – alltid ha stöd i 1 §.

Personuppgifter får enligt *punkt 2* alltid behandlas om de har lämnats till den behöriga myndigheten i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning. Uttrycket

”anmälan, ansökan eller liknande” innefattar alla slag av framställningar till en behörig myndighet. Det gäller både skriftliga framställningar och uppgifter som lämnas muntligen men nedtecknas av någon hos den behöriga myndigheten. Oftast omfattas framställningar av detta slag av bestämmelsen om rättslig grund i 1 § och ska då behandlas med stöd av den bestämmelsen, men i vissa fall kan innehållet i handlingen vara sådant att nödvändighetsrekvisitet i den paragrafen inte är uppfyllt. Eftersom det vanligtvis krävs något slag av handläggning hos den behöriga myndigheten för att hantera en framställan, har det ansetts nödvändigt med en särskild bestämmelse för personuppgiftsbehandling i dessa fall (jfr t.ex. prop. 2009/10:85 s. 324). Behandlingen måste vara nödvändig för handläggningen. Det kan i ett enskilt fall innebära att personuppgifter i ett e-postmeddelande inte får behandlas på annat sätt än att uppgifterna tas emot och därefter omedelbart arkiveras eller gallras. I ett annat fall kan bestämmelsen innebära att personuppgifterna också får behandlas i samband med att framställningen besvaras.

Ändamål

3 §

I paragrafen föreskrivs att personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål och att det ska framgå för vilket ändamål uppgifterna behandlas. Paragrafen genomför delar av artiklarna 4.1 b och 8.2 och behandlas i avsnitt 7.4.

Av *första stycket* framgår att ändamålen för behandling av personuppgifter ska vara särskilda, uttryckligt angivna och berättigade. Ändamålen måste bestämmas redan när uppgiften behandlas första gången, eftersom det är i förhållande till dem som det ska prövas om personuppgifterna som behandlas är adekvata och relevanta och hur många personuppgifter som behöver behandlas (8 §).

Ändamålet får inte blandas ihop med den rättsliga grunden för behandling. Ändamålet ska vara mer konkret. Att ändamålet ska vara särskilt innebär att det måste vara tillräckligt preciserat för att det ska kunna avgöras om de personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen eller om för många personuppgifter behandlas. Ändamålet får alltså inte vara så vagt eller vittomfattande att någon sådan prövning i praktiken inte blir möjlig. Ändamålet kan t.ex. vara förundersökningen om ett visst brott, åtalet för vissa gärningar eller handläggningen av en begäran om domstolsprövning av ett kontaktförbud eller tillträdesförbud. Vidare kan det vara fråga om ett pågående underrättelsearbete om viss, närmare angiven, brottslig verksamhet. Det kan också vara fråga om verkställigheten av ett straff eller handläggningen av ett ingripande på grund av en ordningsstörning.

Att ändamålet ska vara berättigat innebär en koppling till de rättsliga grunderna. Personuppgifter får inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden. Personuppgifter som avser en förundersökning får t.ex. inte längre behandlas för det ändamålet när brottet har preskriberats. Uppgifter om verkställigheten av en påföljd får inte behandlas om påföljden har bortfallit. Däremot kan det vara berättigat för åklagare och domstolar att fortsätta att behandla personuppgifter efter en dom till dess att det står klart att den fått laga kraft.

Om det ändamål för vilket personuppgifterna behandlas inte framgår av sammanhanget eller på annat sätt ska det enligt *andra stycket* tydliggöras genom en särskild upplysning. Behandlas uppgifterna i en förundersökning eller i ett mål eller ärende framgår ändamålet av sammanhanget. Det gäller också många gånger om uppgifterna finns i ett särskilt register eller i en viss uppgiftssamling som skapats för ett visst ändamål.

4 §

I paragrafen regleras förutsättningarna för att personuppgifter ska få behandlas för ett nytt ändamål inom lagens tillämpningsområde. Paragrafen genomför artikel 4.2 och behandlas i avsnitt 7.6.2 och 7.6.5.

Personuppgifter får enligt *första stycket* inte behandlas innan det har säkerställts att det finns en rättslig grund för den nya behandlingen och att kraven i övrigt är uppfyllda. Det nya ändamålet ska alltså bestämmas innan behandlingen för det ändamålet påbörjas.

Av *punkt 1* framgår att det alltid ska finnas en rättslig grund för att behandla personuppgifterna för det nya ändamålet. I 1 § anges vilka rättsliga grunder som är tillåtna. Om personuppgifter behandlas för att utreda ett brott och det upptäcks att personen i fråga har begått ett annat brott, finns det rättslig grund för att behandla personuppgifterna även för att utreda det andra brottet.

Av *punkt 2* framgår att det ska vara nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Med nödvändig avses att det är fråga om något som behövs snarare än något som absolut fordras. Behandlingen kan vara nödvändig exempelvis om det i en förundersökning finns uppgifter som avslöjar planer på fritagning av en häktad och uppgiften därför behöver lämnas till Kriminalvården. Att det ska vara proportionerligt att personuppgifterna behandlas för det nya ändamålet innebär att skälen för att behandla uppgifterna för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för enskilda. Det har också betydelse vilka personuppgifter det är fråga om och i vilken verksamhet de ska användas. Som utgångspunkt torde det anses både nödvändigt och proportionerligt att uppgifter från en förundersökning används för att motverka ny misstänkt brottslig verksamhet eller för att uppfylla en internationell förpliktelse.

Bara om de förutsättningar som räknas upp i *första stycket* är uppfyllda får personuppgifter behandlas för ett nytt ändamål. Någon prövning av om behandlingen för det nya ändamålet är förenlig med det ändamål för vilket uppgifterna ursprungligen behandlades behöver däremot inte göras. Det saknar också betydelse om det är samma eller en annan personuppgiftsansvarig som ska behandla uppgifterna för ett nytt ändamål, så länge det nya ändamålet omfattas av lagens tillämpningsområde.

I *andra stycket* föreskrivs att någon prövning enligt första stycket inte ska göras i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. Exempel på uppgiftsskyldighet gentemot andra myndigheter finns i förordningen (1990:893) om underrättelse om dom i vissa brottmål, m.m. som föreskriver skyldighet att expediera domar, beslut och underrättelser i brottmål till bl.a. Polismyndigheten, Kriminalvården och socialnämnden. Vidare omfattas en myndighets skyldighet enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) att på begäran av

en annan myndighet lämna ut uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. I de fall där det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna personuppgifter ska det däremot prövas om uppgiftslämnandet är nödvändigt och proportionerligt. Prövningen bör dock i sådana fall som regel mynna ut i att det är nödvändigt och proportionerligt att lämna uppgifterna.

5 §

I paragrafen föreskrivs att en behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Den genomför delar av artikel 4.3 och behandlas i avsnitt 7.7.

Paragrafen reglerar bara behöriga myndigheters behandling för statistiska, vetenskapliga eller historiska ändamål inom lagens tillämpningsområde och gäller inte för exempelvis Brottsförebyggande rådets statistikverksamhet. Den gäller heller inte behöriga myndigheters behandling av personuppgifter för syften utanför lagens tillämpningsområde, t.ex. för forskningsändamål.

Vid behandling för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde ska lagens övriga bestämmelser tillämpas på samma sätt som vid annan behandling enligt lagen. De uppgifter som behandlas ska vara adekvata och relevanta och inte för omfattande i förhållande till det vetenskapliga, statistiska eller historiska ändamålet. På samma sätt som man vid behandling för andra ändamål inom lagens tillämpningsområde måste se till att uppgifterna inte behandlas under längre tid än vad som behövs för de ändamålen, får uppgifter som behandlas för statistiska, vetenskapliga eller historiska ändamål inte behandlas under längre tid än vad som behövs för dessa ändamål.

Författningsenlig och korrekt behandling

6 §

I paragrafen föreskrivs att personuppgifter alltid ska behandlas författningsenligt och på ett korrekt sätt. Paragrafen genomför artikel 4.1 a och behandlas i avsnitt 8.1.1.

När det är tillåtet att behandla personuppgifter och vilka krav som ställs på behandlingen framgår inte bara av denna lag och föreskrifter som har meddelats med stöd av den, utan också av de behöriga myndigheternas registerförfattningar och andra författningar som reglerar särskilda register eller särskilda samarbeten inom lagens tillämpningsområde. Även regler om personuppgiftsbehandling i andra författningar kan vara tillämpliga, t.ex. 26 och 27 §§ lagen (1988:688) om kontaktförbud. Regler av nu aktuellt slag har betydelse för bedömningen av både om behandlingen är författningsenlig och vad som är ett korrekt sätt att behandla personuppgifter. I det ligger bl.a. kravet på att det ska göras en kontinuerlig bedömning av att personuppgiftsbehandlingen uppfyller alla formella krav.

Vad som är ett korrekt sätt för behandling styrs emellertid inte bara av författningsregler och den praxis som utbildas kring dem. Tillsynsmyn-

dighetens allmänna råd och uttalanden i fråga om personuppgiftsbehandling har också betydelse, liksom myndigheternas interna regler.

Otillåten behandling av personuppgifter kan i vissa fall vara straffbar enligt bestämmelser i brottsbalken, bl.a. regeln om dataintrång i 4 kap. 9 c §. Det kan då röra sig om externa angrepp eller om att någon som har tillgång till ett it-system överskrider sina befogenheter.

Personuppgifternas kvalitet

7 §

Paragrafen reglerar hur personuppgifter som behandlas ska vara beskaffade. Den genomför delar av artikel 4.1 d och behandlas i avsnitt 8.1.2.

I *första stycket* föreskrivs att de personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

En personuppgift är korrekt om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är får man söka ledning i ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses, exempelvis utredningen av en misshandel eller rättspsykiatrisk undersökning av en viss person. Inom lagens tillämpningsområde måste frågan om en personuppgift är korrekt inte bara vägas mot ändamålen med behandlingen utan även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. För att kunna avgöra om personuppgifterna är korrekta är det också av stor betydelse att veta om de grundar sig på fakta eller på personliga bedömningar. Kravet på att personuppgifter ska vara korrekta innebär inte något hinder mot att samla in exempelvis osäkra underrättelseuppgifter, under förutsättning att personuppgifterna är relevanta för arbetet (se 8 §) och att det framgår att det är osäkert om uppgiften är riktig (se exempelvis 3 kap. 4 § andra stycket polisdatalagen [2010:361]). Att personuppgifter som grundar sig på fakta i så stor utsträckning som möjligt ska särskiljas från uppgifter som grundar sig på personliga bedömningar framgår av 10 §. Det krav som kan ställas när det gäller personuppgifter som behandlas vid utsagor (t.ex. förhör med misstänkta) måste inskränkas till att utsagorna återges på ett korrekt sätt, dvs. så som de har lämnats, och att dokumentationen av dem följer gällande regler.

De personuppgifter som behandlas behöver bara vara uppdaterade om det är nödvändigt. Frågan om det är nödvändigt att de är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen. Exempelvis kan uppgifter om telefonnummer eller andra kontaktuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras. När ärendet har avslutats eller arkiverats är det dock inte nödvändigt att uppdatera kontaktuppgifter.

I *andra stycket* föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet. Motsvarande bestämmelser finns i exempelvis 2 kap. 10 § tredje stycket polisdatalagen och 2 kap. 8 § tredje stycket åklagardatalagen (2015:433). Syftet med bestämmelsen är att förhindra att personers utseende beskrivs i ordalag som kan vara kränkande för individen. Exempel på signalementsbeteckningar som anses acceptabla finns bl.a. i Rikspolisstyrelsens föreskrifter och allmänna råd om fingeravtryck och annan signalementsupptagning (RPSFS 2005:12, FAP 473–1).

Utformningen av bestämmelsen innebär att en behörig myndighet alltid är oförhindrad att, när den får ett tips från allmänheten om en person som kan misstänkas för brott, göra de anteckningar som är nödvändiga för att underlätta identifieringen av personen, t.ex. anteckningar om fysiska kännetecken. I anslutning till dessa anteckningar får även sådana känsliga personuppgifter som avses i 11 § första stycket antecknas, om det är absolut nödvändigt för det arbete som tipset kan komma att leda till.

8 §

Paragrafen reglerar omfattningen av behandlingen av personuppgifter. Den genomför artikel 4.1 c och behandlas i avsnitt 8.1.2.

Av paragrafen framgår att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och att fler personuppgifter inte får behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses, exempelvis utredningen av en stöld eller ett ärende om förordnande av offentlig försvarare. Att personuppgifterna ska vara adekvata och relevanta innebär att ovidkommande uppgifter inte får behandlas. En prövning av om en personuppgift är nödvändig för behandlingen ska göras kontinuerligt av den behöriga myndigheten, inte bara när uppgiften registreras eller på annat sätt samlas in. Även vid en senare behandling ska personuppgiften behövas för just den behandlingen, annars är kravet på adekvans och relevans inte uppfyllt.

Förutom att uppgifterna ska vara adekvata och relevanta får de inte heller vara fler än nödvändigt. Det understryker kravet på att en fortlöpande bedömning görs.

Vid all behandling måste det alltså prövas om det går att utelämna personuppgifter, eller i vart fall att endast använda uppgifter som indirekt går att hänföra till en viss person. Om fullständig avidentifiering är ett fullgott alternativ till att använda direkta eller indirekta personuppgifter är förutsättningarna för att behandla personuppgifterna inte uppfyllda.

Åtskillnad mellan olika slag av personuppgifter

9 §

I paragrafen, som i allt väsentligt har utformats i enlighet med *Lagrådets* förslag, ställs krav på att personuppgifter som rör olika kategorier av registrerade så långt det är möjligt ska särskiljas. Paragrafen genomför artikel 6. Den behandlas i avsnitt 8.1.3.

I paragrafen anges personer som är misstänkta för brott, dömda för brott, brottsoffer och andra som berörs av ett brott som exempel på kategorier av registrerade. Andra som berörs av ett brott kan vara t.ex. vittnen eller vårdnadshavare för målsägande, misstänkta eller vittnen. Det är särskilt viktigt att det framgår om någon är misstänkt för brott eller inte. Det gäller oavsett misstankegrad.

Om det framgår av sammanhanget eller på annat sätt vilken kategori en person tillhör behöver någon särskild upplysning inte lämnas. Om en person har hörts under en förundersökning eller under en brottmålsrättegång och det av sammanhanget framgår att han eller hon har hörts som t.ex. målsägande, tilltalad eller vittne, behöver uppgifterna inte förses med någon tilläggsupplysning.

Kravet på att olika kategorier av uppgifter ska särskiljas innebär att det krävs rutiner hos behöriga myndigheter för att följa upp om en tidigare brottsmisstanke avskrivs i sin helhet, exempelvis i samband med att en förundersökning läggs ned eller om rätten meddelar en frikännande dom.

Varje enskild uppgift måste inte förses med en särskild upplysning, vilket inte heller torde vara praktiskt möjligt. Vid behandling av uppgifter i bild- eller ljudupptagningar eller i löpande text framgår det som regel av sammanhanget till vilka personkategorier olika personer hör. Ibland kan dock en sådan upptagning eller text behöva förses med en upplysning som förtydligar det.

Kravet på att olika uppgifter ska särskiljas gäller så långt det är möjligt. Om en misstänkt fotograferas i stadsmiljö förekommer ofta andra personer på samma fotografi. De kan vara helt okända och då kan det inte krävas att de kategoriseras på något sätt. Det är tillräckligt att det i stället anges vem som är den misstänkte.

10 §

I paragrafen ställs krav på att personuppgifter som grundar sig på fakta så långt det är möjligt ska särskiljas från personuppgifter som grundar sig på personliga bedömningar. Paragrafen genomför artikel 7.1. Den behandlas i avsnitt 8.1.3.

Om det framgår av sammanhanget eller på annat sätt om uppgiften grundar sig på fakta eller personliga bedömningar behöver någon särskild upplysning inte lämnas. Det som uttalas vid ett förhör eller vittnesmål kan grunda sig på bedömningar eller vara faktabaserat. Det kan då utläsas av sammanhanget om det är fråga om fakta eller bedömningar. Detsamma gäller innehållet i intyg och andra liknande handlingar. Kravet gäller också uppgifter som finns i promemorior och analyser. Tas uppgifterna ur sitt sammanhang måste de förses med en särskild upplysning.

Kravet på att personuppgifter som grundar sig på fakta ska särskiljas från personuppgifter som grundar sig på personliga bedömningar gäller så långt det är möjligt. Det kan t.ex. vara omöjligt att värdera vad som är fakta respektive bedömningar i en anmälan om brott som har skickats med post till Polismyndigheten. Det räcker då att det framgår från vem eller på vilket sätt personuppgifterna kommit till Polismyndigheten.

Känsliga personuppgifter

11 §

Paragrafen reglerar tillsammans med 12–14 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Att uppgifterna betecknas som känsliga personuppgifter framgår av 13 §. Paragrafen genomför delar av artikel 10 och behandlas i avsnitt 8.1.4.

Enligt *första stycket* får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte behandlas. Det innebär att det inte är tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda på den grunden att de utifrån etniskt ursprung, politiska åsikter eller något annat i paragrafen angivet förhållande kan hänföras till en viss kategori av människor.

En uppgift om utseende är normalt inte en känslig personuppgift och den får alltså behandlas, med den begränsning som följer av 7 § andra stycket. Om en sådan uppgift samtidigt innebär uppgift om etniskt ursprung omfattas den dock av förbudet. Bestämmelsen hindrar inte att uppgifter om en persons nationalitet behandlas, eftersom en sådan uppgift normalt inte ger upplysning om etniskt ursprung (se prop. 2009/10:85 s. 325). Uppgifter om att en viss person kommer från en viss världsdel eller ett visst land faller också som regel utanför förbudet mot behandling av känsliga personuppgifter. Skulle en sådan personuppgift i det enskilda fallet t.ex. avslöja etniskt ursprung är dock förbudet tillämpligt.

Avbildningar av personer, t.ex. fotografier, kan avslöja många detaljer. Man kan t.ex. se hudfärg eller om personen bär klädsel eller andra kännetecken som är typiska för utövare av en viss religion. Även fysiska funktionsnedsättningar kan framgå av bilder och det kan även framgå att en person är sjuk eller skadad. Bilder på människor i mera normala sammanhang torde inte avslöja känsliga personuppgifter, medan bilder på människor som utövar religiösa, politiska eller sexuella aktiviteter som regel utgör känsliga personuppgifter (jfr Öman m.fl. s. 288).

I *andra stycket* görs det undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Uppgifter om en person som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för ändamålet med behandlingen. Det innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får de kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung om det är av betydelse för utredningen, exempelvis för att utreda hets mot folkgrupp. Under utredning av sexualbrott kan det ibland vara befogat att anteckna uppgifter om den misstänktes sexualliv. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste dock behovet av att göra sådana kompletteringar prövas noga i det enskilda fallet.

Känsliga personuppgifter kan också förekomma i behöriga myndigheters verksamhet på grund av att någon under ett förhör har lämnat en sådan uppgift eller i en inlaga nämnt uppgiften. Det kan vara fråga om helt grundlösa påståenden eller påståenden som inte har någon relevans i sammanhanget. Eftersom myndigheterna inte kan hindra någon från att yttra sig vare sig muntligen eller skriftligen kan känsliga personuppgifter på detta sätt komma att ingå i t.ex. en förundersökning eller en dom. Om det nedtecknade förhöret eller den inkomna handlingen ingår i förundersökningen eller uppgiften antecknas i domen omfattas behandlingen av den känsliga personuppgiften även i dessa fall av undantaget i detta stycke.

12 §

Paragrafen reglerar tillsammans med 13 och 14 §§ i vilken utsträckning två särskilda typer av känsliga personuppgifter får behandlas. Paragrafen genomför delar av artikel 10 och behandlas i avsnitt 8.1.4.

Enligt paragrafen får biometriska uppgifter och genetiska uppgifter endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålen med behandlingen. I t.ex. 4 och 5 kap. polisdata-

lagen (2010:361) finns sådana särskilda föreskrifter som avses i föregående paragraf. I kommentaren till 11 § ges exempel på vad som avses med kravet på att behandlingen är absolut nödvändig. I 1 kap. 6 § definieras vad som avses med biometriska respektive genetiska uppgifter.

13 §

Paragrafen reglerar tillsammans med 11, 12 och 14 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Paragrafen behandlas i avsnitt 8.1.4.

I paragrafen klargörs att sådana personuppgifter som avses i 11 och 12 §§ utgör känsliga personuppgifter. Vidare tydliggörs att sådana uppgifter alltid får behandlas i de fall som avses i 2 §, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i en anmälan, ansökan eller liknande, om det är nödvändigt för myndighetens handläggning. Det innebär bl.a. att det är möjligt för en behörig myndighet att ta emot och besvara anmälningar, ansökningar och liknande skrifter som lämnas i elektronisk form även om de innehåller känsliga personuppgifter. Regleringen innebär också att sådana uppgifter får arkiveras om det är nödvändigt. Som framgår av kommentaren till 2 § är den behandling som är tillåten begränsad.

14 §

Paragrafen reglerar användningen av känsliga personuppgifter vid sökning. Frågan behandlas i avsnitt 8.1.4. Av 11 och 12 §§ framgår vilka personuppgifter som är känsliga personuppgifter.

Enligt paragrafen är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har viss politisk eller religiös åskådning eller sexuell läggning. Uppgifter som beskriver en persons utseende, t.ex. uppgifter om längd, hudfärg eller tatueringar, får användas som sökbegrepp så länge syftet med sökningen inte är att göra en sammanställning av en viss grupp av personer grundat på exempelvis etniskt ursprung eller politisk åskådning.

Även tillåtna sökningar kan resultera i ett urval av personer grundat på känsliga personuppgifter, t.ex. sökningar som görs i registervårdande syfte. I vilken utsträckning det sedan är tillåtet att behandla någon eller några av personuppgifterna i sammanställningen får prövas mot huvudregeln för behandling av känsliga personuppgifter i 11 §.

Rättelse, uppdatering och radering

15 §

I paragrafen föreskrivs vad den personuppgiftsansvarige ska göra för att förhindra att felaktiga eller ofullständiga personuppgifter behandlas, lämnas ut eller görs tillgängliga. Den genomför delar av artiklarna 4.1 d, 7.2 och 7.3 och behandlas i avsnitt 8.1.6. I 4 kap. 9 § regleras vad som gäller när den registrerade begär att personuppgifter ska rättas eller kompletteras.

I *första stycket* föreskrivs att alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felak-

tiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Vad som avses med att uppgifter är korrekta framgår av kommentaren till 7 §. Den personuppgiftsansvarige ska också utan onödigt dröjsmål uppdatera uppgifter som är inaktuella om det är nödvändigt. Bestämmelsen innebär att den personuppgiftsansvarige självmant måste vidta åtgärder för att säkerställa personuppgifternas kvalitet.

Vad som utgör rimliga åtgärder skiljer sig åt beroende på om personuppgifterna är felaktiga, ofullständiga eller inaktuella, eftersom personuppgifter alltid ska vara korrekta men endast behöver vara uppdaterade om det är nödvändigt. Vilka åtgärder som är rimliga att vidta får bedömas mot bakgrund av omständigheterna i varje enskilt fall, som t.ex. ändamålet med behandlingen, vilka personuppgifter som behandlas och vilka konsekvenser en felaktig eller ofullständig uppgift kan få för den enskilde.

När personuppgifter lämnas ut till en behörig myndighet ska mottagaren enligt *andra stycket* så långt det är möjligt ges information som gör att det går att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga. Det gör att mottagaren kan fullgöra sin skyldighet att kontrollera kvaliteten på personuppgifter som kommer från andra behöriga myndigheter. Informationen kan exempelvis ange varifrån personuppgifterna kommer, vad som är känt om uppgiftslämnaren, när och för vilket ändamål personuppgifterna hämtades in och om de grundar sig på fakta eller personliga bedömningar. Andra exempel på information som kan vara relevant för mottagaren är om personuppgiften grundas på misstanke om brott, saken är föremål för domstolsprövning eller avser en lagakraftvunnen dom. Mottagare definieras i 1 kap. 6 §.

16 §

I paragrafen föreskrivs vilka åtgärder som ska vidtas om personuppgifter behandlas på ett otillåtet sätt. Den genomför delar av artiklarna 4.1 d, 7.2 och 7.3 och behandlas i avsnitt 8.1.6. I 4 kap. 10 § regleras vad som gäller när den registrerade begär att motsvarande åtgärder ska vidtas.

I *första stycket* föreskrivs att alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1, 2, 3 § första stycket, 4–6, 8, 11, 12, 14 eller 17 § första stycket utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller när radering krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. När radering kan komma i fråga, förutsättningarna för det och vad som kan vara en rättslig förpliktelse utvecklas i kommentaren till 4 kap. 10 §.

I stället för att personuppgifter som behandlas på ett otillåtet sätt raderas ska enligt *andra stycket* behandlingen av uppgifterna utan onödigt dröjsmål begränsas om uppgifterna behöver finnas kvar av bevisskäl. Vad det innebär utvecklas i kommentaren till 4 kap. 10 §.

Längsta tid som personuppgifter får behandlas

17 §

Paragrafen reglerar hur länge behöriga myndigheter får behandla personuppgifter för ändamål inom lagens tillämpningsområde. Där framgår också hur bestämmelsen förhåller sig till arkivlagstiftningen. Paragrafen genomför artikel 4.1 e och behandlas i avsnitt 8.2.2.

I *första stycket* föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det som avses är ändamålet i det enskilda fallet. Ibland behandlas personuppgifter för flera olika ändamål. Att det inte längre finns behov av att behandla personuppgiften för ett visst ändamål medför inte att behandlingen av den måste upphöra för alla andra ändamål samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål inte att den får fortsätta att behandlas för alla ändamål lika länge. Behovet av att fortsätta att behandla uppgifterna måste prövas kontinuerligt. Om det är tillräckligt att behandla avidentifierade uppgifter är det inte längre tillåtet att behandla personuppgifterna.

Av *andra stycket* framgår att bestämmelsen om längsta tid för behandling inte hindrar att personuppgifterna arkiveras av den behöriga myndigheten eller att arkivmaterial lämnas till en arkivmyndighet. Behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde.

18 §

Paragrafen reglerar vad som gäller om det inte är föreskrivet hur länge behöriga myndigheter får behandla personuppgifter för ändamål inom lagens tillämpningsområde. Paragrafen genomför artikel 5 och behandlas i avsnitt 8.2.2.

Enligt paragrafen ska den personuppgiftsansvarige en gång om året se över behovet av att behandla personuppgifter. Det gäller dock bara om det inte finns någon författningsbestämmelse som reglerar när uppgifterna inte längre får behandlas för ändamål inom lagens tillämpningsområde. Sådana bestämmelser finns i vissa behöriga myndigheters registerförfattningar. Bestämmelser om hur länge personuppgifter får behandlas finns inte bara i lag eller förordning utan kan även finnas i myndighetsföreskrifter som har stöd i bemyndiganden.

Automatiserade beslut

19 §

Paragrafen, som har utformats i enlighet med *Lagrådets* förslag, reglerar automatiserade beslut. Paragrafen genomför delar av artikel 11 och behandlas i avsnitt 8.3.

Av *första stycket* framgår att den som berörs av ett beslut som enbart grundas på automatiserad behandling av personuppgifter som är avsedda att bedöma hans eller hennes egenskaper har rätt att få beslutet prövat på nytt av någon fysisk person. Rätten till information regleras i 4 kap. 4 §.

I *andra stycket* förbjuds automatiserade beslut som enbart grundas på känsliga personuppgifter. Vilka uppgifter som är känsliga personuppgifter framgår av 11 och 12 §§.

Överföring av personuppgifter till en annan medlemsstat

20 §

Paragrafen reglerar möjligheten att ställa upp villkor för behandlingen av personuppgifter. Paragrafen genomför artikel 9.4 och behandlas i avsnitt 8.4.

Om det inte är särskilt föreskrivet får en utlämnande myndighet inte ställa upp villkor i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om myndigheten inte i motsvarande fall får ställa upp samma typ av villkor i förhållande till en mottagare inom Sverige. Paragrafen är bara tillämplig vid utlämnande för ändamål inom lagens tillämpningsområde.

Uppgiftslämnande för rättsstatistik

21 §

Paragrafen, som behandlas i avsnitt 8.5, reglerar behandling av personuppgifter som är nödvändiga för att framställa rättsstatistik. Sådana uppgifter ska enligt paragrafen lämnas till den som ansvarar för att framställa sådan statistik. Enligt 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet ansvarar myndigheten för kriminalstatistiken.

Behandling för ändamål utanför denna lags tillämpningsområde

22 §

Paragrafen anger vad som gäller när fråga uppkommer om att behandla personuppgifter, som behandlas med stöd av lagen, för nya ändamål utanför lagens tillämpningsområde. Paragrafen behandlas i avsnitt 7.6.3–7.6.5.

Personuppgifter som en behörig myndighet behandlar enligt lagen kan behöva lämnas till en enhet inom myndigheten som bedriver verksamhet utanför lagens tillämpningsområde. Personuppgifter som Polismyndigheten behandlar i sin brottsbekämpande verksamhet kan t.ex. behövas för att bedöma en persons lämplighet att få vapenlicens. Ett annat exempel är att uppgifter i Kustbevakningens brottsutredande verksamhet överlämnas till den enhet som hanterar frågor om vattenföroreningsavgift på grund av oljeutsläpp. Vid behandling för att lämna ut personuppgifter för sådana ändamål ska dataskyddsförordningen tillämpas i stället för denna lag. Prövningen av om behandlingen är tillåten ska alltså då göras med utgångspunkt i dataskyddsförordningens bestämmelser.

Innan personuppgifter som behandlas med stöd av lagen behandlas för ett nytt ändamål utanför lagens tillämpningsområde ska det dock enligt *första stycket* säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Denna prövning ska alltså ske utöver de krav som sedan gäller enligt dataskyddsförordningen. Med nödvändigt avses att det är fråga om något som behövs snarare än något som absolut fordras. I kravet på proportionalitet ligger att skälen för att personuppgifterna behandlas för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för den enskilde. Det som står att vinna med behandlingen ska alltså vägas mot intrånget i enskildas integritet. Det har också betydelse vilka personuppgifter det är

fråga om och för vilket syfte de ska användas. Någon prövning av om behandlingen för det nya ändamålet är förenlig med det ändamål för vilket uppgifterna ursprungligen behandlades behöver däremot inte göras. Att behandla personuppgifter för ett nytt ändamål kan vara både nödvändigt och proportionerligt exempelvis om det i Polismyndighetens brottsbekämpande verksamhet finns uppgifter om att en person har sådana kontakter i kriminella kretsar att han eller hon ter sig olämplig för att få tillstånd att bedriva viss verksamhet och uppgifterna därför behöver tillhandahållas för att användas vid prövningen av tillståndsärendet. Vidare får det anses både nödvändigt och proportionerligt att personuppgifter som behandlas med stöd av lagen behandlas för arkivering.

I *andra stycket* föreskrivs att någon prövning enligt första stycket inte ska göras i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. Exempel på uppgiftsskyldighet gentemot annan myndighet finns i 14 kap. 1 § socialtjänstlagen (2001:453) som föreskriver skyldighet att göra anmälan till socialnämnden när nämnden behöver ingripa till barns skydd. Ett annat exempel är den skyldighet som föreskrivs i lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet. Vidare omfattas en myndighets skyldighet enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) att på begäran av en annan myndighet lämna ut uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. I de fall där det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna personuppgifter ska det däremot prövas om uppgiftslämnandet är nödvändigt och proportionerligt. Prövningen bör dock i sådana fall som regel mynna ut i att det är nödvändigt och proportionerligt att lämna uppgifterna.

3 kap. Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

1 §

Paragrafen reglerar personuppgiftsansvarets omfattning. Personuppgiftsansvarig definieras i 1 kap. 6 §. Paragrafen, som genomför artikel 4.4, behandlas i avsnitt 9.1.2.

Paragrafen slår fast det helhetsansvar som den personuppgiftsansvarige har och tydliggör hur långt ansvaret sträcker sig när det gäller behandlingen av personuppgifter. Den närmare innebörden av personuppgiftsansvaret framgår av lagens övriga bestämmelser och föreskrifter som meddelas i anslutning till den. Vem som är personuppgiftsansvarig kan framgå av andra författningar.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under den personuppgiftsansvariges ledning. Med det avses all personuppgiftsbehandling vid den behöriga myndigheten. Det gäller både behandling som utförs genom en aktiv handling, t.ex. insamling eller sökning, och passiv behandling, t.ex. lagring. Ansvaret omfattar däremot inte sådan behandling som den behöriga myndigheten eventuellt utför som personuppgiftsbiträde. Genom att ansvaret knyts till behandling som utförs under den personuppgiftsansvariges ledning tydliggörs att det inte

är den personuppgiftsansvarige, dvs. den behöriga myndigheten, som utför personuppgiftsbehandlingen utan de anställda.

Den personuppgiftsansvarige är också ansvarig för all behandling av personuppgifter som utförs på dennes vägnar. Med det avses främst sådan behandling som den personuppgiftsansvarige har uppdragit åt ett personuppgiftsbiträde att utföra. Den personuppgiftsansvarige kan uppdra åt ett biträde att utföra viss behandling av personuppgifter, men kan inte genom det avsäga sig personuppgiftsansvaret. Personuppgiftsansvaret sträcker sig då utanför den personuppgiftsansvariges egen verksamhet. Personuppgiftsbiträdens behandling ska styras av skriftliga avtal eller andra skriftliga överenskommelser och får endast utföras enligt instruktioner från den personuppgiftsansvarige, se kommentarerna till 16 och 18 §§.

Två eller flera personuppgiftsansvariga kan behandla samma personuppgifter samtidigt för olika ändamål, t.ex. om de har direktåtkomst till personuppgifter i samma system. Varje personuppgiftsansvarig är då ansvarig för den behandling som utförs under dennes ledning eller på dennes vägnar.

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

2 §

Paragrafen genomför artikel 19.1 och reglerar, tillsammans med 3–5 §§, de krav som ställs på personuppgiftsansvariga i fråga om tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas. Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 8 §. Paragrafen behandlas i avsnitt 9.2.1.

Organisatoriska åtgärder som avses i paragrafen är bl.a. att anta interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av itsystem, behandlingar och vidtagna åtgärder och teknisk spårbarhet genom loggning och logguppföljning.

Vilka åtgärder som bör vidtas får avgöras efter en bedömning i enskilda fall. Vid den bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga de är. Även grunden för behandlingen och riskerna med den ska beaktas. Mer långtgående åtgärder kan behövas vid behandling som kan medföra särskilda risker för integritetsintrång eller vid omfattande behandling av en stor mängd personuppgifter.

Skyldigheten att vidta lämpliga åtgärder är inte knuten till en viss tidpunkt, utan något som den personuppgiftsansvarige ständigt ska ha för ögonen. Åtgärder som har vidtagits måste därför kontinuerligt revideras och vid behov förändras.

3 §

Paragrafen, som genomför artikel 20.1, reglerar skyldigheten att beakta principen om inbyggt dataskydd vid behandling av personuppgifter. Paragrafen har utformats i enlighet med *Lagrådets* förslag och behandlas i avsnitt 9.2.1.

Paragrafen innebär att den personuppgiftsansvarige både när medlen för behandlingen bestäms och vid behandlingen, ska vidta åtgärder som medför att dataskyddsprinciper säkerställs och skyddsåtgärder integreras i behandlingen. Skyldigheten är tätt förknippad med de skyldigheter som följer av 2, 4 och 8 §§. Paragrafen kan ses som en precisering av den övergripande skyldigheten i 2 §.

Exempel på grundläggande dataskyddsprinciper som bör säkerställas är uppgiftsminimering, dvs. att så få personuppgifter som möjligt samlas in och hanteras, och att personuppgifter inte behandlas längre än vad som behövs eller används på ett otillåtet sätt. Principerna kan säkerställas i verksamheten genom åtgärder som exempelvis begränsar behandlingen till personuppgifter som endast indirekt pekar ut en individ eller till personuppgifter som är mindre integritetskänsliga. Att använda pseudonymisering, vilket innebär att uppgifterna inte går att koppla till en enskild person utan ytterligare information som hålls avskild, är ett annat exempel. Om det i ett ärendehanteringssystem är möjligt att behandla personuppgifterna utöver vad som är tillåtet med hänsyn till ändamålet bör funktionerna begränsas och spärras innan systemet tas i drift. Funktioner för att avskilja personuppgifter automatiskt är också exempel på inbyggt dataskydd. Andra åtgärder som kan vidtas för att säkerställa dataskyddsprinciper är behörighetsstyrning och kryptering av information. Sådana åtgärder syftar till att begränsa åtkomsten till personuppgifterna så att endast de som behöver uppgifterna för att kunna utföra sina arbetsuppgifter har tillgång till dem.

Integrering av skyddsåtgärder kan avse funktioner för autentisering, t.ex. lösenord, möjlighet att använda kryptering vid kommunikation över internet och på mobila enheter, funktioner för loggning och säkerhetskopiering.

Vilka åtgärder som bör vidtas får avgöras i varje enskilt fall. Vilka faktorer som kan vara av betydelse utvecklas i kommentaren till 2 §. De tekniska möjligheterna och kostnaderna för genomförandet ska också vägas in.

4 §

Paragrafen, som genomför artikel 20.2, fastställer den personuppgiftsansvariges skyldighet att i automatiserade behandlingssystem införa dataskydd som standard. Den behandlas i avsnitt 9.2.1.

Dataskydd som standard innebär att systemet automatiskt styr användaren mot att arbeta integritetssäkert. Grundinställningarna ska vara satta så att inte mer information än nödvändigt samlas in eller visas. Skyldigheten att ha dataskydd som standard tar sikte på mängden insamlade personuppgifter, behandlingens omfattning, hur länge personuppgifterna behandlas och hur tillgängliga de är. Det innebär att den personuppgiftsansvarige ska se till att det i automatiserade behandlingssystem endast är möjligt att samla in de typer av personuppgifter som behövs, att person-

uppgifterna endast kan behandlas på ett sådant sätt och så länge som det är nödvändigt och att uppgifterna endast är tillgängliga för de personer som behöver dem i sitt arbete. Paragrafen kan i likhet med 3 § ses som en precisering av den övergripande skyldigheten i 2 §.

Med automatiserade behandlingssystem avses särskilt för verksamheten utformade eller anpassade behandlingssystem där personuppgifter behandlas mer eller mindre strukturerat, t.ex. verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. För att dataskydd som standard ska kunna införas i automatiserade behandlingssystem krävs det att den personuppgiftsansvarige har tekniska möjligheter och rätt att vidta sådana åtgärder i systemet. Standardprogram som Word, Outlook och Excel är inte att anse som automatiserade behandlingssystem i paragrafens mening och omfattas därför inte av kraven.

Något utrymme för lämplighetsbedömning i det enskilda fallet finns inte. Den personuppgiftsansvarige är skyldig att införa dataskydd som standard oavsett vilken behandling det rör sig om eller vad kostnaderna uppgår till.

5 §

Paragrafen, som genomför artikel 25.1, reglerar den personuppgiftsansvariges skyldighet att säkerställa att det i automatiserade behandlingssystem förs loggar över vissa typer av behandlingar. Paragrafen behandlas i avsnitt 9.2.2.

En logg är en behandlingshistorik som sparas under en viss tid. Det är en teknisk funktion i systemet som ska fungera automatiskt och som inte ska gå att ändra eller påverka på annat sätt. En logg bör vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Syftet med loggning är dels att verka förebyggande, dels att ge den personuppgiftsansvarige möjlighet att kontrollera användningen av systemen och att upptäcka felaktig eller obehörig användning av personuppgifterna. Loggningen bör inte utformas så att den medför onödiga intrång i användarnas integritet.

Krav på loggning vid behandling av personuppgifter följer indirekt av de generella kraven på lämpliga tekniska och organisatoriska åtgärder i både 2 och 8 §§. Förevarande paragraf utgör därmed ett mer preciserat krav på loggning i vissa typer av system. Vad som avses med automatiserade behandlingssystem framgår av kommentaren till 4 §. Standardprogram som Word, Outlook och Excel är i detta sammanhang inte att anse som automatiserade behandlingssystem och omfattas därför inte av kravet på loggning i paragrafen. Inte heller lagringsytor som t.ex. usbminnen och anställdas personliga mappar på den egna datorn omfattas. Krav på loggning i sådan programvara och på sådana lagringsytor följer dock, i den mån det är tekniskt möjligt, av 2 och 8 §§.

Paragrafen innebär att den personuppgiftsansvarige ska säkerställa att de automatiserade behandlingssystem som används möjliggör loggning i den utsträckning som krävs och att informationen faktiskt loggas. Av 2 § följer bl.a. krav på logguppföljning. Logguppföljning ska göras systematiskt och återkommande och vara såväl förebyggande som reaktiv. Den

personuppgiftsansvarige ska se till att det finns rutiner för logguppföljning.

Paragrafen gäller enligt 19 § även för personuppgiftsbiträden.

Tillgången till personuppgifter

6 §

Paragrafen, som har utformats i enlighet med *Lagrådets* förslag, reglerar den interna tillgången till personuppgifter för dem som arbetar under den personuppgiftsansvariges ledning. Den behandlas i avsnitt 9.2.3.

Paragrafen innebär att den personuppgiftsansvarige är skyldig att se till att anställda och andra som deltar i arbetet hos den personuppgiftsansvarige, t.ex. praktikanter eller inhyrd personal, bara ges tillgång till de personuppgifter som krävs för att de ska kunna fullgöra sina arbetsuppgifter. I de behöriga myndigheternas verksamheter behandlas som regel en betydande mängd personuppgifter. De är ofta av integritetskänsligt slag och bör inte spridas till någon som inte är behörig att ta del av uppgifterna. Kravet på behörighetsbegränsning syftar till att minska den interna exponeringen och spridningen av personuppgifterna. Hur det bör göras får bedömas med utgångspunkt i förutsättningarna och den behöriga myndighetens behov. Faktorer som myndighetens och it-systemens storlek och om personuppgifterna är sekretessreglerade eller annars integritetskänsliga ska beaktas.

Paragrafen reglerar inte bara tillgången till den personuppgiftsansvariges egen information. Vid direktåtkomst är det den mottagande myndigheten som ansvarar för att den egna personalen inte ges tillgång till fler personuppgifter i det it-system som åtkomsten avser än vad arbetsuppgifterna motiverar.

Paragrafen gäller enligt 19 § även för personuppgiftsbiträden.

Konsekvensbedömning och förhandssamråd

7 §

Paragrafen, som genomför artiklarna 27.1 och 28.1, slår fast den personuppgiftsansvariges skyldighet att inför vissa behandlingar göra en konsekvensbedömning och samråda med tillsynsmyndigheten. Den behandlas i avsnitt 9.2.4 och 9.2.5.

Av *första stycket* framgår att en konsekvensbedömning ska göras om det kan antas att en ny typ av behandling kommer att medföra särskild risk för intrång i registrerades personliga integritet. En konsekvensbedömning ska också göras om betydande förändringar av redan pågående behandlingar kan antas leda till sådan risk. Vid riskbedömningen bör bl.a. användningen av ny teknik och behandlingens art, omfattning, sammanhang och ändamål beaktas. Exempel på riskfyllda behandlingar som bör föranleda en konsekvensbedömning är inrättandet av storskaliga register som innehåller känsliga personuppgifter eller vissa former av profilering. En konsekvensbedömning ska omfatta relevanta system och processer för behandlingen men inte behandlingen i enskilda fall.

Andra stycket reglerar s.k. förhandssamråd. När en konsekvensbedömning visar att det finns särskild risk för intrång i registrerades personliga integritet eller när typen av behandling innebär särskild risk för intrång,

ska den personuppgiftsansvarige samråda med tillsynsmyndigheten. Samrådet ska äga rum i god tid innan behandlingen påbörjas eller betydande förändringar genomförs. Det bör dock inte äga rum så tidigt att det inte finns något konkret förslag på teknisk lösning för tillsynsmyndigheten att ta ställning till. När förhandssamrådet lämpligen bör äga rum får avgöras i varje enskilt fall och förutsätter en dialog med tillsynsmyndigheten. Tillsynsmyndighetens roll vid förhandssamråd regleras i 5 kap. 4 §.

Säkerheten för personuppgifter

Säkerhetsåtgärder

8 §

I paragrafen, som genomför artiklarna 4.1 f och 29, regleras den personuppgiftsansvariges skyldighet att skydda de personuppgifter som behandlas. Paragrafen behandlas i avsnitt 9.3.

Enligt paragrafen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Personuppgifterna ska särskilt skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. Uppräkningen illustrerar vad säkerhetsåtgärderna ska åstadkomma, men den är inte uttömmande.

Skydd mot obehörig eller otillåten behandling innebär att obehöriga personer ska vägras åtkomst till utrustning som används vid behandling (åtkomstskydd för utrustning), att obehörig läsning, kopiering, ändring eller radering av datamedier ska förhindras (kontroll av datamedier), att obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter ska förhindras (lagringskontroll) och att obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med uppgiftslämnande eller transport av databärare ska förhindras (transportkontroll). Åtgärder ska också vidtas i syfte att säkerställa att personer som är behöriga att använda ett it-system endast har tillgång till personuppgifter som omfattas av deras behörighet (åtkomstkontroll). Den personuppgiftsansvarige ska också säkerställa att det kan kontrolleras och fastställas till vilka myndigheter eller andra organ personuppgifter har överförts och för vilka myndigheter eller andra organ uppgifterna har gjorts tillgängliga (kommunikationskontroll) och att det i efterhand kan kontrolleras och fastställas vilka personuppgifter som förts in i ett it-system, när det har gjorts och av vem (indatakontroll).

Skydd mot förlust, förstöring eller annan oavsiktlig skada innebär bl.a. att de it-system som används ska kunna återställas vid störningar (återställande), att systemen ska fungera och att funktionsfel rapporteras (driftsäkerhet) och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemen (dataintegritet).

Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner. Rutiner för anmälan och uppföljning av personuppgiftsincidenter utgör också sådana åtgärder, se kommentaren till 9 §.

Vilken skyddsnivå som är lämplig får avgöras från fall till fall. Bedömningen är bl.a. beroende av vilka personuppgifter som behandlas och hur integritetskänsliga de är.

Paragrafen gäller enligt 19 § även för personuppgiftsbiträden.

Personuppgiftsincidenter

9 §

Paragrafen, som genomför artikel 30.1, reglerar anmälan av personuppgiftsincidenter till tillsynsmyndigheten. Personuppgiftsincident definieras i 1 kap. 6 §. Paragrafen behandlas i avsnitt 9.4.2.

Bestämmelser om rapportering av incidenter finns också i 10 och 10 a §§ säkerhetsskyddsförordningen (1996:633) och 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Anmälan av personuppgiftsincidenter enligt förevarande paragraf kommer som regel att göras parallellt med anmälan av it-incidenter enligt den sistnämnda förordningen.

I *första stycket* föreskrivs att den personuppgiftsansvarige ska anmäla en inträffad personuppgiftsincident till tillsynsmyndigheten inom 72 timmar. Anmälan ska dock inte göras till tillsynsmyndigheten om incidenten ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen. Undantag från anmälningsskyldigheten gäller således om incidenten ska anmälas enligt säkerhetsskyddsförordningen.

Någon anmälan behöver enligt *andra stycket* inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet. Undantaget kan exempelvis vara tillämpligt om incidenten påverkat en mycket begränsad mängd personuppgifter som inte är av känslig art eller om skyddet för uppgifterna påverkats under så kort tid att obehörig åtkomst inte varit möjlig. Den personuppgiftsansvarige har bevisbördan för att det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

10 §

Paragrafen reglerar den personuppgiftsansvariges skyldighet att underrätta registrerade om en personuppgiftsincident. Underrättelseskyldigheten omfattar bara sådana personuppgiftsincidenter som ska anmälas enligt 9 §. Gäller undantag från anmälningsskyldigheten behöver den registrerade inte underrättas. Informationen kan också begränsas med stöd av 11 §. Paragrafen genomför artikel 31.1, 31.3 och 31.5 och behandlas i avsnitt 9.4.3.

I *första stycket* anges under vilka omständigheter den registrerade ska underrättas. Underrättelseskyldigheten gäller bara om personuppgiftsincidenten medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet. Sådan särskild risk kan exempelvis finnas om känsliga personuppgifter har gjorts tillgängliga för ett stort antal obehöriga personer eller om en större mängd personuppgifter i ett specifikt ärende har ändrats eller förstörts. Hur snabbt den personuppgiftsansvarige bör informera den registrerade beror på omstän-

digheterna i det enskilda fallet. En omedelbar skaderisk kan kräva att de registrerade underrättas omgående. Underrättelsen bör lämnas så snart det är möjligt. Personuppgiftsincidentens art och den registrerades intresse av och möjlighet att själv vidta åtgärder för att begränsa skadan bör beaktas. Även den tid det tar för den personuppgiftsansvarige att vidta akuta åtgärder för att begränsa skadan, avhjälpa fel och liknande kan påverka tidpunkten för underrättelsen.

I *andra stycket* regleras i vilka fall någon underrättelse inte krävs. Den registrerade behöver enligt *punkt 1* inte underrättas om den personuppgiftsansvarige har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av personuppgiftsincidenten. Det kan t.ex. vara fallet om personuppgifterna har skyddats genom kryptering eller om pseudonymisering av personuppgifterna har tillämpats. Ett annat exempel kan vara att säkerhetskopiering gjorts.

Den registrerade behöver enligt *punkt 2* inte heller underrättas om den personuppgiftsansvarige har vidtagit åtgärder som säkerställer att det inte längre finns särskild risk för otillbörligt intrång i registrerades personliga integritet. En sådan åtgärd kan vara att tillgången till ett register har begränsats till dess att den personuppgiftsansvarige har kunnat överblicka konsekvenserna av incidenten.

Om det skulle krävas en oproportionerlig ansträngning att underrätta de registrerade behöver enligt *punkt 3* underrättelse inte heller lämnas. Det skulle kunna vara fallet om en personuppgiftsincident påverkar ett mycket stort antal registrerade. I det sistnämnda fallet ska i stället allmänheten informeras eller en liknande åtgärd vidtas för att de registrerade ska få nödvändig information. Det framgår av *tredje stycket*.

11 §

Paragrafen, som har utformats i enlighet med *Lagrådets* förslag, reglerar i vilka fall information till registrerade enligt 10 § får begränsas. Paragrafen genomför artikel 31.5 och behandlas i avsnitt 9.4.3.

Den personuppgiftsansvarige får enligt *första stycket* avstå från att lämna information om personuppgiftsincidenter i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifterna inte får lämnas ut. Det är främst sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen (2009:400) som avses. Vad det innebär utvecklas i kommentaren till 4 kap. 5 §. I första hand bör informationen senareläggas eller begränsas. Bara om det är absolut nödvändigt med hänsyn till de intressen som anges i paragrafen bör den personuppgiftsansvarige helt underlåta att informera den registrerade.

I *andra stycket* föreskrivs att en personuppgiftsansvarig som inte är en myndighet i motsvarande utsträckning får underlåta att lämna information.

Samarbete med tillsynsmyndigheten

12 §

I paragrafen, som genomför artikel 26, regleras den personuppgiftsansvariges skyldighet att samarbeta med tillsynsmyndigheten. Paragrafen behandlas i avsnitt 9.2.6. Skyldigheten omfattar enbart samarbete med den myndighet som är tillsynsmyndighet enligt lagen, se definitionen i 1 kap. 6 §. Skyldighet att bistå tillsynsmyndigheten regleras också i 5 kap. 5 §. Samarbete med andra tillsynsmyndigheter regleras inte i lagen.

Skyldigheten att samarbeta hör samman med tillsynsmyndighetens undersökningsbefogenheter. Skyldigheten innebär inte bara att den personuppgiftsansvarige ska ge tillsynsmyndigheten tillgång till det material, de resurser och den hjälp som krävs för att den ska kunna utöva tillsyn utan även att den personuppgiftsansvarige ska underlätta för tillsynsmyndigheten att utöva sina undersökningsbefogenheter på ett effektivt sätt. Det kan exempelvis innebära att hjälp ska erbjudas och ges inom rimlig tid. Tillsynsmyndigheten ska också ges möjlighet att ta del av information och material på det sätt som den anser mest lämpligt. Tillsynsmyndigheten förutsätts precisera vilken hjälp myndigheten behöver och sätter därigenom ramarna för samarbetsskyldigheten.

Skyldigheten att samarbeta gäller när tillsynsmyndigheten utför sina författningsreglerade uppgifter. Det innebär att bestämmelsen ska tillämpas när tillsynsmyndigheten utövar allmän tillsyn över personuppgiftsbehandling, handlägger klagomål från registrerade, på begäran kontrollerar om personuppgifter behandlas författningsenligt, bistår en tillsynsmyndighet i en annan medlemsstat och lämnar råd inom ramen för bl.a. förhandssamråd.

Paragrafen gäller enligt 19 § även för personuppgiftsbiträden.

Dataskyddsombud

13 §

Paragrafen reglerar den personuppgiftsansvariges skyldighet att utse dataskyddsombud. Den genomför artiklarna 32.1 och 32.4 och behandlas i avsnitt 9.5.2. Dataskyddsombud definieras i 1 kap. 6 §.

I paragrafen föreskrivs att ett eller flera dataskyddsombud ska utses. Dataskyddsombudet kan vara anställd hos den personuppgiftsansvarige eller en utomstående person. Den personuppgiftsansvarige får inte utse sig själv till dataskyddsombud.

Det finns inget som hindrar att flera personuppgiftsansvariga utser ett gemensamt dataskyddsombud. Det skulle kunna aktualiseras om de personuppgiftsansvariga bedriver liknande verksamhet i nära anslutning till varandra eller utför behandling i ett gemensamt system eller i ett avgränsat samarbete.

Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

I paragrafen, som genomför artikel 34, anges vilka uppgifter dataskyddsombud ska utföra. Paragrafen behandlas i avsnitt 9.5.3.

I *punkt 1* föreskrivs att dataskyddsombud självständigt ska kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör de skyldigheter som åligger personuppgiftsansvariga. Det innebär att ombudet måste förvissa sig om att den personuppgiftsansvarige följer bestämmelserna i lagen och andra författningar som reglerar behandlingen av personuppgifter. Hur omfattande kontrollen bör vara får avgöras efter omständigheterna.

Dataskyddsombuden bör framför allt granska den faktiska hanteringen av personuppgifter. Därutöver bör ombuden exempelvis granska rutinerna för behandling av personuppgifter, hur tillgången till personuppgifter hanteras och vilka krav på utbildning och andra kvalifikationer som den personuppgiftsansvarige ställer på personal som behandlar personuppgifter. Ombuden bör påpeka eventuella brister för den personuppgiftsansvarige så att denne blir medveten om dem och har möjlighet att vidta lämpliga åtgärder.

Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden bör framför allt ha sådan ställning i organisationen att deras synpunkter och råd tas på allvar. De förutsätts också ha goda kunskaper om regelverket om personuppgiftsbehandling.

I *punkt 2* anges att dataskyddsombuden ska informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid sådan behandling. Det handlar främst om att göra den personuppgiftsansvarige och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att informera registrerade, att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Det innebär inte att dataskyddsombuden ska tala om för den personuppgiftsansvarige och medarbetarna hur de ska behandla personuppgifter i enskilda fall.

Om den personuppgiftsansvarige begär det ska dataskyddsombudet också ge råd vid en konsekvensbedömning och kontrollera att bedömningen genomförs på korrekt sätt. Det framgår av *punkt 3*.

Enligt *punkt 4* ska dataskyddsombuden vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter. Syftet med bestämmelsen är att enskilda ska kunna vända sig till en kunnig person inom organisationen i frågor som t.ex. rör information om personuppgiftsbehandlingen och rättelse av felaktiga personuppgifter. Dataskyddsombuden har som kontaktpunkt skyldighet att hjälpa enskilda som vänder sig till myndigheten. I den rollen ligger också att bevaka att den personuppgiftsansvarige fullgör sina skyldigheter gentemot registrerade. Ombuden behöver däremot inte vidta de åtgärder som kan krävas med anledning av förfrågningar eller klagomål från registrerade.

I *punkt 5* föreskrivs att dataskyddsombuden ska samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter. Samarbeta har här i princip samma innebörd som i 12 §, dvs. det handlar om att underlätta tillsynsmyndighetens arbete. I samarbetsskyldigheten ligger

även att ombuden, när det är lämpligt, ska samråda med tillsynsmyndigheten i frågor som rör personuppgiftsbehandling. Det innebär att ombuden vid tveksamheter av olika slag bör fråga tillsynsmyndigheten om råd. Vid förhandssamråd bör arbetsuppgiften främst bestå i att bistå tillsynsmyndigheten med nödvändigt underlag och information och eventuellt stå till förfogande vid frågor angående behandlingen.

Ett dataskyddsombud behöver inte ägna sig uteslutande åt de arbetsuppgifter som anges i paragrafen. Beroende på hur organisationen ser ut kan arbetet som dataskyddsombud kombineras med andra arbetsuppgifter, så länge de inte kommer i konflikt med uppdraget som ombud.

15 §

I paragrafen, som behandlas i avsnitt 15.3, regleras dataskyddsombudens tystnadsplikt.

I *första stycket* föreskrivs att den som fullgör uppgift som dataskyddsombud inte obehörigen får röja det som han eller hon i den rollen har fått kännedom om. Bestämmelsen är tillämplig på den som fullgör uppgift som dataskyddsombud åt någon annan aktör än en myndighet eller annat organ som tillämpar offentlighets- och sekretesslagen.

Om dataskyddsombudet har en sådan anställning eller ett sådant uppdrag som avses i 2 kap. 1 § offentlighets- och sekretesslagen tillämpas i stället den lagen, vilket framgår av *andra stycket*.

Personuppgiftsbiträden

16 §

Av paragrafen, som i allt väsentligt har utformats enligt *Lagrådets* förslag, framgår att personuppgiftsbiträden får anlitas och vad den personuppgiftsansvarige måste göra innan ett personuppgiftsbiträde anlitas. Paragrafen genomför artikel 22.1 och 22.3–22.4 och behandlas i avsnitt 9.6.2.

I *första stycket* föreskrivs att en personuppgiftsansvarig får anlita personuppgiftsbiträden. Det förutsätter dock att det är lämpligt. Om det är lämpligt får avgöras med hänsyn bl.a. till vilka personuppgifter som ska behandlas och om det gäller sekretess för uppgifterna. Av första stycket framgår också att den personuppgiftsansvarige, innan personuppgiftsbiträdet anlitas, ska försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att personuppgiftsbehandlingen ska vara författningsenlig och för att skydda registrerades rättigheter. Kraven omfattar inte bara säkerhetsåtgärder, utan även andra tekniska och organisatoriska åtgärder. Skyldigheten innebär att den personuppgiftsansvarige, innan ett personuppgiftsbiträde anlitas, bl.a. bör förhöra sig om hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna kommer att ha.

I *andra stycket* ställs krav på att det ska ingås ett skriftligt avtal eller någon annan skriftlig överenskommelse som reglerar personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. Eftersom statliga myndigheter, som är att anse som två enheter inom samma juridiska person, i rättslig mening inte kan ingå bindande avtal med varandra får de träffa en skriftlig överenskommelse som regle-

rar behandlingen om en myndighet agerar personuppgiftsbiträde åt en annan.

17 §

Paragrafen, som genomför artikel 22.2, reglerar vad som gäller när ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde. Paragrafen har utformats enligt *Lagrådets* förslag och behandlas i avsnitt 9.6.2.

I paragrafen föreskrivs att ett personuppgiftsbiträde inte utan skriftligt tillstånd från den personuppgiftsansvarige får anlita ett annat personuppgiftsbiträde, ett underbiträde. Ett sådant tillstånd kan gälla biträdets rätt att anlita underbiträden generellt eller i en specifik situation. Syftet med bestämmelsen är att den personuppgiftsansvarige ska känna till vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning.

18 §

Paragrafen, som genomför artikel 22.5 och delar av artikel 23, reglerar vad som gäller vid behandling av personuppgifter hos ett personuppgiftsbiträde. Paragrafen behandlas i avsnitt 9.6.3.

I *första stycket* slås fast den grundläggande principen att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Instruktionerna till biträdet bör vara så tydliga att det inte finns risk för otillåten behandling. Instruktionerna kan exempelvis gälla hur tillgången till personuppgifter hos biträdets anställda ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för dataskydd. Om det finns avvikande regler i annan lagstiftning som föreskriver att personuppgiftsbiträdet är skyldig att utföra viss behandling, t.ex. att lämna ut allmänna handlingar, får behandlingen utföras utan särskilda instruktioner.

I *andra stycket* regleras det fallet där personuppgiftsbiträdet bestämmer ändamålen med och medlen för behandlingen. Personuppgiftsbiträdet är då att anse som personuppgiftsansvarig för den behandlingen. Att den som bestämmer ändamålen med och medlen för behandlingen är att anse som personuppgiftsansvarig framgår av definitionen av personuppgiftsansvarig i 1 kap. 6 §.

19 §

I paragrafen föreskrivs vilka skyldigheter som gäller för personuppgiftsbiträden. Paragrafen, som genomför delar av artiklarna 25, 26 och 29, behandlas i avsnitt 9.6.5.

Hänvisningen till 5 och 6 §§ innebär att personuppgiftbiträden, i likhet med personuppgiftsansvariga, är skyldiga att dels säkerställa att loggar förs i automatiserade behandlingssystem, dels se till att anställda bara ges tillgång till de personuppgifter som krävs för att fullgöra arbetsuppgifterna. Innebörden av bestämmelserna framgår av kommentarerna till 5 och 6 §§.

Vidare gäller skyldigheten enligt 8 § att vidta lämpliga säkerhetsåtgärder även för personuppgiftsbiträden. Innebörden av skyldigheten framgår av kommentaren till den paragrafen.

Personuppgiftsbiträden är också, genom hänvisningen till 12 §, skyldiga att i samma utsträckning som personuppgiftsansvariga samarbeta med tillsynsmyndigheten. Innebörden av skyldigheten framgår av kommentaren till den paragrafen. Personuppgiftsbiträdens skyldighet att samarbeta med tillsynsmyndigheten kan aktualiseras i flera olika situationer. Samarbete kan t.ex. krävas vid tillsyn hos biträdet. Då är samarbetsskyldigheten i princip densamma som för den personuppgiftsansvarige. Samarbetsskyldigheten kan också aktualiseras vid tillsyn hos den personuppgiftsansvarige som biträdet utför personuppgiftsbehandling åt eller inom ramen för den personuppgiftsansvariges förhandssamråd med tillsynsmyndigheten. Skyldigheten innebär att biträdet också måste samarbeta med den personuppgiftsansvarige, eftersom det är en förutsättning för att tillsynsmyndigheten ska kunna utföra sitt arbete.

Att personuppgiftsbiträden åläggs vissa skyldigheter fråntar inte de personuppgiftsansvariga deras ansvar. Den personuppgiftsansvarige är, som framgår av kommentaren till 1 §, ansvarig för den behandling av personuppgifter som personuppgiftsbiträdet utför på dennes vägnar. Den omständigheten att personuppgiftsbiträden ges en direkt skyldighet att vidta vissa åtgärder innebär dock att tillsynsmyndigheten vid brister kan vidta åtgärder mot både personuppgiftsbiträdet och den personuppgiftsansvarige.

Gemensamt personuppgiftsansvar

20 §

Paragrafen, som genomför artikel 21, anger när två eller flera behöriga myndigheter är gemensamt personuppgiftsansvariga. Den behandlas i avsnitt 9.7.2.

I *första stycket* slås det fast att gemensamt personuppgiftsansvar uppkommer när två eller flera behöriga myndigheter gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen. Ett operativt samarbete mellan två eller flera myndigheter, så som sker under ledning av Polismyndigheten i arbetet mot organiserad brottslighet, medför inte i sig att ett gemensamt ansvar för behandlingen uppkommer. Det avgörande är i stället om myndigheterna tillsammans bestämmer ändamålen med och medlen för behandlingen.

I *andra stycket* anges att den registrerade får utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Bemyndigande

21 §

I paragrafen, som behandlas i avsnitt 9.8, bemyndigas regeringen med stöd av 8 kap. 3 § första stycket regeringsformen att meddela föreskrifter om skyldighet att föra register över kategorier av behandlingar av personuppgifter och skyldighet att införa interna rutiner för anmälan av överträdelser.

Rätten till information

Allmän information

1 §

I paragrafen, som genomför artikel 13.1, anges vilken allmän information som på den personuppgiftsansvariges eget initiativ ska göras tillgänglig för registrerade. Informationen, som riktar sig till allmänheten eller en obestämd, större krets av registrerade, kan göras tillgänglig t.ex. på den behöriga myndighetens webbplats. Paragrafen behandlas i avsnitt 10.2.5 och 10.2.6.

Enligt *punkt 1* ska den personuppgiftsansvariges identitet och kontaktuppgifter göras tillgängliga. Med det avses uppgifter om namn, post- och besöksadress, telefonnummer och e-postadress. Alla personuppgiftsansvariga är enligt 3 kap. 13 § skyldiga att utse dataskyddsombud. Enligt *punkt 2* ska dataskyddsombudets kontaktuppgifter anges. Det behöver inte vara en kontaktuppgift direkt till dataskyddsombudet, t.ex. hans eller hennes e-postadress, utan det är tillräckligt att ombudet går att nå med hjälp av uppgifterna.

I *punkt 3* föreskrivs att kategorier av ändamål för behandlingen ska framgå. Det är alltså inte ändamålen med behandlingen av personuppgifter i enskilda fall som avses utan vilka kategorier av ändamål som den behöriga myndigheten behandlar personuppgifter för. Det kan t.ex. vara förundersökning, ärenden om strafföreläggande eller handläggning av brottmål.

I *punkt 4* och *5* föreskrivs att den personuppgiftsansvarige ska upplysa om de rättigheter som enskilda har enligt 3, 9 och 10 §§. Det gäller rätten för registrerade att få information om behandlingen av personuppgifter och att få del av uppgifterna och rätten att begära rättelse, radering eller begränsning av behandlingen. Den personuppgiftsansvarige ska även enligt *punkt 6* upplysa om möjligheten att lämna in klagomål till tillsynsmyndigheten och ange kontaktuppgifterna till myndigheten.

Personrelaterad information

2 §

Paragrafen, som genomför artikel 13.2, anger vilken information som ska lämnas till den registrerade i ett enskilt fall för att han eller hon ska kunna ta till vara sina rättigheter. Det är fråga om personrelaterad information som på den personuppgiftsansvariges eget initiativ ska lämnas till den registrerade. Paragrafen har utformats i enlighet med *Lagrådets* förslag och behandlas i avsnitt 10.2.5 och 10.2.7.

I *första stycket* föreskrivs att den registrerade i ett enskilt fall ska ges viss information för att kunna ta till vara sina rättigheter. Sådana fall som avses i bestämmelsen kan t.ex. vara att den registrerade riskerar att lida rättsförlust om han eller hon inte får del av informationen eller att det av annat skäl är viktigt för honom eller henne att känna till behandlingen för att kunna ta till vara sina rättigheter. Ett annat exempel kan vara att känsliga personuppgifter har behandlats i strid med 2 kap. 11 §. Information behöver inte lämnas vid fel som inte kan antas ha negativ påverkan, t.ex. när personnummer eller adressuppgifter som visat sig vara felaktiga

rättas. För att informationsskyldigheten ska inträda bör normalt krävas att det är fråga om överträdelser av regelverket som kan föranleda skadeståndsansvar, allvarlig kritik eller ingripande från tillsynsmyndigheten eller någon liknande reaktion.

Att informationen är tillgänglig på den personuppgiftsansvariges webbplats eller i en informationsskrift befriar inte den personuppgiftsansvarige från skyldigheten att lämna samma information till en viss registrerad, om informationen behövs för att han eller hon ska kunna ta till vara sina rättigheter.

Enligt *punkt 1* ska information lämnas om den rättsliga grunden för personuppgiftsbehandlingen. Den rättsliga grunden kan t.ex. vara att det är nödvändigt att behandla personuppgifterna vid utredning av brott eller verkställighet av straffrättsliga påföljder.

Punkt 2 föreskriver att kategorier av mottagare av personuppgifterna ska anges. Mottagare definieras i 1 kap. 6 §. Allmän information är tillräcklig, exempelvis till vilken typ av myndighet som personuppgifterna har lämnats eller ska lämnas. Det kan vara t.ex. allmän domstol eller Kriminalvården. Om mottagarkategorin finns i ett tredjeland eller är en internationell organisation ska det anges.

Information ska enligt *punkt 3* lämnas om hur länge personuppgifterna får behandlas. Om det inte är möjligt att ange hur länge uppgifterna får behandlas i det enskilda fallet ska i stället kriterierna för att fastställa det anges. Det kan vara upplysningar om vilka omständigheter eller tidpunkter som styr hur länge uppgifterna får behandlas, t.ex. nedläggning av åtal eller när viss tid förflutit efter det att uppgifterna behandlades första gången.

Även övrig nödvändig information ska lämnas enligt *punkt 4*. Om informationen är nödvändig ska bedömas utifrån den registrerades behov av den för att kunna ta till vara sina rättigheter. Det kan vara en upplysning om rätten att begära att få del av uppgifterna, rätten att begära rättelse, radering eller begränsning av behandlingen och möjligheten att lämna in klagomål till tillsynsmyndigheten.

Av *andra stycket* framgår att den personuppgiftsansvarige vid bedömningen av om information enligt punkt 4 ska lämnas särskilt ska beakta om personuppgifterna har samlats in utan att den registrerade vetat om det.

Av 5 § framgår att informationsskyldigheten får begränsas. I 12 § föreskrivs att avgift inte får tas ut för information enligt förevarande paragraf.

3 §

Paragrafen, som genomför artikel 14, behandlas i avsnitt 10.2.5 och 10.2.8. I paragrafen regleras en enskilds rätt att på begäran få besked om hans eller hennes personuppgifter behandlas, att få del av sådana uppgifter och att få viss information om behandlingen av dem.

I *första stycket* föreskrivs att den som begär det har rätt till skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och få viss i paragrafen uppräknad skriftlig information.

Vem som helst får begära besked av den personuppgiftsansvarige. Vårdnadshavare och andra ställföreträdare kan begära besked för den som inte själv har rätt att göra det. Om en underårig förstår vad åtgärden innebär och själv kan tillgodogöra sig den information som begäran avser bör hans eller hennes begäran godtas. Sökanden har bevisbördan för att begäran har gjorts och tidpunkten för det. Bestämmelsen i 22 § förvaltningslagen (2017:900) kan vara till ledning vid avgörande av frågan om när en begäran ska anses ha gjorts (jfr prop. 1997/98:44 s. 132). Begäran ska besvaras utan onödigt dröjsmål. Beskedet till sökanden ska vara skriftligt och kan lämnas t.ex. via e-post. Det ska avse om personuppgifter som rör sökanden behandlas.

Om sökandens personuppgifter behandlas ska, med de begränsningar som följer av andra stycket och 5–7 §§, han eller hon få del av dem. Rätten omfattar även personuppgifter som utgörs av bild- och ljudupptagningar och personuppgifter i ostrukturerat material som t.ex. löpande text.

Det är de uppgifter som behandlas vid tiden för utlämnandet som ska lämnas ut (jfr prop. 1997/98:44 s. 132). Sökanden ska få tillgång till all information som den personuppgiftsansvarige själv kan få fram om honom eller henne, men det är tillräckligt att använda de sök- och sammanställningsmöjligheter som är faktiskt tillgängliga och rättsligt tillåtna (jfr prop. 1997/98:44 s. 82 f.). Det bör räcka att sökningar görs i myndighetens verksamhetsspecifika behandlingssystem, t.ex. dokument- och ärendehanteringssystem, register och databaser. Om uppgifter är sökbara i standardprogram som Word, Outlook och Excel bör de också omfattas.

För att det ska kunna utrönas om personuppgifter behandlas krävs att det finns sökbara uppgifter som direkt kan hänföras till den person som begär informationen. Sökanden förutsätts därför lämna sådana uppgifter om sin identitet att det blir möjligt att söka efter informationen. Det kan vara fullständigt namn eller person- eller samordningsnummer eller någon annan lika unik identitetsuppgift.

Sökanden kan få del av uppgifterna genom t.ex. en kopia av en handling med de personuppgifter som rör honom eller henne. Den personuppgiftsansvarige har dock ingen skyldighet att lämna ut en kopia om sökandens rättigheter kan säkerställas på annat sätt, t.ex. genom en sammanfattning av vilka personuppgifter som behandlas.

Sökanden ska också informeras om behandlingen av personuppgifterna. Enligt *punkt 1* och *2* ska informationen avse vilka personuppgifter om sökanden som behandlas och, om det är känt, varifrån uppgifterna kommer.

I *punkt 3* föreskrivs att den rättsliga grunden för behandlingen ska anges. Den rättsliga grunden kan t.ex. vara att det är nödvändigt att behandla personuppgifterna vid utredning av brott eller verkställighet av straffrättsliga påföljder. Vidare ska enligt *punkt 4* information om ändamålen med behandlingen lämnas. Det som avses är ändamålen i det enskilda fallet, t.ex. vilket ärende eller vilken förundersökning det är fråga om.

Vidare ska information om mottagare eller kategorier av mottagare av personuppgifterna lämnas enligt *punkt 5*. Mottagare definieras i 1 kap. 6 §. Det som sägs i kommentaren till 2 § gäller även de uppgifter som är aktuella här.

Enligt *punkt 6* ska information också lämnas om hur länge personuppgifterna får behandlas. Det som sägs i kommentaren till 2 § gäller även de uppgifter som är aktuella här.

I *punkt 7* föreskrivs att den personuppgiftsansvarige ska informera om rätten att begära rättelse, radering eller begränsning av behandlingen. Den personuppgiftsansvarige ska även enligt *punkt 8* upplysa om möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till myndigheten. Punkterna motsvarar 1 § 5 och 6 och behandlas i kommentaren till den paragrafen.

I *andra stycket* begränsas rätten att få del av personuppgifter. Om sökanden redan har tagit del av personuppgifterna behöver de inte lämnas ut till honom eller henne. Det har ingen betydelse på vilket sätt sökanden fått del av dem. Det kan t.ex. vara personuppgifter i handlingar som sökanden själv har skickat in till myndigheten eller som myndigheten har expedierat till honom eller henne. Den personuppgiftsansvarige måste emellertid tydligt ange vilka personuppgifter som behandlas och ge sökanden en förteckning över dem. Den personuppgiftsansvarige måste också lämna information om behandlingen enligt första stycket 2–8. Vidare har sökanden rätt att få del av personuppgifterna om han eller hon begär det.

Om en begäran om information är orimlig eller uppenbart ogrundad får den avslås enligt 7 § första stycket.

I 12 § föreskrivs att information enligt förevarande paragraf ska lämnas till den registrerade avgiftsfritt en gång per år och att utlämnande därutöver kan avgiftsbeläggas.

4 §

Paragrafen, som genomför delar av artikel 11, ger den som har varit föremål för ett automatiserat beslut rätt till information. Paragrafen behandlas i avsnitt 10.2.9.

Paragrafen innebär att den registrerade har rätt att på begäran få närmare information av den personuppgiftsansvarige om beslutet. Det kan t.ex. gälla frågor om omständigheterna som ledde fram till beslutet.

I 12 § första stycket föreskrivs att avgift inte får tas ut för information enligt förevarande paragraf.

Begränsning av rätten till information

5 §

Paragrafen, som genomför artiklarna 13.3, 15.1 och 16.4, gör undantag från den personuppgiftsansvariges informationsskyldighet. Paragrafen har utformats i enlighet med *Lagrådets* förslag. Paragrafen är också delvis utformad efter mönster av 27 § personuppgiftslagen och behandlas i avsnitt 10.3.1. I 3 kap. 11 § regleras i vilka fall information till registrerade om personuppgiftsincidenter får begränsas.

Enligt *första stycket* gäller den personuppgiftsansvariges skyldighet att lämna personrelaterad information enligt 2 och 3 §§ inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifterna inte får lämnas ut. Regleringen innebär att den personuppgiftsan-

svarige får begränsa eller utelämna informationen. Det är främst sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen (2009:400) som avses. Även andra bestämmelser om tystnadsplikt och bestämmelser som begränsar möjligheten att använda uppgifter som en svensk myndighet har fått från en myndighet i en annan stat kan begränsa informationsskyldigheten. Undantaget från informationsskyldigheten gäller även vid beslut som har meddelats med stöd av författning, t.ex. beslut om förbehåll enligt 10 kap. 14 § offentlighets- och sekretesslagen. Även andra författningar kan innehålla bestämmelser som gör paragrafen tillämplig, t.ex. 6 kap. 6 § lagen (2010:751) om betaltjänster. Det är dock endast bestämmelser om att uppgifter inte får lämnas som hänför sig till de intressen som räknas upp i paragrafen som inskränker rätten till information. I avsnitt 10.3.1 redovisas ingående vilken prövning den personuppgiftsansvarige ska göra och hur den förhåller sig till de i paragrafen uppräknade intressena.

I *punkt 1* skyddas intresset av att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det rör sig alltså om skydd för allmänna intressen. *Punkt 2* skyddar intresset av att andra rättsliga utredningar eller undersökningar inte hindras. Det kan exempelvis vara fråga om utredning om administrativa avgifter som vattenföroreningsavgift vid oljeutsläpp. I *punkt 3* skyddas nationell säkerhet. Intresset av att skydda annans rättigheter och friheter regleras i *punkt 4*. Det är inte den registrerades rättigheter och friheter som skyddas, utan andra personers.

Den personuppgiftsansvarige är enligt *andra stycket* inte heller skyldig att lämna ut skälen för beslut enligt första stycket och beslut i fråga om rättelse, radering eller begränsning av behandlingen om motiveringen skulle riskera att skada något av de intressen som anges i första stycket.

Eftersom lagen är tillämplig på andra aktörer än myndigheter föreskrivs i *tredje stycket* att även en personuppgiftsansvarig som inte är en myndighet i motsvarande utsträckning får begränsa eller underlåta att lämna information av hänsyn till något av de intressen som anges i första stycket.

6 §

Paragrafen, som har sin grund i artikel 15.1 e, föreskriver undantag från informationsskyldigheten i 3 § för personuppgifter i viss typ av text. Paragrafen behandlas i avsnitt 10.3.3.

Den personuppgiftsansvariges skyldighet att lämna personrelaterad information enligt 3 § gäller enligt *första stycket* inte för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller text som utgör minnesanteckningar eller liknande. Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas. Bild- och ljudupptagningar omfattas inte av undantaget eftersom det bara gäller text. Med text som inte fått sin slutliga utformning avses koncept eller utkast till protokoll, skrivelser, beslut eller liknande. Löpande text som är avsedd att tidvis ändras eller kompletteras och därför aldrig får någon slutlig utformning omfattas inte. Det sistnämnda kan t.ex. vara diarier, journaler, register eller förteckningar som

förs löpande. Med minnesanteckning avses anteckningar som utgör hjälpmedel för handläggningen, t.ex. promemorior och andra anteckningar eller upptagningar som har skapats bara för att förbereda ett ärende för avgörande och som inte har tillfört ärendet något i sak.

Av *andra stycket* framgår att undantaget från informationsskyldigheten inte gäller under vissa förhållanden. Sökanden har då rätt att få del av personuppgifter även i ofärdig löpande text eller i minnesanteckningar och liknande.

Enligt *punkt 1* gäller undantaget inte om personuppgifterna har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Tredje man definieras i 1 kap. 6 §. Det är den version av uppgifterna i t.ex. utkastet som lämnades till tredje man som informationsskyldigheten omfattar, även om utkastet därefter har ändrats.

Enligt *punkt 2* gäller undantaget inte om personuppgifterna behandlas enbart för vetenskapliga, statistiska eller historiska ändamål. Om ett utkast eller en minnesanteckning endast används vid statistikproduktion eller för vetenskapliga eller historiska ändamål inom lagens tillämpningsområde ska alltså information om behandlingen av personuppgifterna lämnas ut. I *punkt 3* anges att undantaget inte heller gäller för personuppgifter som har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Det är tidpunkten för begäran som är avgörande för bedömningen av om något av undantagen gäller. Både ettårsfristen och frågan om uppgifterna har lämnats ut till tredje man eller behandlas för vetenskapliga, statistiska eller historiska ändamål ska bedömas i förhållande till när begäran om information gjordes (jfr prop. 1997/98:44 s. 83 f.).

7 §

Paragrafen, som tillsammans med 12 § genomför delar av artikel 12.4, behandlas i avsnitt 10.3.4. Paragrafen föreskriver att information enligt 3 § inte behöver lämnas om begäran är orimlig eller uppenbart ogrundad.

I *första stycket* föreskrivs att den personuppgiftsansvarige får avslå en begäran att få information om behandlingen av personuppgifter och få del av dem om begäran är orimlig eller uppenbart ogrundad. En begäran kan vara orimlig t.ex. om den upprepas ofta. En begäran kan också vara orimlig om den är så oprecis att det skulle vara närmast omöjligt att besvara den, t.ex. om den rör en större myndighets hela verksamhet. Normalt bör i sådana fall begäran kunna preciseras till viss verksamhet, visst ärende eller någon annan liknande avgränsning. En begäran kan vara uppenbart ogrundad t.ex. om sökanden missbrukar sin rätt till information genom att exempelvis lämna felaktiga eller missvisande uppgifter i sin begäran. Den personuppgiftsansvarige har bevisbördan för att en begäran är orimlig eller uppenbart ogrundad.

I *andra stycket* upplyses att den personuppgiftsansvarige med stöd av 12 § andra stycket i vissa fall får ta ut avgift i stället för att avslå begäran.

Möjligheten att begära kontroll genom tillsynsmyndigheten

8 §

I paragrafen, som behandlas i avsnitt 10.3.1, upplyses om att den registrerade med stöd av 5 kap. 3 § kan begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt.

Rätten till rättelse, radering och begränsning av behandlingen

9 §

Paragrafen reglerar den enskildes rätt att begära rättelse eller komplettering av felaktiga eller ofullständiga personuppgifter och begränsning av behandlingen av personuppgifterna. Den genomför artikel 16.1 och, tillsammans med 10 §, artikel 16.3. Paragrafen behandlas i avsnitt 10.4.1 och 10.4.3. I 2 kap. 15 § regleras personuppgiftsansvarigas skyldighet att på eget initiativ rätta felaktiga eller ofullständiga personuppgifter och uppdatera inaktuella personuppgifter.

Enligt *första stycket* ska den personuppgiftsansvarige på begäran av den registrerade rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Vårdnadshavare och andra ställföreträdare kan begära rättelse eller komplettering åt en registrerad som inte själv har rätt att göra det. I kommentaren till 2 kap. 7 § framgår vad som avses med att en personuppgift är korrekt och vilka bedömningar som ska göras.

Rättelse eller komplettering ska göras utan onödigt dröjsmål. Det innebär att den personuppgiftsansvarige skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt genomföra åtgärden.

Den personuppgiftsansvarige ska enligt *andra stycket* begränsa behandlingen av personuppgifter som rör den registrerade om han eller hon ifrågasätter att de är korrekta. Den registrerade kan ha en annan uppfattning än den personuppgiftsansvarige om huruvida en personuppgift är korrekt. Om korrektheten ifrågasätts är den personuppgiftsansvarige skyldig att försöka klarlägga hur det förhåller sig. Om den personuppgiftsansvariges utredning om den omstridda personuppgiften inte kan slutföras inom den tid som en personuppgift ska rättas eller kompletteras, ska behandlingen begränsas under utredningstiden.

Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av vare sig den personuppgiftsansvarige, ett personuppgiftsbiträde eller någon annan, utom för de ändamål för vilka behandlingen begränsades. Uppgiften får dock lämnas ut med stöd av 2 kap. tryckfrihetsförordningen. Den personuppgiftsansvarige ska vidta åtgärder som visar att behandlingen av personuppgiften har begränsats. En sådan åtgärd kan vara att föra över uppgiften från det datasystem där den behandlas, t.ex. myndighetens verksamhetssystem, till ett arkivsystem. Andra åtgärder kan vara att göra personuppgiften oåtkomlig genom en teknisk begränsning eller annan inskränkning av tillgången till uppgiften. När utredningen om personuppgiften är avslutad ska begränsningen av behandlingen upphöra. Då ska personuppgiften antingen rättas eller fortsätta att behandlas som tidigare.

Paragrafen reglerar den enskildes rätt att vid otillåten behandling av personuppgifter begära radering eller, om personuppgifterna behöver finnas kvar av bevisskäl, begränsning av behandlingen. Den genomför artikel 16.2 och, tillsammans med 9 §, artikel 16.3. Paragrafen behandlas i avsnitt 10.4.2 och 10.4.3. I 2 kap. 16 § regleras personuppgiftsansvarigas skyldighet att på eget initiativ radera eller begränsa behandlingen av personuppgifter som behandlas på otillåtet sätt.

Enligt *första stycket* ska den personuppgiftsansvarige på begäran av den registrerade radera personuppgifter som rör honom eller henne, om de behandlas i strid med 2 kap. 1, 2, 3 § första stycket, 4–6, 8, 11, 12, 14 eller 17 § första stycket eller om det krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. Vårdnadshavare och andra ställföreträdare kan begära radering för en registrerad som inte har rätt att själv göra det.

Om personuppgifter behandlas i strid med någon av de bestämmelser som räknas upp i paragrafen ska de på begäran av den registrerade raderas. Med radering avses att personuppgifter tas bort från informationssamlingar på ett sådant sätt att de inte längre kan återskapas. I de aktuella bestämmelserna föreskrivs bl.a. att personuppgifter ska vara adekvata och relevanta, att inte fler personuppgifter än nödvändigt får behandlas och att de bara får behandlas om det finns en rättslig grund och för särskilt angivna ändamål. Där regleras också behandling av känsliga personuppgifter och hur länge personuppgifter får behandlas. Frågan om en personuppgift ska raderas ska bedömas mot bakgrund av kraven i dessa bestämmelser.

Personuppgifter ska också raderas på begäran av den registrerade om det krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. Rättslig förpliktelse kan avse en skyldighet som rör hur personuppgifter får behandlas enligt denna lag, myndighetens registerförfattning eller annan författning om ett enskilt register, t.ex. lagen (1998:621) om misstankeregister.

Utrymmet för att radera uppgifter i allmänna handlingar begränsas av arkivlagstiftningen genom att det krävs författningsstöd för gallring.

Radering ska göras utan onödigt dröjsmål. Det innebär att den personuppgiftsansvarige skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt radera uppgiften.

Om förutsättningarna för att radera personuppgifterna är uppfyllda, men uppgifterna behöver finnas kvar av bevisskäl, ska enligt *andra stycket* den personuppgiftsansvarige på begäran av den registrerade i stället begränsa behandlingen av uppgifterna.

En begränsning kan bara göras i de fall där personuppgifterna behandlas otillåtet, eftersom det endast är då som radering kan komma i fråga. För att personuppgifterna inte ska raderas ska de behövas som bevisning, t.ex. i en rättsprocess angående otillåten personuppgiftsbehandling. Däremot är det inte tillåtet att ha kvar personuppgifter som ska raderas i syfte att använda dem t.ex. för brottsbekämpning.

Begränsning av behandlingen är inte en permanent åtgärd. När personuppgifterna inte längre behöver finnas kvar av bevisskäl, t.ex. för att

domen eller beslutet i skadeståndsmålet har fått laga kraft, ska begränsningen upphöra och personuppgifterna raderas.

Behandlingen ska begränsas utan onödigt dröjsmål. Hur det kan göras utvecklas i kommentaren till 9 §.

11 §

Enligt paragrafen, som behandlas i avsnitt 10.4.4, avgör den personuppgiftsansvarige vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Paragrafen innebär att den personuppgiftsansvarige – med beaktande av vilken åtgärd som är lagligen möjlig att vidta – ska se till att den lämpligaste åtgärden vidtas oavsett vilken åtgärd som begärs av den registrerade. Vad som är mest lämpligt ska bedömas med utgångspunkt i både verksamhetens behov och den registrerades rätt till skydd för sina personuppgifter.

Avgiftsfri information

12 §

Paragrafen, som tillsammans med 7 § genomför delar av artikel 12.4, föreskriver att information som huvudregel ska vara avgiftsfri. Den behandlas i avsnitt 10.3.4 och 10.5.9.

I *första stycket* slås fast att den information som den personuppgiftsansvarige på eget initiativ ska lämna till en registrerad om behandlingen av hans eller hennes personuppgifter och information om automatiserade beslut ska vara avgiftsfri, medan den information om behandlingen av den registrerades personuppgifter som lämnas på begäran ska vara utan avgift en gång per år.

I *andra stycket* föreskrivs att om någon begär att få information om behandlingen av personuppgifter och få del av dem oftare än en gång per år får den personuppgiftsansvarige ta ut en rimlig avgift för det. Den personuppgiftsansvarige får, i stället för att ta ut avgift, avslå begäran, vilket regleras i 7 § första stycket. Utgångspunkten bör vara att den personuppgiftsansvarige i första hand tar ut avgift och i andra hand avslår begäran om information. Vilken åtgärd som är lämpligast får avgöras med utgångspunkt i omständigheterna i det enskilda fallet. En viktig faktor kan vara hur många framställningar om information som personen har gjort under året och hur lång tid som förflutit efter den senaste framställan. Även omständigheter som hur preciserad eller komplicerad begäran är och vilka skäl han eller hon anger för sin begäran bör beaktas.

Om den personuppgiftsansvarige avser att ta ut avgift bör den som begärt informationen underrättas om det. Den personuppgiftsansvarige bör förhöra sig om begäran vidhålls. Avgiften ska vara rimlig, vilket innebär att den inte får överstiga de administrativa kostnaderna för att besvara begäran.

5 kap. Tillsyn

Tillsynsmyndighetens uppdrag

1 §

Paragrafen, som genomför artikel 41.1 och behandlas i avsnitt 11.5, reglerar tillsynsmyndighetens uppdrag. Den har utformats i enlighet med *Lagrådets* förslag. Definitionen av tillsynsmyndigheten finns i 1 kap. 6 §.

Paragrafen tydliggör att tillsynsmyndigheten ska ha dubbla perspektiv vid sin tillsyn. Den innebär att tillsynsmyndigheten i sin tillsyn ska verka både för att fysiska personers grundläggande rättigheter och friheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom denna lags tillämpningsområde. Vid sin tolkning och tillämpning av regelverket ska tillsynsmyndigheten bl.a. beakta hur tillsynen påverkar informationsutbytet både nationellt och internationellt, t.ex. vid bedömning av vad som utgör lämpliga skyddsåtgärder och en tillräcklig skyddsnivå. Om myndigheten exempelvis i sin tillsyn konstaterar att den personuppgiftsansvarige ska vidta en åtgärd och det finns flera alternativ som är likvärdiga ur integritetssynpunkt, bör den åtgärd som innebär minst hinder för det fria flödet av personuppgifter förordas. Intresseavvägningen ska även speglas i tillsynsmyndighetens föreskrifter, råd och annan information som myndigheten tar fram.

Tillsynsmyndighetens uppgifter

2 §

Paragrafen genomför delar av artiklarna 46 och 50.1 och reglerar, tillsammans med 3 och 4 §§, tillsynsmyndighetens uppgifter. Paragrafen behandlas i avsnitt 11.6.1, 11.6.2 och 11.10.1.

I paragrafen räknas de huvudsakliga tillsynsuppgifterna upp. Tillsynsmyndigheten avgör om och i vilken utsträckning tillsyn ska utövas och hur den ska genomföras. Myndigheten ska agera helt oberoende vid denna bedömning. Det innebär att ingen kan kräva att myndigheten ska utöva tillsyn, förutom när det gäller kontroll enligt 3 §. Det finns inte heller några formella krav på hur tillsynen ska utövas, med undantag från vissa bestämmelser i denna lag och i föreskrifter som beslutas i anslutning till den. Om tillsynsmyndigheten beslutar att inleda ett tillsynsärende tillämpas förvaltningslagen (2017:900) på handläggningen om det inte finns avvikande bestämmelser (se avsnitt 11.8.1).

I *punkt 1* anges tillsynsmyndighetens allmänna uppgift att utöva tillsyn över behandlingen av personuppgifter. Vad det innebär utvecklas i avsnitt 11.7.1. Av *punkt 2* framgår att handläggning av klagomål från registrerade är en tillsynsuppgift. Tillsynsmyndigheten är skyldig att åtminstone hantera inkomna klagomål och ta ställning till om klagomålet bör föranleda någon tillsynsåtgärd och att underrätta klaganden om resultatet. Tillsynsmyndigheten är dock bara skyldig att utreda klagomål i den utsträckning den finner det lämpligt. *Punkt 3* hänvisar till 3 § när det gäller kontroll av om viss behandling är författningsenlig. I *punkt 4* regleras tillsynsmyndighetens skyldighet att på begäran bistå en tillsynsmyndighet i en annan medlemsstat. Det kan exempelvis vara fråga om att

inhämta handlingar från en svensk myndighet eller att undersöka hur personuppgifter som har överförts till Sverige har behandlats. Samarbetet regleras i 9, 10 och 12 §§.

I *andra stycket*, som genomför artikel 45.2, regleras ett undantag för dömande verksamhet. Undantaget behandlas i avsnitt 11.3.2. Undantaget innebär att tillsynsmyndighetens tillsyn inte ska omfatta behandling av personuppgifter inom ramen för domstolarnas dömande verksamhet. Uttrycket dömande verksamhet har samma innebörd som i artikel 45.2. Syftet med den bestämmelsen är enligt skäl 80 till direktivet att garantera domarnas oberoende när de utför sina rättsliga uppgifter. Vidare anges att undantaget bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka.

3 §

I paragrafen, som genomför artiklarna 17.1 och 46.4 och delar av artikel 46.1, regleras tillsynsmyndighetens skyldighet att kontrollera om viss personuppgiftsbehandling är författningsenlig. Paragrafen behandlas i avsnitt 11.6.1 och 11.6.3.

I *första stycket* anges förutsättningarna för kontroll. Om en fysisk person inte fått tillgång till eller information om uppgifter som behandlas om honom eller henne, eller fått uppgifter korrigerade, kan den enskilde begära att tillsynsmyndigheten kontrollerar om uppgifterna behandlas författningsenligt. En förutsättning för att tillsynsmyndigheten ska vara skyldig att utföra kontrollen är att den som begär kontrollen först har begärt information eller en korrigeringsåtgärd av den personuppgiftsansvarige. Juridiska personer har inte rätt att begära kontroll.

Kontrollen ska avse om uppgifter om personen i fråga behandlas och i så fall om de behandlas i enlighet med denna lag och andra författningar som reglerar behandling av personuppgifter inom lagens tillämpningsområde. Med utgångspunkt i uppgifterna i begäran avgör tillsynsmyndigheten hur omfattande kontroll som behövs i det enskilda fallet. Den enskilde själv kan begära kontroll, men kontroll kan också begäras av en vårdnadshavare eller ett ombud, jfr kommentaren till 4 kap. 3 §.

Tillsynsmyndigheten är endast skyldig att underrätta den sökande om att kontrollen har utförts, men inte att röja vad kontrollen har resulterat i.

Enligt *andra stycket* kan tillsynsmyndigheten vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad. En begäran kan vara orimlig om den upprepas för ofta. En begäran kan även vägras om den är så opreciserad att det skulle krävas oproportionerligt stora ansträngningar av tillsynsmyndigheten för att utföra den. En begäran är uppenbart ogrundad om någon av de grundläggande förutsättningarna brister, t.ex. om den som begär kontroll inte först har vänt sig till den personuppgiftsansvarige. Tillsynsmyndigheten har bevisbördan för att begäran är orimlig eller uppenbart ogrundad. Ett beslut att vägra att utföra kontroll kan överklagas till allmän förvaltningsdomstol, se kommentaren till 7 kap. 3 §.

Paragrafen, som genomför delar av artikel 46.1, reglerar tillsynsmyndighetens skyldighet att lämna råd och stöd till personuppgiftsansvariga och till personuppgiftsbiträden. Paragrafen behandlas i avsnitt 11.6.1 och 11.6.4.

Med råd avses både muntliga och skriftliga råd. Det kan vara fråga om allmänna råd eller rådgivning i ett enskilt fall. Det kan även vara fråga om rådgivning vid förhandssamråd enligt 3 kap. 7 §. Rådgivning av sistnämnda slag är tillsynsmyndigheten skyldig att bistå med, medan myndigheten i övrigt ska ge råd och stöd bara när den anser att det är påkallat. Rådgivningen och stödet ska avse personuppgiftsansvarigas och personuppgiftsbiträdens allmänna skyldigheter.

Råd kan t.ex. lämnas genom information på tillsynsmyndighetens hemsida, genom publicering av allmänna råd eller andra riktlinjer eller någon funktion för rådgivning per telefon eller e-post. Paragrafen ger således ingen rätt för personuppgiftsansvariga eller personuppgiftsbiträden att avkräva tillsynsmyndigheten råd i en konkret fråga, om det inte är särskilt reglerat. Förhandssamråd är exempel på det sistnämnda.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

5 §

Paragrafen, som genomför artiklarna 25.3 och 47.1, reglerar tillsynsmyndighetens undersökningsbefogenheter. Den behandlas i avsnitt 11.7.3.

Enligt *punkt 1* har tillsynsmyndigheten rätt att för sin tillsyn från personuppgiftsansvariga och personuppgiftsbiträden få tillgång till alla personuppgifter som behandlas. Det innebär att tillsynsobjektet ska lämna de begärda uppgifterna även om det kräver viss efterforskning. Att tillsynsmyndigheten har rätt att få del av annan information framgår av punkterna 2 och 4 och rätten att få hjälp med de sökningar i behandlingssystem som myndigheten begär regleras i punkten 4.

Punkt 2 ger tillsynsmyndigheten rätt till upplysningar och dokumentation som rör behandling av personuppgifter och vilka åtgärder som har vidtagits för att säkerställa skyddet för personuppgifterna och registrerades personliga integritet. Dokumentationen kan avse exempelvis de register eller loggar som personuppgiftsansvariga och personuppgiftsbiträden ska föra. Det kan också vara fråga om upplysningar om och dokumentation av vilka organisatoriska och tekniska åtgärder som vidtogs i samband med att ett register inrättades eller en viss typ av behandling påbörjades. Det kan också röra sig om åtgärder för att garantera säkerheten, begränsa den interna tillgången till uppgifter eller förhindra otillåten behandling och åtgärder för intern kontroll. Informationen kan avse exempelvis ändamålen med behandlingen eller loggar och förteckningar över pågående behandlingar. Att en myndighet saknar faktisk möjlighet att påverka hur uppgifter hanteras innan de blir tillgängliga hos myndigheten hindrar inte att den är skyldig att redovisa säkerheten vid behandlingen (se HFD 2012 ref. 21).

I *punkt 3* regleras tillsynsmyndighetens rätt att få tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar

samt tillgång till utrustning och andra medel som används för behandlingen. Rätten till tillträde ger inte myndigheten rätt att bereda sig tillträde med tvång. Om den personuppgiftsansvarige eller personuppgiftsbiträdet inte samarbetar kan tillsynsmyndigheten utnyttja sina korrigerande befogenheter enligt 7 §. Tillsynsmyndigheten har också rätt att få tillgång till den utrustning som tillsynsobjektet disponerar för att, med hjälp av tillsynsobjektets personal, kunna göra nödvändiga körningar och kontroller. Punkten ger således inte tillsynsmyndigheten någon rätt att fritt använda tillsynsobjektets utrustning och datasystem.

Punkt 4 klargör att tillsynsmyndigheten har rätt att få hjälp med de sökningar och andra åtgärder som den begär och annan nödvändig hjälp för att genomföra tillsynen. Punkten ger även tillsynsmyndigheten rätt till information som inte har direkt anknytning till behandlingen av personuppgifter men som myndigheten behöver för tillsynen. Informationen kan avse t.ex. verksamhetsplaner som beskriver den verksamhet där behandlingen utförs.

Förebyggande befogenheter

6 §

Paragrafen reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. De åtgärder som regleras i paragrafen är inte av tvingande karaktär. De syftar till att förebygga att framtida behandling av personuppgifter står i strid med regelverket. Paragrafen genomför delar av artikel 47.2 och behandlas i avsnitt 11.7.4, 11.7.5 och 9.2.5.

Av *första stycket* framgår att tillsynsmyndigheten, om det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att motverka risken genom råd, rekommendationer och påpekanden. Det kan vara fråga om ett nytt register som ska inrättas, en ny typ av behandling som ska påbörjas eller en större förändring av pågående behandling. Tillsynsmyndigheten kan också identifiera risker i pågående behandling som skulle kunna innebära att regelverket inte kommer att följas. Rådgivning kan avse såväl formella som informella samråd.

Av 7 § första stycket 1 framgår att de befogenheter som räknas upp i detta stycke även i vissa fall får användas i korrigerande syfte.

Enligt *andra stycket* får tillsynsmyndigheten skriftligen varna för att viss behandling riskerar att strida mot regelverket. En varning är en mer ingripande åtgärd än åtgärderna i första stycket. Varning kan användas för att visa hur allvarligt tillsynsmyndigheten ser på den planerade behandlingen. Tillsynsmyndigheten behöver inte ha uttömt andra förebyggande åtgärder innan den utfärdar en varning. En varning ska vara skriftlig. Av den ska framgå varför tillsynsmyndigheten bedömt att behandlingen inte kommer att vara författningsenlig. Åtgärden är inte tvingande, men den som får en varning förväntas rätta sig efter den. Om tillsynsmyndigheten finner det lämpligt kan den i beslutet om varning erinra om att – om tillsynsobjektet skulle sätta sina planer i verket – det skulle kunna leda till ett beslut om sanktionsavgift om förutsättningarna för det är uppfyllda.

Varning får också utfärdas om pågående behandling riskerar att stå i strid med lag eller annan författning. Det kan t.ex. aktualiseras om det vid förhandssamråd enligt 3 kap. 7 § andra stycket visar sig att det finns risk för att de förändringar som planeras kan göra att den framtida behandlingen inte blir författningsenlig.

Korrigerande befogenheter

7 §

I paragrafen regleras tillsynsmyndighetens korrigerande befogenheter. Paragrafen, som genomför delar av artikel 47.2, behandlas i avsnitt 11.7.4 och 11.7.6.

Tillsynsmyndigheten har möjlighet att successivt använda olika medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig. Förutom de medel som anges i första stycket 1 är befogenheterna tvingande. De sträcker sig från förelägganden till möjligheten att besluta om sanktionsavgift. Befogenheterna anges i stegrande ordning men är inte kopplade till varandra på det sättet att en strängare åtgärd förutsätter att mindre ingripande åtgärder redan har prövats.

De korrigerande befogenheterna får användas när tillsynsmyndigheten konstaterar att den personuppgiftsansvarige behandlar personuppgifter i strid med lag eller annan författning eller på något annat sätt inte fullgör sina skyldigheter. De skyldigheter som avses är framför allt skyldigheterna i 3 kap. Den personuppgiftsansvarige har emellertid också skyldigheter enligt 4 och 8 kap. och skyldighet att bistå tillsynsmyndigheten enligt 5 §. Även underlåtenhet att fullgöra sådana skyldigheter och skyldigheter som regleras i myndigheternas registerförfattningar eller i föreskrifter med anledning av denna lag omfattas.

Enligt *första stycket punkt 1* får tillsynsmyndigheten använda de förebyggande befogenheter som regleras i 6 § första stycket för att försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter. Vilka befogenheter tillsynsmyndigheten kan använda utvecklas i kommentaren till 6 §. Vad som avses med författningsenlig utvecklas i kommentaren till 2 kap. 6 §.

Enligt *punkt 2* får tillsynsmyndigheten förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att viss behandling av personuppgifter ska bli författningsenlig eller för att de ska uppfylla andra skyldigheter. Sådana förelägganden är bindande för mottagaren.

Tillsynsmyndigheten kan t.ex. förelägga den personuppgiftsansvarige att förändra viss personuppgiftsbehandling eller att uppfylla krav på loggning, dokumentations- eller underrättelseskyldighet. Ett föreläggande kan också avse att den personuppgiftsansvarige ska rätta, komplettera eller radera en personuppgift. Tillsynsmyndigheten kan även förelägga den behöriga myndigheten att vidta ytterligare tekniska eller organisatoriska åtgärder för säkerheten vid behandling eller att inrätta en intern ordning för anmälan av överträdelser av bestämmelserna, upprätta konsekvensbedömning eller fullgöra samrådsskyldighet.

Punkt 3 ger tillsynsmyndigheten rätt att förbjuda fortsatt behandling, om den personuppgiftsansvarige eller biträdet allvarligt brister i sina

skyldigheter. Med förbud mot fortsatt behandling avses att uppgifter inte längre får behandlas för de ändamål som den personuppgiftsansvarige har bestämt, utan endast får behandlas i syfte att uppfylla 2 kap. tryckfrihetsförordningen. För förbud bör krävas, förutom att det är fråga om allvarliga brister, att bristerna i fråga inte kan avhjälpas genom andra mindre ingripande åtgärder. En sådan allvarlig brist kan vara att personuppgifter behandlas för ändamål som inte är tillåtna. Att tillsynsmyndigheten inte på begäran får det underlag eller den hjälp som den har rätt till enligt 5 § kan i vissa fall vara en allvarlig brist, t.ex. att myndigheten vägras tillträde. Det kan också vara en allvarlig brist om den personuppgiftsansvarige eller personuppgiftsbiträdet inte rättar sig efter ett föreläggande eller negligerar en skriftlig varning.

Ett förbud enligt punkt 3 kan vara permanent. Tillsynsmyndigheten kan också meddela tillfälligt förbud om den anser att det finns förutsättningar för att bristen, trots att den är allvarlig, ska kunna åtgärdas.

Det ankommer på den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta de tekniska åtgärder som krävs för att personuppgifterna inte längre ska kunna behandlas om fortsatt behandling förbjuds.

Av *punkt 4* framgår att tillsynsmyndigheten får besluta om en sanktionsavgift. De närmare reglerna om det finns i 6 kap.

Beslut enligt första stycket punkterna 2–4 ska vara skriftliga och motiveras. Tillsynsmyndighetens beslut gäller först efter att de har fått laga kraft enligt 8 §. Besluten kan överklagas enligt 7 kap. 3 §.

I *andra stycket* föreskrivs att det av ett föreläggande alltid ska framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas. Om föreläggandet avser rättelse, komplettering, radering eller begränsning av behandlingen bör det framgå av föreläggandet vad som ska göras. Tillsynsmyndigheten får emellertid överlåta åt den granskade myndigheten att avgöra vilka åtgärder som ska vidtas för att behandlingen ska bli författningsenlig eller hur andra skyldigheter ska fullgöras. Det kan vara lämpligt när det är fråga om tekniska eller organisatoriska åtgärder som ska vidtas eller när det annars finns olika alternativ för vilka åtgärder som kan vidtas och hur de bör genomföras.

Verkställighet av beslut

8 §

Paragrafen, som behandlas i avsnitt 11.8.3, reglerar när tillsynsmyndighetens beslut kan verkställas.

Paragrafen innebär ett undantag från förvaltningslagens bestämmelser om verkställighet. Tillsynsmyndighetens beslut ska endast kunna verkställas efter att det har fått laga kraft. Bestämmelsen innebär att förvaltningslagens möjligheter att i vissa fall göra undantag från huvudregeln om att laga kraft är en förutsättning för verkställighet, inte gäller för tillsynsmyndighetens beslut.

9 §

Paragrafen, som genomför artikel 50.4, anger i vilka fall en begäran från en tillsynsmyndighet i en annan medlemsstat om bistånd får vägras. Paragrafen behandlas i avsnitt 11.10.1.

Tillsynsmyndigheten får vägra att lämna en utländsk tillsynsmyndighet det bistånd den begär bara om det skulle strida mot en lag eller en förordning att tillmötesgå den. Det kan vara fallet t.ex. om den svenska lagstiftningen inte medger att tillsynsmyndigheten agerar på det sätt som begärs. Tillsynsmyndigheten får exempelvis inte med tvång eller i hemlighet bereda sig tillträde till de lokaler som en personuppgiftsansvarig disponerar. Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU-rättsakter här i landet med den verkan som följer av EU-fördragen. EU-förordningar är att jämställa med svensk lag.

10 §

I paragrafen, som genomför artikel 50.2, regleras tillsynsmyndighetens befogenheter vid internationellt samarbete. Paragrafen behandlas i avsnitt 11.10.1.

Tillsynsmyndigheten har rätt att utnyttja alla de befogenheter som den har i sin vanliga tillsyn när den bistår en utländsk tillsynsmyndighet. Vilka åtgärder som är lämpliga att vidta får avgöras i det enskilda fallet.

11 §

Paragrafen innehåller en sekretessbrytande bestämmelse som gör det möjligt för tillsynsmyndigheten att lämna information till en utländsk tillsynsmyndighet. Paragrafen behandlas i avsnitt 15.2.4.

Om det är förenligt med svenska intressen får tillsynsmyndigheten lämna ut uppgifter till en behörig tillsynsmyndighet i en annan medlemsstat även om uppgifterna omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). På samma sätt som vid utlämnande med stöd av 8 kap. 3 § 2 samma lag ska en avvägning göras mellan Sveriges intresse av internationellt samarbete på tillsynsområdet och de skäl som talar mot utlämnande. Om det bedöms vara oförenligt med svenska intressen att lämna ut uppgifterna utgör det grund för tillsynsmyndigheten att enligt 9 § vägra lämna begärt bistånd när det gäller den informationen.

12 §

Paragrafen, som genomför delar av artikel 50.3, behandlas i avsnitt 11.10.2. Paragrafen föreskriver att de uppgifter som tillsynsmyndigheten får från en tillsynsmyndighet i en annan medlemsstat inte får användas för något annat ändamål än det för vilket de begärdes. Regleringen innebär ett förbud att använda upplysningarna för något annat ändamål än det som den svenska tillsynsmyndigheten angav i sin begäran. Uppgifterna får t.ex. inte lämnas vidare till andra myndigheter för att användas i deras verksamhet.

6 kap. Administrativa sanktionsavgifter

Överträdelser som kan leda till en sanktionsavgift

1 §

Paragrafen reglerar vid vilka överträdelser en sanktionsavgift får tas ut av en personuppgiftsansvarig. Den genomför, tillsammans med 2–8 §§, artikel 57. Paragrafen behandlas i avsnitt 12.5.1–3. Möjligheten att ålägga personuppgiftsbiträden sanktionsavgift regleras i 2 §.

Flertalet av lagens bestämmelser riktar sig till personuppgiftsansvariga. Även vid ett personuppgiftsbiträdes handlande som lett till överträdelser kan sanktionsavgift tas ut av den personuppgiftsansvarige, eftersom personuppgiftsansvaret enligt 3 kap. 1 § omfattar all behandling som utförs på dennes vägnar.

Tillsynsmyndigheten avgör i det enskilda fallet om en sanktionsavgift bör tas ut, vilket framgår av formuleringen att en avgift får tas ut. I paragrafen anges uttömmande vilka överträdelser av personuppgiftsansvarigas skyldigheter som kan föranleda sanktionsavgift enligt den här lagen och i vilka fall underlåtenhet att vidta åtgärder kan göra det. Både överträdelser av bestämmelser i lagen och bestämmelser som har utfärdats i anslutning till lagen kan leda till en sanktionsavgift.

Ansvaret för överträdelser är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut. Det är tillräckligt att en överträdelse ägt rum. I 4 § anges vilka omständigheter som särskilt ska beaktas vid bedömning av om avgift ska tas ut och avgiftens storlek.

Enligt *första stycket punkt 1* kan en sanktionsavgift utgå för överträdelse av flertalet av de grundläggande bestämmelserna i 2 kap. Det innebär bl.a. att behandling av personuppgifter utan rättslig grund, för ändamål som inte är tillräckligt preciserade och behandling av fler personuppgifter än som behövs eller för längre tid än vad som är nödvändigt kan leda till sanktionsavgift. Detsamma gäller otillåten behandling av känsliga personuppgifter eller underlåtenhet att i tillräcklig utsträckning göra åtskillnad mellan olika slags uppgifter eller att säkerställa personuppgifternas kvalitet, exempelvis genom att inte komplettera ofullständiga uppgifter. Även överträdelse av bestämmelsen om behandling för nya ändamål utanför ramlagens tillämpningsområde kan föranleda sanktionsavgift.

Enligt *punkt 2* kan underlåtenhet att vidta tekniska och organisatoriska åtgärder enligt någon av bestämmelserna i 3 kap. 2–5 §§ eller säkerhetsåtgärder enligt 3 kap. 8 § också leda till en sanktionsavgift. Överträdelsen kan t.ex. bestå i att den personuppgiftsansvarige tar i bruk ett it-system som inte har det inbyggda dataskydd som krävs. Underlåtenhet att begränsa tillgången till personuppgifter internt enligt 3 kap. 6 § eller att göra konsekvensbedömning och förhandssamråda med tillsynsmyndigheten enligt 3 kap. 7 § kan föranleda en sanktionsavgift.

Vid överträdelser av reglerna om överföring till tredjeland eller internationella organisationer kan enligt *punkt 3* en sanktionsavgift också tas ut.

En sanktionsavgift kan vidare enligt *andra stycket* utgå för underlåtenhet att anmäla eller dokumentera inträffade personuppgiftsincidenter.

Vad som är en personuppgiftsincident definieras i 1 kap. 6 §. Anmälningsskyldigheten utvecklas i kommentaren till 3 kap. 9 §.

Vid underlåtenhet att bistå tillsynsmyndigheten enligt någon av punkterna i 5 kap. 5 § får en sanktionsavgift också tas ut av den personuppgiftsansvarige. Det gäller också vid underlåtenhet att följa tillsynsmyndighetens förelägganden eller beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Innan tillsynsmyndigheten beslutar om en sanktionsavgift ska den personuppgiftsansvarige ges tillfälle att yttra sig. Detta följer av förvaltningslagen (2017:900).

2 §

I paragrafen regleras vid vilka överträdelser personuppgiftsbiträden får åläggas en sanktionsavgift. Paragrafen behandlas i avsnitt 12.5.1–3. Personuppgiftsbiträde definieras i 1 kap. 6 §.

De bestämmelser som räknas upp i *första stycket* innefattar uttryckliga skyldigheter för personuppgiftsbiträden. En sanktionsavgift får tas ut om tillgången till personuppgifter inte har begränsats internt eller om personuppgiftsbiträden inte har vidtagit nödvändiga säkerhetsåtgärder. Även underlåtenhet att logga behandling av personuppgifter kan leda till en sanktionsavgift.

Vid underlåtenhet att bistå tillsynsmyndigheten enligt någon av punkterna i 5 kap. 5 § får en sanktionsavgift enligt *andra stycket* också tas ut av personuppgiftsbiträden. Detsamma gäller vid underlåtenhet att följa tillsynsmyndighetens förelägganden eller beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Bestämmelsen anger uttömmande vilka överträdelser som kan leda till en sanktionsavgift enligt den här lagen. Ansvaret är strikt.

Innan sanktionsavgift beslutas ska personuppgiftsbiträdet ges tillfälle att yttra sig. Detta följer av förvaltningslagen (2017:900).

Hur sanktionsavgiften ska bestämmas

3 §

I paragrafen fastställs maximibelopp för sanktionsavgift. Överträdelser av alla regler som kan föranleda sanktionsavgift ska, om det inte finns skäl enligt 5 § att sätta ned avgiften, leda till sanktionsavgift inom dessa ramar. Överträdelser av samma slag kan leda till olika höga sanktionsavgifter inom spannet. I paragrafen anges också hur sanktionsavgiften ska beräknas vid flera överträdelser. Hur avgiften närmare ska bestämmas regleras i 4 §. Paragrafen behandlas i avsnitt 12.6.1.

I *första stycket* anges sanktionsavgiften för mindre allvarliga överträdelser. Avgiften ska i dessa fall uppgå till högst 5 000 000 kronor. I stycket anges uttömmande vilka överträdelser som ska betraktas som mindre allvarliga.

I *andra stycket* anges maximibeloppen för sanktionsavgift för allvarligare överträdelser, vilket är alla överträdelser utom de som anges i första stycket. Avgiften är i dessa fall högst 10 000 000 kronor.

I *tredje stycket* anges hur avgiften ska bestämmas om flera regler har överträtts genom samma personuppgiftsbehandling, eller om en eller

flera regler har överträtts genom sammankopplade personuppgiftsbehandlingar. Det kan t.ex. röra sig om att ett flertal registrerades personuppgifter har behandlats på samma otillåtna sätt eller i ett otillåtet register. Det kan också vara fråga om att en personuppgift som borde ha rättats eller raderats har spritts och sedan blivit föremål för ny behandling. Tredje stycket tar alltså sikte på det fallet att samma behandling av personuppgifter inneburit att flera av de regler som räknas upp i 1 eller 2 § överträtts. Sanktionsavgiften ska då bestämmas efter de samlade överträdelsernas allvar. Maximibeloppet för den allvarligaste överträdelsen får dock inte överskridas. Sanktionsavgiften ska framstå som en rimlig reaktion på de samlade överträdelserna. Till skillnad från vad som gäller vid fastställande av skadestånd ska alltså beloppet inte beräknas för varje enskild överträdelse mot varje registrerad utan med utgångspunkt i vad som är en rimlig total reaktion på överträdelserna.

4 §

I paragrafen anges vilka omständigheter som särskilt ska beaktas vid bedömningen av om någon sanktionsavgift ska tas ut och avgiftens storlek. Samma omständigheter ska beaktas vid båda bedömningarna. Uppräkningen är inte uttömmande. Paragrafen behandlas i avsnitt 12.6.2. Jämkning av avgiften regleras i 5 §.

I *punkt 1* föreskrivs att det ska beaktas om överträdelsen var uppsåtlig eller berodde på oaktsamhet. Som framgår av kommentaren till 1 § är ansvaret strikt. Det ska emellertid inte vara obligatoriskt att ta ut sanktionsavgift när en bestämmelse i ramlagen som kan föranleda avgift har överträtts. Om det kan konstateras att en överträdelse är avsiktlig bör det dock i princip vara uteslutet att avstå från att ta ut en sanktionsavgift. Tillvägagångssättet och om det varit fråga om systematiskt handlande har också betydelse. Det finns skäl att se särskilt allvarligt på överträdelser som har tydlig karaktär av nonchalans mot regelverket eller som innebär att förfaranden som tidigare lett till påpekanden från tillsynsmyndigheten upprepas. Att en överträdelse varit avsiktlig talar också för högre avgift än i andra fall. Exempel på en avsiktlig överträdelse kan vara att en myndighet medvetet inrättar ett register som det inte är tillåtet att föra. Om en myndighet uppmärksammas på att viss personuppgiftsbehandling är otillåten men trots det fortsätter med behandlingen är det också en avsiktlig överträdelse. Däremot kan en överträdelse inte ses som avsiktlig om myndigheten, efter att den blivit medveten om att personuppgiftsbehandlingen inte är tillåten, under en kort tid fortsätter att behandla vissa personuppgifter om det inte är möjligt att omedelbart vidta åtgärder som gör behandlingen författningsenlig.

Om överträdelsen haft sin grund i oaktsamhet talar det för lägre sanktionsavgift, såvida inte oaktsamheten är grov. Ju ringare oaktsamheten är, desto starkare skäl kan det finnas att avstå från att ta ut avgift. Om den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sitt bästa för att agera korrekt men felbedömt rättsläget är utrymmet att avstå från att ta ut en sanktionsavgift också större. Det kan dock inte uteslutas att en sanktionsavgift i vissa fall bör tas ut även om omständigheterna är mildrande. Det kan vara fallet t.ex. om överträdelsen fått eller riskerat att få allvarliga konsekvenser för de registrerade.

Enligt *punkt 2* ska det beaktas vilken skada, fara eller kränkning som överträdelsen inneburit. Det är främst vad överträdelsen fått för följder för de registrerade som avses. Det behöver inte konstateras att skada uppstått utan det räcker att det funnits risk för skada. Som regel blir det fråga om att göra en helhetsbedömning av de potentiella skadeverkningarna. En faktisk skada behöver inte heller vara allvarligare än risken för skada, särskilt om risken varit mycket hög och skadan – om den hade inträffat – skulle ha fått stora konsekvenser.

Även överträdelsens karaktär, svårhetsgrad och varaktighet ska enligt *punkt 3* beaktas. Vid bedömningen av överträdelsens karaktär och svårhetsgrad bör hänsyn tas till en rad omständigheter. Vilket slag av behandling det varit fråga om och vilken typ av uppgifter som behandlats är naturligtvis viktigt (t.ex. om det varit känsliga personuppgifter eller annars integritetskänsliga uppgifter). Även hur många personuppgifter som behandlats är relevant liksom behandlingens omfattning i övrigt (t.ex. om det varit fråga om enstaka uppgifter eller ett register av stor omfattning). Vidare bör hänsyn tas till vilken regel som har överträtts och vikten av det skyddsintresse som den bär upp. Hur behandlingen utförts kan också spela roll, eftersom det t.ex. kan påverka spridningen av uppgifterna. Även hur lång tid behandlingen pågått har betydelse, t.ex. om den personuppgiftsansvarige underlåtit att i rätt tid ta bort särskilt integritetskänsliga uppgifter. Generellt sett innebär längre tids behandling oftast att risken för att uppgifter kunnat spridas ökat. För vilka syften uppgifterna har behandlats kan också ha betydelse (t.ex. om verksamhetsintressen eller andra motiv legat bakom behandlingen). Ju mer central bestämmelsen som överträtts är för registrerades integritetsskydd, ju fler personuppgifter som behandlats och ju längre de behandlats, desto mindre är utrymmet för att avstå att ta ut avgift eller att sätta sanktionsavgiften lägre. Om känsliga personuppgifter behandlats på ett otillåtet sätt finns det i allmänhet skäl att se strängare på överträdelsen. Om överträdelsen kan anses vara ringa bör det finnas utrymme för att inte ta ut avgift eller bestämma avgiften till ett förhållandevis lågt belopp.

I *punkt 4* och *5* räknas andra omständigheter upp som särskilt ska beaktas. Det kan påverka i mildrande riktning om den personuppgiftsansvarige eller personuppgiftsbiträdet har gjort sitt bästa för att förebygga eller begränsa eventuella skadliga verkningar av överträdelsen. Om den personuppgiftsansvarige däremot inte vidtagit några sådana åtgärder alls eller gjort det först efter påtryckningar talar det i motsatt riktning.

Om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare har ålagts att betala sanktionsavgift för samma typ eller liknande överträdelser bör det ses som försvårande.

Att de uppräknade omständigheterna ska beaktas särskilt utesluter inte att det kan finnas andra omständigheter som i det enskilda fallet kan tillmätas betydelse.

5 §

Paragrafen, som föreskriver att sanktionsavgiften kan sättas ned helt eller delvis, behandlas i avsnitt 12.6.2.

Det kan ibland finnas omständigheter som gör att det framstår som oskäligt eller stötande att ta ut en sanktionsavgift, trots att förutsätt-

ningarna för att ta ut avgift är uppfyllda. Paragrafen ger möjlighet att sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift.

Det kan t.ex. röra sig om fall där det har gått så lång tid sedan överträdelsen att det skulle vara oskäligt att ta ut en sanktionsavgift. Avgift kan också te sig oskälig om den samlade reaktionen med hänsyn till att den personuppgiftsansvarige eller personuppgiftsbiträdet även ålagts skadestånd skulle bli oproportionerlig i förhållande till överträdelsen.

Det är däremot inte oskäligt att ta ut en avgift när överträdelsen exempelvis har berott på att den personuppgiftsansvarige eller personuppgiftsbiträdet inte känt till reglerna eller överträdelsen berott på dålig ekonomi, tidsbrist, glömska eller dåliga rutiner.

Omständigheter utom den avgiftsskyldiges kontroll som lett till överträdelsen kan i undantagsfall göra överträdelsen ursäktlig. I fall där någon t.ex. avsiktligen och i hemlighet har manipulerat ett datasystem eller vidtagit liknande åtgärder bör den personuppgiftsansvarige kunna undgå ansvar. Det förutsätter emellertid att den personuppgiftsansvarige har vidtagit nödvändiga säkerhetsåtgärder. Den omständigheten att ett personuppgiftsbiträde har behandlat personuppgifter i strid med regelverket kan dock aldrig leda till att den personuppgiftsansvarige befrias från ansvar, utom i de fall där personuppgiftsbiträdet enligt 3 kap. 18 § andra stycket själv ska betraktas som personuppgiftsansvarig.

Beslut om sanktionsavgift

6 §

Paragrafen behandlas i avsnitt 12.7.1 och 12.7.3.

I *första stycket* föreskrivs att tillsynsmyndigheten beslutar om sanktionsavgift. Tillsynsmyndigheten definieras i 1 kap. 6 §. Av *andra stycket* framgår att sanktionsavgiften tillfaller staten.

7 §

Paragrafen behandlas i avsnitt 12.7.2 och har utformats i enlighet med *Lagrådets* förslag.

Av *första stycket* framgår att möjligheten att besluta om sanktionsavgift bortfaller om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år efter överträdelsen. Så länge otillåten eller felaktig behandling pågår är det fråga om en pågående överträdelse som kan leda till en sanktionsavgift. Den i paragrafen angivna tiden förskjuts då framåt så länge personuppgifterna behandlas. Tidpunkten för överträdelsen kan emellertid få betydelse om överträdelsen avsåg överföring till tredjeland eller om behandlingen har avbrutits. Tiden bör då räknas från när överföringen gjordes eller när behandlingen upphörde.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen (2010:1932).

Betalning av sanktionsavgift

8 §

Paragrafen reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 12.7.3.

Betalning bör normalt göras inom 30 dagar från det att beslutet fick laga kraft. Det bör dock finnas möjlighet för tillsynsmyndigheten att i det enskilda fallet bestämma en längre betalningsfrist. Det kan t.ex. bli aktuellt vid mycket höga belopp. Ett beslut om sanktionsavgift får lämnas till indrivning efter sista betalningsdagen. Vid indrivning tillämpas utsökningsbalken. Om beslutet överklagas bör domstolen inhibera verkställighetsförfarandet till dess att den rättsliga prövningen har avslutats, om betalningsfristen inte har kopplats till att beslutet fått laga kraft.

Bemyndigande

9 §

Paragrafen innehåller ett bemyndigande för regeringen att meddela ytterligare föreskrifter om sanktionsavgifter enligt denna lag. Övervägandena finns i avsnitt 12.7.3.

Föreskrifter som meddelas med stöd av bemyndigandet i denna paragraf ska avse sådana sanktionsavgifter som regleras i ramlagen. Bemyndigandet kan således inte läggas till grund för föreskrifter som utvidgar det sanktionerade området.

7 kap. Skadestånd och överklagande

Skadestånd

1 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen, som har utformats efter mönster av 48 § personuppgiftslagen och genomför artikel 56, behandlas i avsnitt 13.3.2.

Paragrafen är en sådan specialbestämmelse om skadestånd som enligt 1 kap. 1 § skadeståndslagen (1972:207) tar över reglerna i den lagen. Om en ersättningsfråga inte berörs i förevarande paragraf – t.ex. frågan om hur ersättningen för en personskada eller sakskada ska beräknas (5 kap. skadeståndslagen) eller hur ansvaret ska fördelas när flera är skadeståndsskyldiga (6 kap. 4 § skadeståndslagen) – tillämpas de allmänna reglerna i skadeståndslagen.

Rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i denna lag eller föreskrifter som meddelats i anslutning till lagen. För att den personuppgiftsansvarige ska bli ersättningsskyldig behöver den registrerade bevisa att behandling av den registrerades personuppgifter stått i strid med reglerna om personuppgiftsbehandling och att den har skadat eller kränkt honom eller henne.

Den registrerades rätt till skadestånd omfattar ersättning för skada och för kränkning av den personliga integriteten. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses

ideell skada som består i att den enskildes integritet kränkts genom behandlingen.

Det är bara sådan skada eller kränkning som behandlingen av personuppgifter har vållat som ersätts, vilket framgår av att behandlingen ska ha orsakat skada respektive kränkning. Orsakssambandet ska vara adekvat.

Ersättningen för kränkning får uppskattas efter skälighet mot bakgrund av samtliga omständigheter i det enskilda fallet. Sådana faktorer som att det funnits risk för otillbörlig spridning av känsliga eller felaktiga personuppgifter eller att den registrerade genom behandlingen av uppgifterna drabbats av beslut eller åtgärder som kunnat få negativa följder hör till det som bör beaktas. Om det t.ex. skett en namnförväxling vid misstanke om rattfylleri och det lett till en felaktig indragning av körkort kan skadestånd aktualiseras. Har den registrerade själv lämnat en oriktig eller ofullständig personuppgift, kan även detta ha betydelse vid bedömningen.

Gentemot den registrerade är den personuppgiftsansvarige ansvarig för all den behandling som utförs för den personuppgiftsansvariges räkning. Det gäller även när ett personuppgiftsbiträde eller någon annan utfört behandlingen. Anspråk på skadestånd ska således riktas mot den personuppgiftsansvarige även i de fallen. Talan om skadestånd ska, om den personuppgiftsansvarige är en myndighet, riktas mot den juridiska personen, dvs. staten, landstinget eller kommunen. Med myndighet avses detsamma som i regeringsformen, dvs. samtliga statliga och kommunala organ med undantag av riksdagen och de kommunala beslutande församlingarna.

Paragrafen innehåller ingen bestämmelse motsvarande 48 § andra stycket personuppgiftslagen, som innebär att ersättningsskyldigheten kan jämkas om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Det torde dock finnas utrymme för att sätta ned skadestånd med stöd av allmänna skadeståndsrättsliga principer beträffande jämkning.

Överklagande

Överklagande av personuppgiftsansvariga myndigheters beslut

2 §

I paragrafen anges i vilken utsträckning beslut som en myndighet har fattat i egenskap av personuppgiftsansvarig får överklagas. Med myndighet avses i denna paragraf detsamma som i regeringsformen, dvs. samtliga statliga och kommunala organ med undantag av riksdagen och de kommunala beslutande församlingarna. Paragrafen behandlas i avsnitt 13.4 och är utformad i enlighet med *Lagrådets* förslag.

Vilka typer av beslut som får överklagas räknas upp i *första stycket*. Uppräkningen är, som framgår av 4 §, uttömmande. Beslut i fråga om rättelse, komplettering eller radering av personuppgifter eller begränsning av behandlingen av personuppgifter får överklagas om den registrerade har begärt åtgärden och beslutet har gått honom eller henne emot. Rätten att överklaga kan gälla även i de fall där myndigheten vidtagit en annan åtgärd än den som den registrerade begärt.

Beslut som innebär att en personuppgiftsansvarig myndighet, helt eller delvis, inte har tillmötesgått en begäran om personrelaterad information får också överklagas. Detsamma gäller beslut att vägra att pröva ett automatiserat beslut på nytt och beslut att ta ut avgift för viss information.

Besluten ska överklagas till allmän förvaltningsdomstol. Vilken förvaltningsdomstol som är behörig framgår av 14 § lagen (1971:289) om allmänna förvaltningsdomstolar. För prövning i kammarrätten krävs det enligt *andra stycket* prövningstillstånd.

Av *tredje stycket* framgår att det inte finns någon möjlighet att överklaga beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän.

Överklagande av tillsynsmyndighetens beslut

3 §

I paragrafen, som har utformats efter mönster av 51 § personuppgiftslagen, föreskrivs att tillsynsmyndighetens beslut enligt lagen får överklagas till allmän förvaltningsdomstol. Bestämmelsen genomför artikel 53.1 och behandlas i avsnitt 13.7.1.

Utgångspunkten enligt *första stycket* är att tillsynsmyndighetens beslut enligt lagen får överklagas. Det är framför allt fråga om beslut som tillsynsmyndigheten har fattat med stöd av sina korrigerande befogenheter i 5 kap. 7 §. Det kan t.ex. vara beslut om rättelse eller radering. Det kan också vara beslut om sanktionsavgift. Även beslut enligt 5 kap. 3 § andra stycket att vägra utföra kontroll får överklagas. I stycket anges vidare att tillsynsmyndigheten är motpart i domstolen när ett beslut överklagas.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagandeförbud

4 §

Enligt paragrafen, som behandlas i avsnitt 13.4, får inga andra beslut än de som räknas upp i 2 och 3 §§ överklagas.

Uppräkningen är uttömmande. Någon rätt att med stöd av förvaltningslagen överklaga andra beslut som en myndighet eller annan har fattat med stöd av lagen finns alltså inte. Det gäller beslut av personuppgiftsansvariga och personuppgiftsbiträden.

8 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för överföring

1 §

I paragrafen, som genomför artikel 35.1 a, b och d och artikel 35.3, anges förutsättningarna för att få överföra personuppgifter till ett tredjeland eller en internationell organisation. Paragrafen behandlas i avsnitt 14.3.1–3.

Enligt *första stycket* får en behörig myndighet överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Tredjeland och internationell organisation definieras i 1 kap. 6 §.

Med behandlas förstås sådan behandling av personuppgifter som lagen reglerar. Behandling av personuppgifter definieras i 1 kap. 6 §. Överföring är en form av personuppgiftsbehandling. För att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation måste därför de allmänna förutsättningarna för att få behandla personuppgifter i 2 kap. alltid vara uppfyllda, exempelvis kraven på ändamål och personuppgifternas kvalitet.

Med överföring avses att en behörig myndighet skickar, vidarebefordrar eller förmedlar information i elektronisk form till någon som befinner sig i ett tredjeland eller till en internationell organisation. Det är också fråga om en överföring när en behörig myndighet gör information tillgänglig för ett tredjeland eller en internationell organisation genom att informationen tillförs ett gemensamt datasystem, t.ex. en databas hos Interpol. Däremot omfattar paragrafen normalt inte överföringar på papper av personuppgifter som inte har behandlats automatiserat.

Personuppgifter som har samlats in och behandlats automatiserat i Sverige och som skickas till ett personuppgiftsbiträde i tredjeland för vidarebearbetning omfattas av regleringen. Överföring av personuppgifter till ett tredjeland eller en internationell organisation för behandling där avser bl.a. den situationen att uppgifterna inte behandlas automatiserat i Sverige, utan överförs till ett tredjeland eller en internationell organisation för att automatiseras där. Som exempel kan nämnas blanketter, formulär eller undersökningar som fyllts i för hand och som skickas per post till ett personuppgiftsbiträde i ett tredjeland där personuppgifterna läggs in i en databas.

Endast behöriga myndigheter har enligt paragrafen rätt att överföra personuppgifter till ett tredjeland eller en internationell organisation. Behörig myndighet definieras i 1 kap. 6 §.

En behörig myndighet kan även vara en kontaktpunkt hos en behörig myndighet. Polismyndigheten är kontaktpunkt enligt bl.a. FN:s vapenprotokoll och FN:s konvention för bekämpande av nukleär terrorism. Genom sådana kontaktpunkter kan även andra än den egna myndighetens personuppgifter överföras. Kontaktpunkten ansvarar då i sin egenskap av behörig myndighet för att överföringen följer de regler som gäller för överföring av personuppgifter till tredjeland och internationella organisationer. En kontaktpunkt som vidarebefordrar andra myndigheters personuppgifter kan behöva samråda med den myndighet från vilken uppgifterna kommer om det är lämpligt att de överförs till ett tredjeland eller en internationell organisation och vilket skydd personuppgifterna i så fall behöver.

Bestämmelserna om överföring reglerar inte på vems initiativ personuppgifterna överförs, om det är den svenska behöriga myndighetens eller den utländska behöriga myndighetens.

Överföring till ett tredjeland eller en internationell organisation får endast göras om både de i punkterna 1 och 2 angivna villkoren och något av alternativen i punkten 3 samtidigt är uppfyllda.

Punkt 1 innebär en begränsning av de syften för vilka personuppgifter får överföras till ett tredjeland eller en internationell organisation. Överföringen av personuppgifter måste vara nödvändig för ett syfte som omfattas av lagens tillämpningsområde (jfr 1 kap. 2 §). Det är således inte tillåtet att till en behörig myndighet i ett tredjeland eller en internationell organisation överföra personuppgifter i något annat syfte, t.ex. för att uppgifterna behövs i ett migrationsärende.

Nödvändighetsrekvisitet innebär att det ska prövas om personuppgifterna behövs för att en behörig myndighet ska kunna utföra en uppgift som den har ansvar för och som omfattas av denna lags tillämpningsområde. Överföringen kan vara nödvändig för att en svensk myndighet t.ex. ska kunna utreda ett brott som har begåtts här men där viss bevisning finns i ett tredjeland. Ett exempel är att målsäganden eller ett vittne befinner sig i tredjeland och att förhör under förundersökningen behöver hållas där. Ett annat exempel är att personuppgifter rörande någon som är internationellt efterlyst sänds till Interpol.

Överföringen kan också vara nödvändig t.ex. för att en behörig myndighet i ett tredjeland ska kunna lagföra ett brott. Kravet är också uppfyllt om en internationell organisation som är en behörig myndighet behöver personuppgifter för ett syfte som omfattas av tillämpningsområdet. Ett exempel kan vara att det i en svensk förundersökning kommer fram information om en person som kan misstänkas för människohandel i ett tredjeland. Ett annat exempel kan vara en narkotikahärva där en försäljare av narkotika i Sverige berättar om en distributör i ett tredjeland. Svensk behörig myndighet kan i båda fallen överföra personuppgifter till tredjelandet om de behövs för att upptäcka eller utreda brott där. Om en myndighet i ett tredjeland begär att få personuppgifter av en svensk behörig myndighet ska den svenska myndigheten pröva om den utländska myndigheten behöver uppgifterna för ett syfte som omfattas av lagens tillämpningsområde.

Punkt 2 begränsar till vilka utländska adressater personuppgifter får överföras. Personuppgifter får som huvudregel bara överföras till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet.

Av kravet på att överföringen ska göras till en behörig myndighet följer att den myndighet eller organisation som ska ta emot personuppgifterna ska ha som uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Den som personuppgiften överförs till behöver inte ha samma uppgifter som den svenska myndigheten, men ska vara behörig genom att den har en uppgift som omfattas av lagens tillämpningsområde. Exempelvis kan Polismyndigheten lämna personuppgifter till en åklagarmyndighet i ett tredjeland. När det gäller internationella organisationer är det framför allt Interpol som är av intresse. Även vissa utredningsorgan under FN torde kunna ha uppgifter som omfattas av lagens tillämpningsområde, liksom internationella tribunaler. Om en svensk behörig myndighet behöver överföra personuppgifter till en myndighet eller en organisation som inte har en sådan uppgift, t.ex. en migrationsmyndighet i ett tredjeland, är lagen inte tillämplig.

I *punkt 3* ställs dessutom krav på viss skyddsnivå för personuppgifter som överförs till ett tredjeland eller till en internationell organisation. Personuppgifter får alltid överföras till ett tredjeland eller till en internationell organisation för vilket eller vilken kommissionen har beslutat att det finns en adekvat skyddsnivå (se 3 §). Om det inte finns ett sådant beslut får personuppgifterna ändå överföras om uppgifterna kommer att omfattas av tillräckliga skyddsåtgärder hos den som mottar dem (se 4 §). Finns det inte något beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder får personuppgifter överföras endast när ett undantag för särskilda situationer gäller (se 5 §). Överföringsgrunderna är alternativa men ska prövas i den ordning som anges i paragrafen. I första hand ska det alltså prövas om det finns beslut om adekvat skyddsnivå och i andra hand om det finns tillräckliga skyddsåtgärder. Först därefter finns det anledning att se om någon av undantagssituationerna är för handen.

Om personuppgifter ska överföras till en internationell organisation, t.ex. Interpol, är det organisationen som sådan, och inte de enskilda stater som är medlemmar i organisationen, som ska uppfylla kravet på skyddsnivå. Ska personuppgiften skickas till ett tredjeland, men överföringen görs med hjälp av Interpol, ska däremot skyddsnivån i tredjelandet bedömas.

Det finns alltid risk för att skyddet för enskildas integritet försämras när personuppgifter överförs till ett tredjeland eller en internationell organisation som inte har samma dataskyddsnivå som direktivet kräver av medlemsstaterna. Den risken ska därför enligt *andra stycket* alltid beaktas särskilt vid bedömningen av hur viktigt det är att personuppgifterna överförs till tredjelandet eller den internationella organisationen.

2 §

Paragrafen, som genomför artiklarna 35.1 c och 35.2, anger förutsättningarna för att få överföra personuppgifter som en svensk myndighet har fått från en annan medlemsstat till ett tredjeland eller till en internationell organisation. Paragrafen behandlas i avsnitt 14.3.4.

Enligt *första stycket* krävs medgivande från den medlemsstat som en svensk myndighet har fått personuppgifterna från för att uppgifterna ska få överföras till ett tredjeland eller en internationell organisation. Medlemsstat definieras i 1 kap. 6 §. Det behöver inte vara en behörig myndighet i Sverige som har tagit emot personuppgifterna. Paragrafen är även tillämplig på personuppgifter som har lämnats till en annan svensk myndighet och som sedan används i t.ex. brottsbekämpande verksamhet. Personuppgifterna kan ha lämnats till svensk myndighet t.ex. genom att de skickats elektroniskt eller gjorts tillgängliga i ett gemensamt informationssystem.

Medgivandet till överföring ska som huvudregel ges i förväg, innan personuppgifterna överförs till tredjelandet eller den internationella organisationen. Det hindrar dock inte att en myndighet som lämnar personuppgifter till en annan medlemsstat generellt medger att uppgifterna får överföras till ett tredjeland eller en internationell organisation om det skulle bli nödvändigt längre fram. Sådana generella medgivanden kan tänkas bli vanliga i informationsutbytet mellan EU:s medlemsstater. Finns det ett generellt medgivande som omfattar personuppgifterna som

ska överföras, behöver den svenska myndigheten inte göra något ytterligare för att säkerställa att den andra medlemsstaten godtar att uppgifterna överförs till ett tredjeland eller en internationell organisation.

Om det på grund av tidsbrist inte går att i förväg inhämta medgivande från den medlemsstat som lämnat personuppgifterna till Sverige, finns det enligt *andra stycket* möjlighet att ändå överföra uppgifterna till ett tredjeland eller en internationell organisation. För att det ska vara tillåtet krävs det att åtgärden är nödvändig för att avvärja en omedelbar och allvarlig fara för allmän säkerhet i Sverige eller utomlands, eller för att tillgodose andra väsentliga intressen för Sverige eller någon annan medlemsstat. Möjligheten att överföra personuppgifter utan medgivande i förväg ska betraktas som en nödlösning. I kommentaren till 5 § utvecklas vad som avses med en omedelbar och allvarlig fara för allmän säkerhet.

Beslut om adekvat skyddsnivå

3 §

Paragrafen, som genomför artikel 36.1, innehåller den första tillåtna grunden för att överföra personuppgifter till ett tredjeland eller till en internationell organisation. Det är först om förutsättningarna i denna paragraf inte är uppfyllda som alternativen att överföra personuppgifter med stöd av reglerna om tillräckliga skyddsåtgärder i 4 § eller särskilda situationer i 5 § ska prövas. Paragrafen behandlas i avsnitt 14.4.

Enligt paragrafen får personuppgifter alltid överföras till ett tredjeland eller en internationell organisation som enligt ett beslut av kommissionen har en adekvat skyddsnivå för personuppgifter. Om kommissionen har meddelat ett sådant beslut för ett territorium eller en sektor i ett tredjeland får personuppgifter överföras dit. Avgränsningen avgörs av innehållet i kommissionens beslut.

Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation i 1 § ska alltid vara uppfyllda för att personuppgifter ska få överföras med stöd av ett beslut om adekvat skyddsnivå. Det innebär bl.a. att personuppgifter ska överföras mellan behöriga myndigheter. Ska personuppgifter som en svensk myndighet har fått från en annan medlemsstat överföras ska även kraven i 2 § vara uppfyllda.

Om kommissionen beslutar att ett tredjeland, eller en del av det, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå får personuppgifter inte överföras dit med stöd av den nu aktuella paragrafen. Det hindrar dock inte att personuppgifter överförs till tredjelandet eller den internationella organisationen om någon av de andra tillåtna grunderna för överföring är tillämplig.

Tillräckliga skyddsåtgärder

4 §

I paragrafen, som genomför artikel 37.1, behandlas den andra tillåtna grunden för överföring av personuppgifter till ett tredjeland eller en internationell organisation. Paragrafen behandlas i avsnitt 14.5.

Om det inte finns något beslut om adekvat skyddsnivå enligt 3 § får en behörig myndighet i Sverige ändå överföra personuppgifter till en behö-

rig myndighet i ett tredjeland, eller till en internationell organisation som är en behörig myndighet, om det finns tillräckliga skyddsåtgärder för uppgifterna där. Förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation i 1 § ska alltid vara uppfyllda för att personuppgifter ska få överföras på denna grund. Det innebär bl.a. att personuppgifter ska överföras mellan behöriga myndigheter. Ska personuppgifter som en svensk myndighet har fått från en annan medlemsstat överföras ska även kraven i 2 § vara uppfyllda.

Enligt *punkt 1* kan tillräckliga skyddsåtgärder finnas om sådana har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerade. Personuppgifter kan normalt överföras till länder som är anslutna till dataskyddskonventionen eller har ingått bindande avtal om internationellt samarbete som innehåller dataskyddsregler som är tillämpliga på överföringen. Det kan också vara fråga om bilaterala avtal som Sverige ingått med ett tredjeland och som sörjer för att kravet på dataskydd uppfylls och registrerades rättigheter respekteras.

Enligt *punkt 2* får personuppgifter också överföras om den behöriga myndighet som ska ta emot uppgifterna på annat sätt än genom avtal garanterar tillräckligt skydd för dem. Den som ska överföra personuppgifterna till tredjelandet eller den internationella organisationen ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Exempel på sådant som kan vägas in vid bedömningen av om tillräckligt skydd garanteras är bl.a. bindande åtaganden att inte sprida personuppgifterna vidare eller att inte använda personuppgifterna efter viss tidpunkt.

Det är den personuppgiftsansvarige som har bevisbördan för att skyddsnivån är tillräcklig hos den som tar emot personuppgifterna i tredjelandet eller den internationella organisationen. I de fall där personuppgifter överförs till ett tredjeland via en nationell kontaktpunkt i det landet bör bedömningen av om tillräckligt skydd för uppgifterna garanteras avse situationen hos den som slutligen ska ta emot dem. Om det inte är känt till vilken behörig myndighet i tredjelandet som kontaktpunkten kommer att vidarebefordra personuppgifterna får bedömningen i stället göras utifrån vilket dataskydd kontaktpunkten erbjuder.

Överföring i särskilda situationer

5 §

Paragrafen genomför artiklarna 38.1 och 38.2. Den behandlas i avsnitt 14.6 och är utformad i enlighet med *Lagrådets* förslag.

Paragrafen reglerar möjligheten att överföra personuppgifter till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet när det varken finns beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder för uppgifterna. Kravet är då att det ska vara fråga om en särskild situation. Undantagen för särskilda situationer gäller även samlingar av överföringar. Med samling avses här flera överföringar som på något sätt är sammankopplade, antingen därför att det är flera personuppgifter som överförs inom ramen för ett ärende, eller för att det är en personuppgift som överförs till flera adressater. En överföring kan också innehålla flera personuppgifter och därmed utgöra en samling, t.ex. ett utdrag från ett register. Det viktiga när det gäller

samlingar av överföringar är att det i efterhand går att kontrollera vilka personuppgifter som har överförts.

Överföringen ska enligt *första stycket* vara nödvändig i någon av de särskilda situationer som räknas upp i punkterna 1–4. Punkterna är alternativa. I punkterna 2 och 3 föreskrivs att överföringen ska vara nödvändig i det enskilda fallet. Oavsett vilken situation som är för handen ska förutsättningarna för överföring till tredjeland och internationella organisationer i 1 § alltid vara uppfyllda. Det innebär bl.a. att överföringen ska göras mellan behöriga myndigheter och i ett syfte som omfattas av lagens tillämpningsområde. Även förutsättningarna i 2 § ska vara uppfyllda om personuppgifter som kommer från en annan medlemsstat ska överföras.

I *punkt 1* regleras två situationer som kan göra överföringen nödvändig. Det är dels för att värna vitala intressen för den registrerade eller någon annan fysisk person, dels för att värna andra berättigade intressen som den registrerade har. I det sistnämnda fallet gäller alltså inte skyddet till förmån för någon annan än den vars personuppgifter ska överföras. Den som är misstänkt för ett brott kan ha ett berättigat intresse av att viss bevisning som finns i ett tredjeland inhämtas därifrån. Ett vittne som befinner sig i ett tredjeland kan ha ett berättigat intresse av att hans eller hennes personuppgifter överförs dit för att ett förhör ska kunna komma till stånd där.

När det gäller skyddet för vitala intressen kan det gälla både för den som personuppgiften avser och för någon annan fysisk person. Det kan t.ex. handla om att överföra uppgifter om en person som misstänks planera ett sprängdåd eller ett värdetransportrån i ett tredjeland. Ett annat exempel är att någon som har rymt från ett fängelsestraff utgör ett hot mot en målsägande eller ett vittne som bor i tredjeland och polisen där behöver få kännedom om det för att kunna skydda personen. Även andra för den enskilde väsentliga intressen som inte är direkt avgörande för liv och död, t.ex. hälsa och ekonomiska intressen, kan värnas med stöd av undantaget för vitala intressen.

Punkt 2 tillgodoser behöriga myndigheters behov av att i ett enskilt fall kunna överföra personuppgifter till ett tredjeland eller en internationell organisation som inte uppfyller kraven på adekvat skyddsnivå eller garanterar tillräckligt skydd för personuppgifterna. Som exempel på när personuppgifter kan behöva överföras i ett enskilt fall för ett ändamål som omfattas av lagens tillämpningsområde kan nämnas bevisupptagning vid utländsk domstol, kvarstad på och beslag av egendom som finns i ett tredjeland och husrannsakan i en bostad eller lokal som är belägen där. Ett annat exempel kan vara att överföringen är nödvändig i ett brottmål för att kunna delge en i tredjeland bosatt målsägande kallelse till rättegång vid svensk domstol.

Åtgärden behöver inte vara nödvändig för att tillgodose svenska myndigheters behov och intressen. Det kan finnas förutsättningar för att tillämpa punkten om ett tredjeland behöver få tillgång till svenska personuppgifter, t.ex. uppgift om att en viss person är dömd för sexuellt utnyttjande av barn. Personuppgifter kan lämnas både på begäran och på den svenska myndighetens eget initiativ.

Punkt 3 innebär att personuppgifter kan överföras till ett tredjeland eller en internationell organisation om överföringen är nödvändig i ett enskilt fall för att kunna fastställa, göra gällande eller försvara ett rättsligt

anspråk. Det rättsliga anspråket ska vara hänförligt till ett ändamål som omfattas av lagens tillämpningsområde. Exempel på sådana rättsliga anspråk är bl.a. skadestånd i anledning av brott.

Ett exempel på när det kan vara nödvändigt att överföra personuppgifter enligt *punkt 4* för att avvärja en omedelbar och allvarlig fara för allmän säkerhet är om det finns information om förestående allvarliga störningar i samhällslivet som har samband med brott eller andra särskilda händelser som kan vålla omfattande ordningsstörning, t.ex. gatukravaller och plundring. Det kan vara fråga om allmän säkerhet i Sverige eller i någon annan stat. Om det är fråga om en omedelbar fara för allmän säkerhet utomlands ligger det i sakens natur att den som vill överföra personuppgifterna har fått veta något av intresse som det är viktigt att tredjelandet eller den internationella organisationen får information om direkt, t.ex. planer på terroristattentat eller flygplanskapning eller risk för kravaller i samband med en fotbollsmatch. Den överförande myndigheten kan naturligtvis bara beakta sådant som den känner till vid prövningen av om personuppgifterna får överföras. Att det sedan i efterhand visar sig att överföringen inte var nödvändig, t.ex. därför att faran aldrig realiserades, innebär inte att överföringen var otillåten.

Enligt *andra stycket* ska en intresseavvägning göras när personuppgifter ska överföras enligt punkt 2 eller 3. De intressen som ska vägas mot varandra är skyddet för den registrerades rättigheter och friheter och det allmännas intresse av att överföringen görs. Om den registrerades intresse väger tyngre än det allmännas får personuppgifterna inte överföras. Ett exempel där den registrerades intresse väger tyngre kan vara om han eller hon riskerar dödsstraff, kroppsstraff eller tortyr om hans eller hennes personuppgifter överförs till en behörig myndighet i ett tredjeland.

Vidareöverföring

6 §

Paragrafen reglerar, tillsammans med 7 §, vidareöverföring av personuppgifter till ett tredjeland eller en internationell organisation. Med vidareöverföring förstås överföring av personuppgifter mellan tredjeländer och internationella organisationer av sådana personuppgifter som överförts dit av en medlemsstat. Paragrafen, som genomför artikel 35.1, behandlas i avsnitt 14.7.

I paragrafen anges förutsättningarna för att en svensk behörig myndighet ska få tillåta en vidareöverföring av personuppgifter som myndigheten fått från en annan medlemsstat enligt 2 § första stycket, t.ex. genom att de skickas elektroniskt eller att de har gjorts tillgängliga i ett gemensamt datasystem, och som sedan har överförts till ett tredjeland eller till en internationell organisation som i sin tur vill vidareöverföra uppgifterna till ett tredjeland eller en internationell organisation.

För det första måste det vara en behörig myndighet i Sverige som ger tillåtelse till vidareöverföringen. Dessutom krävs det att den behöriga myndigheten i den medlemsstat som lämnade personuppgifterna till en svensk myndighet har medgett att uppgifterna får vidareöverföras. En annan behörig myndighet i den andra medlemsstaten kan också medge

vidareöverföring. Om medgivande saknas får den svenska behöriga myndigheten inte tillåta att personuppgifterna vidareöverförs.

Något formkrav för hur medgivandet ska lämnas finns inte. Ett medgivande skulle därför kunna lämnas muntligen. Någon form av dokumentation, t.ex. genom en tjänsteanteckning, torde dock vara nödvändig för att tillsynsmyndigheten i efterhand ska kunna kontrollera om nödvändigt medgivande fanns innan den svenska behöriga myndigheten tillät vidareöverföringen.

I 10 § regleras möjligheten för en svensk behörig myndighet att ställa upp villkor för tredjelandets eller den internationella organisationens användning av personuppgifterna.

7 §

I paragrafen, som tillsammans med 6 § genomför artikel 35.1, anges vad en svensk myndighet ska beakta när den tar ställning till en fråga från en annan medlemsstat om att ett tredjeland eller en internationell organisation ska få vidareöverföra personuppgifter som har överförts dit av den andra medlemsstaten. Paragrafen behandlas i avsnitt 14.7.

Paragrafen ska alltså tillämpas på personuppgifter som har sitt ursprung i en svensk myndighet. Personuppgifterna har sedan överlämnats till en annan medlemsstat som i sin tur har överfört dem till ett tredjeland eller en internationell organisation som vill vidareöverföra uppgifterna. Det är alltid en svensk behörig myndighet som ska medge vidareöverföringen. Med det avses antingen den svenska behöriga myndigheten som ursprungligen lämnade personuppgifterna till den andra medlemsstaten eller en annan svensk behörig myndighet. Om exempelvis Polismyndigheten har lämnat personuppgifter till en annan medlemsstat, som överfört uppgifterna till ett tredjeland som vill vidareöverföra dem, men ärendet handläggs av svensk åklagare när förfrågan om vidareöverföring görs är det naturligt att Åklagarmyndigheten prövar frågan om vidareöverföring. Om personuppgifterna har sitt ursprung i en annan myndighet som inte är behörig i lagens mening, t.ex. Skatteverkets beskattningsverksamhet eller Tullverkets verksamhet under Effektiv handel, bör den myndigheten rådfrågas om medgivande till vidareöverföring ska lämnas. Den rådfrågade myndigheten bör då, utifrån vad som är känt för den, beakta motsvarande omständigheter som den behöriga myndigheten ska ta hänsyn till.

Vid bedömningen av om medgivande till vidareöverföring ska lämnas, ska enligt paragrafen alla omständigheter som har samband med vidareöverföringen beaktas. Av naturliga skäl kan hänsyn tas endast till sådana omständigheter som är kända när bedömningen görs. Det krävs inte att myndigheten gör omfattande efterforskningar för att få fram alla omständigheter som skulle kunna ha betydelse för om medgivande ska lämnas.

I paragrafen pekas ut några omständigheter som ska tillmätas särskild vikt när en svensk behörig myndighet ska ta ställning till en förfrågan från en annan medlemsstat om vidareöverföring kan medges. Brottets allvar ska ses i ljuset av varför vidareöverföringen är nödvändig. Är exempelvis vidareöverföringen nödvändig för att förebygga brott är det allvaret i det brottet som ska beaktas. Om personuppgifter vidareöverförs till ett tredjeland för att den allmänna ordningen och säkerheten där ska

kunna upprätthållas, är det i stället allvaret i faran som hotar ordningen eller säkerheten som ska beaktas. Även det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten ska beaktas. När det gäller skyddsnivån för personuppgifter, bör bl.a. lagstiftningen i tredjelandet beaktas. Uppräkningen av omständigheter i paragrafen är inte avsedd att vara uttömmande.

Det finns i och för sig inget som hindrar att en svensk behörig myndighet i förväg generellt medger att personuppgifter får vidareöverföras om det skulle komma att behövas. Det kan tvärtom ligga i den svenska myndighetens intresse att personuppgifterna får stor spridning om det t.ex. är fråga om en efterlyst person som eftersöks. En behörig myndighet ska dock, om den lämnar generella medgivanden till vidareöverföring, beakta att olika tredjeländer och internationella organisationer kan ha olika nivå på skyddet för personuppgifter och att olika personuppgifter kan behöva olika starkt skydd.

Överföring till andra än behöriga myndigheter

8 §

Paragrafen, som genomför artikel 39.1 a–c och e, är ett undantag från kravet i 1 § första stycket 2 att överföring av personuppgifter till tredjeland ska göras till behöriga myndigheter. Om förutsättningarna i paragrafen är uppfyllda får personuppgifter överföras även till andra än behöriga myndigheter. Det kan t.ex. vara företag och privatpersoner i ett tredjeland. Överföring till andra än behöriga myndigheter får dock göras endast om samtliga i första stycket punkterna 1–3 angivna förutsättningar är uppfyllda. Dessutom ska de övriga förutsättningarna i 1 och 2 §§ vara uppfyllda. Paragrafen behandlas i avsnitt 14.8 och är utformad i enlighet med *Lagrådets* förslag.

Enligt *första stycket punkt 1* ska överföringen vara absolut nödvändig för att den svenska myndigheten ska kunna utföra en uppgift som anges i 1 kap. 2 §. Kravet på absolut nödvändighet innebär att överföringen inte kan underlåtas. Det kan vara fallet bl.a. vid brådskande delgivning av en fysisk person i ett tredjeland genom ett delgivningsföretag som är etablerat där. Ett annat exempel kan vara att Tullverket i sin underrättelseverksamhet kan behöva kontakta ett hotell eller ett transportföretag i ett tredjeland för att snabbt få fram information. Överföring kan också vara nödvändig för att en svensk myndighet ska kunna underrätta en målsägande enligt förundersökningskungörelsen (1947:948) när en gripen, anhållen eller häktad avviker eller ett frihetsberövande hävs, eller enligt fängelseförordningen (2010:2010) när en intagen har permission, rymmer, fritas eller friges.

Kravet i *punkt 2* innebär en skyldighet för den svenska myndighet som överför personuppgifterna till någon som inte är en behörig myndighet att underrätta den som ska ta emot uppgifterna om för vilket eller vilka specifika ändamål de får behandlas.

Enligt *punkt 3* krävs slutligen att den svenska myndigheten bedömer att det skulle vara ineffektivt eller på något annat sätt olämpligt att i stället överföra personuppgifterna till en behörig myndighet i tredjelandet. Det kan vara något i tidigare kontakter med den behöriga myndigheten i det landet eller andra indikationer som ger anledning att tro att syftet med

överföringen kan komma att förfelas eller att det på något annat sätt skulle vara olämpligt att överföra personuppgifterna via den behöriga myndigheten. Däremot är bestämmelsen inte tillämplig enbart om det skulle ta längre tid att kanalisera personuppgifterna via en behörig myndighet därför att det t.ex. krävs en formell framställning om rättslig hjälp i brottmål.

Ett exempel är de mycket vanliga överföringarna som Polismyndigheten gör till internetoperatörer för att förhindra och utreda internetrelaterad brottslighet. Det skulle vara ineffektivt om varje sådan överföring skulle behöva göras genom en behörig myndighet i mottagarlandet både med hänsyn till mängden förfrågningar och den brådska som ofta råder. Ett annat exempel är information som lämnas till en bank för att förhindra att banken utnyttjas för brottsliga penningöverföringar. I sådana fall kan kontakt behöva tas omedelbart. När det gäller underrättelser till målsägande enligt förundersökningskungörelsen skulle det kunna medföra problem för målsäganden om underrättelserna alltid kanaliseras via tredjelandets behöriga myndigheter.

Enligt *andra stycket* ska det göras en intresseavvägning mellan den registrerades intresse av skydd mot kränkning av rättigheter och friheter och det allmännas intresse av att överföringen kommer till stånd. Om den enskildes skyddsintresse väger tyngre får överföringen inte göras. Ett exempel kan vara om personen som uppgifterna avser riskerar förföljelse på grund av sin religion eller politiska åskådning om personuppgifterna överförs till någon annan än en behörig myndighet i ett tredjeland. Intresseavvägningen motsvarar den som enligt 5 § andra stycket ska göras när personuppgifter ska överföras i vissa särskilda situationer.

Begränsningen i *tredje stycket* innebär att en annan aktör som är behörig myndighet enligt definitionen i 1 kap. 6 § inte får överföra personuppgifter till andra än behöriga myndigheter.

Villkor om användningsbegränsning

9 §

I paragrafen anges vad som gäller om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och överföringen försetts med villkor för användningen av uppgifterna. Paragrafen behandlas i avsnitt 14.9.1.

Om tredjelandet eller den internationella organisationen som överfört personuppgifterna med stöd av en bindande överenskommelse har ställt upp särskilda villkor för hur en viss personuppgift får behandlas, t.ex. av vem eller på vilket sätt uppgiften får användas eller hur länge den får behandlas, ska enligt paragrafen villkoren följas av svenska myndigheter. Det gäller oavsett vad som annars är föreskrivet i lag eller annan författning. Ett begränsande villkor följer med personuppgiften om den lämnas vidare till en annan myndighet (se JO 2007/08 s. 57). Den myndighet som lämnar personuppgifter vidare anses vara skyldig att informera om begränsningen. Likartade bestämmelser om användningsbegränsning finns bl.a. i 5 kap. 1 § lagen (2000:562) om internationell rättslig hjälp i brottmål och 6 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete.

Enligt paragrafen får en svensk behörig myndighet, när den överför personuppgifter till ett tredjeland eller en internationell organisation, ställa upp villkor som begränsar tredjelandets eller den internationella organisationens möjlighet att använda uppgifterna. Paragrafen behandlas i avsnitt 14.9.2.

Förutsättningen för att få ställa upp sådana villkor är dels att de inte strider mot en bindande internationell överenskommelse, dels att det krävs med hänsyn till den enskildes rätt eller från allmän synpunkt. Det får dock bara göras i enskilda fall.

Det kan vara aktuellt att ställa upp villkor om den överförande svenska myndigheten vill försäkra sig om att tredjelandet inte vidareöverför uppgifterna till ett annat tredjeland eller en internationell organisation utan att först inhämta tillstånd från den svenska myndigheten (se kommentaren till 6 §). Ett annat exempel kan vara att en svensk myndighet har fått personuppgifter från en annan medlemsstat med villkor som begränsar användningen. Om den svenska behöriga myndigheten, med den andra medlemsstatens medgivande, då vill överföra uppgifterna till ett tredjeland eller en internationell organisation är det naturligt att den svenska myndigheten föreskriver motsvarande villkor för tredjelandet eller den internationella organisationen.

Liknande bestämmelser finns bl.a. i 5 kap. 2 § lagen (2000:562) om internationell rättslig hjälp i brottmål och 6 kap. 4 § lagen (2017:496) om internationellt polisiärt samarbete.

Övergångsbestämmelser

Övergångsbestämmelserna behandlas i avsnitt 6.1.4, 17.1 och 17.2.

Punkt 1 föreskriver när lagen ska träda i kraft och *punkt 2* att 2013 års lag då ska upphöra att gälla.

I *punkt 3*, som har utformats i enlighet med *Lagrådets* förslag, föreskrivs att bestämmelsen om loggning i 3 kap. 5 § tillämpas från och med den 6 maj 2023 på sådana automatiserade behandlingssystem som inrättats före den 6 maj 2016.

En sanktionsavgift får enligt *punkt 4* beslutas endast för överträdelser som har skett efter ikraftträdandet. Bestämmelsen tydliggör att sanktionsavgift inte får beslutas för en överträdelse som har begåtts före ikraftträdandet, även om sanktionsavgift skulle betraktas som en mildare åtgärd än ett straff.

Enligt *punkt 5* ska äldre föreskrifter fortfarande gälla för överträdelser av bestämmelser om personuppgiftsbehandling som har skett före ikraftträdandet. Den gäller endast för sådana överträdelser som varit straffbara enligt 49 § personuppgiftslagen (1998:204). Vid bedömningen av om det varit fråga om en överträdelse ska de krav som gällde för personuppgiftsbehandling vid tidpunkten för överträdelsen tillämpas.

I *punkt 6* föreskrivs att äldre föreskrifter fortfarande ska gälla för överklagande av beslut om behandling av personuppgifter inom denna lags tillämpningsområde som har meddelats före ikraftträdandet. Med äldre föreskrifter avses här personuppgiftslagen, personuppgiftsförordningen (1998:1191) eller särskilda överklagandebestämmelser i de behöriga myndigheternas registerförfattningar. Punkten tar inte bara sikte på själva

 överklagandet utan också på vilket regelverk som ska tillämpas när överklagandet prövas. Äldre föreskrifter ska tillämpas även i det fallet.

18.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

9 kap.

2 §

Paragrafen, som behandlas i avsnitt 6.1.4 och 15.2.6, innehåller en upplysning om att det finns bestämmelser som gör det möjligt att ställa upp villkor om användningsbegränsning i andra författningar.

Hänvisningen till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen tas bort.

Punkterna 10–13 är enbart omnumrerade.

Punkt 14, som är ny, innehåller en hänvisning till brottsdatalagen (2018:000).

17 kap.

Internationellt samarbete avseende behandling av personuppgifter

7 c §

Paragrafen, som är ny, reglerar sekretessen hos den myndighet som utövar tillsyn enligt brottsdatalagen (2018:000) när den samarbetar med tillsynsmyndigheter i vissa andra stater. Paragrafen har i allt väsentligt utformats enligt *Lagrådets* förslag. Vad som avses med tillsynsmyndigheten framgår av 1 kap. 6 § brottsdatalagen. Paragrafen behandlas i avsnitt 15.2.2 och 15.2.3.

I *första stycket* föreskrivs att sekretess gäller i tillsynsmyndighetens verksamhet enligt 5 kap. brottsdatalagen för uppgift som, utan samband med en svensk begäran, har lämnats av en tillsynsmyndighet i en stat inom Europeiska ekonomiska samarbetsområdet (EES) eller i Schweiz. Det kan exempelvis vara uppgifter som kan ge inblick i enskilda ärenden hos ett utländskt tillsynsobjekt eller avslöja hur arbetet bedrivs där. Sekretessen skyddar alltså utländska intressen. Att uppgiften ska ha lämnats utan samband med en svensk begäran om bistånd innebär att den kan ha lämnats i en utländsk begäran om svenskt bistånd, att den kan härröra från fortsatta kontakter efter en sådan begäran eller att den kan ha lämnats av en utländsk tillsynsmyndighet utan att denna begär något bistånd av den svenska tillsynsmyndigheten. Det kan t.ex. vara fråga om en uppgift som den utländska tillsynsmyndigheten lämnat spontant.

Sekretessen gäller om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs. Vid bedömningen bör vägas in vilken effekt offentliggörande av uppgiften skulle antas få på det framtida samarbetet och på den svenska tillsynsmyndighetens möjligheter att få bistånd i sin tillsyn från tillsynsmyndigheter i andra EES-stater eller i Schweiz.

I *andra stycket* anges att sekretessen gäller i högst 40 år för uppgift i allmän handling.

18.3 Förslaget till lag om ändring i domstolsdatalagen (2015:728)

5 §

Paragrafen reglerar förhållandet till Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur. Paragrafen behandlas i avsnitt 6.1.4.

Paragrafen ändras så att hänvisningen till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen tas bort.

18.4 Förslaget till lag om ändring i lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning

1 kap.

4 §

Paragrafen reglerar undantag från lagens 1 kap. 2 §, som utsträcker dataskyddsförordningens tillämpningsområde, när det gäller vissa personuppgiftsincidenter. Övervägandena finns i avsnitt 17.1.

Paragrafen ändras så att hänvisningen till säkerhetsskyddslagen (1996:627) ersätts av en hänvisning till säkerhetsskyddslagen (2018:000).

18.5 Förslaget till lag om ändring i brottsdatalagen (2018:000)

3 kap.

9 §

Paragrafen reglerar anmälan av personuppgiftsincidenter till tillsynsmyndigheten. Övervägandena finns i avsnitt 17.1.

Paragrafen ändras så att hänvisningen till säkerhetsskyddslagen (1996:627) ersätts av en hänvisning till säkerhetsskyddslagen (2018:000).

4.5.2016 SV Europeiska unionens officiella tidning L 119/89

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/680

av den 27 april 2016

om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16.2,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Regionkommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Skyddet för fysiska personer med avseende på behandling av personuppgifter är en grundläggande rättighet. I artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Principerna och reglerna för skyddet för fysiska personer med avseende på behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras rättigheter och grundläggande friheter, särskilt deras rätt till skydd av personuppgifter. Detta direktiv är avsett att bidra till att skapa ett område med frihet, säkerhet och rättvisa.

(3) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamlingen och delningen av personuppgifter har ökat avsevärt. Tekniken gör det möjligt att i en aldrig tidigare skådad omfattning behandla personuppgifter i verksamheter såsom förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställighet av straffrättsliga påföljder.

(4) Det fria flödet av personuppgifter mellan behöriga myndigheter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten inom unionen, samt överföringar av sådana personuppgifter till tredjeländer och internationella organisationer, bör underlättas samtidigt som en hög skyddsnivå för personuppgifter säkerställs. Denna utveckling kräver en stark och mer sammanhängande ram för skyddet av personuppgifter inom unionen, uppbackad av kraftfullt tillsynsarbete.

(5) Europaparlamentets och rådets direktiv 95/46/EG ([3]) är tillämpligt på all behandling av personuppgifter i medlemsstaterna, såväl inom den offentliga som inom den privata sektorn. Det är emellertid inte tillämpligt på behandling av personuppgifter "som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten", t.ex. verksamhet på områdena för straffrättsligt samarbete och polissamarbete.

([1]) EUT C 391, 18.12.2012, s. 127.
([2]) Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.
([3]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

(6) Rådets rambeslut 2008/977/RIF ([1]) är tillämpligt på områdena för straffrättsligt samarbete och polissamarbete. Tillämpningsområdet för det rambeslutet begränsas till behandling av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna.

(7) Att säkerställa en enhetlig och hög skyddsnivå för fysiska personers personuppgifter och underlätta utbytet av personuppgifter mellan behöriga myndigheter i medlemsstaterna är av avgörande betydelse för att säkerställa ett effektivt straffrättsligt samarbete och polissamarbete. Därför bör skyddet för fysiska personers rättigheter och friheter i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, vara likvärdigt i alla medlemsstater. Ett effektivt skydd av personuppgifter i hela unionen förutsätter att de registrerades rättigheter stärks och att skyldigheterna för dem som behandlar personuppgifter, ökar, samt likvärdiga befogenheter för att övervaka och säkerställa efterlevnaden av bestämmelserna om skydd av personuppgifter i medlemsstaterna.

(8) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter samt om det fria flödet för personuppgifter.

(9) Med stöd av denna grund fastställs i Europaparlamentets och rådets förordning (EU) 2016/679 ([2]) allmänna bestämmelser om skydd av fysiska personer i samband med behandling av personuppgifter och om det fria flödet för sådana uppgifter inom unionen.

(10) I förklaring nr 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antog Lissabonfördraget, bekräftade konferensen att det med hänsyn till dessa områdens särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget.

(11) Det är därför lämpligt att dessa områden behandlas i ett direktiv som fastställer särskilda regler om skydd för fysiska personer i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, med respekt för den särskilda karaktären hos denna verksamhet. Sådana behöriga myndigheter kan omfatta inte bara offentliga myndigheter såsom rättsliga myndigheter, polis eller andra brottsbekämpande myndigheter, utan också alla andra organ eller enheter som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning enligt detta direktiv. Förordning (EU) 2016/679 bör tillämpas när ett sådant organ eller en sådan enhet behandlar personuppgifter för andra ändamål än de som avses i detta direktiv. Förordning (EU) 2016/679 är därför tillämplig i fall då ett organ eller en enhet samlar in personuppgifter för andra ändamål och behandlar dessa personuppgifter ytterligare för att iaktta sina rättsliga skyldigheter. Exempelvis behåller finansinstitut vissa personuppgifter som de behandlar i syfte att utreda, avslöja eller lagföra brott, och tillhandahåller dessa personuppgifter för behöriga nationella myndigheter endast i särskilda fall och i enlighet med medlemsstaternas nationella rätt. Ett organ eller en enhet som behandlar personuppgifter för sådana myndigheters räkning inom detta direktivs tillämpningsområde bör vara bundet av ett avtal eller annan rättsakt och de bestämmelser som är tillämpliga på personuppgiftsbiträden enligt detta direktiv, medan tillämpningen av förordning (EU) 2016/679 förblir opåverkad när det gäller personuppgiftsbiträdets behandling av personuppgifter som inte omfattas av detta direktivs tillämpningsområde.

(12) Polisens och andra brottsbekämpande myndigheters verksamhet är främst inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, inbegripet polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande

([1]) Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

([2]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (se sidan 1 i detta nummer av EUT).

myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott. Medlemsstaterna får åt behöriga myndigheter anförtro andra uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inklusive att skydda mot och förebygga hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för förordning (EU) 2016/679.

(13) Ett brott i den mening som avses i detta direktiv bör utgöra ett självständigt begrepp i unionsrätten enligt Europeiska unionens domstols (nedan kallad *domstolen*) tolkning.

(14) Eftersom detta direktiv inte bör tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, bör verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) inte betraktas som verksamhet som omfattas av detta direktivs tillämpningsområde.

(15) För att säkerställa en enhetlig skyddsnivå för fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan behöriga myndigheter, bör detta direktiv innehålla harmoniserade bestämmelser om skydd och fri rörlighet för personuppgifter som behandlas för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Tillnärmningen av medlemsstaternas nationella rätt bör inte leda till försämringar i det personuppgiftsskydd de tillhandahåller, utan i stället ha till syfte att säkerställa en hög skyddsnivå inom unionen. Inget ska hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än dem som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

(16) Detta direktiv påverkar inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar. Enligt förordning (EU) 2016/679 får personuppgifter i allmänna handlingar som förvaras av en offentlig myndighet eller ett offentligt eller privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med unionsrätten eller medlemsstatens nationella lagstiftning som den offentliga myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter.

(17) Det skydd som ska tillhandahållas enligt detta direktiv bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter.

(18) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av detta direktiv.

(19) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([1]) är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i förordning (EU) 2016/679.

(20) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning ange vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter, särskilt när det gäller personuppgifter som ingår i ett domstolsbeslut eller i protokoll avseende straffrättsliga förfaranden.

([1]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

(21) Principerna för dataskydd bör gälla all information som rör en identifierad eller identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av någon annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer som kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskydd bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte längre är identifierbar.

(22) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning i allmänhetens intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut bör alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser om dataskydd som är tillämpliga på behandlingens ändamål.

(23) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken som ger unik information om denna enskilda persons fysiologi eller hälsa och vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information. Eftersom genetiska uppgifter är komplexa och känsliga finns det en stor risk för att den personuppgiftsansvarige missbrukar och återanvänder dem för olika ändamål. All diskriminering på grundval av genetiska särdrag bör i princip vara förbjuden.

(24) Personuppgifter om hälsa bör innefatta alla uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den enskilda personen som samlats in i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ([1]), ett nummer, en symbol eller ett kännetecken som personen tilldelats för att unikt identifiera den fysiska personen för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökningar av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prover, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling, eller den registrerades fysiologiska eller biomedicinska tillstånd oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

(25) Samtliga medlemsstater är anslutna till Internationella kriminalpolisorganisationen (Interpol). För att kunna fullgöra sitt uppdrag mottar, lagrar och cirkulerar Interpol personuppgifter i syfte att hjälpa behöriga myndigheter att förebygga, förhindra och bekämpa internationell brottslighet. Därför är det lämpligt att stärka samarbetet mellan unionen och Interpol genom att främja ett effektivt utbyte av personuppgifter med respekt för de grundläggande rättigheterna och friheterna vid automatiserad behandling av personuppgifter. När personuppgifter överförs från unionen till Interpol samt till länder som har delegerade medlemmar i Interpol bör detta direktiv, framför allt bestämmelserna om internationella överföringar, gälla. Detta direktiv bör inte påverka de särskilda bestämmelserna i rådets gemensamma ståndpunkt 2005/69/RIF ([2]) och rådets beslut 2007/533/RIF ([3]).

(26) Varje behandling av personuppgifter måste vara laglig, korrekt och öppen i förhållande till berörda fysiska personer och endast genomföras för särskilda lagstadgade ändamål. Detta hindrar i sig inte brottsbekämpande myndigheter från att genomföra verksamhet såsom hemliga utredningar eller videoövervakning. Sådan verksamhet kan genomföras i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa

([1]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([2]) Rådets gemensamma ståndpunkt 2005/69/RIF av den 24 januari 2005 om utbyte av vissa uppgifter med Interpol (EUT L 27, 29.1.2005, s. 61).
([3]) Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, förutsatt att verksamheten har fastställts i lag och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den fysiska personens berättigade intressen. Dataskyddsprincipen om korrekt behandling är ett begrepp som är skilt från rätten till en opartisk domstol enligt artikel 47 i stadgan och rätten till en rättvis rättegång enligt artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata och relevanta för de ändamål som de behandlas för. Det bör i synnerhet säkerställas att de uppgifter som insamlats inte är orimligt omfattande och att de inte sparas längre än vad som är nödvändigt för det ändamål för vilket uppgifterna behandlas. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att uppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Medlemsstaterna bör inrätta lämpliga skyddsåtgärder för personuppgifter som lagras under längre perioder, för arkivändamål av allmänt intresse, för vetenskapliga, statistiska eller historiska ändamål.

(27) Om behöriga myndigheter ska kunna förebygga, förhindra, utreda och lagföra brott är det nödvändigt att de behandlar personuppgifter som insamlats inom ramen för förebyggande, förhindrande, utredning och lagföring av specifika brott i ett bredare sammanhang för att utveckla förståelsen för kriminell verksamhet och göra kopplingar mellan olika upptäckta brott.

(28) För att bibehålla behandlingens säkerhet och förhindra behandling som innebär en överträdelse av detta direktiv bör personuppgifter behandlas på ett sätt som säkerställer en lämplig säkerhets- och konfidentialitetsnivå samt förhindrar obehörigt tillträde till eller obehörig användning av personuppgifter och den utrustning som används för behandlingen, med beaktande av tillgänglig teknik och den tekniska utvecklingen samt genomförandekostnader i förhållande till riskerna och den typ av personuppgifter som ska skyddas.

(29) Personuppgifter bör samlas in för särskilda, uttryckligt angivna och berättigade ändamål som omfattas av detta direktivs tillämpningsområde och bör inte behandlas för andra ändamål än att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av detta direktiv men som inte är det ändamål som uppgifterna insamlades för, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet.

(30) Principen om uppgifters korrekthet bör tillämpas med hänsyn till den typ av behandling det är fråga om och syftet med denna. Särskilt i domstolsförfaranden baseras utsagor som innehåller personuppgifter på fysiska personers subjektiva uppfattning, och kan inte alltid verifieras. Följaktligen bör inte korrekthetskravet röra korrektheten i en utsaga, utan endast det faktum att en viss utsaga har gjorts.

(31) Behandling av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete innebär av naturliga skäl att personuppgifter om olika kategorier av registrerade behandlas. Därför är det viktigt att i tillämpliga fall och i möjligaste mån göra en klar åtskillnad mellan personuppgifter om olika kategorier av registrerade, t.ex. brottsmisstänkta, brottsdömda och brottsoffer samt andra som berörs av ett brottmål, t.ex. vittnen, personer med relevant information eller personer med kontakter eller band till brottsmisstänkta och brottsdömda. Detta bör inte hindra tillämpningen av rätten till oskuldspresumtion som garanteras i stadgan och i Europakonventionen, tolkade enligt rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna.

(32) De behöriga myndigheterna bör säkerställa att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. För att säkerställa skydd för fysiska personer, korrekthet, fullständighet eller i vilken grad personuppgifterna är aktuella och tillförlitlighet i de personuppgifter som överförs eller görs tillgängliga, bör de behöriga myndigheterna i möjligaste mån föra in nödvändiga uppgifter vid all överföring av personuppgifter.

(33) När det i detta direktiv hänvisas till medlemsstaternas nationella rätt, en rättslig grund eller lagstiftningsåtgärd innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den

berörda medlemsstatens konstitutionella ordning. Medlemsstaternas nationella rätt, den rättsliga grunden eller lagstiftningsåtgärden bör emellertid i dessa fall vara tydlig och precis, och dess tillämpning förutsägbar för dem som omfattas av den i enlighet med rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna. Medlemsstaternas nationella rätt som reglerar behandlingen av personuppgifter inom tillämpningsområdet för detta direktiv bör åtminstone specificera målen, vilka personuppgifter som ska behandlas, behandlingens ändamål, förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för förstöring av dem så att tillräckliga garantier mot risken för missbruk och godtycklighet ges.

(34) Behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, bör omfatta varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter som utförs i dessa syften, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, justering eller sammanförande, begränsning av behandlingen, radering eller förstöring. Framför allt bör bestämmelserna i detta direktiv gälla personuppgifter som vid tillämpningen av detta direktiv överförs till en mottagare som inte omfattas av detta direktiv. Med sådana mottagare bör avses fysiska eller juridiska personer, myndigheter, institutioner eller andra organ som den behöriga myndigheten lagligen lämnar ut personuppgifterna till. Om personuppgifter ursprungligen samlats in av en behörig myndighet för något av detta direktivs ändamål, bör förordning (EU) 2016/679 vara tillämplig på behandlingen av dessa uppgifter för andra ändamål än de som anges i detta direktiv om behandlingen är godkänd enligt unionsrätten eller nationell rätt. Framför allt bör bestämmelserna i förordning (EU) 2016/679 gälla överföring av personuppgifter för ändamål som inte omfattas av detta direktiv. Förordning (EU) 2016/679 bör gälla när personuppgifter behandlas av en mottagare som varken är eller agerar i egenskap av behörig myndighet i den mening som avses i detta direktiv och som lagligen mottagit personuppgifter av en behörig myndighet. Vid tillämpningen av detta direktiv bör medlemsstaterna också närmare kunna ange tillämpningen av bestämmelserna i förordning (EU) 2016/679 på de villkor som anges i den förordningen.

(35) För att vara laglig bör behandlingen av personuppgifter enligt detta direktiv vara nödvändig för att utföra en uppgift av allmänt intresse som en behörig myndighet ansvarar för enligt unionsrätten eller medlemsstaternas nationella rätt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Denna verksamhet bör omfatta skydd av intressen som är av grundläggande betydelse för den registrerade. Utförandet av uppgifterna att förebygga, förhindra, utreda, avslöja eller lagföra brott, som de behöriga myndigheterna institutionellt har tilldelats enligt lag, gör det möjligt för dem att kräva eller beordra att fysiska personer efterlever de begäranden som gjorts. I detta fall bör den registrerades samtycke, enligt definitionen i förordning (EU) 2016/679, inte utgöra en rättslig grund för behöriga myndigheters behandling av personuppgifter. Om den registrerade är skyldig att fullgöra en rättslig förpliktelse har den registrerade inte någon genuin och fri valmöjlighet, och således är det inte möjligt att betrakta den registrerades reaktion som en frivillig viljeyttring. Detta bör inte hindra medlemsstaterna från att i lag fastställa att den registrerade får tillåta behandling av sina personuppgifter vid tillämpning av detta direktiv, såsom DNA-testning inom ramen för brottsutredningar eller övervakning av var den registrerade befinner sig med elektronisk fotboja för verkställighet av straffrättsliga påföljder.

(36) Medlemsstaterna bör föreskriva att om det i den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställs särskilda villkor som under särskilda omständigheter är tillämpliga på behandlingen av personuppgifter, såsom användning av hanteringskoder, bör den överförande behöriga myndigheten informera den mottagare till vilken uppgifterna överförs om dessa villkor och om kravet att respektera dem. Sådana villkor kan till exempel innefatta ett förbud mot att överföra personuppgifter till andra mottagare eller använda dem i andra syften än de för vilka de överfördes till mottagaren eller att informera den registrerade vid en begränsning av rätten till information utan förhandsgodkännande från den överförande behöriga myndigheten. Dessa skyldigheter bör även gälla för överföringar från den överförande behöriga myndigheten till mottagare i tredjeländer eller internationella organisationer. Medlemsstaterna bör säkerställa att den överförande behöriga myndigheten inte tillämpar dessa villkor på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för sådana villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den medlemsstat där den behöriga myndigheten är belägen.

(37) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta ett särskilt skydd eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i detta direktiv inte innebär att unionen

godtar teorier som söker fastställa förekomsten av skilda människoraser. Dessa personuppgifter bör inte behandlas såvida inte behandlingen omfattas av lämpliga skyddsåtgärder för den registrerades lagstadgade rättigheter och friheter och medges i fall som är tillåtna enligt lag, eller behandlingen, om den ännu inte är tillåten enligt lag, är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Lämpliga skyddsåtgärder för den registrerades rättigheter och friheter kan till exempel inbegripa möjligheten att samla in dessa uppgifter endast i samband med andra uppgifter om den berörda fysiska personen, möjligheten att säkra de insamlande uppgifterna, striktare regler om tillgång till uppgifterna för den behöriga myndighetens personal på lämpligt sätt, och förbud mot att översända sådana uppgifter. Behandling av sådana uppgifter bör även tillåtas enligt lag när den registrerade uttryckligen har gett sitt samtycke i fall där uppgiftsbehandlingen är särskilt inkräktande för honom eller henne. Den registrerades samtycke bör dock inte i sig utgöra någon rättslig grund för behöriga myndigheters behandling av sådana känsliga personuppgifter.

(38) Den registrerade bör ha rätt att inte bli föremål för ett beslut angående bedömning av personliga aspekter rörande honom eller henne som uteslutande grundas på automatiserad behandling och som har negativa rättsliga följder eller i betydande grad påverkar honom eller henne. Denna form av uppgiftsbehandling bör under alla omständigheter omfattas av lämpliga skyddsåtgärder, inbegripet skild information till den registrerade och rätt till personlig kontakt, särskilt för framförande av egna synpunkter, rätten att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätten att överklaga beslutet. Profilering som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden på de villkor som fastställs i artiklarna 21 och 52 i stadgan.

(39) För att den registrerade ska kunna utöva sina rättigheter bör all information till denne vara lättåtkomlig, t.ex. via den personuppgiftsansvariges webbplats, och lättbegriplig, på ett klart och tydligt språk. Denna information bör anpassas till de behov som sårbara människor, t.ex. barn, har.

(40) Det bör finnas arrangemang som underlättar för registrerade att utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv, bl.a. rutiner för att kostnadsfritt begära och i tillämpliga fall få, särskilt, kostnadsfri tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen. Personuppgiftsansvariga bör vara skyldiga att besvara en begäran från den registrerade utan onödigt dröjsmål, om inte de personuppgiftsansvariga tillämpar begränsningar av den registrerades rättigheter i enlighet med detta direktiv. Om en begäran är uppenbart ogrundad eller orimlig, som i fall då en registrerad utan skäl och vid upprepade tillfällen begär uppgifter eller om denne missbrukar sin rätt till information genom att exempelvis i sin begäran tillhandahålla felaktig eller missvisande information, bör den personuppgiftsansvarige dessutom kunna ta ut en rimlig avgift eller vägra att tillmötesgå begäran.

(41) När den personuppgiftsansvarige begär att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas bör denna information endast behandlas för detta specifika ändamål och bör inte lagras längre än vad som krävs för detta ändamål.

(42) Åtminstone följande information bör göras tillgänglig för den registrerade: Vem som är personuppgiftsansvarig, att behandling sker, syftena med behandlingen, rätten att lämna in klagomål och rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandlingen. Informationen kan anges på den behöriga myndighetens webbplats. Dessutom bör den registrerade, i specifika fall och för att göra det möjligt för honom eller henne att utöva sina rättigheter, informeras om behandlingens rättsliga grund och om hur länge uppgifterna kommer att lagras, i den utsträckning som den ytterligare informationen är nödvändig, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, för att garantera en korrekt behandling när det gäller den registrerade.

(43) Fysiska personer bör ha rätt att få tillgång till uppgifter som insamlats som rör dem samt att på enkelt sätt och med rimliga intervall kunna utöva denna rätt för att hålla sig underrättade om att behandling sker och kunna kontrollera att den är laglig. Därför bör varje registrerad ha rätt att känna till och underrättas om de ändamål för vilka uppgifterna behandlas, hur länge behandlingen kommer att pågå och vilka som kommer att få del av uppgifterna, inbegripet mottagare i tredjeländer. Om denna underrättelse omfattar information om personuppgifternas ursprung bör denna information inte avslöja fysiska personers identitet, framför allt konfidentiella källor. För att denna rättighet ska respekteras är det tillräckligt att den registrerade innehar en komplett sammanfattning av dessa uppgifter i begripligt format, det vill säga ett format som gör det möjligt för den registrerade att få kännedom om dessa uppgifter och kontrollera att de är korrekta och behandlade i enlighet med detta direktiv så

att den sökande kan utöva de rättigheter som han eller hon tilldelas enligt detta direktiv. En sådan sammanfattning skulle kunna tillhandahållas i form av en kopia av de personuppgifter som håller på att behandlas.

(44) Medlemsstaterna bör ha möjlighet att genom lagstiftning vidta åtgärder som innebär att informationen till de registrerade senareläggs, begränsas eller utelämnas eller att deras tillgång till sina personuppgifter helt eller delvis begränsas, i den utsträckning och så länge som en sådan åtgärd utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, och syftet är att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, skydd för allmän eller nationell säkerhet eller skydd för andra personers rättigheter och friheter. Den personuppgiftsansvarige bör genom en konkret och individuell granskning i varje enskilt fall bedöma om rätten till tillgång delvis eller helt bör begränsas.

(45) En vägran eller begränsning av tillgång bör i princip meddelas den registrerade skriftligen och inkludera de faktiska eller rättsliga skäl som beslutet grundar sig på.

(46) All begränsning av den registrerades rättigheter måste vara förenlig med stadgan och med Europakonventionen, tolkade enligt rättspraxis från domstolen respektive Europeiska domstolen för de mänskliga rättigheterna, och i synnerhet respektera kärnan i dessa rättigheter och friheter.

(47) Fysiska personer bör ha rätt att få felaktiga personuppgifter som rör dem rättade, särskilt faktauppgifter, samt rätt att få dem raderade om behandlingen av uppgifterna utgör en överträdelse av detta direktiv. Rätten till rättelse bör emellertid inte påverka exempelvis innehållet i ett vittnesmål. En fysisk person bör också ha rätt till begränsning av behandlingen när han eller hon bestrider korrektheten av en personuppgift och det inte kan fastställas huruvida denna är korrekt eller när personuppgiften måste sparas som bevisning. Framför allt bör behandlingen av personuppgifter begränsas snarare än att uppgifterna raderas om det i ett visst fall finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades legitima intressen. I ett sådant fall bör begränsade uppgifter endast behandlas för det ändamål som hindrade att de raderades. Behandling av personuppgifter kan exempelvis begränsas genom att man flyttar de valda uppgifterna till ett annat databehandlingssystem, till exempel för arkivering, eller gör de valda uppgifterna otillgängliga. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel. Att behandlingen av personuppgifter är begränsad bör anges inom systemet på sådant sätt att det tydligt framgår att behandlingen av personuppgifterna är begränsad. Sådan rättelse, radering av personuppgifter eller begränsning av behandlingen bör meddelas till de mottagare till vilka uppgifterna har lämnats ut och till de behöriga myndigheter från vilka de oriktiga uppgifterna härrörde. De personuppgiftsansvariga bör också avstå från vidare spridning av sådana uppgifter.

(48) Om en personuppgiftsansvarig nekar en registrerad dennes rätt till information, tillgång till, rättelse, eller radering av personuppgifter eller till begränsning av behandlingen bör den registrerade ha rätt att begära att den nationella tillsynsmyndigheten kontrollerar behandlingens laglighet. De registrerade bör informeras om denna rättighet. När en tillsynsmyndighet agerar för de registrerades räkning, bör tillsynsmyndigheten åtminstone informera dem om att tillsynsmyndigheten har utfört alla nödvändiga kontroller eller översyner. Tillsynsmyndigheten bör också informera de registrerade om rätten att begära rättslig prövning.

(49) När personuppgifter behandlas inom ramen för en brottsutredning eller domstolsförfaranden vid brottmål, bör medlemsstaterna kunna föreskriva att rätten till information, tillgång, rättelse och radering samt till begränsning av behandlingen utövas i enlighet med nationella bestämmelser om rättsliga förfaranden.

(50) Den personuppgiftsansvarige bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och bör kunna visa att behandlingen är förenlig med detta direktiv. I samband med dessa åtgärder bör behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter beaktas. De åtgärder som den personuppgiftsansvarige vidtar bör omfatta utarbetande och genomförande av särskilda skyddsåtgärder för behandling av personuppgifter om sårbara fysiska personer, t.ex. barn.

(51) Risker för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av uppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller uppgifter som omfattas av tystnadsplikt, obehörigt hävande av

pseudonymisering, eller annan betydande ekonomisk eller social nackdel; eller om registrerade kan komma att berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter; om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter eller biometriska uppgifter behandlas för att unikt identifiera en person eller om uppgifter om hälsa eller uppgifter om sexualliv och sexuell läggning eller fällande domar i brottmål samt brott eller därmed sammanhängande säkerhetsåtgärder behandlas; om det förekommer en bedömning av personliga aspekter, exempelvis analyser och förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler; eller om personuppgifter rörande sårbara fysiska personer, framför allt barn, behandlas; eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(52) Riskens sannolikhetsgrad och allvar bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas enligt en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen medför hög risk. Med hög risk avses en särskild risk för menlig inverkan på registrerades rättigheter och friheter.

(53) Skyddet för fysiska personers rättigheter och friheter i samband med behandlingen av personuppgifter kräver lämpliga tekniska och organisatoriska åtgärder för att säkerställa att kraven i detta direktiv uppfylls. Genomförandet av sådana åtgärder bör inte enbart bero på ekonomiska hänsyn. För att kunna visa överensstämmelse med detta direktiv bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, som i synnerhet följer principerna om inbyggt dataskydd och dataskydd som standard. Om den personuppgiftsansvarige har genomfört en konsekvensbedömning avseende dataskydd i enlighet med detta direktiv bör resultatet beaktas vid utarbetandet av dessa åtgärder och förfaranden. Sådana åtgärder kan bland annat bestå av pseudonymisering snarast möjligt. Pseudonymisering vid tillämpning av detta direktiv kan utgöra ett verktyg som kan underlätta det fria flödet av personuppgifter inom området med frihet, säkerhet och rättvisa.

(54) Skyddet för de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och registerförarnas ansvar, också i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt detta direktiv, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

(55) Ett personuppgiftsbiträdes behandling bör styras av en rättsakt som omfattar ett avtal som binder personuppgiftsbiträdet till den personuppgiftsansvarige och där det särskilt anges att personuppgiftsbiträdet endast bör agera på instruktion av den personuppgiftsansvarige. Personuppgiftsbiträdet bör beakta principen om inbyggt dataskydd och dataskydd som standard.

(56) För att visa överensstämmelse med detta direktiv bör de personuppgiftsansvariga eller registerförarna föra register över alla kategorier av behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt för myndigheten så att det kan tjäna som grund för övervakningen av behandlingen. Personuppgiftsansvariga eller personuppgiftsbiträden som behandlar personuppgifter i icke-automatiserade behandlingssystem bör ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen är laglig, möjliggöra egenkontroll och säkerställa dataintegritet och datasäkerhet.

(57) Loggar bör åtminstone föras över behandlingar i automatiserade behandlingssystem såsom insamling, ändring, läsning, utlämning, inklusive överföringar, sammanförande eller radering. Identifieringen av den person som läst eller lämnat ut personuppgifter bör loggas och från denna identifiering skulle det kunna vara möjligt att fastställa motiveringen till behandlingen. Loggarna bör endast användas för att kontrollera om behandlingen av uppgifterna är tillåten, för egenkontroll, för att garantera dataintegritet och datasäkerhet samt för straffrättsliga förfaranden. Egenkontroll omfattar även behöriga myndigheters interna disciplinära förfaranden.

(58) En konsekvensbedömning avseende dataskydd bör genomföras av den personuppgiftsansvarige om det är sannolikt att uppgiftsbehandlingen, på grund av sin karaktär, sin omfattning eller sina ändamål, medför en hög risk för de registrerades rättigheter och friheter, vilken i synnerhet bör omfatta planerade åtgärder, skyddsåtgärder och mekanismer för att säkerställa skyddet av personuppgifter och för att styrka efterlevnaden av detta direktiv. Konsekvensbedömningarna bör omfatta relevanta system och processer för behandling men inte enskilda fall.

(59) I syfte att säkerställa ett effektivt skydd av de registrerades rättigheter och friheter bör den personuppgiftsansvarige eller personuppgiftsbiträdet i vissa fall samråda med tillsynsmyndigheten före behandlingen.

(60) För att upprätthålla säkerheten och förhindra behandling som bryter mot detta direktiv bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera de risker som behandlingen är förknippad med och bör vidta åtgärder, såsom kryptering, för att mildra dem. Åtgärderna bör leda till en lämplig säkerhetsnivå, inklusive konfidentialitetsnivå, med beaktande av den senaste utvecklingen och till genomförandekostnaderna med hänsyn till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av riskerna när det gäller datasäkerhet bör man beakta de risker som uppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller olagliga handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, som framför allt kan leda till fysisk, materiell eller immateriell skada. Den personuppgiftsansvarige och personuppgiftsbiträdet bör säkerställa att behandlingen av personuppgifter inte utförs av obehöriga personer.

(61) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan betydande ekonomisk eller social nackdel för den berörda fysiska personen. Så snart en personuppgiftsansvarig blir medveten om en personuppgiftsincident bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om möjligt, inom 72 timmar efter att ha fått kännedom om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan visa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om anmälan inte kan göras inom 72 timmar bör skälen till fördröjningen åtföljа anmälan och informationen får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(62) Fysiska personer bör utan onödigt dröjsmål underrättas om personuppgiftsincidenten sannolikt leder till en högre risk för deras rättigheter och friheter så att de kan vidta nödvändiga försiktighetsåtgärder. Underrättelsen bör innehålla en beskrivning av personuppgiftsincidentens art samt rekommendationer till den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter. Exempelvis kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omgående medan behovet att vidta lämpliga åtgärder vid fortlöpande eller likartade uppgiftsincidenter kan motivera längre tid för underrättelsen. Om man inte kan undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder eller skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter genom att senarelägga eller begränsa informationen till den berörda fysiska personen om en personuppgiftsincident skulle denna information under exceptionella omständigheter kunna utelämnas.

(63) Den personuppgiftsansvarige bör utse en person att hjälpa denne att övervaka den interna efterlevnaden av de bestämmelser som antas i enlighet med detta direktiv, förutom om en medlemsstat beslutar att undanta domstolar och andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin dömande verksamhet. Denna person kan vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning inom dataskyddslagstiftning och praxis i fråga om dataskydd för att förvärva sakkunskap på detta område. Den nödvändiga nivån på sakkunskapen bör särskilt fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige. Hans eller hennes uppgift kan utföras på deltid eller heltid. Flera personuppgiftsansvariga kan, med beaktande av organisationsstruktur och storlek, gemensamt utse ett dataskyddsombud, t.ex. vid gemensamma resurser i centralenheter. Denna person kan också utnämnas till olika befattningar inom de berörda personuppgiftsansvarigas struktur. Denna person bör hjälpa den personuppgiftsansvarige och de anställda som behandlar personuppgifter genom att ge information och råd till dem angående efterlevnaden av deras respektive skyldigheter i fråga om dataskydd. Dataskyddsombudet i fråga bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt i enlighet med medlemsstaternas nationella rätt.

(64) Medlemsstaterna bör säkerställa att överföringar till ett tredjeland eller en internationell organisation endast får äga rum om detta är nödvändigt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller för att verkställa straffrättsliga påföljder, inklusive för att skydda mot samt förebygga och förhindra hot mot den

allmänna säkerheten, och den personuppgiftsansvarige i tredjelandet eller den internationella organisationen är en myndighet som är behörig i den mening som avses i detta direktiv. En överföring bör endast utföras av behöriga myndigheter som agerar som personuppgiftsansvariga, utom när personuppgiftsbiträden uttryckligen har getts i uppdrag att göra en överföring för personuppgiftsansvarigas räkning. En sådan överföring kan äga rum när kommissionen har beslutat att skyddsnivån i ett tredjeland eller en internationell organisation är adekvat eller när lämpliga skyddsåtgärder föreligger, eller när undantag för särskilda situationer gäller. Det är viktigt att den skyddsnivå som fysiska personer garanteras inom unionen genom detta direktiv inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeländer eller internationella organisationer, vilket inbegriper fall av vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga eller personuppgiftsbiträden i samma eller i ett annat tredjeland eller en annan internationell organisation.

(65) Om personuppgifter överförs från en medlemsstat till tredjeländer eller internationella organisationer bör en sådan överföring i princip ske först efter det att den medlemsstat från vilken uppgifterna insamlades har gett sitt tillstånd till överföringen. För ett effektivt samarbete i fråga om brottsbekämpning krävs att, om ett hot mot en medlemsstats eller ett tredjelands allmänna säkerhet eller en medlemsstats väsentliga intressen är så överhängande att det är omöjligt att i tid inhämta ett förhandstillstånd, den behöriga myndigheten bör få överföra de relevanta personuppgifterna till det berörda tredjelandet eller internationella organisationen utan sådant förhandstillstånd. Medlemsstaterna bör föreskriva att eventuella särskilda villkor som rör överföringen bör vidarebefordras till tredjeländer eller internationella organisationer. För vidare överföring av personuppgifter bör det krävas förhandstillstånd från den behöriga myndighet som utförde den ursprungliga överföringen. När den behöriga myndighet som utförde den ursprungliga överföringen fattar beslut om en begäran om tillstånd för vidare överföring bör den vederbörligen beakta alla relevanta faktorer, inklusive hur allvarligt brottet är, de särskilda villkor på vilka, och det ändamål för vilket, uppgifterna ursprungligen överfördes, arten och villkoren för verkställandet av den straffrättsliga påföljden, samt nivån på skyddet av personuppgifter i det tredjeland eller den internationella organisation som personuppgifterna vidare överförs till. Den behöriga myndighet som utförde den ursprungliga överföringen bör också ha möjlighet att tillämpa särskilda villkor för vidare överföring. Dessa särskilda villkor kan beskrivas, t.ex. i hanteringskoder.

(66) Kommissionen bör med verkan för hela unionen kunna fastställa att vissa tredjeländer, ett visst territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation kan erbjuda en adekvat dataskyddsnivå, och på så sätt skapa rättssäkerhet och enhetlighet i hela unionen vad gäller dessa tredjeländer eller internationella organisationer som anses erbjuda en sådan skyddsnivå. I dessa fall bör överföringar av personuppgifter till dessa länder kunna ske utan särskilt tillstånd, utom när en annan medlemsstat från vilken uppgifterna insamlades måste ge tillstånd till överföringen.

(67) I enlighet med de grundläggande värderingar som unionen vilar på, särskilt skyddet av de mänskliga rättigheterna, bör kommissionen i sin bedömning av ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland beakta i vilken omfattning ett visst tredjeland iakttar rättsstatsprincipen, möjligheten till rättslig prövning samt internationella människorättsliga normer och standarder samt landets allmänna lagstiftning och sektorslagstiftning, vilket inbegriper lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i det tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen, i synnerhet när uppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning samt sörja för mekanismer för samarbete med medlemsstaternas dataskyddsmyndigheter och de registrerade bör tillförsäkras effektiva och verkställbara rättigheter samt effektiva administrativa och rättsliga rättsmedel.

(68) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har ingått bör kommissionen också beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med Europeiska dataskyddsstyrelsen, inrättad genom förordning

(EU) 2016/679 (nedan kallad *styrelsen*) vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer. Kommissionen bör också beakta alla relevanta kommissionsbeslut om adekvat skyddsnivå som antagits i enlighet med artikel 45 i förordning (EU) 2016/679.

(69) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar. I sina beslut om adekvat skyddsnivå bör kommissionen föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör göras i samråd med tredjelandet eller den internationella organisationen i fråga och bör beakta all relevant utveckling i tredjelandet eller den internationella organisationen.

(70) Kommissionen bör även kunna konstatera att ett tredjeland eller ett territorium eller en specificerad sektor inom ett tredjeland, eller en internationell organisation, inte längre säkerställer en adekvat dataskyddsnivå. Följaktligen bör överföringar av personuppgifter till det tredjelandet eller den internationella organisationen förbjudas om inte kraven i detta direktiv rörande överföring som är föremål för lämpliga skyddsåtgärder och undantag i särskilda situationer är uppfyllda. Bestämmelser bör fastställas för förfaranden för samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.

(71) Överföringar som inte grundar sig på ett sådant beslut om adekvat skyddsnivå bör endast tillåtas om lämpliga skyddsåtgärder garanteras i ett rättsligt bindande instrument, som säkerställer skyddet av personuppgifterna eller om den personuppgiftsansvarige har gjort en bedömning av alla omständigheter kring en uppgiftsöverföring och på grundval av denna bedömning anser att lämpliga skyddsåtgärder föreligger vad avser skyddet av personuppgifter. Sådana rättsligt bindande instrument kan t.ex. vara rättsligt bindande bilaterala avtal som har ingåtts av medlemsstaterna och genomförts inom deras rättsordning och som kan åberopas av registrerade som omfattas av denna och som sörjer för att kraven i fråga om dataskydd uppfylls och att registrerades rättigheter respekteras, inbegripet rätten till en effektiv administrativ eller rättslig prövning. Den personuppgiftsansvarige bör vid bedömningen av alla omständigheter kring uppgiftsöverföringen kunna beakta samarbetsavtal som ingåtts mellan Europol eller Eurojust och tredjeländer, som medger utbyte av personuppgifter. Den personuppgiftsansvarige bör också kunna beakta att överföringen av personuppgifter kommer att omfattas av tystnadplikt och principen om specificitet, vilket säkerställer att personuppgifterna inte kommer att behandlas i andra syften än för överföringen. Dessutom bör den personuppgiftsansvarige beakta att personuppgifterna inte kommer att användas för att göra framställningar om, meddela eller verkställa dödsstraff eller någon form av grym och omänsklig behandling. Även om dessa villkor kan betraktas som tillräckliga skyddsåtgärder för överföringen av uppgifter bör den personuppgiftsansvarige kunna begära ytterligare skyddsåtgärder.

(72) Om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder saknas kan en överföring eller en kategori av överföringar endast äga rum i särskilda situationer om överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller för att skydda den registrerades berättigade intressen om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta, eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller i ett tredjeland, eller om det är nödvändigt i ett enskilt fall för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive för att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten, eller i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk. Dessa undantag bör tolkas restriktivt och bör inte möjliggöra upprepade, omfattande eller strukturella överföringar av personuppgifter eller storskaliga överföringar av uppgifter, utan begränsas till uppgifter som är absolut nödvändiga. Sådana överföringar bör dokumenteras och på begäran göras tillgängliga för tillsynsmyndigheten så att man kan övervaka om överföringen är laglig.

(73) Medlemsstaternas behöriga myndigheter tillämpar gällande bilaterala eller multilaterala internationella avtal som ingåtts med tredjeländer på området för straffrättsligt samarbete och polissamarbete för utbyte av relevant information för att de ska kunna fullgöra de uppgifter som de anförtrotts enligt lag. Detta sker i princip genom eller åtminstone i samarbete med tredjeländernas berörda myndigheter, i vissa fall även i avsaknad av ett bilateralt eller multilateralt internationellt avtal. I specifika enskilda fall är emellertid de ordinarie förfaranden som kräver kontakt med myndigheten i tredjelandet ineffektiva eller olämpliga, framför allt för att överföringen inte skulle kunna utföras i tid eller för att myndigheten i tredjelandet inte respekterar rättsstatsprincipen eller internationella människorättsliga normer och standarder, så att medlemsstaternas behöriga myndigheter skulle kunna besluta att överföra personuppgifterna direkt till de mottagare som är etablerade i dessa tredjeländer. Detta kan till exempel vara fallet om det finns ett akut behov av att överföra personuppgifter för att rädda livet på en person som riskerar att utsättas för ett brott eller för att förhindra en överhängande fara för brottslighet, inbegripet terrorism. Även om denna överföring mellan behöriga myndigheter och mottagare som är etablerade i tredjeländer endast

äger rum i särskilda enskilda fall bör det i detta direktiv föreskrivas villkor för att reglera sådana fall. Dessa bestämmelser bör inte betraktas som undantag från något befintligt bilateralt eller multilateralt internationellt avtal på området för straffrättsligt samarbete och polissamarbete. Dessa bestämmelser bör vara tillämpliga utöver övriga bestämmelser i detta direktiv, särskilt bestämmelserna om när personuppgifter får behandlas och bestämmelserna i kapitel V.

(74) När personuppgifter förs över gränserna kan detta öka risken för att fysiska personer inte ska kunna utöva sina dataskyddsrättigheter för att skydda sig mot olaglig användning eller olagligt utlämnande av dessa uppgifter. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller genomföra utredningar avseende verksamheter utanför sina egna gränser. Deras strävan att samarbeta i ett gränsöverskridande sammanhang kan också försvåras på grund av otillräckliga preventiva eller korrigerande befogenheter och oenhetliga rättsliga regelverk. Närmare samarbete mellan tillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information med sina utländska motparter.

(75) För att skydda fysiska personer med avseende på behandling av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar tillsynsmyndigheter som kan utföra sitt uppdrag fullständigt oberoende. Tillsynsmyndigheterna bör övervaka tillämpningen av detta direktiv och bör bidra till enhetlig tillämpning av dessa i hela unionen, för att skydda fysiska personer när deras personuppgifter behandlas. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen.

(76) Medlemsstaterna får anförtro en tillsynsmyndighet som de redan har inrättat i enlighet med förordning (EU) 2016/679 ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta direktiv.

(77) Medlemsstaterna bör kunna inrätta mer än en tillsynsmyndighet för att återspegla sin konstitutionella, organisatoriska och administrativa struktur. Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som krävs för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

(78) Tillsynsmyndigheterna bör vara föremål för oberoende kontroll- eller övervakningsmekanismer i fråga om sina utgifter, förutsatt att denna finansiella kontroll inte påverkar deras oberoende.

(79) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas i medlemsstaternas nationella rätt och bör i synnerhet föreskriva att de ska utnämnas antingen av den berörda medlemsstatens parlament eller dess regering eller dess statschef på grundval av ett förslag från regeringen eller en minister eller parlamentet eller dess kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen genom ett öppet förfarande. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, bör avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. För att säkerställa tillsynsmyndighetens oberoende bör personalurvalet göras av tillsynsmyndigheten, och kunna innefatta ett ingripande från ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts uppgiften.

(80) Detta direktiv är visserligen tillämpligt på nationella domstolars och andra rättsliga myndigheters verksamheter, men tillsynsmyndigheterna bör inte ha behörighet att övervaka behandling av personuppgifter inom ramen för domstolars dömande verksamhet. Syftet är att garantera domarnas oberoende när de utför sina rättsliga uppgifter. Detta undantag bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka. Medlemsstaterna bör också kunna föreskriva att tillsynsmyndigheten inte ska vara behörig att övervaka andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet, exempelvis allmänna åklagarmyndigheter. Under alla omständigheter är domstolarnas och andra oberoende rättsliga myndigheters efterlevnad av bestämmelserna i detta direktiv alltid föremål för en oberoende kontroll i enlighet med artikel 8.3 i stadgan.

(81) Tillsynsmyndigheterna bör hantera klagomål som anförs av registrerade och utreda ärendena i fråga eller överföra dem till den behöriga övervakande myndigheten. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta.

(82) För att man ska kunna övervaka efterlevnaden av och verkställa detta direktiv på ett effektivt, tillförlitligt och enhetligt sätt i hela unionen enligt EUF-fördraget, i enlighet med den tolkning som domstolen gjort, bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och rådgivande befogenheter, som utgör nödvändiga medel för utförandet av deras uppgifter. Emellertid bör deras befogenheter inte inkräkta på särskilda regler för straffrättsliga förfaranden, inbegripet utredning och lagföring av brott, eller domstolsväsendets oberoende. Utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt bör tillsynsmyndigheterna också ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av detta direktiv eller delta i rättsliga förfaranden. Tillsynsmyndigheternas befogenheter bör utövas i överensstämmelse med lämpliga rättssäkerhetsgarantier som fastställs i unionsrätten och i medlemsstaternas nationella rätt samt opartiskt, korrekt och inom rimlig tid. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnaden av detta direktiv, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar den berörda personen negativt vidtas, och utformas så att onödiga kostnader och alltför stora olägenheter för denne undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella rätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Antagande av ett rättsligt bindande beslut bör bli föremål för domstolsprövning i den medlemsstat där den tillsynsmyndighet som antog beslutet är belägen.

(83) Tillsynsmyndigheterna bör bistå varandra när de utför sina uppgifter och ge ömsesidigt bistånd för att säkerställa att de bestämmelser som antas i enlighet med detta direktiv efterlevs och tillämpas på ett enhetligt sätt.

(84) Styrelsen bör bidra till detta direktivs enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen och främja samarbetet mellan tillsynsmyndigheterna i hela unionen.

(85) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet och till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan, om den registrerade anser att hans eller hennes rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Den behöriga tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta. För att förenkla inlämnandet av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

(86) Varje fysisk eller juridisk person bör ha rätt till ett effektivt rättsmedel vid behörig nationell domstol mot en tillsynsmyndighets beslut som har rättsliga följder för denna person. Ett sådant beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Denna rätt inbegriper dock inte tillsynsmyndigheters övriga åtgärder som inte är rättsligt bindande, såsom yttranden som avgetts eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot en tillsynsmyndighet bör väckas vid domstol i den medlemsstat där tillsynsmyndigheten är etablerad och bör prövas i enlighet med den nationella rätten i den medlemsstaten. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att rättsligt eller faktiskt pröva alla frågor som rör de tvister som anhängiggjorts vid dem.

(87) Om en registrerad anser att hans eller hennes rättigheter enligt detta direktiv har kränkts bör han eller hon ha rätt att ge ett organ som syftar till att skydda registrerades rättigheter och intressen vad gäller skyddet av deras

personuppgifter, och som inrättats i enlighet med den nationella rätten i en medlemsstat, i uppdrag att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet och utöva rätten till rättsmedel. De registrerades rätt att bli företrädda bör inte påverka medlemsstatens nationella processrätt enligt vilken det kan vara obligatoriskt att registrerade företräds inför nationell domstol av en advokat enligt definitionen i rådets direktiv 77/249/EEG ([1]).

(88) Personer som lider skada till följd av behandling som står i strid med de bestämmelser som antas i enlighet med detta direktiv bör få ersättning av den personuppgiftsansvarige eller av någon annan myndighet som är behörig enligt medlemsstaternas nationella rätt. Begreppet *skada* bör tolkas brett mot bakgrund av domstolens rättspraxis och på ett sätt som fullt ut återspeglar detta direktivs mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Vid hänvisning till behandling som är olaglig eller står i strid med de bestämmelser som antas i enlighet med detta direktiv omfattas även behandling som inte är i överensstämmelse med de genomförandeakter som antagits i enlighet med detta direktiv. Registrerade bör få full och effektiv ersättning för den skada de lidit.

(89) Om någon fysisk eller juridisk person överträder detta direktiv bör detta leda till sanktioner, oavsett om personen i fråga omfattas av privaträtt eller offentlig rätt. Medlemsstaterna bör säkerställa att sanktioner är effektiva, proportionella och avskräckande och bör vidta alla åtgärder som krävs för att sanktionerna ska verkställas.

(90) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter vad gäller adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom ett tredjeland eller en internationell organisation och för format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([2]).

(91) Mot bakgrund av att dessa rättsakter har allmän räckvidd bör granskningsförfarandet användas vid antagandet av genomförandeakter om adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom detta tredjeland eller en internationell organisation och om format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.

(92) Kommissionen bör när tvingande skäl till skyndsamhet föreligger i vederbörligen motiverade fall anta omedelbart tillämpliga genomförandeakter avseende ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation där en adekvat skyddsnivå inte längre kan säkerställas.

(93) Eftersom målen för detta direktiv, nämligen att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och för att säkerställa ett fritt utbyte av personuppgifter mellan behöriga myndigheter inom unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(94) Särskilda bestämmelser i unionsakter på området för straffrättsligt samarbete och polissamarbete som antagits före dagen för antagandet av detta direktiv, och som reglerar behandlingen av personuppgifter mellan medlemsstaterna eller tillträdet för utsedda myndigheter i medlemsstaterna till informationssystem som inrättats i

([1]) Rådets direktiv 77/249/EEG av den 22 mars 1977 om underlättande för advokater att effektivt begagna sig av friheten att tillhandahålla tjänster (EGT L 78, 26.3.1977, s. 17).

([2]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

enlighet med fördragen, bör kvarstå oförändrade, till exempel de särskilda bestämmelser om skydd av personuppgifter som tillämpas i enlighet med rådets beslut 2008/615/RIF ([1]), eller artikel 23 i konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ([2]). Eftersom artikel 8 i stadgan och artikel 16 i EUF-fördraget kräver att den grundläggande rätten till skydd av personuppgifter bör säkerställas på ett enhetligt sätt i hela unionen bör kommissionen utvärdera situationen vad gäller förhållandet mellan detta direktiv och rättsakter, antagna före dagen för antagandet av detta direktiv, som reglerar behandling av personuppgifter mellan medlemsstaterna eller tillträde för utsedda myndigheter i medlemsstater till informationssystem som inrättats i enlighet med fördragen, i syfte att bedöma om dessa särskilda bestämmelser behöver anpassas till detta direktiv. Vid behov bör kommissionen lägga fram förslag i syfte att säkerställa enhetliga rättsregler angående behandlingen av personuppgifter.

(95) För att säkerställa ett övergripande och enhetligt skydd av personuppgifter i unionen bör internationella avtal som medlemsstaterna ingått före dagen för detta direktivs ikraftträdande, och som överensstämmer med relevant unionsrätt som var tillämplig före den dagen, fortsätta att gälla till dess att de ändras, ersätts eller upphävs.

(96) Medlemsstaterna bör medges en period på högst två år från dagen för ikraftträdandet av detta direktiv för att införliva det. Behandling som redan pågår den dagen bör bringas i överensstämmelse med detta direktiv inom en period av två år från det att detta direktiv träder i kraft. I fall där sådan behandling överensstämmer med unionsrätt som var tillämplig före dagen för ikraftträdandet av detta direktiv bör dock inte kraven i detta direktiv rörande förhandssamråd med tillsynsmyndigheten gälla för behandling som redan pågick vid den tidpunkten, eftersom dessa krav, p.g.a. sin natur, är sådana att de ska uppfyllas före själva behandlingen. Om medlemsstaterna tillämpar den längre genomförandeperioden som löper ut sju år efter detta direktivs ikraftträdande för fullgörandet av loggningsskyldigheterna för automatiserade behandlingssystem som inrättats före den dagen bör den personuppgiftsansvarige eller personuppgiftsbiträdet ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen av uppgifterna är laglig, möjliggöra egenkontroll samt säkerställa dataintegritet och datasäkerhet.

(97) Detta direktiv påverkar inte bestämmelserna om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi i Europaparlamentets och rådets direktiv 2011/93/EU ([3]).

(98) Rambeslut 2008/977/RIF bör därför upphävas.

(99) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Förenade kungariket och Irland inte bundna av de bestämmelser i detta direktiv som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget i det fall då Förenade kungariket och Irland inte är bundna av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.

(100) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i detta direktiv och omfattas inte av den tillämpning av regler som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för kapitlen 4 och 5 i avdelning V i tredje delen i EUF-fördraget. Eftersom detta direktiv bygger på av Schengenregelverket, som omfattas av avdelning V i tredje delen av EUF-fördraget, ska Danmark i enlighet med artikel 4 i protokollet inom en tid av sex månader efter antagandet av detta direktiv besluta huruvida landet ska genomföra det i sin nationella lagstiftning.

(101) När det gäller Island och Norge utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([4]).

([1]) Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 1).
([2]) Rådets akt av den 29 maj 2000 om att i enlighet med artikel 34 i Fördraget om Europeiska unionen upprätta konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 1).
([3]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).
([4]) EGT L 176, 10.7.1999, s. 36.

(102) När det gäller Schweiz utgör detta direktiv, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av bestämmelserna i Schengenregelverket ([1]).

(103) När det gäller Liechtenstein utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ([2]).

(104) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan som erkänns i EUF-fördraget, särskilt rätten till respekt för privatlivet och familjelivet, rätten till skydd av personuppgifter, rätt till ett effektivt rättsmedel och till en opartisk domstol. De inskränkningar som gjorts av dessa rättigheter överensstämmer med artikel 52.1 i stadgan eftersom de är nödvändiga för att uppnå av unionen erkända mål av allmänt intresse eller för att skydda andras rättigheter och friheter.

(105) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument, har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella införlivandeåtgärderna. Med avseende på detta direktiv anser lagstiftaren att översändandet av sådana dokument är berättigat.

(106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ([3]).

(107) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning genomföra bestämmelser om registrerades utövande av sina rättigheter vad gäller information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden samt eventuella begränsningar av dessa rättigheter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och mål

1. I detta direktiv fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

2. Enligt detta direktiv ska medlemsstaterna

a) skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och

b) säkerställa att behöriga myndigheters utbyte av personuppgifter inom unionen, när sådant utbyte krävs enligt unionsrätten eller medlemsstaternas nationella rätt, varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

([1]) EUT L 53, 27.2.2008, s. 52.
([2]) EUT L 160, 18.6.2011, s. 21.
([3]) EGT C 192, 30.6.2012, s. 7.

3. Detta direktiv ska inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

Artikel 2

Tillämpningsområde

1. Detta direktiv ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1.

2. Detta direktiv ska tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register.

3. Detta direktiv tillämpas inte på behandling av personuppgifter

a) som utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) som utförs av unionens institutioner, organ och byråer.

Artikel 3

Definitioner

I detta direktiv avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar enskild person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer, eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4. *profilering*: varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

7. *behörig myndighet*:

   a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

   b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten,

8. *personuppgiftsansvarig*: en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivs i unionsrätten eller medlemsstaternas nationella rätt,

9. *personuppgiftsbiträde*: en fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

10. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

11. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

12. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

13. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

14. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

15. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 41,

16. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder,

KAPITEL II

Principer

Artikel 4

Principer för behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

d) vara korrekta och, om nödvändigt, uppdaterade; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål,

e) inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas,

f) behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

2. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

3. Behandling som utförs av samma eller en annan personuppgiftsansvarig kan inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1 under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

4. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, punkterna 1, 2 och 3.

Artikel 5

Tidsgränser för lagring och översyn

Medlemsstaterna ska föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna efterlevs.

Artikel 6

Åtskillnad mellan olika kategorier av registrerade

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, i tillämpliga fall och så långt det är möjligt, ska göra en klar åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom

a) personer avseende vilka det finns tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott,

b) personer som dömts för brott,

c) brottsoffer eller personer avseende vilka det finns vissa omständigheter som ger anledning att anta att de kan vara brottsoffer, och

d) andra som berörs av ett brott, såsom personer som kan komma att kallas att vittna i samband med brottsutredningar eller senare straffrättsliga förfaranden, personer som kan ge information om brott eller personer med kontakter med eller band till någon av de personer som avses i a och b.

Artikel 7

Åtskillnad mellan personuppgifter och kontroll av kvaliteten på personuppgifterna

1. Medlemsstaterna ska föreskriva att personuppgifter som grundar sig på fakta så långt det är möjligt ska åtskiljas från personuppgifter som grundar sig på personliga bedömningar.

2. Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska därför i den mån det är praktiskt möjligt kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga. Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan nödvändig information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga och tillförlitliga samt i vilken utsträckning de är aktuella.

3. Om det visar sig att felaktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts ska mottagaren omedelbart underrättas om detta. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16.

Artikel 8

Laglig behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt.

2. Medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för detta direktiv ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

Artikel 9

Särskilda villkor för uppgiftsbehandling

1. Personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. ska inte behandlas för andra ändamål än de som anges i artikel 1.1 såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska förordning (EU) 2016/679 tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

2. Om de behöriga myndigheterna enligt medlemsstaternas nationella rätt anförtros utförandet av andra uppgifter än de som utförs för de ändamål som anges i artikel 1.1, ska förordning (EU) 2016/679 vara tillämplig på behandlingen för dessa ändamål, inklusive för arkivändamål av allmänt intresse, för historiska eller vetenskapliga forskningsändamål eller för statistiska ändamål, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

3. Om den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställer särskilda villkor för behandling, ska medlemsstaten föreskriva att den överförande behöriga myndigheten ska informera mottagaren om dessa särskilda villkor och om kravet att respektera dem.

4. Medlemsstaterna ska föreskriva att den överförande behöriga myndigheten inte ska tillämpa villkor enligt punkt 3 på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för de villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den överförande behöriga myndighetens medlemsstat.

Artikel 10

Behandling av särskilda kategorier av personuppgifter

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och endast

a) om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt,

b) för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller

c) om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

Artikel 11

Automatiserat individuellt beslutsfattande

1. Medlemsstaterna ska föreskriva att beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida.

2. Beslut som avses i punkt 1 i den här artikeln får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 10, såvida inte lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen har vidtagits.

3. Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 ska förbjudas i enlighet med unionsrätten.

KAPITEL III

Den registrerades rättigheter

Artikel 12

Information om och villkor för utövandet av den registrerades rättigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade all information som avses i artikel 13 och alla meddelanden enligt artiklarna 11, 14–18 och 31 som avser behandling i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma format som begäran.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt artiklarna 11 och 14–18.

3. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål skriftligen ska informera den registrerade om uppföljningen av hans eller hennes begäran.

4. Medlemsstaterna ska föreskriva att den information som tillhandahålls enligt artikel 13 och alla meddelanden eller åtgärder som vidtas enligt artiklarna 11, 14–18 och 31 ska tillhandahållas kostnadsfritt. Om en registrerads begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift med beaktande av de administrativa kostnaderna för tillhandahållandet av informationen eller meddelandet eller vidtagandet av den åtgärd som begärs, eller

b) vägra att tillmötesgå begäran.

Den personuppgiftsansvarige ska visa att begäran är uppenbart ogrundad eller orimlig.

5. Om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 14 eller 16, får den personuppgiftsansvarige begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas.

Artikel 13

Information som ska göras tillgänglig för eller lämnas till den registrerade

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda.

d) Rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.

e) Rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

2. Utöver den information som avses i punkt 1, ska medlemsstaterna i lag föreskriva att den personuppgiftsansvarige i specifika fall ska lämna följande information till den registrerade, för att göra det möjligt för honom eller henne att utöva sina rättigheter:

a) Behandlingens rättsliga grund.

b) Den period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.

c) I tillämpliga fall, kategorierna av mottagare av personuppgifterna, inbegripet i tredjeländer eller internationella organisationer.

d) Vid behov ytterligare information, i synnerhet om personuppgifterna samlas in utan den registrerades vetskap.

3. Medlemsstaterna får anta lagstiftningsåtgärder som gör att informationen till den registrerade enligt punkt 2 senareläggs, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

4. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av något av leden i punkt 3.

Artikel 14

Den registrerades rätt till tillgång till personuppgifter

Med förbehåll för artikel 15 ska medlemsstaterna föreskriva att den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse av huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

a) Ändamålen med behandlingen och dess rättsliga grund.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.

e) Rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifter eller begränsning av behandling av personuppgifter som rör den registrerade.

f) Rätten att lämna in klagomål till tillsynsmyndigheten samt tillsynsmyndighetens kontaktuppgifter.

g) Information om vilka personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar.

Artikel 15

Begränsningar av rätten till tillgång

1. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar den registrerades rätt till tillgång i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, förundersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

2. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av undantagen i punkt 1 a–e.

3. I de fall som avses i punkterna 1 och 2 ska medlemsstaterna föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål ska informera den registrerade skriftligen om varje vägran eller begränsning av tillgång och om skälen för vägran eller begränsningen. Denna information kan utelämnas om tillhandahållandet skulle undergräva ett ändamål enligt punkt 1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslutet. Denna information ska göras tillgänglig för tillsynsmyndigheterna.

Artikel 16

Rätt till rättelse eller radering av personuppgifter och begränsning av behandling

1. Medlemsstaterna ska föreskriva att den registrerade ska ha rätt att utan onödigt dröjsmål av den personuppgiftsansvarige få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen ska medlemsstaterna föreskriva att den registrerade ska ha rätt att få ofullständiga personuppgifter kompletterade, inbegripet genom att tillhandahålla en kompletterande inlaga.

2. Medlemsstaterna ska kräva att den personuppgiftsansvarige utan onödigt dröjsmål ska radera personuppgifter och ge den registrerade rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få till stånd radering av personuppgifter som rör honom eller henne om behandlingen står i strid med de bestämmelser som antas enligt artiklarna 4, 8 och 10 eller om personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

3. I stället för radering ska den personuppgiftsansvarige begränsa behandling om

a) den registrerade bestrider personuppgifternas korrekthet och korrektheten inte kan fastställas, eller

b) personuppgifterna måste sparas som bevisning.

Om behandlingen begränsas enligt första stycket led a ska den personuppgiftsansvarige underrätta den registrerade innan begränsningen av behandlingen upphävs.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige underrättar den registrerade skriftligen om eventuell vägran att rätta, radera eller begränsa behandlingen och om skälen till vägran. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar skyldigheten att tillhandahålla sådan information i den utsträckning som en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheterna att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska meddela varje rättelse av oriktiga personuppgifter till den behöriga myndighet från vilken de oriktiga personuppgifterna kommer.

6. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, när personuppgifter har rättats, raderats eller begränsats i enlighet med punkterna 1, 2 och 3, ska underrätta mottagarna och att mottagarna ska rätta eller radera personuppgifterna eller begränsa den behandling som utförs under deras ansvar.

Artikel 17

Den registrerades utövande av rättigheter och kontroll genom tillsynsmyndigheten

1. I de fall som avses i artiklarna 13.3, 15.3 och 16.4 ska medlemsstaterna anta bestämmelser om att den registrerades rättigheter även kan utövas genom den behöriga tillsynsmyndigheten.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om hans eller hennes möjlighet att utöva sina rättigheter genom tillsynsmyndigheten enligt punkt 1.

3. När den rättighet som avses i punkt 1 utövas ska tillsynsmyndigheten åtminstone underrätta den registrerade om att alla nödvändiga kontroller eller en översyn genom tillsynsmyndigheten har ägt rum. Tillsynsmyndigheten ska också informera den registrerade om hans eller hennes rätt att begära rättslig prövning.

Artikel 18

Den registrerades rättigheter i brottsutredningar och straffrättsliga förfaranden

Medlemsstaterna får föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med medlemsstaternas nationella rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 19

Den personuppgiftsansvariges skyldigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang och ändamål, samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa, och kunna visa, att behandlingen utförs i enlighet med detta direktiv. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

Artikel 20

Inbyggt dataskydd och dataskydd som standard

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av den senaste utvecklingen och genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål, samt de risker, av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter som behandlingen utgör, både vid tidpunkten för beslut om vilka medel behandlingen ska utföras med och vid tidpunkten för själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för genomförande av dataskyddsprinciper, såsom uppgiftsminimering, på ett effektivt sätt och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, för att uppfylla kraven i detta direktiv och skydda den registrerades rättigheter.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige genomför lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Artikel 21

Gemensamt personuppgiftsansvariga

1. Medlemsstaterna ska föreskriva att två eller flera personuppgiftsansvariga har gemensamt ansvar för registret, om de gemensamt fastställer behandlingens ändamål och medel. De ska under öppna former fastställa sitt respektive ansvar för efterlevnaden av detta direktiv, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artikel 13, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget ska en kontaktpunkt för de registrerade utses. Medlemsstaterna får fastslå vem av de gemensamt personuppgiftsansvariga som kan fungera som enda kontaktpunkt för de registrerade i fråga om utövandet av deras rättigheter.

2. Oavsett formerna för det arrangemang som avses i punkt 1 får medlemsstaterna föreskriva att den registrerade får utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv med avseende på var och en av de personuppgiftsansvariga.

Artikel 22

Personuppgiftsbiträde

1. Medlemsstaterna ska, om en behandling ska genomföras på en personuppgiftsansvarigs vägnar, föreskriva att den personuppgiftsansvarige endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i detta direktiv och säkerställer att den registrerades rättigheter skyddas.

2. Medlemsstaterna ska föreskriva att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet alltid informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. Medlemsstaterna ska föreskriva att ett personuppgiftsbiträdes behandling ska regleras genom ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. Avtalet eller den andra rättsakten ska särskilt föreskriva att personuppgiftsbiträdet

a) endast handlar enligt instruktioner från den personuppgiftsansvarige,

b) säkerställer att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) på lämpligt sätt ska bistå den personuppgiftsansvarige att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,

d) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och raderar befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt,

e) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att denna artikel efterlevs,

f) respekterar de villkor som avses i punkterna 2 och 3 för anlitande av ett annat personuppgiftsbiträde.

4. Det avtal eller den andra rättsakt som avses i punkt 3 ska vara skriftligt, inbegripet i elektronisk form.

5. Om ett personuppgiftsbiträde i strid med detta direktiv fastställer ändamålen och medlen för behandlingen ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

Artikel 23

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Medlemsstaterna ska föreskriva att personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast får behandla dessa uppgifter enligt instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 24

Register över behandling

1. Medlemsstaterna ska föreskriva att alla personuppgiftsansvariga ska föra ett register över alla kategorier av verksamheter i samband med behandling som de ansvarar för. Detta register ska innehålla samtliga följande uppgifter:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga och dataskyddsombudet.

b) Ändamålen med behandlingen.

c) De kategorier av mottagare som personuppgifterna har lämnats ut till eller ska lämnas ut till, inbegripet mottagare i tredjeländer eller internationella organisationer.

d) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

e) Användning av profilering, i tillämpliga fall.

f) I tillämpliga fall, kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation.

g) En uppgift om den rättsliga grunden för den behandling, inbegripet överföringar, för vilken personuppgifterna är avsedda.

h) Om möjligt, de planerade tidsfristerna för radering av de olika personuppgiftskategorierna.

i) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

2. Medlemsstaterna ska föreskriva att alla personuppgiftsbiträden ska upprätthålla ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, vilket ska omfatta följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller registerförarna, för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar samt, i tillämpliga fall, för dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen, om den personuppgiftsansvarige uttryckligen begär detta.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra registren tillgängliga för tillsynsmyndigheten.

Artikel 25

Loggning

1. Medlemsstaterna ska säkerställa att loggar förs över åtminstone följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna.

2. Loggarna bör endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra loggarna tillgängliga för tillsynsmyndigheten.

Artikel 26

Samarbete med tillsynsmyndigheten

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet på begäran ska samarbeta med tillsynsmyndigheten vid utförandet av dess uppgifter.

Artikel 27

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska medlemsstaterna säkerställa att den personuppgiftsansvarige före behandlingen utför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att detta direktiv efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 28

Förhandssamråd med tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten före behandling av personuppgifter som kommer att ingå i ett nytt register som ska inrättas, om

a) en konsekvensbedömning avseende dataskydd enligt artikel 27 visar att behandlingen skulle leda till en hög risk om inte den registeransvarige vidtar åtgärder för att minska risken, eller om

b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.

2. Medlemsstaterna ska föreskriva att tillsynsmyndigheten ska rådfrågas under utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

3. Medlemsstaterna ska föreskriva att tillsynsmyndigheten får upprätta en förteckning över de olika typer av uppgiftsbehandling som omfattas av förhandssamråd enligt punkt 1.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige till tillsynsmyndigheten lämnar in den konsekvensbedömning avseende dataskydd som avses i artikel 27 och, på begäran, eventuell övrig information som gör att tillsynsmyndigheten kan göra en bedömning av behandlingens överensstämmelse och särskilt av riskerna för skyddet av den registrerades personuppgifter och av därmed sammanhängande skyddsåtgärder.

5. Medlemsstaterna ska, om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 i denna artikel inte skulle vara förenlig med de bestämmelser som antas i enlighet med detta direktiv, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, föreskriva att tillsynsmyndigheten inom en period på högst sex veckor från det att begäran om samråd mottagits ska ge den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 47. Denna period får förlängas med en månad beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 29

Säkerhet i samband med behandling

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller de särskilda kategorier av personuppgifter som avses i artikel 10.

2. När det gäller automatiserad behandling ska varje medlemsstat föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet, efter en bedömning av riskerna, ska vidta åtgärder i syfte att

a) vägra varje obehörig person åtkomst till utrustning för behandling som används för behandling (*åtkomstskydd för utrustning*),

b) förhindra obehörig läsning, kopiering, ändring eller radering av datamedier (*kontroll av datamedier*),

c) förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (*lagringskontroll*),

d) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring (*användarkontroll*),

e) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet (*åtkomstkontroll*),

f) säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring (*kommunikationskontroll*),

g) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes (*indatakontroll*),

h) förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (*transportkontroll*),

i) säkerställa att de system som används kan återställas vid störningar (*återställande*),

j) säkerställa att systemet fungerar, att funktionsfel rapporteras (*driftsäkerhet*) och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet (*dataintegritet*).

Artikel 30

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, anmäler den till tillsynsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar, ska den åtföljas av en motivering till förseningen.

2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

3. Den anmälan som avses i punkt 1 ska åtminstone

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antal registrerade som berörs samt de kategorier av och det ungefärliga antal personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller annan kontaktpunkt där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten,

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, i tillämpliga fall, åtgärder för att mildra dess potentiella negativa effekter.

4. Om, och i den utsträckning, det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter som avses i punkt 1, inbegripet omständigheterna rörande personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

6. Medlemsstaterna ska föreskriva att den information som avses i punkt 3, om personuppgiftsincidenten rör personuppgifter som har överförts av eller till den personuppgiftsansvarige i en annan medlemsstat, utan onödigt dröjsmål ska meddelas den personuppgiftsansvarige i den medlemsstaten.

Artikel 31

Information till den registrerade om en personuppgiftsincident

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, om personuppgiftsincidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter, utan onödigt dröjsmål ska informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i den här artikeln ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 30.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 ska inte krävas om något av följande villkor är uppfyllda:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som gör personuppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dem, såsom kryptering.

b) Om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4. Om personuppgiftsbiträdet inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det, eller besluta att något av de villkor som avses i punkt 3 är uppfyllt.

5. Den information till den registrerade som avses i punkt 1 i den här artikeln kan senareläggas, begränsas eller utelämnas på de villkor och av de skäl som avses i artikel 13.3.

Avsnitt 3

Dataskyddsombud

Artikel 32

Utnämning av dataskyddsombudet

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Medlemsstaterna får undanta domstolars och andra oberoende rättsliga myndigheters dömande verksamhet från denna skyldighet.

2. Dataskyddsombudet ska utnämnas på grundval av sina yrkesmässiga kvalifikationer och, i synnerhet, sin sakkunskap om lagstiftning och praxis i fråga om dataskydd samt förmåga att fullgöra de uppgifter som avses i artikel 34.

3. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter med hänsyn tagen till organisationsstruktur och storlek.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 33

Dataskyddsombudets ställning

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 34 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

Artikel 34

Dataskyddsombudets uppgifter

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska anförtro dataskyddsombudet åtminstone följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige och de anställda som utför behandling om deras skyldigheter enligt detta direktiv och annan unionsrätt eller medlemsstaters bestämmelser om dataskydd.

b) Att övervaka efterlevnaden av detta direktiv, annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd och av den personuppgiftsansvariges strategier för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 27.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 28, och, om så är lämpligt, samråda i andra frågor.

KAPITEL V

Överföringar av personuppgifter till tredjeländer eller internationella organisationer

Artikel 35

Allmänna principer för överföringar av personuppgifter

1. Medlemsstaterna ska föreskriva att de behöriga myndigheterna endast ska överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation, inklusive för vidare överföring till ett annat tredjeland eller en annan internationell organisation, under förutsättning att de nationella bestämmelser som antas i enlighet med andra bestämmelser i detta direktiv respekteras och endast om de villkor som fastställs i detta kapitel uppfylls, nämligen:

a) Överföringen är nödvändig för de ändamål som anges i artikel 1.1.

b) Personuppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är en behörig myndighet för de ändamål som avses i artikel 1.1.

c) Den aktuella medlemsstaten, om personuppgifter överförs eller görs tillgängliga från en annan medlemsstat, har gett förhandstillstånd till överföringen i enlighet med medlemsstaternas nationella rätt.

d) Kommissionen har antagit ett beslut om adekvat skyddsnivå i enlighet med artikel 36 eller, om inget sådant beslut föreligger, när lämpliga skyddsåtgärder har vidtagits eller föreligger enligt artikel 37 eller, om inget beslut om adekvat skyddsnivå enligt artikel 36 föreligger och inga lämpliga skyddsåtgärder enligt artikel 37 har vidtagits, när undantag för särskilda situationer gäller i enlighet med artikel 38.

e) Att den behöriga myndighet som gjorde den ursprungliga överföringen eller en annan behörig myndighet i samma medlemsstat vid vidare överföring till ett annat tredjeland eller en internationell organisation godkänner vidareöverföringen efter vederbörligt beaktande av alla relevanta faktorer, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i tredjelandet till vilket eller den internationella organisationen till vilken personuppgifterna förts vidare.

2. Medlemsstaterna ska föreskriva att överföringar utan förhandstillstånd av en annan medlemsstat i enlighet med punkt 1 c tillåts endast om överföringen av personuppgifter är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och förhandstillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska underrättas utan dröjsmål.

3. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den skyddsnivå för fysiska personer som säkerställs genom detta direktiv inte undergrävs.

Artikel 36

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Medlemsstaterna ska föreskriva att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva ett särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt samt offentliga myndigheters tillgång till personuppgifter liksom tillämpningen av denna lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser och regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det tredjeland eller inom den internationella organisation som berörs, rättspraxis, och effektiva och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, med ansvar för att säkerställa och kontrollera att dataskyddsbestämmelserna följs, inklusive lämpliga verkställighetsbefogenheter, ge registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om skyddsnivån är adekvat, genom en genomförandeakt, besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation, säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Den territoriella och sektoriella tillämpningen ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter dra tillbaka, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet, ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 58.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Medlemsstaterna ska föreskriva att ett beslut enligt punkt 5 inte ska påverka överföringar av personuppgifter till tredjelandet, territoriet eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga, enligt artiklarna 37–38.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

Artikel 37

Överföring som omfattas av lämpliga skyddsåtgärder

1. Om det inte föreligger något beslut enligt artikel 36.3 ska medlemsstaterna föreskriva att en överföring av personuppgifter till ett tredjeland eller en internationell organisation får ske om

a) lämpliga skyddsåtgärder för personuppgifter har fastställts i ett rättsligt bindande instrument, eller

b) den personuppgiftsansvarige har bedömt alla omständigheter kring en överföring av personuppgifter och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

2. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om kategorier av överföringar enligt punkt 1 b.

3. När en överföring grundas på punkt 1 b, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 38

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 36 eller lämpliga skyddsåtgärder enligt artikel 37, ska medlemsstaterna föreskriva att en överföring eller en kategori av överföringar av personuppgifter till ett tredjeland eller en internationell organisation får ske endast om överföringen är nödvändig

a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,

b) för att skydda den registrerades berättigade intressen, om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta,

c) för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland,

d) i enskilda fall för de ändamål som anges i artikel 1.1. eller

e) i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk som hänför sig till de ändamål som anges i artikel 1.1.

2. Personuppgifter får inte överföras om den överförande behöriga myndigheten fastställer att den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset av en sådan överföring som avses i punkt 1 d och e.

3. När en överföring grundas på punkt 1, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 39

Överföringar av personuppgifter till mottagare som är etablerade i tredjeländer

1. Genom undantag från artikel 35.1 b och utan att det påverkar tillämpningen av internationella avtal som avses i punkt 2 i den här artikeln, får det i unionsrätten eller medlemsstaternas nationella rätt föreskrivas att de behöriga myndigheter som avses i artikel 3.7 a, i enskilda och särskilda fall, får överföra personuppgifter direkt till mottagare som är etablerade i tredjeländer endast om de övriga bestämmelserna i detta direktiv efterlevs och samtliga följande villkor är uppfyllda:

a) Överföringen är absolut nödvändig för att utföra en uppgift som en överförande behörig myndighet ansvarar för i enlighet med unionsrätten eller medlemsstaternas nationella rätt för de ändamål som anges i artikel 1.1.

b) Den överförande behöriga myndigheten har fastställt att ingen av den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresse som nödvändiggör överföringen i det aktuella fallet.

c) Den överförande behöriga myndigheten anser att överföring till en myndighet som är behörig för de ändamål som avses i artikel 1.1 i tredjelandet är ineffektivt eller olämpligt, i synnerhet eftersom överföringen inte kan göras inom rimlig tid.

d) Den myndighet i tredjelandet som är behörig för de ändamål som avses i artikel 1.1 har utan dröjsmål informerats, såvida detta inte är ineffektivt eller olämpligt.

e) Den överförande behöriga myndigheten har informerat mottagaren om det eller de specifika ändamål för vilka och personuppgifterna ska behandlas av den senare förutsatt att den behandlingen är nödvändig.

2. Med ett internationellt avtal som avses i punkt 1 avses varje gällande bilateralt eller multilateralt internationellt avtal mellan medlemsstater och tredjeländer inom området för straffrättsligt samarbete och polissamarbete.

3. Den överförande behöriga myndigheten ska informera tillsynsmyndigheten om överföringar enligt denna artikel.

4. Överföringar som grundar sig på punkt 1 ska dokumenteras.

Artikel 40

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och medlemsstaterna vidta lämpliga åtgärder för att

a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,

b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,

c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,

d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 41

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av detta direktiv, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen samt att underlätta det fria flödet av sådana uppgifter inom unionen (*tillsynsmyndighet*).

2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av detta direktiv i hela unionen. För det ändamålet ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.

3. Medlemsstaterna får föreskriva att en tillsynsmyndighet som har inrättats enligt förordning (EU) 2016/679 ska vara den tillsynsmyndighet som avses i detta direktiv och ta på sig ansvaret för de uppgifter som ska utföras av den tillsynsmyndighet som inrättas enligt punkt 1 i denna artikel.

4. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda myndigheterna i fråga i den styrelse som avses i artikel 51.

Artikel 42

Oberoende

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med detta direktiv.

2. Medlemsstaterna ska föreskriva att dess tillsynsmyndigheters ledamot eller ledamöter i utförandet av sina uppgifter och i utövandet av sina befogenheter enligt detta direktiv ska stå fria från utomstående påverkan, direkt såväl som indirekt, och varken begära eller ta emot instruktioner av någon.

3. Medlemsstaternas tillsynsmyndigheters ledamot eller ledamöter ska avhålla sig från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.

4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.

5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.

6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet är föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

Artikel 43

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utses genom ett öppet förfarande av

— deras parlament

— deras regering

— deras statschef, eller

— ett oberoende organ som enligt medlemsstaternas nationella rätt anförtrotts utnämningen.

2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att de ska kunna utföra sitt uppdrag och utöva sina befogenheter.

3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den nationella rätten i den berörda medlemsstaten.

4. En ledamot ska avsättas endast på grund av allvarlig försummelse eller när ledamoten inte längre uppfyller de krav som ställs för att kunna utföra sina uppgifter.

Artikel 44

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska i lag fastställa samtliga följande:

a) Varje tillsynsmyndighets inrättande.

b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.

c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.

d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 6 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.

e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder,

f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapporter från fysiska personer om överträdelser av detta direktiv.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 45

Behörighet

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den i enlighet med detta direktiv inom sin egen medlemsstats territorium.

2. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet. Medlemsstaterna får föreskriva att deras tillsynsmyndighet inte ska vara behörig att utöva tillsyn över andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet.

Artikel 46

Uppgifter

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inom sitt territorium ska

a) övervaka och verkställa tillämpningen av de bestämmelser som antas i enlighet med detta direktiv och dess genomförandeåtgärder,

b) öka allmänhetens medvetenhet och kunskaper om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen,

c) i enlighet med medlemsstaternas nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsmässiga och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling,

d) öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt detta direktiv,

e) på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt detta direktiv, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål,

f) behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 55, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet,

g) kontrollera att behandling enligt artikel 17 är laglig och inom en rimlig period informera den registrerade om resultatet av kontrollen enligt artikel 17.3 eller om skälen till att kontrollen inte har genomförts,

h) samarbeta, inbegripet genom att utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att detta direktiv tillämpas och verkställs på ett enhetligt sätt,

i) utföra undersökningar om tillämpningen av detta direktiv, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan offentlig myndighet,

j) följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik,

k) ge råd om sådan behandling av personuppgifter som avses i artikel 28, och

l) bidra till styrelsens verksamhet.

2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder, såsom att tillhandahålla ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 47

Befogenheter

1. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva undersökningsbefogenheter. Dessa befogenheter ska minst inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

2. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva korrigerande befogenheter, till exempel för att:

a) Utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att stå i strid med de bestämmelser som antas i enlighet med detta direktiv.

b) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med de bestämmelser som antas enligt detta direktiv, om lämpligt på ett visst sätt och inom en viss tid, bland annat genom att beordra rättelse, eller radering av personuppgifter eller begränsning av behandling enligt artikel 16.

c) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, uppgiftsbehandlingen.

3. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva befogenheter att ge den personuppgiftsansvarige råd i enlighet med det förfarande för förhandssamråd som avses i artikel 28 och att på eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med dess nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställts i unionsrätten och medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har befogenhet att göra rättsliga myndigheter uppmärksamma på överträdelser av de bestämmelser som antas i enlighet med detta direktiv och att, när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden, i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med detta direktiv.

Artikel 48

Rapportering av överträdelser

Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska inrätta effektiva mekanismer för att uppmuntra till konfidentiell rapportering av överträdelser av detta direktiv.

Artikel 49

Verksamhetsrapport

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av ålagda sanktioner. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstaternas nationella rätt. Den ska göras tillgänglig för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete

Artikel 50

Ömsesidigt bistånd

1. Medlemsstaterna ska föreskriva att tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa detta direktiv på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska särskilt omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om att genomföra samråd, inspektioner och utredningar.

2. Medlemsstaterna ska föreskriva att varje tillsynsmyndighet ska vidta alla lämpliga åtgärder för att kunna besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.

3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med och skälen till denna. Information som utbytts får endast användas för det syfte för vilket den har begärts.

4. En tillsynsmyndighet som tar emot begäran får bara vägra att tillmötesgå begäran om

a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller

b) det skulle stå i strid med detta direktiv eller med den unionsrätt eller medlemsstatens nationella rätt som den tillsynsmyndighet som mottar begäran omfattas av att tillmötesgå begäran.

5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.

6. Varje tillsynsmyndighet som tar emot begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.

7. Tillsynsmyndigheter som tar emot begäran får inte ta ut någon avgift för åtgärder som de vidtagit efter en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.

8. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

Artikel 51

Styrelsens uppgifter

1. Styrelsen som inrättats genom förordning (EU) 2016/679 ska i samband med uppgiftsbehandling som omfattas av detta direktivs tillämpningsområde ha följande uppgifter:

a) Ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, till exempel om eventuella förslag till ändring av detta direktiv.

b) På eget initiativ, på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av detta direktiv och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av detta direktiv.

c) Utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 47.1 och 47.3.

d) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke för att konstatera personuppgiftsincidenter och fastställa det otillbörliga dröjsmål som avses i artikel 30.1 och 30.2 och för de särskilda omständigheter under vilka ett personuppgiftsbiträde eller en personuppgiftsansvarig är skyldig att anmäla personuppgiftsincidenten.

e) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att orsaka en hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 31.1.

f) Se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden b och c.

g) Avge ett yttrande till kommissionen för bedömningen av huruvida skyddsnivån i ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation är adekvat, inbegripet för en bedömning av huruvida det tredjelandet, det territoriet, den specificerade sektorn eller den internationella organisationen inte längre säkerställer en adekvat skyddsnivå.

h) Främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna.

i) Främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna, och där så är lämpligt även med tillsynsmyndigheter i tredjeland och internationella organisationer.

j) Främja utbyte av kunskap och dokumentation om lagstiftning och bästa praxis på området för dataskydd med tillsynsmyndigheter med ansvar för dataskydd i hela världen.

Vad gäller första stycket led g ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med territoriet eller den specificerade sektorn i det tredjelandet eller med den internationella organisationen.

2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.

3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och exempel på bästa praxis till kommissionen och till den kommitté som avses i artikel 58.1, samt offentliggöra dem.

4. Kommissionen ska hålla styrelsen underrättad om de åtgärder den vidtagit som en följd av styrelsens yttranden, riktlinjer, rekommendationer och bästa praxis.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 52

Rätt att lämna in ett klagomål till en tillsynsmyndighet

1. Utan att det påverkar andra administrativa prövningsförfaranden eller rättsmedel ska medlemsstaterna föreskriva att alla registrerade personer som anser att behandling som avser dem står i strid med de bestämmelser som antas i enlighet med detta direktiv har rätt att lämna in ett klagomål till en enda tillsynsmyndighet.

2. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska överlämna det till den behöriga tillsynsmyndigheten utan onödigt dröjsmål, om klagomålet inte inlämnats till den myndighet som är behörig enligt artikel 45.1. Den registrerade ska informeras om överlämnandet.

3. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska tillhandahålla ytterligare hjälp på den registrerades begäran.

4. Den registrerade ska underrättas av den behöriga tillsynsmyndigheten om klagomålets handläggning och dess resultat, inbegripet rätten till rättsmedel enligt artikel 53.

Artikel 53

Rätt till ett effektivt rättsmedel mot en tillsynsmyndighets beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska medlemsstater föreskriva att en fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje registrerad person ha rätt till ett effektivt rättsmedel om den enligt artikel 45.1 behöriga tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller om tillsynsmyndigheten inte informerar den registrerade om handläggningen eller resultatet av det klagomål som inlämnats enligt artikel 52.

3. Medlemsstaterna ska föreskriva att talan mot en tillsynsmyndighet ska väckas vid domstol i den medlemsstat där tillsynsmyndigheten har sitt säte.

Artikel 54

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet enligt artikel 52, ska medlemsstaterna föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter enligt de bestämmelser som antas enligt detta direktiv har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med dessa bestämmelser.

Artikel 55

Företrädande av registrerade personer

Medlemsstaterna ska i enlighet med medlemsstaternas nationella processrätt se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, och vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter vad gäller skyddet av deras personuppgifter, i uppdrag att lämna in klagomålet för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

Artikel 56

Rätt till ersättning

Medlemsstaterna ska föreskriva att var och en som lidit materiell eller immateriell skada till följd av en olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de nationella bestämmelser som antas i enlighet med detta direktiv ska ha rätt till ersättning för denna skada från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Artikel 57

Sanktioner

Medlemsstaterna ska föreskriva sanktioner för överträdelser av bestämmelser som antas enligt detta direktiv och ska vidta de åtgärder som krävs för att säkerställa att dessa sanktioner genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande.

KAPITEL IX

Genomförandeakter

Artikel 58

Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats enligt artikel 93 i förordning (EU) 2016/679. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt, ska artikel 8 i förordning (EU) nr 182/2011 jämförd med artikel 5 i den förordningen tillämpas.

KAPITEL X

Slutbestämmelser

Artikel 59

Upphävande av rambeslut 2008/977/RIF

1. Rambeslut 2008/977/RIF ska upphöra att gälla från och med den 6 maj 2018.

2. Hänvisningar till det upphävda beslut som avses i punkt 1 ska anses som hänvisningar till detta direktiv.

Artikel 60

Gällande unionsrättsakter

Detta direktiv ska inte påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som trädde i kraft den 6 maj 2016 eller tidigare, vilka reglerar behandling medlemsstaterna emellan och medlemsstaternas utsedda myndigheters tillgång till informationssystem som inrättats på grundval av fördragen och som är relevanta för detta direktivs tillämpningsområde.

Artikel 61

Förhållande till tidigare ingångna internationella avtal på området för straffrättsligt samarbete och polissamarbete

Internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 6 maj 2016 och som är förenliga med unionsrätten så som den tillämpades före den dagen ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 62

Kommissionens rapporter

1. Kommissionen ska senast den 6 maj 2022 och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av detta direktiv till Europaparlamentet och rådet. Rapporten ska offentliggöras.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen i synnerhet granska tillämpningen av kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer samt hur bestämmelserna fungerar, och därvid särskilt beakta beslut som antagits i enlighet med artiklarna 36.3 och 39.

3. För de ändamål som avses i punkterna 1 och 2 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.

4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.

5. Dessa rapporter får vid behov överlämnas tillsammans med lagstiftningsförslag om ändring, i syfte att ändra detta direktiv med särskild hänsyn till informationsteknikens utveckling och informationssamhällets framsteg.

6. Kommissionen ska senast den 6 maj 2019 se över andra rättsakter som antagits av unionen och som reglerar de behöriga myndigheternas behandling för att uppnå de mål som anges i artikel 1.1, inklusive de som avses i artikel 60, i syfte att bedöma om de behöver anpassas till detta direktiv och att, i förekommande fall, lägga fram förslag till ändring av dessa rättsakter för att säkerställa ett enhetligt tillvägagångssätt för skydd av personuppgifter inom detta direktivs tillämpningsområde.

Artikel 63

Införlivande

1. Medlemsstaterna ska senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast överlämna texten till dessa bestämmelser till kommissionen. De ska tillämpa dessa bestämmelser från och med den 6 maj 2018.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Genom undantag från punkt 1 får medlemsstaterna föreskriva att de automatiserade behandlingssystem som inrättades före den 6 maj 2016 undantagsvis, när det innebär oproportionella ansträngningar, ska bringas i överensstämmelse med artikel 25.1 senast den 6 maj 2023.

3. Genom undantag från punkterna 1 och 2 i denna artikel får en medlemsstat under exceptionella omständigheter bringa ett automatiserat behandlingssystem som avses i punkt 2 i denna artikel i överensstämmelse med artikel 25.1 inom en specifik tidsperiod efter den period som avses i punkt 2 i den här artikeln om det annars skulle uppstå allvarliga problem för driften av detta specifika automatiserade behandlingssystem. Den berörda medlemsstaten ska underrätta kommissionen om skälen till dessa allvarliga problem och skälen till den angivna tidsperioden inom vilken den ska bringa detta specifika automatiserade databehandlingssystem i överensstämmelse med artikel 25.1. Den angivna perioden ska under inga omständigheter inte vara senare än 6 maj 2026.

4. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i medlemsstaternas nationella rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 64

Ikraftträdande

Detta direktiv träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 65

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*

Sammanfattning SOU 2017:29

Uppdraget

Europeiska unionen har enats om en genomgripande dataskyddsreform som ska vara genomförd under våren 2018. Reformen omfattar dels en allmän dataskyddsförordning, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet. En konsekvens av reformen är att personuppgiftslagen kommer att upphävas och att all lagstiftning om personuppgiftsbehandling behöver ses över och anpassas.

Utredningens uppdrag är att föreslå hur det nya direktivet ska genomföras i svensk rätt. Eftersom regleringen i förordningen inte omfattar det som regleras i direktivet är en viktig uppgift att genom den nya lagstiftningen avgränsa tillämpningsområdet i förhållande till förordningen.

Alla myndigheter som kommer att tillämpa den lagstiftning som genomför direktivet kommer även att tillämpa förordningen. Utredningen har därför strävat efter att ha samma terminologi och likartade lösningar som i förordningen, när båda rättsakterna innehåller samma eller liknande artiklar och det inte finns sakliga skäl att välja en annan lösning för direktivets del.

Uppdraget har genomförts i nära kontakt med Dataskyddsutredningen, som har till uppgift att senare i vår lägga fram de förslag till kompletterande reglering som dataskyddsförordningen kan kräva och att utreda vissa andra generella frågor som dataskyddsreformen väcker. Under arbetet har utredningen också haft kontakt med alla andra pågående utredningar vilkas arbete kan påverkas av vår utrednings förslag.

En ny ramlag

Utredningen föreslår att direktivet i huvudsak genomförs genom en ny ramlag, brottsdatalagen. Syftet med lagen är både att skydda fysiska personers grundläggande fri- och rättigheter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt. Lagen ska – i likhet med personuppgiftslagen – vara generellt tillämplig inom det område som direktivet reglerar. Lagen ska även vara subsidiär. De myndigheter som bedriver verksamhet inom lagens tillämpningsområde har i allmänhet särskilda registerförfattningar som reglerar personuppgiftsbehandlingen. Utredningen kommer att i slutbetänkandet föreslå de anpassningar som krävs med anledning av ramlagen i de registerförfattningar som ingår i utredningens uppdrag. Registerförfattningarna kommer att gälla utöver brottsdatalagen.

Lagen kompletteras med en förordning, som genomför vissa detaljbestämmelser i direktivet.

Tillämpningsområdet

Lagen ska tillämpas av myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder vid behandling av personuppgifter. Lagen ska också gälla för personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. De som har sådana arbetsuppgifter betecknas behöriga myndigheter. Lagen ska även tillämpas av andra aktörer som har fått i uppgift att utöva myndighet för något av de nämnda syftena.

De behöriga myndigheternas behandling av personuppgifter kommer dock bara att styras av lagen när de behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Dataskyddsförordningen kommer att bli tillämplig i övrigt, t.ex. när Polismyndigheten behandlar personuppgifter i tillståndsärenden eller när en allmän domstol handlägger ett tvistemål. Det som blir avgörande för om lagen är tillämplig är dels om det är en behörig myndighet som behandlar personuppgifterna, dels syftet med behandlingen. Gränsdragningsfrågor som rör lagens tillämpningsområde diskuteras ingående i kapitel 8.

Lagen ska i huvudsak gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad.

Lagen ska inte tillämpas på Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Undantag ska också gälla för Polismyndigheten om den övertagit en uppgift som rör nationell säkerhet från Säkerhetspolisen. Något motsvarande undantag för andra myndigheter vid deras behandling av uppgifter som rör nationell säkerhet görs inte.

Principer för behandlingen av personuppgifter

Det ska alltid finnas en rättslig grund för att personuppgifter ska få behandlas med stöd av ramlagen. Den huvudsakliga grunden att behandlingen av personuppgifterna ska vara nödvändig för att en behörig myndighet ska kunna utföra en sådan arbetsuppgift som gör lagen tillämplig. Arbetsuppgiften ska framgå av en bindande unionsrättsakt, en lag, en förordning eller ett särskilt beslut av regeringen. Den andra rättsliga grunden är om behandlingen krävs för diarieföring eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Personuppgifter får dessutom bara behandlas för särskilda, uttryckligt angivna, och berättigade ändamål.

Det ställs krav på att personuppgifterna ska behandlas författningsenligt och på ett korrekt sätt. De personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade. De ska också vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler uppgifter än nödvändigt får inte behandlas och inga uppgifter får behandlas längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Det är tillåtet att behandla personuppgifter för ett nytt ändamål som ligger inom lagens tillämpningsområde, men det måste alltid först prövas om det finns en tillåten rättslig grund för den nya behandlingen och om den är nödvändig och proportionerlig för det nya ändamålet. Det behöver däremot inte prövas om det nya ändamålet är förenligt med det ursprungliga.

Lagen föreskriver att olika typer av personuppgifter ska särskiljas – t.ex. uppgifter om misstänkta respektive brottsoffer – och att personuppgifter som grundar sig på fakta ska skiljas från personuppgifter som grundar sig på personliga bedömningar.

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning betecknas känsliga personuppgifter. Enligt huvudregeln får sådana uppgifter inte behandlas, men om uppgifter om en person redan behandlas får de, på samma sätt som i dag, kompletteras med känsliga personuppgifter, under förutsättning att det är absolut nödvändigt för ändamålet med behandlingen.

Biometriska uppgifter som används i identifieringssyfte och genetiska uppgifter är också känsliga personuppgifter. Sådana uppgifter får enbart behandlas om det är särskilt föreskrivet.

Det är förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. För att det inte ska vara möjligt att med stöd av offentlighetsprincipen få tillgång till en sådan sammanställning, föreslår utredningen en särskild sekretessregel som innebär att det gäller absolut sekretess för uppgifter i sådana sammanställningar.

Personuppgiftsansvariga åläggs att vidta alla rimliga åtgärder för att rätta personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Det regleras också under vilka förutsättningar personuppgifter som behandlas på ett otillåtet sätt ska raderas och när behandlingen av dem i stället ska begränsas.

Personuppgiftsansvarigas skyldigheter

De skyldigheter som personuppgiftsansvariga har i dag kommer till stor del att gälla även i fortsättningen. Vissa regler blir dock mer preciserade och det tillkommer också vissa nya skyldigheter. Kraven på säkerhets- och skyddsåtgärder blir mer preciserade, liksom kravet på att det ska finnas en behandlingshistorik. Det ställs exempelvis krav på inbyggt dataskydd och dataskydd som standard. Det införs också en generell bestämmelse om att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Till de nya skyldigheterna hör att personuppgiftsansvariga ska dokumentera alla personuppgiftsincidenter och anmäla de incidenter som kan antas påverka registrerades integritet till tillsynsmyndigheten. Det gäller dock inte sådana incidenter som rör nationell säkerhet.

Det införs också ett generellt krav på att personuppgiftsansvariga som planerar en ny typ av behandling eller att genomföra betydande förändringar i pågående behandling ska göra en bedömning av konsekvenserna för registrerades personliga integritet och, beroende på framför allt risken

för intrång, samråda med tillsynsmyndigheten innan behandlingen påbörjas eller förändras.

Alla personuppgiftsansvariga ska utse dataskyddsombud. Ombudens arbetsuppgifter anges i lagen.

En annan nyhet är att förutsättningarna för gemensamt personuppgiftsansvar regleras. Utredningen föreslår att gemensamt personuppgiftsansvar endast får förekomma om det följer av lag eller förordning eller om regeringen i ett enskilt fall har beslutat om det.

Enskildas rättigheter

När det gäller enskildas rättigheter kommer till stora delar samma reglering som i dag att gälla, men rätten till information blir tydligare i vissa avseenden. Genom att lagen är subsidiär kommer reglerna om information i straffrättsliga förfaranden att ha företräde framför ramlagens bestämmelser om information.

Utgångspunkten är att den som vill kontrollera om hans eller hennes personuppgifter behandlas får vända sig till den personuppgiftsansvarige, som utan onödigt dröjsmål ska lämna skriftligt besked om uppgifterna behandlas. Om så är fallet har den registrerade rätt att få del av uppgifterna och få viss information om behandlingen. Informationsskyldigheten gäller dock inte om uppgifterna inte får lämnas ut på grund av att vissa i lagen angivna intressen kan skadas. Om det finns grund för att inte lämna informationen får även skälen för det utelämnas.

Personuppgifter i ofärdig text eller som utgör minnesanteckningar omfattas som regel inte av informationsskyldigheten. Detsamma gäller personuppgifter som sökanden redan har tagit del av.

Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. En motsvarande skyldighet gäller i fråga om radering av personuppgifter som behandlas på ett otillåtet sätt eller om radering krävs för att den personuppgiftsansvarige ska fullgöra en rättslig förpliktelse. I vissa fall ska behandlingen av personuppgifterna i stället begränsas. Om det finns stöd för att begränsa informationen till den registrerade får den personuppgiftsansvarige också utelämna skälen för beslut om korrigeringsåtgärder.

Tillsynen över personuppgiftsbehandling

Utredningen tar inte ställning till vilken myndighet som ska utses till tillsynsmyndighet eller hur myndigheten ska organiseras, eftersom det har utretts i annan ordning. Utredningen behandlar enbart frågan hur verksamheten ska bedrivas.

Tillsynsmyndighetens dubbla perspektiv – att både verka för att fysiska personers grundläggande rättigheter och friheter skyddas och att underlätta det fria flödet av personuppgifter – lyfts fram. Myndighetens uppdrag, huvuduppgifter och befogenheter regleras i ramlagen. En viktig utgångspunkt är att tillsynsmyndighetens oberoende ska värnas, vilket görs bäst om det inte regleras när och hur tillsyn ska inledas respektive avslutas och hur den ska bedrivas.

Tillsynsmyndigheten ska utöva allmän tillsyn över personuppgiftsbehandling, handlägga klagomål från registrerade, på begäran av fysiska personer kontrollera om deras personuppgifter behandlas författningsenligt, på begäran bistå utländska tillsynsmyndigheter och ge råd och stöd åt personuppgiftsansvariga och personuppgiftsbiträden.

Tillsynsmyndighetens undersökningsbefogenheter, som inkluderar rätt att få tillgång till personuppgifter som behandlas och dokumentation om behandlingen och om säkerhets- och skyddsåtgärder, tillträde till lokaler där personuppgifter behandlas och rätt till biträde av den personuppgiftsansvarige eller personuppgiftsbiträdet vid tillsynen, blir tydligare.

Det görs också tydlig skillnad mellan tillsynsmyndighetens förebyggande och korrigerande befogenheter. Till de förebyggande befogenheterna, som inte är bindande, hör råd, rekommendationer och påpekanden. Tillsynsmyndigheten får också möjlighet att utfärda skriftlig varning om att det finns risk för att viss behandling kan komma att stå i strid med regelverket.

Till de korrigerande befogenheterna, som är bindande för den personuppgiftsansvarige eller personuppgiftsbiträdet, hör förelägganden, förbud mot fortsatt behandling och beslut om sanktionsavgift.

Tillsynsmyndighetens internationella samarbete regleras också i ramlagen. I anslutning till det föreslås en sekretessbrytande regel som ger myndigheten möjlighet att, om det ligger i svenskt intresse, lämna ut uppgifter som är sekretessbelagda när tillsynsmyndigheten begär bistånd av en utländsk tillsynsmyndighet. Vidare föreslås en ny sekretessregel som ska gälla hos tillsynsmyndigheten i tillsynsverksamhet enligt lagen för uppgifter som en utländsk tillsynsmyndighet har lämnat i samband med en begäran om svenskt bistånd med tillsyn. Sekretessen gäller om det kan antas att möjligheterna för den svenska tillsynsmyndigheten att bedriva tillsyn motverkas om uppgiften röjs.

Sanktioner

Utredningen anser att överträdelser av bestämmelserna om personuppgiftsbehandling i ramlagen inte ska straffsanktioneras. Det ska i stället införas en ny administrativ sanktion i form av sanktionsavgift. Det motsvarar vad som gäller vid överträdelse av bestämmelserna i dataskyddsförordningen.

Sanktionsavgift får tas ut av personuppgiftsansvariga och i vissa fall av personuppgiftsbiträden. Sanktionsavgift får tas ut av personuppgiftsansvariga vid överträdelse av de grundläggande bestämmelserna till skydd för enskildas integritet. Det gäller bl.a. om personuppgifter behandlas utan rättslig grund eller utan ett särskilt angivet och berättigat ändamål, om personuppgifterna inte uppfyller kraven på att vara korrekta, aktuella, adekvata och relevanta eller om fler uppgifter än nödvändigt behandlas eller om de behandlas längre än vad som är nödvändigt med hänsyn till ändamålen. Det gäller också om den personuppgiftsansvarige inte vidtar tillräckliga säkerhets- och skyddsåtgärder eller om personuppgifter överförs till tredjeland eller internationella organisationer i strid med regelverket.

Sanktionsavgift får också tas ut om den personuppgiftsansvarige inte bistår tillsynsmyndigheten vid tillsyn eller inte rättar sig efter tillsynsmyndighetens förelägganden eller beslut.

Regleringen av sanktionsavgift bygger på strikt ansvar, men sanktionsavgift behöver inte tas ut vid varje överträdelse. Vid bedömningen av om sanktionsavgift ska tas ut och till vilket belopp den ska bestämmas ska särskild hänsyn tas till bl.a. om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet och vad som gjorts för att begränsa skadan.

Sanktionsavgiften ska bestämmas till lägst 25 000 kronor och högst 10 000 000 kronor för mindre allvarliga överträdelser och det dubbla vid andra överträdelser.

Tillsynsmyndigheten ska besluta om sanktionsavgift och sanktionsavgiften ska tillfalla staten.

Rättsmedel och skadestånd

Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning som behandling av personuppgifter i strid med ramlagen med tillhörande förordning har orsakat. Jämkning av skadeståndsskyldigheten ska, i motsats till vad som är fallet i dag, inte vara möjlig.

Vissa beslut som en myndighet fattat i egenskap av personuppgiftsansvarig ska kunna överklagas. Det gäller beslut i fråga om rättelse, komplettering, radering eller begränsning av behandlingen, beslut att inte lämna ut information på begäran av en registrerad, att ta ut avgift för sådan information eller att inte medge omprövning av automatiserade beslut. Regleringen motsvarar i allt väsentligt det som gäller i dag.

Tillsynsmyndighetens beslut enligt lagen får också överklagas.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd vid överklagande av både personuppgiftsansvariga myndigheters och tillsynsmyndighetens beslut.

Det införs också en möjlighet för registrerade att föra s.k. dröjsmålstalan om tillsynsmyndigheten dröjer med att handlägga klagomål. Om en registrerad har lämnat in ett klagomål till tillsynsmyndigheten och den inte inom tre månader har tagit ställning till om klagomålet ska föranleda tillsyn, har den registrerade rätt att inom två veckor antingen få ett skriftligt besked i den frågan eller ett särskilt beslut om att begäran om besked avslås. Om tillsynsmyndigheten har avslagit begäran får den registrerade överklaga beslutet till allmän förvaltningsdomstol. Om domstolen bifaller talan ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna den registrerade besked i frågan om tillsyn kommer att utövas. Domstolen ska däremot inte ta ställning i frågan om tillsyn ska utövas.

Överföring till tredjeland och internationella organisationer

I ramlagen regleras vad som ska gälla vid överföring av personuppgifter till tredjeland och internationella organisationer. Med tredjeland avses i lagen andra stater än EU:s medlemsstater, Island, Liechtenstein, Norge och Schweiz.

Behöriga myndigheter får överföra personuppgifter som behandlas automatiserat till ett tredjeland eller en internationell organisation eller överföra uppgifterna dit för att de ska behandlas automatiserat där. Det ställs upp en rad villkor för att uppgifterna ska få överföras. Personuppgifter får endast överföras om överföringen är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Överföringen ska enligt huvudregeln riktas till en behörig myndighet i ett tredjeland eller en internationell organisation som är en behörig myndighet. Dessutom krävs det att kommissionen har meddelat ett beslut om att det tredjelandet eller den internationella organisationen har adekvat skyddsnivå för personuppgifter eller, om det inte finns ett sådant beslut, personuppgifterna omfattas av tillräckliga skyddsåtgärder. I vissa särskilda undantagssituationer får dock personuppgifter överföras även om det inte finns ett beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder. Det gäller bl.a. om det är nödvändigt för att skydda den registrerades eller en annan fysisk persons vitala intressen, för att en behörig myndighet i ett enskilt fall ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller för att avvärja en omedelbar eller allvarlig fara för allmän säkerhet.

Vidare regleras vad som ska göras om ett tredjeland eller en internationell organisation vill vidareöverföra personuppgifter till ett tredjeland eller en internationell organisation och möjligheten att i vissa fall överföra personuppgifter till andra än behöriga myndigheter.

Konsekvenser

Förslagen bedöms förbättra skyddet för enskildas integritet. Förbättrat dataskydd ger samtidigt möjlighet till ökat informationsutbyte mellan brottsbekämpande myndigheter både nationellt och mellan medlemsstaterna, vilket är positivt för det brottsförebyggande arbetet. De ekonomiska konsekvenserna för berörda myndigheter bedöms rymmas inom de befintliga ekonomiska ramarna.

Ikraftträdande och övergångsbestämmelser

Den nya lagen föreslås träda i kraft den 1 maj 2018. Det krävs särskilda övergångsbestämmelser, dels för det nya sanktionssystemet, dels för mål och ärenden som rör behandlingen av personuppgifter som har påbörjats före lagens ikraftträdande men inte hunnit slutföras. Det krävs också övergångsbestämmelser för mål som har överklagats men inte hunnit slutföras och för ersättning för skador som har vållats före ikraftträdandet.

Förslag till brottsdatalag (2018:000)

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (dataskyddsdirektivet).

Lagens tillämpningsområde

2 § Denna lag gäller för behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också för behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

3 § Lagen gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

4 § Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Avvikande bestämmelser i annan författning

5 § Om det i en annan lag eller en förordning finns bestämmelser som avviker från denna lag, ska de bestämmelserna gälla.

Uttryck i lagen

6 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Behörig myndighet	1. En myndighet som har till uppgift att a) förebygga, förhindra eller upptäcka brottslig verksamhet, b) utreda eller lagföra brott, c) verkställa straffrättsliga påföljder, eller d) upprätthålla allmän ordning och säkerhet, eller 2. en annan aktör som utövar myndighet för något av de syften som anges i 1.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.
Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av

	en överenskommelse mellan två eller flera stater.
Medlemsstat	En stat som är medlem i Europeiska unionen och Island, Liechtenstein, Norge och Schweiz.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.
Registrerad	Den fysiska person som personuppgiften rör.
Tillsynsmyndighet	Myndighet som regeringen utser att enligt dataskyddsdirektivet utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.
Tredjeland	En stat som inte är en medlemsstat.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgift som rör hälsa	Personuppgift som rör en per-

sons fysiska eller psykiska hälsa, inkluderande information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

2 kap. Behandling av personuppgifter

Behandling för ändamål inom denna lags tillämpningsområde

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa en straffrättslig påföljd eller upprätthålla allmän ordning och säkerhet. Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt den behöriga myndigheten att ansvara för en sådan uppgift.

2 § Utöver vad som sägs i 1 § får personuppgifter behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Ändamål för behandling av personuppgifter

3 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.

Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

4 § Innan personuppgifter får behandlas för ett nytt ändamål inom denna lags tillämpningsområde ska det säkerställas att

1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen, och
2. behandlingen är nödvändig och proportionerlig för det nya ändamålet.

5 § En behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Grundläggande krav på behandlingen av personuppgifter

Laglig och korrekt behandling

6 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifters kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Åtskillnad mellan olika slag av personuppgifter

9 § Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade, som personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott, särskiljas. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

10 § Så långt det är möjligt ska personuppgifter som grundar sig på fakta skiljas från personuppgifter som grundar sig på personliga bedömningar. Om grunden inte framgår av sammanhanget eller på annat sätt ska den tydliggöras genom en särskild upplysning.

Känsliga personuppgifter

11 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket när det är absolut nödvändigt för ändamålet med behandlingen.

12 § Biometriska uppgifter som används för att identifiera en person och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

13 § Personuppgifter som avses i 11 och 12 §§ betecknas i denna lag som känsliga personuppgifter. Känsliga personuppgifter får behandlas med stöd av 2 §.

14 § Det är förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter.

Åtgärder för att säkerställa personuppgifternas kvalitet

15 § Alla rimliga åtgärder ska vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

När personuppgifter lämnas ut till en behörig myndighet ska mottagaren så långt det är möjligt ges information som gör det möjligt att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga.

16 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1, 2, 3 § första stycket, 4–6, 8, 11, 12, 14 eller 17 § första stycket utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska den personuppgiftsansvarige i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Längsta tid som personuppgifter får behandlas

17 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

18 § Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för andra ändamål än arkivändamål, ska den personuppgiftsansvarige årligen se över behovet av att fortsatt behandla personuppgifterna.

Automatiserade beslut

19 § Om ett beslut, som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne, enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet omprövat av någon person.

Automatiserade beslut får inte enbart grundas på känsliga personuppgifter.

Villkor om användningsbegränsning

20 § Om det inte är särskilt föreskrivet får villkor för behandling av personuppgifter inte ställas upp i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om det inte i motsvarande fall får ställas upp samma typ av villkor i förhållande till en svensk mottagare.

Behandling för ändamål utanför denna lags tillämpningsområde

21 § Av artikel 2.1 d i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, framgår att dataskyddsförord-

ningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför denna lags tillämpningsområde.

Föreskrifter

22 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. underrättelseskyldighet, eller
2. åtgärder för att säkerställa att personuppgifter inte behandlas längre än nödvändigt.

3 kap. Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

1 § Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

2 § Den personuppgiftsansvarige ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

3 § Både vid beslut om hur behandlingen ska utföras och vid behandlingen ska den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder, se till att dataskyddsprinciper säkerställs på ett effektivt sätt och att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

4 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem som regel endast är möjligt att behandla de personuppgifter som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

5 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

6 § Den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

7 § Kan en typ av ny behandling, eller betydande förändringar avseende redan pågående behandling, antas medföra särskild risk för intrång i registrerades personliga integritet, ska den personuppgiftsansvarige innan

behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Säkerheten för personuppgifter

Skyddsåtgärder

8 § Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Personuppgiftsincidenter

9 § Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten rör nationell säkerhet.

Anmälan behöver inte göras om det kan antas att personuppgiftsincidenten inte har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

10 § Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten.

Underrättelseskyldigheten enligt första stycket gäller inte om den personuppgiftsansvarige

1. har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av incidenten,
2. har säkerställt att det inte längre finns särskild risk för otillbörligt intrång i registrerades personliga integritet, eller
3. skulle behöva göra oproportionerliga ansträngningar för att underrätta alla berörda.

I fall som avses i andra stycket 3 ska allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade får nödvändig information.

11 § Den personuppgiftsansvarige får underlåta att lämna information enligt 10 § i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. annans fri- och rättigheter skyddas.

Första stycket gäller även för en personuppgiftsansvarig som inte är en myndighet i motsvarande fall som avses i offentlighets- och sekretesslagen (2009:400).

Samarbete med tillsynsmyndigheten

12 § Den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till den.

Dataskyddsombud

13 § Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

14 § Dataskyddsombud ska

1. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge den personuppgiftsansvarige råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

15 § Om den personuppgiftsansvarige bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

16 § [Tystnadsplikt för dataskyddsombud]

Personuppgiftsbiträden

17 § Den personuppgiftsansvarige får, om det är lämpligt, anlita personuppgiftsbiträden. När ett personuppgiftsbiträde anlitas, ska den personuppgiftsansvarige försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter.

18 § Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde får inte utan skriftligt tillstånd av den personuppgiftsansvarige anlita ett annat personuppgiftsbiträde.

19 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Om ett personuppgiftsbiträde i strid med den personuppgiftsansvariges instruktioner fastställer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

20 § Det som sägs om den personuppgiftsansvariges skyldigheter i 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden.

Gemensamt personuppgiftsansvar

21 § Två eller flera behöriga myndigheter får vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Bemyndigande

22 § Regeringen får meddela föreskrifter om skyldigheten att föra register över kategorier av behandling av personuppgifter och skyldigheten att införa interna rutiner för anmälan av överträdelser.

Föreskrifter

23 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. åtgärder som avses i 2–5, 7 och 8 §§,
2. tillgången till personuppgifter,
3. anmälan om personuppgiftsincidenter,
4. underrättelser till registrerade om personuppgiftsincidenter, och
5. innehållet i avtal och överenskommelser enligt 18 §.

4 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Den personuppgiftsansvarige ska göra följande allmänna information tillgänglig för registrerade.

1. Den personuppgiftsansvariges identitet och kontaktuppgifter.
2. Dataskyddsombudets kontaktuppgifter.
3. Ändamålen med behandlingen.
4. Rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§.
6. Möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

2 § Den personuppgiftsansvarige ska i specifika fall lämna följande information till den registrerade, om det behövs för att han eller hon ska kunna ta tillvara sina rättigheter.

1. Den rättsliga grunden för behandlingen.
2. Kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer.
3. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
4. Övrig nödvändig information.

Vid bedömningen av om information enligt första stycket 4 ska lämnas ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap.

3 § Den personuppgiftsansvarige ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om sökanden som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§.
8. Möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

4 § Den som har varit föremål för ett sådant beslut som avses i 2 kap. 19 § får av den personuppgiftsansvarige begära närmare information om beslutet.

Begränsning av rätten till information

5 § Informationsskyldigheten i 2 och 3 §§ gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. annans fri- och rättigheter skyddas.

Om förutsättningarna i första stycket är uppfyllda, är den personuppgiftsansvarige inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 9 eller 10 §.

Undantagen från informationsskyldigheten enligt första och andra styckena gäller även för en personuppgiftsansvarig som inte är en myndighet i motsvarande fall som avses i offentlighets- och sekretesslagen (2009:400).

6 § Informationsskyldigheten i 3 § gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje man, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

7 § Om en begäran enligt 3 § är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Av 12 § andra stycket framgår att den personuppgiftsansvarige i vissa fall får ta ut avgift i stället för att avslå begäran.

Möjligheten att begära kontroll genom tillsynsmyndigheten

8 § I 5 kap. 3 § finns bestämmelser om att en fysisk person får begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt.

Rätten till rättelse, radering och begränsning av behandlingen

9 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

10 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne om de behandlas i strid med 2 kap. 1, 2, 3 § första stycket, 4–6, 8, 11, 12, 14 eller 17 § första stycket. Detsamma gäller om radering krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

11 § Den personuppgiftsansvarige avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

12 § Information enligt 1, 2 och 4 §§ ska lämnas utan avgift. Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 3 § oftare än en gång per år, får den personuppgiftsansvarige ta ut en rimlig avgift eller avslå begäran enligt 7 § första stycket.

Föreskrifter

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. information enligt 1–4 §§,
2. avgift för information som avses i 3 §, och
3. kraven på en begäran enligt 3, 4, 9 eller 10 §.

5 kap. Tillsyn

Tillsynsmyndighetens uppdrag

1 § Tillsynsmyndigheten ska verka både för att fysiska personers grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom denna lags tillämpningsområde.

Tillsynsmyndighetens uppgifter

2 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling,
2. handlägga klagomål från registrerade,
3. utföra kontroll enligt 3 §, och
4. på begäran bistå en tillsynsmyndighet i en annan medlemsstat.

3 § Tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär sådan kontroll ska visa att han eller hon har begärt information enligt 4 kap. 3 § eller en åtgärd enligt 4 kap. 9 eller 10 §.

Myndigheten får vägra att utföra sådan kontroll som avses i första stycket om begäran är orimlig eller uppenbart ogrundad.

4 § Tillsynsmyndigheten ska ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd och när det i övrigt är påkallat.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

5 § Tillsynsmyndigheten har rätt att av personuppgiftsansvariga och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

6 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

7 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 6 § första stycket försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
3. förbjuda fortsatt behandling om bristen är allvarlig, eller
4. besluta om sanktionsavgift enligt 6 kap.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Kommunikation

8 § Innan tillsynsmyndigheten fattar ett beslut enligt 7 § första stycket 2–4, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

Besked angående handläggningen av ett klagomål

9 § Om tillsynsmyndigheten inte inom tre månader från den dag då ett klagomål kom in till myndigheten har tagit ställning till om tillsyn ska utövas i anledning av klagomålet, ska myndigheten på skriftlig begäran av den registrerade antingen lämna besked i den frågan eller i ett särskilt beslut avslå begäran.

Besked eller beslut enligt första stycket ska meddelas inom två veckor från den dag då begäran kom in till myndigheten.

10 § Om tillsynsmyndigheten har avslagit en begäran enligt 9 §, får den registrerade begära nytt besked tidigast tre månader efter det att myndighetens beslut meddelades. Om den registrerade innan dess på nytt begär besked avseende samma klagomål, ska myndigheten avvisa begäran.

Samarbete med tillsynsmyndigheter i andra medlemsstater

11 § En begäran om bistånd från en tillsynsmyndighet i en annan medlemsstat får vägras endast om det skulle strida mot en bindande unionsrättsakt, en lag eller en förordning att tillmötesgå den.

12 § När tillsynsmyndigheten utövar tillsyn enligt 2 § 4 har den de befogenheter som anges i 5–7 §§.

13 § Tillsynsmyndigheten får, om det är förenligt med svenska intressen, lämna ut en uppgift till en behörig tillsynsmyndighet i annan medlemsstat, även om uppgiften är sekretessbelagd enligt offentlighets- och sekretesslagen (2009:400).

14 § Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat får inte användas för något annat ändamål än det för vilket informationen begärdes.

Ansökan hos allmän förvaltningsdomstol

15 § Om tillsynsmyndigheten vid handläggningen av ett ärende bedömer att det finns särskilda skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av denna lag, får myndigheten hos allmän förvaltningsdomstol ansöka om att en åtgärd som anges i 7 § första stycket 2–4 ska vidtas.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Föreskrifter

16 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. kraven på en begäran enligt 3 §,
2. anmälningsskyldighet, och
3. samarbete med tillsynsmyndigheter i andra medlemsstater.

6 kap. Administrativa sanktionsavgifter

Överträdelser som kan föranleda sanktionsavgift

1 § Sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av bestämmelser i

1. 2 kap. 1–5, 7–12, 14–18 eller 19 § andra stycket,
2. 3 kap. 2–8 §§, eller
3. 8 kap. 1–6 eller 8 §.

Sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar sådana incidenter eller underlåter att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller att följa tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

2 § Sanktionsavgift får tas ut av ett personuppgiftsbiträde vid överträdelse av 3 kap. 5, 6 eller 8 §.

Sanktionsavgift får också tas ut om ett personuppgiftsbiträde underlåter att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Hur sanktionsavgiften ska bestämmas

3 § Sanktionsavgiften ska vid överträdelser av 3 kap. 6 eller 7 § eller av bestämmelser om dokumentation av personuppgiftsincidenter vara minst 25 000 kronor och högst 10 000 000 kronor.

Vid överträdelser av övriga bestämmelser som anges i 1 och 2 §§ ska avgiften vara minst 50 000 kronor och högst 20 000 000 kronor.

Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlingar, ska sanktionsavgiften bestämmas efter överträdelsernas allvar. Sanktionsavgiften får aldrig överstiga maximibeloppet för den allvarligaste överträdelsen.

4 § Vid bedömningen av om sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas ska särskild hänsyn tas till

1. om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa skadan, och
5. om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala sanktionsavgift.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift.

Beslut om sanktionsavgift

6 § Tillsynsmyndigheten beslutar om sanktionsavgift.

Sanktionsavgiften tillfaller staten.

7 § Sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Föreskrifter

8 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om handläggningen av beslut om och verkställighet av sanktionsavgift.

7 kap. Skadestånd och rättsmedel

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den, har orsakat.

Överklagande

Överklagande av beslut som fattats av en myndighet i egenskap av personuppgiftsansvarig

2 § Beslut i fråga om rättelse eller komplettering enligt 4 kap. 9 § första stycket, radering enligt 4 kap. 10 § första stycket, eller begränsning av behandlingen enligt 4 kap. 9 § andra stycket eller 10 § andra stycket, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 4 kap. 3 eller 4 §, att ta ut avgift enligt 4 kap. 12 § andra stycket eller att inte medge omprövning av ett automatiserat beslut enligt 2 kap. 19 § första stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Första stycket gäller inte beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

Dröjsmålstalan

3 § Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 5 kap. 9 § får överklagas till allmän förvaltningsdomstol.

Om domstolen bifaller överklagandet, ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna den registrerade besked i fråga om tillsyn kommer att utövas.

Domstolens beslut får inte överklagas.

Överklagande av andra beslut av tillsynsmyndigheten

4 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till den får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som inte får överklagas

5 § Andra beslut enligt denna lag än de som anges i 2–4 §§ får inte överklagas.

8 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Grundläggande förutsättningar för överföring

1 § En behörig myndighet får överföra personuppgifter som behandlas till ett tredjeland eller en internationell organisation. Det gäller även överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet, och
3. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 3 §, eller

b) tillräckliga skyddsåtgärder enligt 4 §, eller

c) ett undantag för särskilda situationer enligt 5 §.

En behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation ska särskilt beakta risken för att enskilda får försämrat skydd för sina personuppgifter.

2 § Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

Om medgivande enligt första stycket på grund av tidsbrist inte kan inhämtas i förväg, får personuppgifter ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller en annan medlemsstat.

Tillåtna grunder för överföring

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

4 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter, eller
2. den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får en överföring, eller en samling av överföringar, av personuppgifter göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. skydda den registrerades eller en annan fysisk persons vitala intressen, eller andra berättigade intressen för den registrerade,
2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller
4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Vidareöverföring

6 § En svensk behörig myndighet får inte tillåta att sådana personuppgifter som anges i 2 § första stycket, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation, om inte en behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras.

7 § När en behörig myndighet ska ta ställning till om personuppgifter som behandlats i Sverige och därefter lämnats till en annan medlemsstat, som överfört dem till ett tredjeland eller en internationell organisation, får vidareöverföras till ett tredjeland eller en internationell organisation, ska alla kända omständigheter som har samband med vidareöverföringen beaktas. Särskild vikt ska läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten och nivån på skyddet av personuppgifter i det tredjelandet eller hos den internationella organisationen dit uppgifterna ska vidareöverföras.

Överföring till andra än behöriga myndigheter

8 § En behörig myndighet, med undantag för en annan aktör som utövar myndighet, får i ett enskilt fall, trots kravet i 1 § 2, överföra personuppgifter till någon som inte är en behörig myndighet i ett tredjeland. Personuppgifterna får överföras endast om

1. det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en arbetsuppgift enligt 1 kap. 2 § som den har ansvar för,
2. den svenska myndigheten informerar den som ska ta emot personuppgifterna om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas, och
3. det skulle vara ineffektivt eller olämpligt att överföra dem till behörig myndighet i det tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Villkor om användningsbegränsning

9 § Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och gäller på grund av en överenskommelse med det tredjelandet eller den internationella organisationen villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

10 § En svensk behörig myndighet får, vid överföring av personuppgifter till ett tredjeland eller en internationell organisation, i ett enskilt fall ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt.

Föreskrifter

11 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. information till annan medlemsstat när personuppgifter överförts utan förhandsmedgivande enligt 2 § andra stycket,
2. information till behörig myndighet i tredjeland när personuppgifter överförts enligt 8 §, och
3. dokumentation av överföringar och information om sådana till tillsynsmyndigheten.

---

1. Denna lag träder i kraft den 1 maj 2018.
2. Genom lagen upphävs lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.
3. Bestämmelsen i 3 kap. 5 § om loggning behöver inte tillämpas på automatiserade behandlingssystem som inrättats före den 6 maj 2018 förrän den 1 maj 2023.
4. Sanktionsavgift enligt 6 kap. får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

5. För överträdelser av bestämmelser om personuppgiftsbehandling som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet som begåtts före ikraftträdandet gäller fortfarande äldre föreskrifter.

6. Ärenden om tillsyn över personuppgiftsbehandling och som Datainspektionen eller Säkerhets- och integritetsskyddsnämnden inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.

7. Äldre föreskrifter gäller fortfarande för överklagande av beslut som meddelats före ikraftträdandet och som rör behandling av personuppgifter för brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet.

8. Bestämmelserna om skadestånd i 48 § i personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats vid behandling av personuppgifter som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet före ikraftträdandet.

Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs att 5 kap. 2 § lagen (2000:562) om internationell rättslig hjälp i brottmål ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 kap.	
2 §[1]	
Rättslig hjälp som lämnas en annan stat enligt denna lag får i enskilda fall förenas med villkor som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt. Detsamma gäller när rättslig hjälp, utan samband med ett ärende, lämnas en annan stat i form av uppgifter och bevisning för att användas vid utredning av brott eller i ett rättsligt förfarande med anledning av brott.	
Villkor som avses i första stycket får inte ställas upp om de strider mot en internationell överenskommelse som är bindande för Sverige.	Villkor som avses i första stycket får inte ställas upp om de strider mot en internationell överenskommelse som är bindande för Sverige. *I brottsdatalagen (2018:000) finns bestämmelser om att villkor om hur personuppgifter får behandlas inte får ställas upp i vissa fall.*

Denna lag träder i kraft den 1 maj 2018.

[1] Senaste lydelse 2005:491.

Förslag till
lag om ändring i lagen (2000:1219) om internationellt tullsamarbete

Härigenom föreskrivs att 2 kap. 7 § lagen (2000:1219) om internationellt tullsamarbete ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
7 §	
Uppgifter som lämnas ut enligt 6 § får i enskilda fall förenas med villkor för användandet, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt.	
Villkor som avses i första stycket får inte strida mot en sådan internationell överenskommelse som avses i 1 kap. 1 §.	Villkor som avses i första stycket får inte strida mot en sådan internationell överenskommelse som avses i 1 kap. 1 §. *I brottsdatalagen (2018:000) finns bestämmelser om att villkor om hur personuppgifter får behandlas inte får ställas upp i vissa fall.*

Denna lag träder i kraft den 1 maj 2018.

Förslag till lag om ändring i lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar

Härigenom föreskrivs att 6 § lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 §[1]	
Överlämnande av uppgifter eller bevisning från en svensk myndighet till en gemensam utredningsgrupp som inrättats med stöd av denna lag får i enskilda fall förenas med villkor som är nödvändiga av hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt.	
Villkor som avses i första stycket får inte ställas upp om de strider mot den överenskommelse enligt 1 § första stycket som är tillämplig.	Villkor som avses i första stycket får inte ställas upp om de strider mot den överenskommelse enligt 1 § första stycket som är tillämplig. *I brottsdatalagen (2018:000) finns bestämmelser om att villkor om hur personuppgifter får behandlas inte får ställas upp i vissa fall.*

Denna lag träder i kraft den 1 maj 2018.

[1] Senaste lydelse 2005:494.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 9 kap. 2 § och 35 kap. 24 § ska ha följande lydelse,

dels att det i lagen ska införas två nya paragrafer, 17 kap. 7 c § och 35 kap. 4 b §, med följande lydelse.

Lydelse enligt prop. 2016/17:139

9 kap.

2 §

Bestämmelser som begränsar möjligheten att använda vissa uppgifter som en svensk myndighet har fått från en myndighet i en annan stat finns i

1. lagen (1990:314) om ömsesidig handräckning i skatteärenden,
2. lagen (2017:000) om internationellt polisiärt samarbete,
3. lagen (2000:344) om Schengens informationssystem,
4. lagen (2000:562) om internationell rättslig hjälp i brottmål,
5. lagen (2000:1219) om internationellt tullsamarbete,
6. lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar,
7. lagen (2011:1537) om bistånd med indrivning av skatter och avgifter inom Europeiska unionen,
8. lagen (1998:620) om belastningsregister,
9. lagen (2012:843) om administrativt samarbete inom Europeiska unionen i fråga om beskattning,
10. lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen,
11. lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet, *och*
12. lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton.

Föreslagen lydelse

9 kap.

2 §

Bestämmelser som begränsar möjligheten att använda vissa uppgifter som en svensk myndighet har fått från en myndighet i en annan stat finns i

1. lagen (1990:314) om ömsesidig handräckning i skatteärenden,
2. lagen (2017:000) om internationellt polisiärt samarbete,
3. lagen (2000:344) om Schengens informationssystem,
4. lagen (2000:562) om internationell rättslig hjälp i brottmål,
5. lagen (2000:1219) om internationellt tullsamarbete,
6. lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar,
7. lagen (2011:1537) om bistånd med indrivning av skatter och avgifter inom Europeiska unionen,
8. lagen (1998:620) om belastningsregister,
9. lagen (2012:843) om administrativt samarbete inom Europeiska unionen i fråga om beskattning,
10. lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet,
11. lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton, *och*
12. *brottsdatalagen (2018:000).*

Nuvarande lydelse

17 kap.

7 c §

Sekretess gäller hos tillsynsmyndigheten i tillsynsverksamhet enligt 5 kap. brottsdatalagen (2018:000) för uppgift som har lämnats i sam-

Föreslagen lydelse

band med en begäran om svenskt bistånd från en tillsynsmyndighet i en medlemsstat som medlemsstat definieras i den lagen, om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

35 kap.

4 b §

Sekretess gäller hos en behörig myndighet enligt brottsdatalagen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag.

För uppgift i en allmän handling gäller sekretessen högst sjuttio år.

24 §

Den tystnadsplikt som följer av 4 b § inskränker rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 11 § och den tystnadsplikt som följer av ett förbehåll som gjorts med stöd av 9 § andra stycket inskränker *rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen* att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 11 § och den tystnadsplikt som följer av ett förbehåll som gjorts med stöd av 9 § andra stycket inskränker rätten att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 15 och 16 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift vars röjande kan antas medföra fara för att någon utsätts för våld eller lider annat allvarligt men.

Denna lag träder i kraft den 1 maj 2018.

Förslag till
lag om ändring i lagen (2017:000) om internationellt polisiärt samarbete

Härigenom föreskrivs i fråga om lagen (2017:000) om internationellt polisiärt samarbete

dels att 6 kap. 2 § ska upphöra att gälla,

dels att 6 kap. 4 § ska ha följande lydelse.

Lydelse enligt prop. 2016/17:139	*Föreslagen lydelse*
6 kap.	
4 §	
En svensk brottsbekämpande myndighet får i enskilda fall ställa upp villkor som begränsar möjligheten att använda uppgifter eller bevisning som lämnas till en annan stat eller en mellanfolklig organisation, om det krävs med hänsyn till enskildas rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.	En svensk brottsbekämpande myndighet får i enskilda fall ställa upp villkor som begränsar möjligheten att använda uppgifter eller bevisning som lämnas till en annan stat eller en mellanfolklig organisation, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige. *I brottsdatalagen (2018:000) finns bestämmelser om att villkor om hur personuppgifter får behandlas inte får ställas upp i vissa fall.*

Denna lag träder i kraft den 1 maj 2018.

Förteckning över remissinstanserna (SOU 2017:29)

Följande remissinstanser har kommit in med yttrande över SOU 2017:29 Brottsdatalag: Riksdagens ombudsmän, Svea hovrätt, Hovrätten för Västra Sverige, Södertörns tingsrätt, Eskilstuna tingsrätt, Helsingborgs tingsrätt, Umeå tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Linköping, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Övervakningsnämnd Stockholm Centrum, Brottsförebyggande rådet, Brottsoffermyndigheten, Rättsmedicinalverket, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Migrationsverket, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Försäkringskassan, Socialstyrelsen, Inspektionen för vård och omsorg, Statens institutionsstyrelse, Pensionsmyndigheten. Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Länsstyrelsen Skåne, Länsstyrelsen Stockholm, Länsstyrelsen Värmland, Länsstyrelsen Västernorrland, Stockholms läns landsting, Västerbottens läns landsting, Avesta kommun, Göteborgs kommun, Laholms kommun, Luleå kommun, Malmö kommun, Norrköpings kommun, Sala kommun, Stockholms kommun, Åmåls kommun, Statskontoret, Uppsala universitet, juridiska fakulteten, Umeå universitet, juridiska institutionen, Naturvårdsverket, Havs- och vattenmyndigheten, Post- och telestyrelsen, Sjöfartsverket, Riksarkivet, Sveriges advokatsamfund. Sveriges Akademikers Centralorganisation (SACO) och Sacoförbundet Sveriges läkarförbund, Arbetsgivarverket, Sveriges Kommuner och Landsting (SKL), Svenska Journalistförbundet, Tidningsutgivarna, dataskydd.net.

Följande remissinstanser har avstått från att yttra sig respektive inte hörts av: Blekinge läns landsting, Alingsås kommun, Borgholms kommun, Danderyds kommun, Falu kommun, Hallstahammars kommun, Helsingborgs kommun, Karlstads kommun, Kiruna kommun, Lycksele kommun, Ronneby kommun, Sandvikens kommun, Sundsvalls kommun, Tierps kommun, Tranås kommun, Trelleborgs kommun, Uppsala kommun, Värnamo kommun, Växjö kommun, Örebro kommun, Östersunds kommun, Landsorganisationen i Sverige (LO), Tjänstemännens centralorganisation (TCO), Svenskt Näringsliv, Sveriges Förenade Ordningsvakter, IT&Telekomföretagen, Civil Rights Defenders.

Uppdraget

Europeiska unionen har enats om en genomgripande dataskyddsreform som ska vara genomförd under våren 2018. Reformen omfattar dels en allmän dataskyddsförordning, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet. En konsekvens av reformen är att personuppgiftslagen kommer att upphävas och att all lagstiftning om personuppgiftsbehandling behöver ses över och anpassas.

Utredningens uppdrag är att föreslå hur det nya direktivet ska genomföras i svensk rätt genom en ny ramlagstiftning och att anpassa registerförfattningarna för myndigheterna i rättskedjan till de nya förutsättningarna. Utredningen ska också överväga om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat.

Brottsdatalagen förutsätter en ny struktur

I delbetänkandet Brottsdatalag (SOU 2017:29) föreslår utredningen en ny lag, brottsdatalagen, som kommer att fylla ungefär samma funktion som personuppgiftslagen gör i dag i verksamhet som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet. I brottsdatalagen finns de grundläggande bestämmelserna om hur personuppgifter får behandlas. Där regleras även personuppgiftsansvarigas skyldigheter, enskildas rättigheter och tillsynen över personuppgiftsbehandling. Brottsdatalagen innehåller vidare bestämmelser om administrativa sanktionsavgifter, skadestånd och rättsmedel.

Registerförfattningarna för myndigheterna i rättskedjan utgår i dag från personuppgiftslagen, antingen genom att registerförfattningen gäller i stället för personuppgiftslagen men hänvisar till bestämmelser i den eller genom att registerförfattningen gäller utöver personuppgiftslagen. Utredningen föreslår att registerförfattningarna ska gälla utöver brottsdatalagen och innehålla bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i den lagen. Bestämmelser i registerförfattningarna om bl.a. syfte, automatiserad behandling, personuppgiftsombud, behandling av känsliga personuppgifter och tillgången till personuppgifter ska därför upphävas. Det föranleder omfattande redaktionella ändringar i registerförfattningarna.

De registerförfattningar som reglerar personuppgiftsbehandling både inom och utanför brottsdatalagens tillämpningsområde renodlas så att de bara gäller vid personuppgiftsbehandling inom tillämpningsområdet. Det gäller lagen om behandling av personuppgifter inom kriminalvården, kustbevakningsdatalagen och åklagardatalagen. För domstolarna skapas i stället en ny lag för den personuppgiftsbehandling som ligger inom tillämpningsområdet. För att det ska vara tydligt att registerförfattningarna gäller utöver brottsdatalagen ges de nya namn.

Anpassningar och andra ändringar i de brottsbekämpande myndigheternas registerförfattningar

Tillämpningsområdet

I dag utgår tillämpningsområdet i de brottsbekämpande myndigheternas registerförfattningar från i vilken verksamhet personuppgiftsbehandlingen utförs. Det som kommer att bli avgörande för tillämpningen är i stället dels om myndigheten agerar i egenskap av behörig myndighet enligt brottsdatalagen, dels i vilket syfte personuppgifterna behandlas. Tillämpningsområdet blir därmed smalare än i dag, eftersom inte all personuppgiftsbehandling som utförs inom ramen för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet omfattas, t.ex. utlämnande av allmänna handlingar enligt tryckfrihetsförordningen eller för ändamål utanför brottsdatalagens tillämpningsområde.

Tillåtna rättsliga grunder och behandling för nya ändamål

Regleringen av för vilka ändamål de brottsbekämpande myndigheterna får behandla personuppgifter är i dag uppdelad i primära och sekundära ändamål. Regleringen föreslås i stort sett vara oförändrad när det gäller de primära ändamålen men det tydliggörs att det är fråga om bestämmelser om rättslig grund.

Innan personuppgifter behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt brottsdatalagen alltid prövas om det finns en tillåten rättslig grund för den nya behandlingen och om den är nödvändig och proportionerlig för det nya ändamålet. Det behöver däremot inte prövas om det nya ändamålet är förenligt med det ursprungliga. När personuppgifter behandlas för ändamål utanför tillämpningsområdet ska dataskyddsförordningen tillämpas. Utredningen föreslår att en prövning av nödvändighet och proportionalitet ska göras även innan personuppgifter behandlas för ändamål utanför brottsdatalagens tillämpningsområde. Någon prövning behöver dock inte göras om skyldighet att lämna uppgifter följer av lag eller förordning. Uppräkningen i de sekundära ändamålsbestämmelserna av i vilka situationer personuppgifter får tillhandahållas ersätts alltså av en särskild prövning både vid behandling för ändamål inom och utanför brottsdatalagens tillämpningsområde.

Behandling av känsliga personuppgifter

Brottsdatalagen förbjuder sökningar i personuppgifter i syfte att få fram ett personurval grundat på känsliga personuppgifter. I registerförfattningarna ska det göras undantag från förbudet som är anpassade till respektive myndighets behov av att kunna behandla känsliga personuppgifter. Brottsbekämpande myndigheter ska få använda t.ex. uppgifter som beskriver en persons utseende eller brottsrubriceringar ska vara tillåtet vid sökning i alla slags personuppgifter. Vid sökning i uppgifter som inte är gemensamt tillgängliga, dvs. som bara ett fåtal personer har tillgång till, ska sökning i syfte att ta fram personurval grundade på vissa känsliga personuppgifter få göras.

Längsta tid för behandling

I registerförfattningarna finns det bestämmelser om bevarande och gallring. De syftar till att skydda den personliga integriteten och reglerar inte bevarande och gallring i arkivlagens mening. De ska därför formuleras om så att det framgår att det är fråga om dataskyddsbestämmelser. Regleringen ska utgå från hur länge personuppgifter får behandlas. Någon ändring av hur länge olika typer av personuppgifter får behandlas görs i princip inte.

Utökade möjligheter till elektroniskt utlämnande

Regleringen av i vilken utsträckning personuppgifter får lämnas ut på medium för automatiserad behandling moderniseras för att möta de ökade behoven av att kunna kommunicera elektroniskt. Det blir tillåtet att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Viss reglering flyttas till registerförfattningarna

Bestämmelserna om Polismyndighetens behandling av personuppgifter i registret över tillträdesförbud vid idrottsarrangemang flyttas till polisens brottsdatalag. Lagen om register över tillträdesförbud vid idrottsarrangemang renodlas så att den bara reglerar idrottsorganisationernas personuppgiftsbehandling.

Regleringen av Polismyndighetens, Säkerhetspolisens och Tullverkets behandling av personuppgifter som tillhandahålls av transportföretag flyttas till respektive myndighets registerförfattning.

En ny lag för domstolarna

Domstolsdatalagen reglerar i dag personuppgiftsbehandling både inom och utanför brottsdatalagens tillämpningsområde i domstolarnas rättskipande och rättsvårdande verksamhet. Den del av domstolarnas personuppgiftsbehandling som ligger inom tillämpningsområdet ska regleras i en ny lag, domstolarnas brottsdatalag. Den nya lagen utformas med domstolsdatalagen som mönster men anpassas till den systematik och terminologi som finns i övriga registerförfattningar inom brottsdatalagens tillämpningsområde. Vissa frågor som hittills reglerats i förordning lyfts upp i lagen.

Allmän domstol ska tillämpa lagen när personuppgifter behandlas i syfte att handlägga mål och ärenden om utredning av eller lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Allmän förvaltningsdomstol ska tillämpa lagen när personuppgifter behandlas i syfte att handlägga mål och ärenden om verkställighet av häktning eller straffrättsliga påföljder. Till skillnad från i dag omfattar tillämpningsområdet inte personuppgiftsbehandling i den administrativa verksamheten som avser att på begäran lämna ut uppgifter ur mål eller ärenden.

Innan domstolar behandlar personuppgifter för nya ändamål inom brottsdatalagens tillämpningsområde ska de pröva om behandlingen är nödvändig och proportionerlig för det nya ändamålet. Vid behandling för

nya ändamål utanför brottsdatalagens tillämpningsområde gäller dataskyddsförordningen. Någon prövning av om behandlingen är nödvändig och proportionerlig behöver inte göras om domstolsdatalagen ska tillämpas. En sådan prövning krävs däremot i andra fall, om inte skyldighet att lämna uppgifter följer av lag eller förordning.

Domstolarna ska inte tillämpa sökförbudet i brottsdatalagen. I stället ska motsvarande sökförbud som i domstolsdatalagen, som förbjuder användningen av uppgifter som avslöjar känsliga personuppgifter och uppgifter om brott eller misstanke om brott och nationell anknytning som sökbegrepp, gälla. Samma undantag från förbudet som finns i domstolsdatalagen ska gälla.

Regleringen av Kriminalvårdens personuppgiftsbehandling

Kriminalvårdens reglering har en annan struktur än övriga registerförfattningar, eftersom större delen finns i förordning. Regleringen anpassas till brottsdatalagen och blir mer lik övriga registerförfattningar. Utredningens uppdrag har dock inte omfattat att göra en total översyn av regleringen och någon ny lag föreslås därför inte, trots att alla bestämmelser ändras och lagen får en helt ny struktur.

Lagen ska tillämpas när kriminalvården behandlar personuppgifter i syfte att verkställa häktning eller straffrättsliga påföljder eller biträda andra behöriga myndigheter när de utför arbetsuppgifter som omfattas av brottsdatalagens tillämpningsområde eller för att fullgöra internationella åtaganden. På samma sätt som för de brottsbekämpande myndigheterna ska behandling för nya ändamål föregås av en prövning av om behandlingen är nödvändig och proportionerlig för det nya ändamålet, oavsett om ändamålet ligger inom eller utanför brottsdatalagens tillämpningsområde.

Regleringen av säkerhetsregistret flyttas till lagen, moderniseras och görs mer generell. Uppgifter om den som är häktad eller verkställer fängelsestraff ska få registreras om personen utgör en säkerhetsrisk. Även uppgifter om personer som en registrerad har viss anknytning till ska få behandlas om det är absolut nödvändigt. Om det finns risk för att någon som verkställer en påföljd inom kriminalvården utövar våld eller hot mot personer i kriminalvårdens lokaler ska uppgifter om honom eller henne också få behandlas i säkerhetsregistret. Det görs undantag från sökförbudet i brottsdatalagen för sökningar i säkerhetsregistret i syfte att få fram personurval grundat på vissa känsliga personuppgifter.

Bestämmelserna om Kriminalvårdens underrättelseskyldighet bryts ut ur registerförordningen och placeras i en ny förordning.

En ny lag för Säkerhetspolisen

Regleringen utgår från dagens reglering och brottsdatalagen

Utredningen föreslår att det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter, Säkerhetspolisens datalag, som ersätter regleringen i polisdatalagen. Den regleringen ska bilda mönster för den nya lagen, som ska vara heltäckande och därför blir betydligt mer omfat-

tande än dagens reglering. Den nya lagen följer i princip brottsdatalagens systematik och innehåll. Det innebär att bestämmelserna om grundläggande krav på behandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, rättsmedel och överföring av personuppgifter till tredjeland i stort sett överensstämmer med brottsdatalagens bestämmelser.

Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. När Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra brott ska myndigheten tillämpa brottsdatalagen och polisens brottsdatalag.

Rättslig grund för behandling av personuppgifter

Regleringen av för vilka ändamål Säkerhetspolisen får behandla personuppgifter är i dag uppdelad i primära och sekundära ändamål. Regleringen behålls i stort sett oförändrad men det tydliggörs att det är fråga om bestämmelser om rättslig grund – rättslig grund för behandling och rättslig grund för utlämnande.

Behandling av känsliga personuppgifter

Huvudregeln är att Säkerhetspolisen på samma sätt som i dag inte ska få behandla känsliga personuppgifter. Om uppgifter om en person redan behandlas ska de dock få kompletteras med känsliga personuppgifter om det är absolut nödvändigt.

Säkerhetspolisen får i dag använda uppgifter som avslöjar känsliga personuppgifter som sökbegrepp om det är absolut nödvändigt. Utredningen föreslår att samma sökförbud som i brottsdatalagen ska gälla för Säkerhetspolisen, dvs. att det ska vara förbjudet att göra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Från förbudet görs det undantag. Det ska vara tillåtet att använda brottsrubriceringar, uppgifter om tillvägagångssätt vid brott och uppgifter som beskriver en persons utseende vid sökning. Även sökningar i syfte att få fram personurval grundat på flertalet känsliga personuppgifter ska tillåtas, om sökningen är absolut nödvändig.

Elektroniskt utlämnande

Säkerhetspolisen ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Säkerhetspolisen ska få medge Polismyndigheten, Försvarsmakten och Försvarets radioanstalt direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften. Även underrättelse- och säkerhetstjänster inom EU och EES ska få medges direktåtkomst till uppgifter som Säkerhetspolisen behandlar för vissa syften om det behövs för samarbetet mot terrorism. Sådan direktåtkomst ska dock endast få medges till personuppgifter i en avskild uppgiftssamling och regeringen ska underrättas innan direktåtkomst medges.

Längsta tid för behandling

Personuppgifter ska inte få behandlas under längre tid än vad som behövs för något eller några av de syften för vilka Säkerhetspolisen får behandla personuppgifter. Huvudregeln ska på samma sätt som i dag vara att personuppgifter som har gjorts gemensamt tillgängliga inte får behandlas längre än tio år efter det år då den senaste registreringen avseende personen gjordes. Uppgifter om personer som ännu inte fyllt 18 år ska dock inte få behandlas längre än fem år från den senaste registreringen. Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken ska inte få behandlas längre än 40 år efter det år då den senaste registreringen gjordes. På samma sätt som i dag ska Säkerhetspolisen kunna besluta att personuppgifter får behandlas under längre tid om det finns särskilda skäl.

Tillsyn över Säkerhetspolisens personuppgiftsbehandling

Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden ska på i huvudsak samma sätt som i dag utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling.

Datainspektionen ska utöva allmän tillsyn över personuppgiftsbehandling enligt den nya lagen och ge råd och stöd till Säkerhetspolisen. Inspektionen ska i huvudsak ha samma befogenheter som enligt brottsdatalagen. Säkerhetspolisen ska dock inte kunna påföras administrativ sanktionsavgift.

Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling och på begäran av enskild kontrollera om behandlingen av personuppgifter är författningsenlig.

Ikraftträdande och övergångsbestämmelser

De nya registerförfattningarna och ändringarna i de befintliga registerförfattningarna föreslås träda i kraft den 1 maj 2018. Det krävs särskilda övergångsbestämmelser för det nya sanktionssystemet och för ersättning för skador som har vållats före ikraftträdandet. Till de nya lagarna krävs det övergångsbestämmelser dels för mål och ärenden som rör behandlingen av personuppgifter som har påbörjats före ikraftträdandet men inte hunnit slutföras, dels för mål som har överklagats men som inte har hunnit slutföras inom den tiden.

Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs att 1 b § lagen (1998:620)[1] om belastningsregister ska upphöra att gälla vid utgången av april 2018.

[1] Senaste lydelse av 1 b § 2013:331.

Förslag till lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs att 1 b § lagen (1998:621)[1] om misstankeregister ska upphöra att gälla vid utgången av april 2018

[1] Senaste lydelse av 1 b § 2013:332.

Förslag till
lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 2 och 18 §§, 35 kap. 1, 4 a, 4 b §, 10 och 10 b §§ och 37 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
2 §[1]	
Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. *7 § 1* eller *6 kap. 1 § 1 polisdatalagen* (2010:361), om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.	Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. *1 § första stycket 1 polisens brottsdatalag* (2010:361) eller 2 *kap. 1 § första stycket 1 Säkerhetspolisens datalag (2018:000)*, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.
Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till	Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till *sådan verksamhet som avses i*
1. *sådan verksamhet som avses i 2 kap. 5 § 1 skattebrottsdatalagen (2017:452)*,	1. *2 kap. 1 § första stycket 1 Kustbevakningens brottsdatalag (2012:145)*,
2. *sådan verksamhet som avses i* 2 kap. *5 § 1 tullbrottsdatalagen* (2017:447), eller	2. 2 kap. *1 § första stycket 1 Tullverkets brottsdatalag* (2017:447), eller
3. *sådan verksamhet som avses i 3 kap. 2 § 1 kustbevakningsdatalagen (2012:145)*.	3. *2 kap. 1 § första stycket 1 Skatteverkets brottsdatalag (2017:452)*.
Sekretess enligt första stycket gäller inte för uppgift som hänför sig till verksamhet hos Säkerhetspolisen och som har förts in i en allmän handling före år 1949.	
För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.	

[1] Senaste lydelse 2017:456.

18 §[2]

Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisdatalagen* (2010:361).

Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisens brottsdatalag* (2010:361).

Lydelse enligt prop. 2016/17:208

Föreslagen lydelse

35 kap.

1 §

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,

3. angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt *4* kap. *polisdatalagen* (2010:361) eller som annars behandlas med stöd av de bestämmelserna eller uppgifter som behandlas av Säkerhetspolisen med stöd av *6 kap. samma lag*,

5. register som förs av Polismyndigheten enligt *5* kap. *polisens brottsdatalag* (2010:361) eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen med stöd av *Säkerhetspolisens datalag (2018:000)*,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt *skattebrottsdatalagen* (2017:452) eller som annars behandlas där med stöd av samma lag,

7. register som förs av Skatteverket enligt *Skatteverkets brottsdatalag* (2017:452) eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, *eller*

9. register som förs av Tullverket enligt *tullbrottsdatalagen* (2017:447) eller som annars behandlas där med stöd av samma

9. register som förs av Tullverket enligt *Tullverkets brottsdatalag* (2017:447) eller som annars behandlas där med stöd av samma

[2] Senaste lydelse 2010:369.

lag, *eller*

10. register som förs enligt lagen (2010:362) om polisens allmänna spaningsregister.

lag.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Nuvarande lydelse	*Föreslagen lydelse*
4 a §[3]	
Sekretess gäller i verksamhet som avser förande av *register* enligt *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang* för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till *denne* lider men.	Sekretess gäller i verksamhet som avser förande av *tillträdesförbudsregistret* enligt *5 kap. polisens brottsdatalag (2010:361)* för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till *honom eller henne* lider men.
För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.	

Lydelse enligt SOU 2017:29	*Föreslagen lydelse*
4 b §	
Sekretess gäller hos en behörig myndighet enligt brottsdatalagen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag.	Sekretess gäller hos *1.* en behörig myndighet enligt brottsdatalagen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag, och *2. Säkerhetspolisen för uppgift i ett sådant personurval som avses i 2 kap. 12 § Säkerhetspolisens datalag (2018:000).*
För uppgift i en allmän handling gäller sekretessen högst sjuttio år.	För uppgift i en allmän handling gäller sekretessen *i* högst sjuttio år.

[3] Senaste lydelse 2015:53.

Nuvarande lydelse	*Föreslagen lydelse*
10 §[4]	
Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut	
1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,	
2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) *samt* i förordning som har meddelats med stöd i den lagen,	2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) *och* i förordning som har meddelats med stöd i den lagen,
	3. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken,
3. enligt vad som föreskrivs i	*4.* enligt vad som föreskrivs i
– lagen (1998:621) om misstankeregister,	
– *polisdatalagen* (2010:361),	– *polisens brottsdatalag* (2010:361),
– *skattebrottsdatalagen (2017:452),*	– *Kustbevakningens brottsdatalag (2012:145),*
– *tullbrottsdatalagen (2017:447),*	– *åklagarväsendets brottsdatalag (2015:433),*
– *kustbevakningsdatalagen (2012:145),*	– *Tullverkets brottsdatalag (2017:447),*
– *åklagardatalagen (2015:433),*	– *Skattverkets brottsdatalag (2017:452),*
	– *Säkerhetspolisens datalag (2018:000), eller*
– förordningar som har stöd i dessa lagar, *eller*	– förordningar som har stöd i dessa lagar.
4. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.	
10 b §[5]	
Sekretessen enligt 4 a § hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang*.	Sekretessen enligt 4 a § hindrar inte att en uppgift lämnas ut till en idrottsorganisation enligt vad som föreskrivs i 2 *kap. 14* § *polisens brottsdatalag (2010:361).*

[4] Senaste lydelse 2017:456.
[5] Senaste lydelse 2015:53.

37 kap.

7 §[6]

Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisdatalagen* (2010:361).	Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisens brottsdatalag* (2010:361).

1. Denna lag träder i kraft den 1 maj 2018.

2. Äldre bestämmelser gäller fortfarande för uppgifter i handlingar som har omhändertagits för arkivering före ikraftträdandet av denna lag.

[6] Senaste lydelse 2010:369.

Förslag till lag om ändring i brottsdatalagen (2018:000)

Härigenom föreskrivs i fråga om brottsdatalagen (2018:000)

dels att nuvarande 2 kap. 21 § ska betecknas 2 kap. 22 § och att rubriken före nuvarande 2 kap. 21 § ska placeras före nya 2 kap. 22 §, nuvarande 2 kap. 22 § ska betecknas 2 kap. 23 § och att rubriken före nuvarande 2 kap. 22 § ska placeras före nya 2 kap. 23 §,

dels att 2 kap. 4, 13 och 18 §§, 6 kap. 1 § och nya 2 kap. 22 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 21 § och 3 kap. 16 §, och en ny rubrik före 2 kap. 21 § av följande lydelse.

Lydelse enligt SOU 2017:29	*Föreslagen lydelse*
2 kap.	
4 §	
Innan personuppgifter får behandlas för ett nytt ändamål inom denna lags tillämpningsområde ska det säkerställas att	
1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen, och	1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen och
2. behandlingen är nödvändig och proportionerlig för det nya ändamålet.	
	I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning behöver någon prövning enligt första stycket inte göras. Det gäller dock inte uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen.
13 §	
Personuppgifter som avses i 11 och 12 §§ betecknas *i denna lag* som känsliga personuppgifter. Känsliga personuppgifter får behandlas med stöd av 2 §.	Personuppgifter som avses i 11 och 12 §§ betecknas som känsliga personuppgifter. Känsliga personuppgifter får behandlas med stöd av 2 §.
18 §	
Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för *andra* ändamål *än arkivändamål*, ska den personuppgiftsansvarige årligen se över behovet av att fortsatt behandla personuppgifterna.	Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för ändamål *inom denna lags tillämpningsområde*, ska den personuppgiftsansvarige årligen se över behovet av att fortsatt behandla personuppgifterna.

Utlämnande av personuppgifter

21 §

Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

22 §

Av artikel *2.1 d* i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, framgår att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför denna lags tillämpningsområde.

Av artikel *2.2 d* i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, framgår att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför denna lags tillämpningsområde.

Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att behandlingen är nödvändig och proportionerlig för det ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning behöver någon prövning enligt andra stycket inte göras. Det gäller dock inte uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen.

3 kap.

16 §

Den som fullgör uppgift som dataskyddsombud får inte obehörigen röja eller utnyttja det som han eller hon då har fått veta om enskilds personliga eller ekonomiska förhållanden.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

6 kap.

1 §

Sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av bestämmelser i

1. 2 kap. 1–5, 7–12, 14–18 *eller* 19 § andra stycket,	1. 2 kap. 1–5, 7–12, 14–18 *§*, 19 § andra stycket *eller 22 § andra stycket*,
2. 3 kap. 2–8 *§§*, eller	2. 3 kap. 2–8 *§*, eller

3. 8 kap. 1–6 eller 8 §.

Sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar sådana incidenter eller underlåter att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller att följa tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Denna lag träder i kraft den 1 maj 2018.

Förteckning över remissinstanserna (SOU 2017:74)

Följande remissinstanser har kommit in med yttrande över SOU 2017:74 Brottsdatalag – kompletterande lagstiftning: Riksdagens ombudsmän, Svea hovrätt, Hovrätten för Västra Sverige, Södertörns tingsrätt, Eskilstuna tingsrätt, Helsingborgs tingsrätt, Umeå tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Linköping, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Övervakningsnämnd Stockholm Centrum, Brottsförebyggande rådet, Brottsoffermyndigheten, Rättsmedicinalverket, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Migrationsverket, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Försäkringskassan, Socialstyrelsen, Inspektionen för vård och omsorg, Statens institutionsstyrelse, Pensionsmyndigheten, Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Arbetsgivarverket, Länsstyrelsen Skåne, Länsstyrelsen Värmland, Länsstyrelsen Västernorrland, Avesta kommun, Hallstahammars kommun, Kiruna kommun, Luleå kommun, Norrköpings kommun, Sala kommun, Stockholms kommun, Statskontoret, Uppsala universitet, juridiska fakulteten, Umeå universitet, juridiska institutionen, Naturvårdsverket, Havs- och vattenmyndigheten, Post- och telestyrelsen, Sjöfartsverket, Riksarkivet, Sveriges advokatsamfund, Svenska Journalistförbundet, Tidningsutgivarna, Dataskydd.net, Svenska Fotbollförbundet och Riksidrottsförbundet.

Följande remissinstanser har avstått från att yttra sig respektive inte hörts av: Länsstyrelsen Stockholm, Blekinge läns landsting, Stockholms läns landsting, Västerbottens läns landsting, Alingsås kommun, Borgholms kommun, Danderyds kommun, Falu kommun, Göteborgs kommun, Helsingborgs kommun, Karlstads kommun, Laholms kommun, Lycksele kommun, Malmö kommun, Ronneby kommun, Sandvikens kommun, Sundsvalls kommun, Tierps kommun, Tranås kommun, Trelleborgs kommun, Uppsala kommun, Värnamo kommun, Växjö kommun, Åmåls kommun, Örebro kommun, Östersunds kommun, Sveriges Akademikers Centralorganisation (SACO), Landsorganisationen i Sverige (LO), Tjänstemännens centralorganisation (TCO), Svenskt Näringsliv, Sveriges Kommuner och Landsting (SKL), Sveriges Förenade Ordningsvakter, IT&Telekomföretagen, Civil Rights Defenders och Svenska Ishockeyförbundet.

Sammanfattning SOU 2016:65

Bakgrund

I vårt moderna och teknikutvecklade samhälle behandlas personuppgifter dagligen i en mycket stor omfattning, av både privatpersoner, företag och myndigheter. Överföringen av personuppgifter mellan aktörer i olika länder ökar också i omfattning. Samtidigt som sådan behandling ofta medför en positiv förenkling och effektivisering, och många gånger är nödvändig för att en verksamhet ska kunna bedrivas ändamålsenligt, medför all personuppgiftsbehandling risker för intrång i den enskildes personliga integritet. Uppgifter som av den enskilde kan uppfattas som känsliga och integritetskränkande kan t.ex. behandlas i olika slags register, uppkomma genom kameraövervakning eller publiceras i inlägg på internet. För att skydda enskildas integritet finns därför ett behov av bestämmelser som bland annat begränsar vilka personuppgifter som får behandlas och för vilka ändamål, och som föreskriver att en otillåten behandling ska rättas eller upphöra. Det är vidare viktigt att de personuppgiftsansvariga har tillräcklig kunskap om gällande bestämmelser kring personuppgiftsbehandling och att det finns en fungerande ordning som verkar för att bestämmelserna följs.

Dessa behov kan delvis tillgodoses genom en väl fungerande tillsyn, som därmed bidrar till att skyddet för den enskildes personliga integritet stärks. I de fall personuppgifter har behandlats på ett otillåtet sätt kan tillsynen också innebära t.ex. att den enskilde får felaktiga uppgifter rättade och tillerkänns kompensation i form av skadestånd, eller att den personuppgiftsansvarige föreläggs att upphöra med en felaktig behandling.

Den alltmer omfattande behandlingen av personuppgifter också på en internationell nivå har inte minst inom EU lett till ett ökat fokus på behovet av skydd för den enskildes personliga integritet. I EU:s nyligen genomförda dataskyddsreform har frågor om tillsyn och tillsynsmyndigheternas befogenheter ett ökat fokus.

Vårt uppdrag

I vårt uppdrag har ingått att kartlägga den tillsyn över behandling av personuppgifter som i dag bedrivs av dels en central tillsynsmyndighet med ett övergripande tillsynsansvar, dels några andra myndigheter med ett tillsynsansvar inom avgränsade sakområden. Vi har dessutom haft i uppdrag att analysera för- och nackdelar med ett i högre grad samlat tillsynsansvar och att utreda hur skyddet för den enskildes personliga integritet kan förstärkas genom att tillsynen över behandling av personuppgifter i högre grad samlas hos en myndighet. Härutöver har vi haft att lämna förslag som innebär att Sverige lever upp till vissa av de krav som ställs på nationella tillsynsmyndigheter i den dataskyddsförordning och det nya dataskyddsdirektiv som har blivit resultatet av EU:s dataskyddsreform.

Den granskning av behandling av personuppgifter som bedrivs vid Statens inspektion för försvarsunderrättelseverksamheten (Siun) har inte omfattats av vårt uppdrag.

Uppdraget i sin helhet framgår av utredningens direktiv (bilaga 1 och 2).

I det följande redovisar vi en sammanfattning av våra överväganden och förslag. Vi kan dock redan nu konstatera att våra förslag har en stark koppling till frågor som regleras i de nyligen beslutade EU-rättsakterna på dataskyddsområdet. Detta innebär att de utredningar som har i uppdrag att föreslå vilka anpassningar som är nödvändiga med anledning av rättsakterna kan ha anledning att på nytt överväga de frågor som omfattas av vårt uppdrag.

Är det möjligt att samla all tillsyn hos en myndighet?

Vi har i enlighet med uppdraget genomfört en kartläggning av dagens tillsyn över behandling av personuppgifter. Kartläggningsarbetet redovisas i kapitel 6. Vi har valt att uppfatta uppdraget så att kartläggningsarbetet på ett så heltäckande sätt som möjligt ska redovisa alla de myndigheter som åtminstone teoretiskt kan sägas ha ett tillsynsuppdrag som omfattar behandlingen av personuppgifter i den granskade verksamheten. Det innebär att kartläggningen omfattar inte bara myndigheter som exempelvis Datainspektionen och Säkerhets- och integritetsskyddsnämnden (SIN), som helt eller till stor del ägnar sig åt tillsyn över personuppgiftsbehandling. Några av de myndigheter som ingår i redovisningen har ett huvudsakligt tillsynsuppdrag inom helt andra områden än dataskydd och skyddet för den personliga integriteten. Ytterligare några är inte huvudsakligen tillsynsmyndigheter utan har tilldelats ett visst tillsynsansvar utöver sina andra uppgifter.

I kapitel 8 redovisar vi våra iakttagelser med anledning av kartläggningen. Det gäller bland annat frågan om var det finns gränsdragningsproblem mellan olika myndigheters tillsynsuppdrag, och våra slutsatser när det gäller vilka för- och nackdelar det skulle innebära att samla all tillsyn över behandling av personuppgifter hos en myndighet.

Vår kartläggning visar att den centrala tillsynsmyndigheten Datainspektionen har ett mycket brett och omfattande tillsynsområde som innefattar personuppgiftsbehandling inom både privat och offentlig verksamhet. Datainspektionen har behörighet att utöva tillsyn över all behandling av personuppgifter. Utöver renodlad tillsynsverksamhet bedriver Datainspektionen ett förebyggande arbete som syftar till att öka kunskapen om de bestämmelser som ska skydda den enskildes personliga integritet vid behandling av personuppgifter. Om de personuppgiftsansvariga har god kännedom om vad som gäller vid personuppgiftsbehandlingen ökar förutsättningarna för ett gott integritetsskydd utan behov av ingripanden från en tillsynsmyndighet.

Vid sidan av Datainspektionens tillsyn utövar en handfull andra myndigheter tillsyn över sådan personuppgiftsbehandling som förekommer i vissa särskilda verksamheter. Tillsynen kompletterar eller ersätter här Datainspektionens tillsyn. Ett sådant tillsynsansvar har bland annat Post- och telestyrelsen (PTS), SIN, Konsumentverket, Centrala etikprövningsnämnden och länsstyrelserna.

Vi har kunnat konstatera vissa brister när det gäller fördelningen av tillsynsansvar mellan Datainspektionen å ena sidan och PTS, SIN, Cen-

trala etikprövningsnämnden samt Inspektionen för vård och omsorg (IVO) å den andra. Lagstiftningen är vidare i några fall utformad på ett sådant sätt att några myndigheter kan sägas ha ett i vart fall teoretiskt tillsynsansvar även över behandling av personuppgifter, trots att tillsynen i dessa fall i realiteten uteslutande bedrivs av Datainspektionen och något annat inte torde ha varit avsikten.

Vi har övervägt om ett ännu mera samlat tillsynsansvar skulle kunna vara en fördel när det gäller effektivitet, resursutnyttjande och enhetlighet i tillsynsarbetet. Om det bara fanns en enda myndighet som hade ansvar för tillsynen av den personliga integriteten skulle det onekligen vara tydligt vilken myndighet som bär ansvaret. Det skulle också kunna ses som en fördel för tillsynsobjekten om en mera samlad tillsyn innebar att de skulle slippa bli föremål för tillsyn från olika håll.

Vår kartläggning visar emellertid att tillsynen redan i dag till stor del är samlad hos en myndighet, Datainspektionen, som också har ett övergripande ansvar när det gäller skyddet för den personliga integriteten. Att även ett antal andra myndigheter har ett till vissa områden avgränsat tillsynsansvar har ofta motiverats med att den personuppgiftsbehandling det då handlar om utgör en del av och har en naturlig och nära koppling till den verksamhet som i övrigt är föremål för myndighetens ansvarsområde och tillsyn. Detta gäller exempelvis för den tillsyn som utförs av PTS, Konsumentverket och Lotteriinspektionen. Den personuppgiftsbehandling som är föremål för särskild tillsyn, utöver eller vid sidan av den tillsyn som utförs av Datainspektionen, kan vidare avse en verksamhet där det har ansetts att det krävs speciell kunskap om och erfarenhet av den granskade verksamheten. Tillsynen är i dessa fall inriktad på områden som kan ge upphov till särskilda risker från integritetssynpunkt. Detta gäller den tillsyn som utförs av SIN. Det kan dessutom vara omöjligt att särskilja de åtgärder som innebär att en personuppgift har behandlats från andra åtgärder som också är föremål för en viss myndighets tillsyn. De behandlingsregler i lagen om elektronisk kommunikation (2003:389) som är föremål för tillsyn av PTS kan exempelvis, men behöver inte, innehålla personuppgifter som går att koppla till en fysisk person.

Sammanfattningsvis tydliggör kartläggningen att behandling av personuppgifter i dag förekommer inom alla delar av samhället, i en mycket stor omfattning och i mycket varierande typer av verksamheter. Det är när det gäller viss sådan verksamhet värdefullt och rent av nödvändigt att tillsynen bedrivs av en myndighet som har särskilda expertkunskaper på det område där behandlingen äger rum. Att uppdra åt en enda myndighet att utöva tillsyn över all personuppgiftsbehandling, oavsett i vilket sammanhang och i vilken verksamhet den förekommer, skulle enligt vår bedömning inte ge ett bättre skydd för enskildas personliga integritet. Man skulle i stället gå miste om fördelarna med att inom vissa för enskildas personliga integritet särskilt viktiga områden kunna utnyttja expertmyndigheternas kunskap om de granskade verksamheterna. Till detta kommer att det många gånger inte ens är möjligt att särskilja åtgärder som innebär att personuppgifter behandlas från andra åtgärder som också är föremål för tillsyn.

Vår slutsats är därför att det inte är möjligt eller ens lämpligt att samla all tillsyn över behandling av personuppgifter hos en enda myndighet. Datainspektionen bör även i fortsättningen vara den centrala myndighe-

ten när det gäller personuppgiftsbehandling, men viss tillsyn härutöver även i fortsättningen utföras av andra myndigheter.

Även om vi alltså inte föreslår att all tillsyns ska utföras av en enda myndighet har vi övervägt frågan om det finns skäl att ge Datainspektionen ett nytt namn för att därigenom betona myndighetens roll som den centrala tillsynsmyndigheten när det gäller skyddet av den personliga integriteten. Vi har emellertid efter att ha vägt för- och nackdelarna med ett namnbyte stannat för att inte lägga fram ett sådant förslag.

Vissa anpassningar till EU:s dataskyddsreform

Den nya allmänna dataskyddsförordningen[15] och ett nytt direktiv om skydd för personuppgifter på det brottsbekämpande området[16] har antagits av Europaparlamentet och rådet. Förordningen ska börja tillämpas den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018. Både förordningen och direktivet innehåller nya och utvidgade regleringar som gäller de nationella tillsynsmyndigheterna. Vi redovisar i kapitel 9 våra överväganden i de delar av uppdraget som gäller vissa anpassningar efter förordningens och direktivets bestämmelser om tillsyn.

Svensk rätt uppfyller enligt vår bedömning dataskyddsförordningens och det nya dataskyddsdirektivets krav på att tillsynsmyndigheten ska vara fullständigt oberoende. Vi föreslår att Datainspektionen ska utses till svensk nationell tillsynsmyndighet enligt både förordningen och direktivet. Som sådan ska Datainspektionen delta i det arbete som kommer att bedrivas av den europeiska dataskyddsstyrelsen. Detta bör regleras i myndighetens instruktion.

Svensk rätt motsvarar dessutom i allt väsentligt enligt vår bedömning de krav som dataskyddsförordningen och det nya dataskyddsdirektivet uppställer om tillsynsmyndighetens organisation och utnämningen respektive avsättandet av tillsynsmyndighetens chef. Detta gäller bland annat kraven på ett öppet rekryteringsförfarande, skydd mot godtyckligt avskedande och förbud mot förtroendeskadliga bisysslor, där allmänna författningsregleringar redan finns. Vi föreslår härutöver att det införs en bestämmelse i myndighetens instruktion om att chefen för Datainspektionen anställs genom beslut av regeringen för en period om minst fyra år, med obegränsad möjlighet till förlängning.

Vi menar att det för närvarande saknas behov av att föreskriva att Datainspektionen ska ha ytterligare befogenheter utöver dem som följer av dataskyddsförordningen och att det inte finns något utrymme eller behov av en kompletterande reglering om myndighetens uppgifter i in-

[15] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (i detta betänkande kallat dataskyddsförordningen).
[16] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter (i detta betänkande kallat [det nya] dataskyddsdirektivet).

struktionen. Vi föreslår, med hänvisning till EU-rättsakternas krav på tillsynsmyndighetens oberoende, att Datainspektionens instruktion inte längre ska ange att myndighetens verksamhet särskilt ska inriktas på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud.

När det gäller Datainspektionens resursbehov med anledning av dataskyddsreformen konstaterar vi att det är för tidigt att mer exakt uppskatta storleken av resursbehovet. Det pågår ett arbete, både inom Datainspektionen och på annat håll, med att utreda och överväga vilka konsekvenser de nya rättsakterna får för hur tillsynen ska vara utformad i framtiden. Detta gäller inte minst de pågående utredningarna om anpassningar med anledning av dataskyddsförordningen och det nya dataskyddsdirektivet[17] som ska redovisa sina överväganden nästa år. Mot bakgrund av de uppskattningar som i nuläget går att göra anser vi att Datainspektionens beräkningar bör ligga till grund för det fortsatta arbetet med att bedöma myndighetens resursbehov.

Förstärkning av skyddet för den enskildes personliga integritet genom vissa förändringar av tillsynsansvaret

Den omständigheten att vi inte ansett det vara till gagn för den personliga integriteten att samla all tillsyn hos en och samma myndighet hindrar inte att det inom den nuvarande myndighetsstrukturen kan finnas skäl att överväga en viss förändring av ansvarsfördelningen genom en överföring av tillsynsuppgifter mellan myndigheter. Våra överväganden i dessa dela redovisas i kapitel 10. Vi föreslår att tillsynsansvaret i några fall överförs från andra tillsynsmyndigheter till Datainspektionen. Genom att på detta sätt ytterligare samla tillsynsansvar hos Datainspektionen skapas enligt vår bedömning en mer ändamålsenlig tillsyn som ger ett starkare skydd för den enskildes personliga integritet. Problem med parallella tillsynsuppdrag kan härigenom undvikas och tillsynsuppgifter med ett naturligt samband kan samlas hos en och samma myndighet. Att tillsynen till viss del ytterligare samlas hos Datainspektionen stärker och tydliggör vidare myndighetens roll som central tillsynsmyndighet.

Vi föreslår mot denna bakgrund att tillsynen över bestämmelserna i lagen (2003:389) om elektronisk kommunikation om abonnentförteckningar och s.k. cookies ska utföras av Datainspektionen i stället för av PTS. Kopplingen till sektorn elektronisk kommunikation är här svagare och prövningen tar i stället sikte på mer allmänna dataskyddsrättsliga överväganden. Datainspektionen får härigenom ett mer samlat tillsynsansvar över behandling av personuppgifter. I tillsynsärenden som även i fortsättningen ska ligga kvar hos PTS kan enligt vår mening ett ökat samråd med Datainspektionen i frågor om innebörden av centrala dataskyddsrättsliga begrepp vara av värde. Det kan också bli aktuellt att hänskjuta frågor från PTS till Datainspektionen för avgörande. Möjligheterna till samråd och hänskjutande följer redan av lagstiftningen och

[17] Dir. 2016:15 och 2016:21.

kräver ingen ytterligare reglering. Även uppgifter som omfattas av sekretess torde enligt vår bedömning kunna lämnas över.

Vi föreslår vidare att tillsynen över den öppna polisens personuppgiftsbehandling i brottsbekämpande verksamhet inte längre ska ingå i SIN:s uppdrag utan i fortsättningen utföras endast av Datainspektionen. De praktiska problemen med parallella tillsynsuppdrag har när det gäller den öppna polisens personuppgiftsbehandling visat sig inte uppvägas av de fördelar för den personliga integriteten som man eftersträvade när SIN:s tillsynsuppdrag utvidgades till att även omfatta denna uppgift. Löpande kontakter och samordning i syfte att undvika kolliderande tillsynsinsatser tar i anspråk resurser hos båda myndigheterna som annars hade kunnat ägnas åt tillsyn. Det finns också en risk att de två myndigheterna kan komma till olika slutsatser i fråga om en viss typ av behandling eller, som en följd av beslutens olika karaktär, att Datainspektionens beslut efter överklagande ändras medan SIN:s i princip likalydande uttalande i samma fråga fortfarande gäller och inte kan överklagas. De båda myndigheterna har inte heller samma maktmedel till sitt förfogande när det gäller att säkerställa att tillsynen blir effektiv. Det är bara Datainspektionen som i dag har de befogenheter som såvitt vi nu kan bedöma krävs enligt det nya dataskyddsdirektivet.

Både Datainspektionen och SIN ska dock även i fortsättningen ha behörighet att utöva tillsyn över Säkerhetspolisens behandling av personuppgifter i brottsbekämpande verksamhet. Vi föreslår att SIN:s tillsyn därvid ska omfatta all personuppgiftsbehandling, inte bara sådan som följer av vissa lagar. Skyldigheten för SIN att i vissa fall göra en anmälan till Datainspektionen får anses gälla bara när det finns behov av ett rättsligt bindande och överklagbart beslut om exempelvis rättelse eller förbud mot fortsatt behandling. En sådan tolkning av omfattningen av SIN:s anmälningsskyldighet ryms enligt vår mening inom den nuvarande författningsregleringen.

Till skillnad från SIN har Datainspektionen i dag ingen skyldighet att på en enskilds begäran kontrollera lagenligheten av personuppgiftsbehandlingar. Det nya dataskyddsdirektivet kommer emellertid att medföra vissa sådana skyldigheter för den centrala tillsynsmyndigheten. Detta kommer att gälla även beträffande den personuppgiftsbehandling som sker hos andra myndigheter än Polismyndigheten. Vi anser att överväganden om den närmare utformningen av Datainspektionens skyldighet att på begäran av en enskild kontrollera om han eller hon har varit föremål för behandling av personuppgifter inom den öppna polisens brottsbekämpande verksamhet bör göras av den utredning som har i uppdrag att genomföra direktivet i svensk rätt.

Våra förslag i denna del innebär att SIN:s verksamhet och uppdrag såvitt avser tillsyn över behandling av personuppgifter återgår till den ordning som gällde före 2012. Utöver tillsynen över Säkerhetspolisens personuppgiftsbehandling kommer SIN även i fortsättningen dessutom att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet, samt på begäran av en enskild kontrollera om han eller hon i strid med lag har utsatts för hemliga tvångsmedel eller varit föremål för Säkerhetspolisens personuppgiftsbehandling. SIN:s

verksamhet består dessutom av de uppdrag som de två särskilda organen Registerkontrolldelegationen och Skyddsregistreringsdelegationen har.

Några ytterligare myndigheters tillsyn

Vi har kunnat konstatera att Datainspektionen och Centrala etikprövningsnämnden inte är helt överens om var gränsen går mellan de båda myndigheternas tillsynsansvar när det gäller forskning som innefattar behandling av personuppgifter. Vi har övervägt om oklarheterna bör åtgärdas genom en lagändring. Vi menar emellertid att ansvarsfördelningen framgår av den nuvarande lagstiftningen och dess förarbeten och att det därför saknas behov av någon ytterligare reglering. Datainspektionen ska utöva tillsyn över om den personuppgiftsbehandling som utförs inom ramen för viss forskning är förenlig med personuppgiftslagen, medan Centrala etikprövningsnämnden ska granska om forskning bedrivs i enlighet med etikprövningslagen. Det senare gäller även om forskningen innefattar behandling av personuppgifter.

Datainspektionen och IVO har ett delvis överlappande tillsynsansvar, men myndigheterna har i grunden helt olika uppdrag. För att tillgodose skyddet av den personliga integriteten vid behandling av personuppgifter i de verksamheter som omfattas av IVO:s tillsynsansvar är det viktigt att sådana frågor prövas av Datainspektionen. Det är därför angeläget att IVO samråder med Datainspektionen så snart det i IVO:s verksamhet uppkommer frågor om en viss personuppgiftsbehandlings lagenlighet. En sådan samrådsskyldighet är redan författningsreglerad men vi konstaterar att det finns behov av att den upprätthålls och utvecklas.

Den rättsliga regleringen är som vi kunnat konstatera i vissa fall utformad så att den ger sken av att några ytterligare myndigheter ska utöva tillsyn även över behandling av personuppgifter trots att detta sannolikt inte medvetet varit avsikten. Myndigheterna ifråga utför inte heller i realiteten någon sådan tillsyn. Detta innebär emellertid inte att det uppkommer några brister i tillsynen över behandling av personuppgifter eller för skyddet av den personliga integriteten, eftersom tillsyn utförs av Datainspektionen även i dessa fall.

Slutligen konstaterar vi att det finns anledning att se över Datainspektionens tillsynsansvar enligt inkassolagen, i syfte att renodla och stärka Datainspektionens roll som central tillsynsmyndighet på området för integritetsskydd vid behandling av personuppgifter.

Frågan om ett integritetsskyddsråd

I vårt uppdrag har ingått att lämna förslag som innebär att den myndighet som ska ha det huvudsakliga ansvaret för tillsynen över behandling av personuppgifter är förberedd för att kunna fullgöra de uppgifter som Integritetskommittén (Ju 2014:09) kan komma att föreslå att ett integritetsskyddsråd ska ha.

Integritetskommittén redovisade i ett delbetänkande i juni 2016 (SOU 2016:41) sina överväganden bland annat i frågan om ett integritetsskyddsråd (bet s. 646 f.). Kommittén anser att det inte bör inrättas något integritetsskyddsråd med huvuduppgift att verka för en säkrare avväg-

ning av motstående intressen i lagstiftningen. Kommittén konstaterar att Datainspektionen redan i dag har ett övergripande ansvar för skyddet av personuppgifter, vilket bland annat innebär att myndigheten regelmässigt är remissinstans (både när det gäller formella remisser och delningar från departementen) och ofta finns representerad i utredningar som gäller sådana frågor. Det finns enligt kommittén dessutom ett flertal andra myndigheter och organisationer, såsom Justitiekanslern, Riksdagens ombudsmän, Myndigheten för samhällsskydd och beredskap, PTS, SIN samt Advokatsamfundet, som också granskar förslag till ny lagstiftning ur ett integritetsskyddsperspektiv. Detta bidrar enligt kommittén till att integritetsskyddsperspektivet lyfts fram i lagstiftningsarbetet och att bristfälliga avvägningar uppmärksammas.

Integritetskommittén föreslår emellertid att Datainspektionen ska få i uppdrag att årligen lämna en rapport till regeringen som sammanställer och analyserar den mest aktuella och betydelsefulla utvecklingen som påverkar den personliga integriteten. Regeringen ska därefter i sin tur överlämna rapporten till riksdagen i form av en skrivelse som också innehåller regeringens kommentarer till rapporten.

Vi har med anledning av Integritetskommitténs ställningstagande i denna del ansett att det inte finns skäl för oss att lämna förslag som gäller ett integritetsskyddsråds uppgifter.

Konsekvenser av våra förslag

Ett omfattande arbete pågår, både inom Regeringskansliet och i ett stort antal utredningar, som på olika sätt berör den personliga integriteten och tillsyn över behandling av personuppgifter. Detta arbete avser till stora delar anpassningar till EU:s nyligen beslutade dataskyddsreform. Resultatet kan komma att få betydelse för Datainspektionens och andra myndigheters arbete och organisation. Den nya dataskyddsförordningen och det nya dataskyddsdirektivet innehåller omfattande bestämmelser om de nationella tillsynsmyndigheternas uppgifter, befogenheter och inbördes samverkan, som såvitt vi kan bedöma kommer att innebära utökade uppgifter för främst Datainspektionen.

Det är mot denna bakgrund svårt att i nuläget göra annat än preliminära uppskattningar av de ekonomiska konsekvenserna av våra förslag. Genomförandet av våra förslag och de förslag som kan bli resultatet av övriga utredningar måste rimligen ske samordnat.

Det pågående arbetet med att även i andra utredningar analysera vilka anpassningar och författningsregleringar som är nödvändiga med anledning av EU:s dataskyddsreform, och nödvändigheten av att göra samlade överväganden om behovet och utformningen av författningsregleringar, innebär att vi nu inte lämnar något annat förslag om när våra föreslagna författningsförändringar bör träda i kraft än att senast maj 2018 framstår som en rimlig utgångspunkt.

Lagförslag i SOU 2016:65

Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs i fråga om lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet att 1 § ska ha följande lydelse.

1 §

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Denna lag träder i kraft den xxx.

Förteckning över remissinstanserna (SOU 2016:65)

Följande remissinstanser har kommit in med yttrande över SOU 2016:65 Ett samlat ansvar för tillsyn över den personliga integriteten: Riksdagens ombudsmän, Kammarrätten i Stockholm, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Revisorsnämnden, Datainspektionen, Statens inspektion för försvarsunderrättelseverksamheten, Socialstyrelsen, Inspektionen för vård och omsorg, Myndigheten för familjerätt och föräldraskapsstöd, Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Lotteriinspektionen, Länsstyrelsen Skåne, Länsstyrelsen Stockholm, Länsstyrelsen Västra Götalands län, Konsumentverket, Fastighetsmäklarinspektionen, Lunds universitet, Göteborgs universitet, Stockholms universitet, Centrala etikprövningsnämnden, Naturvårdsverket, Statens energimyndighet, Affärsverket svenska kraftnät, Energimarknadsinspektionen, Post- och telestyrelsen, Transportstyrelsen, Skogsstyrelsen, Utredningen Översyn av regelverken för forskningsetik och gränsområdet mellan klinisk forskning och hälso- och sjukvård (U 2016:02), Sveriges advokatsamfund, IT&Telekomföretagen, Sveriges Konsumenter, Civil Rights Defenders och Dataskydd.net.

Följande remissinstanser har avstått från att yttra sig respektive inte hörts av: Saco, Eniro 118 118 AB, Bisnode Sverige AB, Telia Company AB, Tele2 Sverige AB, Telenor Sverige AB, Hi3G Access AB, IAB Sverige.

Därutöver har Arbetsgivarverket och Sveriges läkarförbund kommit in med yttranden.

Lagrådsremissens lagförslag

Förslag till brottsdatalag

Härigenom föreskrivs[1] följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, här benämnt dataskyddsdirektivet.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

4 § Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Lagen gäller inte heller i sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, i den ursprungliga lydelsen.

Avvikande bestämmelser i annan författning

5 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Uttryck i lagen

6 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Behörig myndighet	1. En myndighet som har till uppgift att a) förebygga, förhindra eller upptäcka brottslig verksamhet, b) utreda eller lagföra brott, c) verkställa straffrättsliga påföljder, eller d) upprätthålla allmän ordning och säkerhet, eller 2. en annan aktör som utövar myndighet för något av de syften som anges i 1.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsombud	Den som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.

Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.
Medlemsstat	En stat som är medlem i Europeiska unionen samt Island, Liechtenstein, Norge och Schweiz.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter.
Registrerad	Den fysiska person som personuppgiften gäller.
Tillsynsmyndighet	Myndighet som regeringen utser att enligt dataskyddsdirektivet utöva tillsyn över behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.
Tredjeland	En stat som inte är en medlemsstat.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.

Uppgift som rör hälsa	Personuppgift som rör en persons fysiska eller psykiska hälsa, inklusive information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

2 kap. Behandling av personuppgifter

Behandling för ändamål inom denna lags tillämpningsområde

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa en straffrättslig påföljd eller upprätthålla allmän ordning och säkerhet. Arbetsuppgiften ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt den behöriga myndigheten att utföra en sådan uppgift.

2 § Utöver vad som sägs i 1 § får personuppgifter behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Ändamål för behandling av personuppgifter

3 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.

Om det ändamål som personuppgifterna behandlas för inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning.

4 § Innan personuppgifter får behandlas för ett nytt ändamål inom denna lags tillämpningsområde ska det säkerställas att

1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen, och
2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

5 § En behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Grundläggande krav på behandlingen av personuppgifter

Laglig och korrekt behandling

6 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifters kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Åtskillnad mellan olika slag av personuppgifter

9 § Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade, som personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott, särskiljas. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

10 § Så långt det är möjligt ska personuppgifter som grundar sig på fakta särskiljas från personuppgifter som grundar sig på personliga bedömningar. Om grunden inte framgår av sammanhanget eller på annat sätt ska den tydliggöras genom en särskild upplysning.

Känsliga personuppgifter

11 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket när det är absolut nödvändigt för ändamålet med behandlingen.

12 § Biometriska uppgifter och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

13 § Personuppgifter som avses i 11 och 12 §§ utgör känsliga personuppgifter. Känsliga personuppgifter får alltid behandlas med stöd av 2 §.

14 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

15 § Alla rimliga åtgärder ska vidtas för att personuppgifter som med hänsyn till ändamålet med behandlingen är felaktiga eller ofullständiga utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

När personuppgifter lämnas ut till en behörig myndighet ska mottagaren så långt det är möjligt ges information som gör det möjligt att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga.

16 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar som bevis, ska den personuppgiftsansvarige i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Längsta tid som personuppgifter får behandlas

17 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Bestämmelsen i första stycket hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

18 § Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för ändamål inom denna lags tillämpningsområde, ska den personuppgiftsansvarige årligen se över behovet av att fortsätta behandla personuppgifterna.

Automatiserade beslut

19 § Om ett beslut har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne och beslutet enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att på begäran få beslutet omprövat av någon fysisk person.

Automatiserade beslut får inte enbart grundas på känsliga personuppgifter.

Villkor om användningsbegränsning

20 § Om det inte är särskilt föreskrivet får villkor för behandling av personuppgifter inte ställas upp i förhållande till en mottagare i en annan medlemsstat eller ett EU-organ, om det inte i motsvarande fall får ställas upp samma typ av villkor i förhållande till en svensk mottagare.

Utlämnande av personuppgifter

21 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Behandling för ändamål utanför denna lags tillämpningsområde

22 § Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

Föreskrifter

23 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. underrättelseskyldighet gentemot mottagare av sådana personuppgifter som dels omfattas av användningsbegränsningar, dels anges i 15 § första stycket och 16 § första stycket, eller
2. åtgärder för att säkerställa att personuppgifter inte behandlas längre än nödvändigt.

3 kap. Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

1 § Den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

2 § Den personuppgiftsansvarige ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

3 § Både vid beslut om hur behandlingen ska utföras och vid behandlingen ska den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen sker författningsenligt och att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

4 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem som regel endast är möjligt att behandla de personuppgifter som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

5 § Den personuppgiftsansvarige ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

6 § Den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

7 § Om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra särskild risk för intrång i den registrerades personliga integritet, ska den personuppgiftsansvarige innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Säkerheten för personuppgifter

Säkerhetsåtgärder

8 § Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Personuppgiftsincidenter

9 § Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet.

10 § Om en personuppgiftsincident som ska anmälas enligt 9 § första stycket har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige utan onödigt dröjsmål underrätta den registrerade om incidenten.

Underrättelseskyldigheten enligt första stycket gäller inte om den personuppgiftsansvarige

1. har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder på de personuppgifter som påverkades av incidenten,

2. har säkerställt att det inte längre finns särskild risk för otillbörligt intrång i registrerades personliga integritet, eller

3. skulle behöva göra oproportionerliga ansträngningar för att underrätta alla berörda.

I fall som avses i andra stycket 3 ska allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade får nödvändig information.

11 § Den personuppgiftsansvarige får avstå från att lämna information enligt 10 § i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans fri- och rättigheter skyddas.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

Samarbete med tillsynsmyndigheten

12 § Den personuppgiftsansvarige ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till den.

Dataskyddsombud

13 § Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

14 § Dataskyddsombud ska

1. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid behandling av personuppgifter,
3. på begäran ge den personuppgiftsansvarige råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,
4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och
5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

15 § Den som fullgör uppgift som dataskyddsombud får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

Personuppgiftsbiträden

16 § Den personuppgiftsansvarige får, om det är lämpligt, anlita personuppgiftsbiträden. När ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda den registrerades rättigheter.

17 § Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde får inte utan skriftligt tillstånd från den personuppgiftsansvarige anlita ett annat personuppgiftsbiträde.

18 § Ett personuppgiftsbiträde och de som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Om ett personuppgiftsbiträde fastställer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

19 § Det som sägs om den personuppgiftsansvariges skyldigheter i 5, 6, 8 och 12 §§ gäller även för personuppgiftsbiträden.

Gemensamt personuppgiftsansvar

20 § Två eller flera behöriga myndigheter är gemensamt personuppgiftsansvariga om de gemensamt fastställer ändamålen med och medlen för personuppgiftsbehandlingen.

Den registrerade får utöva sina rättigheter enligt lagen mot var och en av de gemensamt personuppgiftsansvariga.

Bemyndigande

21 § Regeringen får meddela föreskrifter om skyldighet att föra register över kategorier av behandling av personuppgifter och skyldighet att införa interna rutiner för anmälan av överträdelser.

Föreskrifter

22 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. åtgärder som avses i 2–5, 7 och 8 §§,
2. tillgången till personuppgifter,
3. anmälan om personuppgiftsincidenter,
4. underrättelser till registrerade om personuppgiftsincidenter, och
5. innehållet i avtal och överenskommelser enligt 17 §.

4 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Den personuppgiftsansvarige ska göra följande allmänna information tillgänglig för den registrerade:

1. den personuppgiftsansvariges identitet och kontaktuppgifter,
2. dataskyddsombudets kontaktuppgifter,
3. typer av ändamål för behandlingen,
4. rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av uppgifterna,
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
6. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

Personrelaterad information

2 § Den personuppgiftsansvarige ska i specifika fall lämna följande information till den registrerade, om det behövs för att han eller hon ska kunna ta tillvara sina rättigheter:

1. den rättsliga grunden för behandlingen,
2. kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
3. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
4. övrig nödvändig information.

Vid bedömningen av om information enligt första stycket 4 ska lämnas ska det särskilt beaktas om personuppgifterna samlats in utan den registrerades vetskap.

3 § Den personuppgiftsansvarige ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om sökanden som behandlas,
2. varifrån personuppgifterna kommer,
3. den rättsliga grunden för behandlingen,
4. ändamålen med behandlingen,
5. mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,
6. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det,
7. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 9 och 10 §§, och
8. möjligheten att lämna in klagomål till tillsynsmyndigheten samt kontaktuppgifterna till myndigheten.

Utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

4 § Den som har varit föremål för ett sådant beslut som avses i 2 kap. 19 § har rätt att på begäran få närmare information om beslutet av den personuppgiftsansvarige.

Begränsning av rätten till information

5 § Informationsskyldigheten i 2 och 3 §§ gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut av hänsyn till intresset av att

1. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,
2. andra rättsliga utredningar eller undersökningar inte hindras,
3. nationell säkerhet skyddas, eller
4. någon annans fri- och rättigheter skyddas.

Om förutsättningarna i första stycket är uppfyllda, är den personuppgiftsansvarige inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 9 eller 10 §.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantagen i första och andra styckena även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

6 § Informationsskyldigheten i 3 § gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje man, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för vetenskapliga, statistiska eller historiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

7 § Om en begäran enligt 3 § är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Av 12 § andra stycket framgår att den personuppgiftsansvarige i vissa fall får ta ut avgift i stället för att avslå begäran.

Möjligheten att begära kontroll genom tillsynsmyndigheten

8 § I 5 kap. 3 § finns bestämmelser om att en fysisk person får begära att tillsynsmyndigheten kontrollerar om hans eller hennes personuppgifter behandlas författningsenligt.

Rätten till rättelse, radering och begränsning av behandlingen

9 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

10 § Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne, om de behandlas i strid med 2 kap. 1, 2, 3 § första stycket eller någon av 4–6 §§ eller 8, 11, 12, 14 eller 17 § första stycket. Detsamma gäller om det krävs radering för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men uppgifterna behöver finnas kvar som bevis, ska den personuppgiftsansvarige på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

11 § Den personuppgiftsansvarige avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

12 § Information enligt 1, 2 och 4 §§ ska lämnas utan avgift. Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 3 § oftare än en gång per år, får den personuppgiftsansvarige ta ut en rimlig avgift eller avslå begäran enligt 7 § första stycket.

Föreskrifter

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. information enligt 1–4 §§,
2. avgift för att lämna ut information som avses i 3 §, och
3. kraven på en begäran enligt 3, 4, 9 eller 10 §.

5 kap. Tillsyn

Tillsynsmyndighetens uppdrag

1 § Tillsynsmyndigheten ska verka både för att fysiska personers grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom denna lags tillämpningsområde.

Tillsynsmyndighetens uppgifter

2 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling inom denna lags tillämpningsområde,
2. handlägga klagomål från registrerade,
3. utföra kontroll enligt 3 §, och
4. på begäran bistå en tillsynsmyndighet i en annan medlemsstat.

Tillsynen ska inte omfatta domstolarnas behandling av personuppgifter som sker inom ramen för den dömande verksamheten.

3 § Tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. Den som begär en sådan kontroll ska visa att han eller hon har begärt information enligt 4 kap. 3 § eller en åtgärd enligt 4 kap. 9 eller 10 §.

Myndigheten får vägra att utföra kontrollen om begäran är orimlig eller uppenbart ogrundad.

4 § Tillsynsmyndigheten ska vid förhandssamråd enligt 3 kap. 7 § och när det i övrigt är påkallat ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

5 § Tillsynsmyndigheten har rätt att av personuppgiftsansvariga och personuppgiftsbiträden på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

6 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

7 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 6 § första stycket försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter,
2. förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
3. förbjuda fortsatt behandling om bristen är allvarlig, eller
4. besluta om en sanktionsavgift enligt 6 kap.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Verkställighet av beslut

8 § Tillsynsmyndighetens beslut får inte verkställas omedelbart.

Samarbete med tillsynsmyndigheter i andra medlemsstater

9 § En begäran om bistånd från en tillsynsmyndighet i en annan medlemsstat får vägras endast om det skulle strida mot en lag eller en förordning att tillmötesgå den.

10 § När tillsynsmyndigheten utövar tillsyn enligt 2 § 4 har den de befogenheter som anges i 5–7 §§.

11 § Tillsynsmyndigheten får, om det är förenligt med svenska intressen, lämna ut en uppgift till en behörig tillsynsmyndighet i annan medlemsstat, även om uppgiften är sekretessbelagd enligt offentlighets- och sekretesslagen (2009:400).

12 § Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat får inte användas för något annat ändamål än det för vilket informationen begärdes.

Föreskrifter

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om kraven på en begäran enligt 3 § och samarbete med tillsynsmyndigheter i andra medlemsstater.

6 kap. Administrativa sanktionsavgifter

Överträdelser som kan leda till en sanktionsavgift

1 § En sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av någon av

1. 2 kap. 1–5, 7–12 eller 14–18 §§, 19 § andra stycket eller 22 §,
2. 3 kap. 2–8 §§, eller
3. 8 kap. 1–6 §§ eller 8 §.

En sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar en sådan incident, låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

2 § En sanktionsavgift får tas ut av ett personuppgiftsbiträde vid överträdelse av 3 kap. 5, 6 eller 8 §.

En sanktionsavgift får också tas ut om ett personuppgiftsbiträde låter bli att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller inte följer tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Hur sanktionsavgiften ska bestämmas

3 § Sanktionsavgiften ska vid överträdelser av 3 kap. 6 eller 7 § eller av bestämmelser om dokumentation av personuppgiftsincidenter bestämmas till högst 5 000 000 kronor.

Vid överträdelser av övriga bestämmelser som anges i 1 och 2 §§ ska avgiften bestämmas till högst 10 000 000 kronor.

Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling, eller om en eller flera bestämmelser har överträtts genom sammankopplade personuppgiftsbehandlingar, ska sanktionsavgiften bestämmas efter överträdelsernas allvar. Sanktionsavgiften får aldrig överstiga maximibeloppet för den allvarligaste överträdelsen.

4 § Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas ska särskild hänsyn tas till

1. om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa skadan, och
5. om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift.

Beslut om sanktionsavgift

6 § Tillsynsmyndigheten beslutar om sanktionsavgift.

Sanktionsavgiften tillfaller staten.

7 § Någon sanktionsavgift får inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Betalning av sanktionsavgift

8 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Bemyndigande

9 § Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt denna lag.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Överklagande

Överklagande av personuppgiftsansvariga myndigheters beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 4 kap. 9 § första stycket, radering enligt 4 kap. 10 § första stycket, eller begränsning av behandlingen enligt 4 kap. 9 § andra stycket eller 10 § andra stycket, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 4 kap. 3 §, att ta ut avgift enligt 4 kap. 12 § andra stycket eller att inte medge omprövning av ett automatiserat beslut enligt 2 kap. 19 § första stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Första stycket gäller inte beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som inte får överklagas

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

8 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Grundläggande förutsättningar för överföring

1 § En behörig myndighet får överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,

2. riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet, och

3. omfattas av

a) ett beslut om adekvat skyddsnivå enligt 3 §,

b) tillräckliga skyddsåtgärder enligt 4 §, eller

c) ett undantag för särskilda situationer enligt 5 §.

En behörig myndighet som avser att överföra personuppgifter till ett tredjeland eller en internationell organisation, ska särskilt beakta risken för att enskilda får ett försämrat skydd för sina personuppgifter.

2 § Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

Om medgivandet på grund av tidsbrist inte kan inhämtas i förväg, får personuppgifter ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för andra väsentliga intressen för Sverige eller någon annan medlemsstat.

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit under de förutsättningar som anges i 1 och 2 §§. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

4 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter, under de förutsättningar som anges i 1 och 2 §§, ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier till skydd för den registrerades rättigheter, eller

2. den behöriga myndighet som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns något beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får en överföring, eller en samling av överföringar, av personuppgifter, under de förutsättningar som anges i 1 och 2 §§, göras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. skydda den registrerades eller någon annan fysisk persons vitala intressen, eller andra berättigade intressen som den registrerade har,

2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet,

3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller

4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Vidareöverföring

6 § En svensk behörig myndighet får inte tillåta att sådana personuppgifter som anges i 2 § första stycket, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation, om inte någon behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras.

7 § När en behörig myndighet ska ta ställning till om personuppgifter som behandlats i Sverige och därefter lämnats till en annan medlemsstat, som överfört dem till ett tredjeland eller en internationell organisation, får vidareöverföras till ett tredjeland eller en internationell organisation, ska alla kända omständigheter som har samband med vidareöverföringen beaktas. Särskild vikt ska läggas vid brottets allvar, allvaret i faran för allmän säkerhet, det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten och nivån på skyddet av personuppgifter i det tredjelandet eller hos den internationella organisationen som uppgifterna ska vidareöverföras till.

Överföring till andra än behöriga myndigheter

8 § En behörig myndighet som inte är en annan aktör som utövar myndighet får i ett enskilt fall överföra personuppgifter till någon som inte är en behörig myndighet i ett tredjeland. Personuppgifterna får överföras endast om de övriga förutsättningarna i 1 och 2 §§ är uppfyllda och om

1. det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en arbetsuppgift enligt 1 kap. 2 § som den har ansvar för,

2. den svenska myndigheten informerar den som ska ta emot personuppgifterna om det eller de specifika ändamål för vilket eller vilka uppgifterna får behandlas, och

3. det skulle vara ineffektivt eller olämpligt att överföra dem till en behörig myndighet i tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Villkor om användningsbegränsning

9 § Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och gäller på grund av en överenskommelse med det tredjelandet eller den internationella organisationen villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

10 § En svensk behörig myndighet får vid överföring av personuppgifter till ett tredjeland eller en internationell organisation i ett enskilt fall ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs med hänsyn till den enskildes rätt eller från allmän synpunkt. Sådana villkor får inte strida mot en internationell överenskommelse som är bindande för Sverige.

Föreskrifter

11 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. information till en annan medlemsstat när personuppgifter överförts utan förhandsmedgivande enligt 2 § andra stycket,

2. information till en behörig myndighet i ett tredjeland när personuppgifter överförts enligt 8 §, och

3. dokumentation av överföringar och information om sådana till tillsynsmyndigheten.

---

1. Denna lag träder i kraft den 1 augusti 2018.

2. Genom lagen upphävs lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

3. Bestämmelsen i 3 kap. 5 § om loggning tillämpas första gången från och med den 6 maj 2023 i fråga om automatiserade behandlingssystem som inrättats före den 6 maj 2016.

4. En sanktionsavgift enligt 6 kap. får beslutas endast för överträdelser som har skett efter ikraftträdandet.

5. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

6. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs att 1 b § lagen (1998:620) om belastningsregister[1] ska upphöra att gälla vid utgången av juli 2018.

[1] Senaste lydelse av 1 b § 2013:331.

Förslag till
lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs att 1 b § lagen (1998:621) om misstankeregister[1] ska upphöra att gälla vid utgången av juli 2018.

[1] Senaste lydelse av 1 b § 2013:332.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 9 kap. 2 § ska ha följande lydelse,

dels att det i lagen ska införas en ny paragraf, 17 kap. 7 c §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
2 §[1]	
Bestämmelser som begränsar möjligheten att använda vissa uppgifter som en svensk myndighet har fått från en myndighet i en annan stat finns i	
1. lagen (1990:314) om ömsesidig handräckning i skatteärenden,	
2. lagen (2017:496) om internationellt polisiärt samarbete,	
3. lagen (2000:344) om Schengens informationssystem,	
4. lagen (2000:562) om internationell rättslig hjälp i brottmål,	
5. lagen (2000:1219) om internationellt tullsamarbete,	
6. lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar,	
7. lagen (2011:1537) om bistånd med indrivning av skatter och avgifter inom Europeiska unionen,	
8. lagen (1998:620) om belastningsregister,	
9. lagen (2012:843) om administrativt samarbete inom Europeiska unionen i fråga om beskattning,	
10. lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen,	
11. lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet,	*10.* lagen (2015:63) om utbyte av upplysningar med anledning av FATCA-avtalet,
12. lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton,	*11.* lagen (2015:912) om automatiskt utbyte av upplysningar om finansiella konton,
13. lagen (2017:182) om automatiskt utbyte av land-för-land-rapporter på skatteområdet, *och*	*12.* lagen (2017:182) om automatiskt utbyte av land-för-land-rapporter på skatteområdet,
14. lagen (2017:1000) om en europeisk utredningsorder.	*13.* lagen (2017:1000) om en europeisk utredningsorder, *och*
	14. brottsdatalagen (2018:000).

[1] Senaste lydelse 2017:1012.

17 kap.

7 c §

Sekretess gäller hos tillsynsmyndigheten i tillsynsverksamhet enligt 5 kap. brottsdatalagen (2018:000) för uppgift som har lämnats utan samband med en svensk begäran om utländskt bistånd från en tillsynsmyndighet i en medlemsstat som medlemsstat definieras i den lagen, om det kan antas att den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Denna lag träder i kraft den 1 augusti 2018.

Förslag till
lag om ändring i domstolsdatalagen (2015:728)

Härigenom föreskrivs att 5 § domstolsdatalagen (2015:728) ska ha följande lydelse.

Lydelse enligt prop. 2017/18:113	*Föreslagen lydelse*
5 §	
De avvikande bestämmelser som finns i *lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen, ska tillämpas i stället för bestämmelserna i denna lag. Detsamma gäller i fråga om* Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur.	De avvikande bestämmelser som finns i Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur, *ska tillämpas i stället för bestämmelserna i denna lag*.

Denna lag träder i kraft den 1 augusti 2018.

Förslag till
lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

Härigenom föreskrivs att 6 kap. 2 § lagen (2017:496) om internationellt polisiärt samarbete ska upphöra att gälla vid utgången av juli 2018.

Förslag till
lag om ändring i lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs i fråga om lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning

dels att punkt 4 i ikraftträdande- och övergångsbestämmelserna ska upphöra att gälla,

dels att 1 kap. 4 § ska ha följande lydelse.

Lydelse enligt prop. 2017/18:105	*Föreslagen lydelse*
1 kap.	
4 §	
Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen *(1996:627)* eller föreskrifter som har meddelats i anslutning till den lagen.	Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen *(2018:000)* eller föreskrifter som har meddelats i anslutning till den lagen.

Denna lag träder i kraft den 1 april 2019 i fråga om 1 kap. 4 § och i övrigt den 1 augusti 2018.

Förslag till
lag om ändring i brottsdatalagen (2018:000)

Härigenom föreskrivs att 3 kap. 9 § brottsdatalagen (2018:000) ska ha följande lydelse.

Lydelse enligt lagförslag 2.1	*Föreslagen lydelse*
3 kap.	
9 §	
Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen *(1996:627)* eller föreskrifter som har meddelats i anslutning till den lagen.	Senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen *(2018:000)* eller föreskrifter som har meddelats i anslutning till den lagen.
Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet.	Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet.

Denna lag träder i kraft den 1 april 2019.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2018-03-23

Närvarande: F.d. justitieråden Gustaf Sandström och Lena Moore samt justitierådet Anders Eka

Brottsdatalag

Enligt en lagrådsremiss den 1 mars 2018 har regeringen (Justitiedepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. brottsdatalag,
2. lag om ändring i lagen (1998:620) om belastningsregister,
3. lag om ändring i lagen (1998:621) om misstankeregister,
4. lag om ändring i offentlighets- och sekretesslagen (2009:400),
5. lag om ändring i domstolsdatalagen (2015:728),
6. lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete,
7. lag om ändring i lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning,
8. lag om ändring i brottsdatalagen (2018:000).

Förslagen har inför Lagrådet föredragits av kanslirådet Anna Westin och rättssakkunnige Henrik Engvall.

Förslagen föranleder följande yttrande av Lagrådet:

Förslaget till brottsdatalag

Inledande synpunkter

Förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen

I 1 kap. 5 § anges att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från lagen tillämpas den bestämmelsen. Paragrafen motsvarar 2 § personuppgiftslagen. Båda dessa paragrafer har rubriken Avvikande bestämmelser i annan författning.

I 7 § första stycket personuppgiftslagen finns dessutom – under rubriken Förhållandet till tryck- och yttrandefriheten – en bestämmelse som anger att lagen inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I 8 § samma lag finns en motsvarande bestämmelse när det gäller offentlighetsprincipen. Enligt 1 kap. 7 § i förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) ska förordningen och lagen inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Remissförslaget innehåller inte någon bestämmelse som på liknande sätt behandlar relationen till grundlagarna. Eftersom förslaget således avviker från vad som gällt enligt personuppgiftslagen och från vad som är avsett att gälla enligt dataskyddslagen aktualiseras frågan hur brottsdatalagen förhåller sig till tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

När det gäller förhållandet till de båda mediegrundlagarna finns det vidare skäl att särskilt framhålla att Justitiekanslern torde träffas av definitionen i 1 kap. 6 § i förslaget och följaktligen vara en behörig myndighet när Justitiekanslern fullgör uppgifter som åklagare avseende tryck- och yttrandefrihetsbrott. Detta har inte berörts i remissen.

Det nu anförda medför behov av att under den fortsatta beredningen ytterligare överväga förslagets förhållande till den tryck- och yttrandefrihetsrättsliga regleringen.

Upplysningsbestämmelserna

Flertalet av de föreslagna kapitlen avslutas med en paragraf som har rubriken Föreskrifter (se 2 kap. 23 §, 3 kap. 22 §, 4 kap. 13 §, 5 kap. 13 § och 8 kap. 11 §). Bestämmelserna innefattar inte något bemyndigande av föreskriftsrätt. Avsikten är endast att upplysa om den föreskriftsrätt som tillkommer regeringen enligt 8 kap. 7 § regeringsformen.

Upplysningsbestämmelser med detta syfte förekommer numera ofta. De föreslagna bestämmelserna avviker emellertid från det som är det vanliga genom att vissa mer precist angivna områden räknas upp (i flertalet fall dessutom i en punktuppställning).

Även om avsikten med upplysningsbestämmelserna är att bidra till ökad klarhet är risken snarast att de, genom den utformning som de har getts, leder till motsatt effekt. Genom att vissa förhållandevis detaljerat beskrivna områden anges uppkommer hos läsaren frågan vad som gäller för regeringens föreskriftsrätt på de områden som inte omnämns (se exempelvis 3 kap. 22 §).

Lagrådet förordar att de föreslagna paragraferna får utgå. Om ett behov av bestämmelser av detta slag bedöms finnas i lagen bör den erinran om regeringens föreskriftsrätt som bestämmelserna är avsedda att ge uttryck för utformas på ett mer generellt sätt. Detaljerade uppgifter om vilka områden som regeringens kommande föreskrifter kan förväntas ta sikte på kan då beskrivas i författningskommentaren.

Under alla förhållanden framstår den rubrik som har valts – Föreskrifter – som mindre passande. Den träffar mycket brett och tillför inget egentligt informationsinnehåll till bestämmelserna.

Om upplysningsbestämmelser av detta slag ska finnas i lagen måste således både paragrafernas utformning och valet av rubrik övervägas under den fortsatta beredningen.

1 kap. 1 §

Ett syfte med lagen anges vara ”att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter”. I direktivet används här uttrycket ”grundläggande rättigheter och friheter” (artikel 1.2 a) och i de olika artiklarna omväxlande ”grundläggande rättigheter och friheter”, ”rättigheter och friheter” och ”rättigheter”.

För att göra det tydligt att det är fråga om rättigheter och friheter i direktivets mening (jfr artikel 8 om skydd av personuppgifter i EU:s stadga om de grundläggande rättigheterna), och inte i någon annan mening, kan styckena i förevarande paragraf lämpligen byta plats så att direktivet nämns i första stycket och andra stycket inleds med orden ”Syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med …”

Uttrycket ”fri- och rättigheter” bör där det förekommer i lagtexten ersättas med ”rättigheter och friheter”.

1 kap. 6 §

Definitionen av Behörig myndighet

Punkterna 1 och 2 är inte i sak kongruenta i det att en myndighet är behörig när den ”har till uppgift att” medan det för en annan aktör krävs att den (i det enskilda fallet) ”utövar” myndighet.

Lagrådet förordar att definitionen förtydligas så att det framgår att myndigheten respektive aktören är behörig endast när den behandlar personuppgifter för sådana syften, inte när uppgifterna behandlas för något annat syfte (t.ex. när Polismyndigheten utfärdar pass, jfr författningskommentaren till 2 §). I stället för ”utövar myndighet” bör ”anförtrotts myndighetsutövning” användas i punkt 2 (se artikel 3.7.b i direktivet).

Lagrådet föreslår följande definition.

1. En myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller

2. en annan aktör som har anförtrotts myndighetsutövning för ett syfte som anges i 1, när den behandlar personuppgifter för ett sådant syfte.

Definitionen av Tillsynsmyndighet

I 5 kap. 9–12 §§ finns bestämmelser om ”tillsynsmyndighet i en annan medlemsstat” som inte bör omfattas av definitionen. Eftersom den svenska tillsynsmyndigheten i lagtexten genomgående anges i bestämd form bör den anges i bestämd form i definitionen, ”Tillsynsmyndig-

heten”. Definitionen kan enligt Lagrådets mening förkortas enligt följande.

Myndighet som regeringen utser att utöva tillsyn över behandling av personuppgifter inom dataskyddsdirektivets tillämpningsområde.

2 kap. 1 §

Paragrafen är lång och svårläst och nyckelorden, ”om det är nödvändigt”, skyms.

Syftet framgår av 1 kap. 2 § och av definitionen av behörig myndighet i 1 kap. 6 §. Uttrycket ”i syfte att” bör utgå.

Ordet ”arbetsuppgift” är inadekvat när det gäller den behöriga myndigheten. Vid föredragningen har förklarats att avsikten varit att undvika sammanblandning med ordet uppgift i betydelsen personuppgift. Ordet arbetsuppgift bör ersättas med uppgift (jfr definitionen av behörig myndighet i 1 kap. 6 §, ”En myndighet som har till uppgift att ...”). Det finns ingen risk för missförstånd, särskilt inte om uttrycket ”sin uppgift” används.

Andra meningen genomför artikel 8.1 i direktivet. Enligt den bestämmelsen ska den behöriga myndighetens uppgift att bekämpa brott m.m. framgå av (unionsrätt eller av) medlemstaternas nationella rätt för att personuppgiftsbehandlingen ska vara laglig. Det kravet behöver inte anges särskilt i förevarande paragraf. Det har dock vid föredragningen uppgetts att bestämmelsen behövs för att klargöra vad som gäller när myndigheter samverkar på dataskyddsdirektivets tillämpningsområde. Ett sådant förtydligande bör tas in i ett andra stycke och formuleras enligt följande.

Lagrådet föreslår att paragrafen ges följande lydelse.

Personuppgifter får behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Med en behörig myndighets uppgift i första stycket avses en uppgift som framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra en sådan uppgift.

2 kap. 9 §

Paragrafen, som även bör omnämna tilltalad, kan förtydligas enligt följande.

Så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade särskiljas så att det framgår om personen är misstänkt, tilltalad, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori personen hör, ska det tydliggöras genom en särskild upplysning.

2 kap. 11–13 §§

Benämningen (känsliga personuppgifter) bör flyttas från 13 § till 11 §. Lagrådet föreslår att paragraferna formuleras enligt följande.

11 § Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt biometriska uppgifter, genetiska uppgifter och uppgifter som rör hälsa, sexualliv eller sexuell läggning (känsliga personuppgifter) får endast behandlas i fall som anges i 12 och 13 §§.

12 § Om uppgifter om en person behandlas får de kompletteras med sådana uppgifter som anges i 11 § när det är absolut nödvändigt för ändamålet med behandlingen. Biometriska uppgifter och genetiska uppgifter får dock behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

13 § Känsliga personuppgifter får alltid behandlas med stöd av 2 §.

2 kap. 19 §

Eftersom uttrycket omprövning inte används i nya förvaltningslagen (se prop. 2016/17:180 s. 223) bör uttrycket inte användas här. ”Fysisk person” bör ersättas med ”någon person” (jfr 29 § personuppgiftslagen). Första stycket bör avslutas enligt följande. ”…få beslutet prövat på nytt av någon person”.

2 kap. 22 §

Enligt paragrafen ska det göras en prövning när personuppgifter som behandlas med stöd av lagen ska behandlas för ändamål utanför lagens tillämpningsområde. Det ska säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet, dvs. samma prövning som enligt 2 kap. 4 § ska göras innan personuppgifter behandlas för ett nytt ändamål inom lagens tillämpningsområde. Enligt remissen (avsnitt 7.6.4) är det rimligt att samma prövning görs i båda fallen.

Det som föreslås är en extra prövning som ska göras innan behandlingen för det nya ändamålet påbörjas. Regleringen saknar stöd i direktivet och EU:s dataskyddsförordning. Hur prövningen förhåller sig – rättsligt och praktiskt – till den nya prövning som ska göras enligt dataskyddsförordningen är oklart.

Lagrådet kan därför inte tillstyrka den föreslagna paragrafen utan anser att den ska utgå.

3 kap. 3 §

I paragrafen behöver inte kravet att behandlingen sker författningsenligt upprepas (jfr 2 §). Paragrafen kan förtydligas enligt följande.

Den personuppgiftsansvarige ska när medlen för behandlingen bestäms och vid behandlingen, genom lämpliga tekniska och organisatoriska åtgärder, se till att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

3 kap. 6 §

Lagrådet föreslår att orden ”varje tjänsteman” ersätts med ”var och en”; jfr 10 § i förslag till lag om behandling av personuppgifter i Arbetsmiljöverkets informationssystem om arbetsskador i prop. 2017/18:112 och 7 § i förslaget till kriminalvårdsdatalag i lagrådsremiss Kriminalvårdsdatalag – en ny lag med anpassning till EU:s dataskyddsförordning.

3 kap. 16 och 17 §§

Det bör i 16 § förtydligas att det handlar om att den personuppgiftsansvarige är skyldig att förvissa sig om att biträdet har den kompetens som krävs och det redan innan biträdet anlitas.

Bestämmelserna i 17 § om att ett personuppgiftsbiträde behandlar personuppgifter på den personuppgiftsansvarigas vägnar och att det ska träffas ett avtal mellan den personuppgiftsansvarige och biträdet bör lämpligen placeras i 16 §.

Lagrådet föreslår att bestämmelserna utformas enligt följande.

16 § Den personuppgiftsansvarige får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på den personuppgiftsansvariges vägnar. Innan ett personuppgiftsbiträde anlitas ska den personuppgiftsansvarige försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda den registrerades rättigheter.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

17 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från den personuppgiftsansvarige.

4 kap. 2 §

Lagrådet föreslår att ”i specifika fall” i första styckets inledning utgår; att det rör sig om ett enskilt fall framgår av fortsättningen, ”när det behövs för att han eller hon ska kunna….”. Alternativt bör uttrycket ersättas med ”i ett enskilt fall”.

6 kap. 4 och 5 §§

I paragraferna finns bestämmelser om hur sanktionsavgift ska bestämmas i det enskilda fallet.

Brottsdatalagen grundas på EU:s dataskyddsdirektiv och tar sikte på personuppgifter som behandlas i den brottsbekämpande verksamhet som

Polismyndigheten och andra myndigheter bedriver. För annan verksamhet hos en sådan myndighet förutsätts i stället EU:s dataskyddsförordning med anknytande inhemska föreskrifter komma att gälla (jfr prop. 2017/18:105 till lag med kompletterande bestämmelser till EU:s dataskyddsförordning). Den sammantagna regleringen blir därmed komplex och svårtillämpad.

När det gäller sanktioner vid överträdelser av bestämmelserna om personuppgifter har man i de båda EU-rättsakterna stannat för olika lösningar. I förordningen finns obligatoriska bestämmelser om administrativa sanktionsavgifter som inte ger utrymme för nationella särlösningar. Direktivet å andra sidan överlämnar åt medlemsstaterna att välja hur regelöverträdelser ska sanktioneras med gängse krav på effektivitet, proportionalitet m.m.

I lagrådsremissen föreslås nu att ett system med sanktionsavgifter ska införas för de brottsbekämpande myndigheterna i deras egenskap av personuppgiftsansvariga. Även personuppgiftsbiträden kan, oavsett om biträdet är en myndighet eller en näringsidkare, träffas av avgift.

Det finns anledning att här återge de bedömningar och ställningstaganden som gjorts i det betänkande (SOU 2017:29) som ligger till grund för lagrådsremissen eftersom remissen i de aktuella delarna helt följer betänkandet.

I betänkandet motiveras utförligt varför sanktionsavgifter bör användas som sanktion. I sammanhanget konstateras att vissa myndigheter kan komma att tillämpa såväl förordningen som den lag som genomför direktivet och att det då är svårt att motivera att helt olika sanktionssystem ska gälla för likartade överträdelser (när betänkandet lämnades våren 2017 hade regeringen inte tagit ställning till möjligheten att låta myndigheter omfattas av förordningens regler om sanktionsavgifter). Vidare framhålls att det finns skäl att vid utformningen av ett nytt sanktionssystem beakta vad som gäller enligt förordningen eftersom i princip samtliga omständigheter som räknas upp i artikel 83.2 i förordningen kan vara av större eller mindre betydelse för frågan om avgift ska tas ut och storleken på avgiften.

Den föreslagna avgiftsmodellen bygger på att särskild hänsyn ska tas till fem kriterier, beskrivna i ganska allmänna ordalag. Enligt en följande paragraf får sanktionsavgiften sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift. Remissinstanserna har inte haft några synpunkter på beräkningssättet. Regeringen har i lagrådsremissen ordagrant följt utredningens förslag till lagtext.

Det sägs i betänkandet och upprepas i lagrådsremissen att det inte är möjligt att skapa helt identiska sanktionssystem eftersom tillämpningsområdet för förordningen och direktivet skiljer sig åt. Enligt Lagrådets mening utesluter inte den omständigheten att tillämpningsområdet i olika avseenden skiljer sig åt att förordningens teknik för att bestämma vad

som ska påverka avgiftsuttaget kan användas också i den nya lagen. En sådan samordning skulle göra sanktionssystemet mer överblickbart för berörda myndigheter och underlätta tillämpningen för tillsynsmyndigheten och domstolarna.

Lagrådet kan därför inte tillstyrka den nu föreslagna avgiftsmodellen utan anser att möjligheten att så långt det går samordna sättet att ta ut sanktionsavgifter bör undersökas. Detta kan innebära att 4 och 5 §§ ersätts med en bestämmelse om att vederbörlig hänsyn ska tas till de omständigheter som anges i a–k i artikel 83.2 i EU:s dataskyddsförordning vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas.

6 kap. 7 §

Lagrådet förordar att en bestämmelse om delgivning motsvarande den som finns i 6 kap. 4 § i förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning tas in i paragrafen som ett nytt andra stycke enligt följande. ”Ett beslut om sanktionsavgift ska delges”.

8 kap. 8 §

Undantaget i paragrafens inledning för en behörig myndighet ”som inte är en annan aktör som utövar myndighet” bör utgå och undantaget i stället regleras i ett nytt tredje stycke enligt följande.

Första och andra styckena gäller inte en sådan annan aktör som är behörig myndighet enligt definitionen i 1 kap. 6 §.

Ikraftträdande- och övergångsbestämmelserna

Enligt punkten 3 i ikraftträdande- och övergångsbestämmelserna ska bestämmelsen i 3 kap. 5 § om loggning tillämpas första gången från och med den 6 maj 2023 i fråga om automatiserade behandlingssystem som inrättats före den 6 maj 2016. Uttrycket ”första gången” bör utgå.

Förslaget till lag om ändring i offentlighets- och sekretesslagen

17 kap. 7 c §

Första stycket bör förenklas enligt följande.

Sekretess gäller i tillsynsmyndighetens verksamhet enligt 5 kap. brottsdatalagen (2018:000) för uppgift som, utan samband med en svensk begäran, har lämnats av en tillsynsmyndighet i en stat inom Europeiska ekonomiska samarbetsområdet (EES) eller i Schweiz, om det kan antas att tillsynsmyndighetens möjlighet att bedriva tillsyn motverkas om uppgiften röjs.

Övriga lagförslag

Lagrådet lämnar förslagen utan erinran.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 19 april 2018

Närvarande: statsminister Löfven, ordförande, och statsråden Lövin, Y Johansson, M Johansson, Baylan, Hallengren, Bucht, Hultqvist, Hellmark Knutsson, Bolund, Damberg, Bah Kuhnke, Strandhäll, Shekarabi, Fridolin, Eriksson, Linde, Skog, Ekström, Fritzon, Eneroth

Föredragande: statsrådet M Johansson

Regeringen beslutar proposition Brottsdatalag