

# Regeringens proposition

## 2008/09:16



Godkännande av Dataskyddsrambeslutet

Prop.  
2008/09:16

---

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 18 september 2008

*Fredrik Reinfeldt*

*Beatrice Ask*  
(Justitiedepartementet)

## Propositionens huvudsakliga innehåll

I propositionen föreslås att riksdagen ska godkänna ett inom Europeiska unionen upprättat utkast till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (Dataskyddsrambeslutet).

Utkastet till rambeslut förpliktar medlemsstaterna att behandla sådana uppgifter som utbyts mellan staterna på de nämnda områdena på visst sätt. Det innehåller bestämmelser som avser att förstärka skyddet av information vid behandling av personuppgifter som överförs. Rambeslutet utgör, när det gäller dataskydd, ett komplement till andra instrument om informationsutbyte inom ramen för polisiärt och straffrättsligt samarbete.

Utkastet innehåller bestämmelser om allmänna utgångspunkter för behandlingen av personuppgifter, behandling av känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. I stora delar motsvarar utkastet till rambeslut det s.k. dataskyddsdirektivet, som har genomförts i svensk rätt genom personuppgiftslagen. Utkastet innehåller härutöver bl.a. särskilda skyddsbestämmelser avsedda att begränsa möjligheterna att behandla utbytta personuppgifter.

I propositionen görs en preliminär bedömning av vilka lagändringar som kan bli nödvändiga med anledning av rambeslutet. Propositionen innehåller inga lagförslag.

1	Förslag till riksdagsbeslut .....	5
2	Ärendet och dess beredning .....	6
3	Sammanfattning av innehållet i utkastet till rambeslut .....	7
4	Gällande rätt .....	9
4.1	Inledning .....	9
4.2	Grundläggande bestämmelser om behandling av personuppgifter .....	10
4.3	Personuppgiftslagen .....	10
4.3.1	Lagens tillämpningsområde .....	10
4.3.2	Grundläggande krav för behandlingen .....	11
4.3.3	Tillåten och otillåten behandling .....	11
4.3.4	Information och rättelse .....	12
4.3.5	Säkerhet vid behandlingen .....	13
4.3.6	Överföring av personuppgifter till tredjeland .....	13
4.3.7	Tillsyn .....	13
4.3.8	Sanktioner .....	14
4.4	Behandling av personuppgifter inom polisen .....	14
4.4.1	Allmänt om polisens behandling av personuppgifter .....	14
4.4.2	Polisdatalagen .....	15
4.4.3	Andra registerförfattningar .....	16
4.5	Andra myndigheters behandling av personuppgifter för brottsbekämpning .....	17
4.5.1	Tullverket .....	17
4.5.2	Kustbevakningen .....	19
4.5.3	Skatteverket .....	19
4.5.4	Åklagarväsendet .....	20
4.6	Lagstiftning om behandling av personuppgifter inom andra verksamhetsområden som berörs av rambeslutet .....	22
4.6.1	Allmänna utgångspunkter .....	22
4.6.2	Kriminalvården .....	22
4.6.3	Domstolsväsendet .....	24
4.7	Lagstiftning om internationellt samarbete .....	25
4.7.1	Inledning .....	25
4.7.2	Regler om användningsbegränsningar .....	26
4.7.3	Lagstiftning om samarbete i den brottsbekämpande verksamheten .....	26
4.7.4	Lagen om internationellt tullsamarbete .....	28
4.7.5	Lagen om internationell rättslig hjälp i brottmål .....	29
5	Genomförande av rambeslutet .....	29
5.1	Inget genomgripande behov av ny lagstiftning .....	29
5.2	Rambeslutets syfte och tillämpningsområde .....	30
5.2.1	Syftet med rambeslutet .....	30

5.2.2	Rambeslutets tillämpningsområde.....	31
5.2.3	Definitioner .....	33
5.3	Huvudregler om tillåtna ändamål för behandling av uppgifter .....	33
5.3.1	Innehållet i rambeslutet .....	33
5.3.2	Behovet av lagändringar.....	34
5.4	Begränsningar i rätten att behandla uppgifter.....	35
5.4.1	Inledning.....	35
5.4.2	Behandling av känsliga personuppgifter.....	35
5.4.3	Behandling av uppgifter för datoriserade beslut .....	36
5.4.4	Allmänna begränsningar för vidarebehandling .....	37
5.4.5	Begränsningar i den överförande statens nationella rätt.....	41
5.4.6	Skyldighet att iakttä överförande stats gallringsfrister.....	41
5.4.7	Begränsningar i rätten att överföra uppgifter till tredjeland eller till internationella organisationer .....	42
5.4.8	Begränsningar i rätten att överföra uppgifter till privata parter.....	43
5.4.9	Sammanfattning.....	44
5.5	Gallring.....	45
5.5.1	Innehållet i rambeslutet .....	45
5.5.2	Behovet av lagändringar.....	45
5.6	Information till den registrerade .....	45
5.6.1	Innehållet i rambeslutet .....	45
5.6.2	Behovet av lagändringar.....	46
5.7	Korrigerig av personuppgifter .....	47
5.7.1	Innehållet i rambeslutet .....	47
5.7.2	Behovet av lagändringar .....	48
5.8	Tillgång till rättsmedel .....	50
5.9	Säkerhet och skydd vid uppgiftsbehandling .....	51
5.9.1	Innehållet i rambeslutet .....	51
5.9.2	Behovet av lagändringar.....	52
5.10	Tillsyn.....	53
5.10.1	Innehållet i rambeslutet .....	53
5.10.2	Behovet av lagändringar.....	54
5.11	Skadestånd.....	55
5.12	Sanktioner.....	56
5.12.1	Innehållet i rambeslutet .....	56
5.12.2	Behovet av lagändringar .....	56
5.13	Övriga frågor .....	58
6	Godkännande av rambeslutet .....	58
7	Ekonomiska konsekvenser .....	65
Bilaga 1	Utkast till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.....	66

Bilaga 2	Utkast till rådsbeslut.....	110	Prop. 2008/09:16
Bilaga 3	Sammanfattning av promemorian.....	111	
Bilaga 4	Förteckning över remissinstanserna .....	112	
	Utdrag ur protokoll vid regeringssammanträde den 18 september 2008.....	113	

# 1 Förslag till riksdagsbeslut

Prop. 2008/09:16

Regeringen föreslår att riksdagen godkänner det inom Europeiska unionen upprättade utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ("Dataskyddsrambeslutet").

Den 4 november 2004 antog Europeiska rådet det s.k. Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen. Rådet uttalade där att en förstärkning av frihet, säkerhet och rättvisa kräver en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning. En princip bör vara att en tjänsteman vid en brottsbekämpande myndighet i en medlemsstat ska göra befintlig information tillgänglig för motsvarande befattningshavare i en annan stat om han eller hon behöver informationen för att utföra sina uppgifter.

Ett effektivare polissamarbete och rättsligt samarbete måste emellertid balanseras mot grundläggande rättigheter, bl.a. rätten till ett privatliv och rätten till skydd av personuppgifter. I Haagprogrammet uppmanades kommissionen att lägga fram förslag till genomförandet av principen om tillgänglighet för att förbättra det gränsöverskridande utbytet av information om brottsbekämpning mellan medlemsstaterna, under strikt iakttagande av centrala villkor i fråga om skydd av personuppgifter. Detta återspeglas i rådets och kommissionens handlingsplan för genomförande av Haagprogrammet.

Den 4 oktober 2005 presenterade kommissionen ett förslag till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Efter ingående förhandlingar i rådet, där medlemsstaterna inte kunde enas, omarbetades förslaget på ett genomgripande sätt under det tyska ordförandeskapet våren 2007. De fortsatta förhandlingarna fördes med det omarbetade förslaget som utgångspunkt.

De materiella bestämmelserna i utkastet till rambeslut är till stora delar identiska med motsvarande artiklar i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter (dataskyddsdirektivet).

Förutom medlemsstaterna inom Europeiska unionen har även Island, Norge och Schweiz deltagit i förhandlingarna om utkastet till rambeslut, som ett led i det utvidgade Schengensamarbetet.

Europaparlamentet har yttrat sig över det ursprungliga förslaget den 27 september 2006 och över det reviderade förslaget den 6 juni 2007. Europeiska datatillsynsmannen har avgett tre yttranden över utkastet till rambeslut, den 19 december 2005, den 29 november 2006 och den 27 april 2007.

I slutet av år 2007 nåddes en politisk principöverenskommelse om innehållet i utkastet till rambeslut, med reservation för vissa ändringar bl.a. i preambeln. Sverige lämnade i samband med det en parlamentarisk granskningsreservation. Europaparlamentet yttrade sig därefter på nytt i februari 2008. I juni 2008 gjordes en granskning av texten av Europeiska unionens språkexperter, de s.k. juristlingvisterna.

Utkastet till rambeslut i dess senaste lydelse på svenska finns i *bilaga 1*. Det bör noteras att numreringen av skälen i preambeln och artikelnumreringen i utkastet på grund av revideringar inte överensstämmer med numreringen i det utkast till rambeslut som har varit

föremål för remissbehandling. I *bilaga 2* finns ett utkast till rådsbeslut innefattande ett uttalande från rådet. Prop. 2008/09:16

En faktagenomnämning om förslaget har överlämnats till riksdagen (2005/06:FPM44 Skydd av personuppgifter i europeisk brottsbekämpning). Regeringen har under förhandlingsarbetet fortlöpande informerat och samrått med riksdagen. Företrädare för Justitiedepartementet har sammanträtt med Justitiekommittén och justitieministern har vid sammanträde i EU-nämnden redogjort för förhandlingsarbetet och den svenska positionen.

Eftersom utkastet innehåller bestämmelser som innebär att det behöver göras ändringar i svensk lag, krävs riksdagens godkännande innan Sverige kan rösta för ett antagande av rambeslutet i rådet (jfr 10 kap. 2 § regeringsformen). Mot bakgrund av det har en utredare biträtt Justitiedepartementet med att ta fram departementspromemorian Antagande av rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (Ds 2008:30), i det följande benämnd promemorian. I promemorian föreslås att riksdagen ska godkänna utkastet till rambeslut samt redovisa översiktligt vilket behov av lagändringar ett kommande rambeslut skulle leda till. En sammanfattning av promemorian finns i *bilaga 3*. Promemorian har remissbehandlats. En sammanställning av remissyttrandena finns tillgänglig i Justitiedepartementet (dnr Ju2008/3356/PO). En förteckning över remissinstanserna finns i *bilaga 4*.

Denna proposition beskriver innehållet i utkastet till rambeslut och redogör för hur beslutet förhåller sig till svensk rätt. I propositionen föreslås att riksdagen ska godkänna utkastet. Några lagförslag presenteras inte. Däremot innehåller propositionen en översiktlig beskrivning av i vilka avseenden ett antagande av rambeslutet bedöms kräva lagändringar. Regeringen avser att senare återkomma till riksdagen med förslag till lagändringar.

### 3 Sammanfattning av innehållet i utkastet till rambeslut

Utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (Dataskyddsrambeslutet, i fortsättningen rambeslutet) utgör ett komplement till olika instrument om utvidgat polisiärt samarbete och rättsligt samarbete inom Europeiska unionen med inriktning på utökad gränsöverskridande informationsutbyte.

Inledningsvis framhålls i beslutet att gemensamma insatser inom polissamarbetet och rörande straffrättsligt samarbete gör det nödvändigt att behandla information samtidigt som det måste finnas regler om skydd för personuppgifter. Gemensamma normer för behandling och skydd av personuppgifter kan både bidra till ett effektivare samarbete och värna grundläggande rättigheter som rätten till privatliv och rätten till skydd för personuppgifter. Det uttalas att befintliga instrument på europeisk nivå

inte är tillräckliga. Dataskyddsdirektivet är inte tillämpligt på behandling av personuppgifter inom det nu aktuella området.

Syftet med rambeslutet, vilket framgår av *artikel 1*, är att säkerställa en hög skyddsnivå för fysiska personers fri- och rättigheter när det gäller behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete. Rambeslutet är endast tillämpligt på uppgifter som har överförts till eller gjorts tillgängliga mellan medlemsstaterna eller mellan medlemsstater och myndigheter och informationssystem som har inrättats i enlighet med avdelning VI i EU-fördraget om polissamarbete och straffrättsligt samarbete, t.ex. Europol. Det framgår dock av *skäl 8* att det är medlemsstaternas avsikt att den nivå på dataskydd som gäller för nationell behandling motsvarar vad som föreskrivs i rambeslutet. Rambeslutet hindrar dock inte medlemsstaterna från att ha ett starkare skydd för behandling av personuppgifter än vad som anges i rambeslutet. Vidare bör tillnärmningen inte leda till ett svagare skydd för personuppgifter än det som medlemsstaternas nuvarande lagstiftning ger utan tvärtom syfta till att garantera en hög skyddsnivå inom hela unionen (*skäl 10*).

Endast behandling av personuppgifter som utförs helt eller delvis automatiskt samt annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register faller inom tillämpningsområdet. Från tillämpningsområdet undantas också viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet.

I *artikel 3* läggs vissa grundläggande principer för personuppgiftsbehandling fast, bl.a. huvudregeln att uppgifter inte får behandlas för något annat ändamål än det ursprungliga, dvs. det ändamål för vilket de överfördes eller gjordes tillgängliga. Personuppgifter får dock alltid vidarebehandlas av behöriga myndigheter för historiska, statistiska eller vetenskapliga ändamål under förutsättning att medlemsstaterna föreskriver lämpliga säkerhetsåtgärder, t.ex. aidentifiering av uppgifterna. Annan vidarebehandling är bara tillåten om det nya ändamålet inte är oförenligt med det ursprungliga och kräver som huvudregel enligt *artikel 11* den registrerades samtycke eller den överförande statens medgivande. Vidarebehandling får dock – om kraven i artikel 3 är uppfyllda – alltid ske för att förebygga, utreda, avslöja eller lagföra andra brott eller verkställa andra straffrättsliga påföljder än de för vilka uppgifterna överfördes. Likaså får vidarebehandling ske för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten.

*Artiklarna 4 och 5* innehåller bestämmelser om rättelse, radering och blockering av personuppgifter liksom om regelbunden kontroll av nödvändigheten av lagringen av uppgifterna. Kopplat till detta är bestämmelserna i *artikel 8* om åtgärder som ska vidtas av överförande myndigheter för att säkerställa att de personuppgifter som överförs är korrekta.

*Artikel 6* reglerar rätten att behandla s.k. känsliga uppgifter, dvs. uppgifter om t.ex. ras eller etniskt ursprung. Sådana uppgifter får endast behandlas när det är absolut nödvändigt och om det i den nationella lagstiftningen tillhandahålls tillräckliga skyddsåtgärder. I *artikel 7* anges att ett automatiserat beslutsförfarande som innefattar behandling av uppgifter som omfattas av rambeslutet är tillåtet endast om det föreskrivs i en lag där det även föreskrivs bestämmelser till skydd för den



registrerades legitima intressen. Även *artiklarna 9 och 12* innehåller bestämmelser om begränsningar i rätten att behandla uppgifter. Där framgår att den överförande staten har möjlighet att meddela tidsfrister för gallring av uppgifter och att vissa begränsningar i rätten att utbyta uppgifter mellan myndigheter i den överförande statens nationella rätt ska iakttas av den mottagande staten.

I *artiklarna 13 och 14* regleras under vilka förutsättningar uppgifter får överföras till tredjeland, internationella organ och privata subjekt i medlemsstaterna. Som huvudregel förutsätter sådan överföring dels att det finns en adekvat skyddsnivå för behandlingen av uppgifter hos mottagaren och att den medlemsstat från vilken uppgifterna härrör ha gett sitt samtycke till överföringen.

*Artiklarna 16–20* reglerar den registrerades rättigheter i olika avseenden, bl.a. rätt till information, rättelse, skadestånd och tillgång till rättsmedel. För att säkerställa genomförandet av rambeslutet ska medlemsstaterna enligt *artikel 24* föreskriva effektiva, proportionella och avskräckande sanktioner mot den som bryter mot bestämmelser som har antagits med anledning av rambeslutet.

*Artiklarna 21 och 22* reglerar viss tystnadsplikt samt föreskriver krav på säkerhet i samband med behandlingen av uppgifter. Enligt *artikel 25* skall varje medlemsstat utse en eller flera nationella tillsynsmyndigheter som ska ansvara för rådgivning och kontroll av behandlingen av uppgifter som omfattas av beslutet.

*Artikel 26* behandlar förhållandet mellan rambeslutet och andra överenskommelser med tredjeland och *artikel 28* reglerar förhållandet mellan rambeslutet och befintliga rättsakter. Slutligen återfinns bestämmelser om genomförande och utvärdering av rambeslutet i *artiklarna 27 och 29*.

## 4 Gällande rätt

### 4.1 Inledning

Rambeslutet innehåller ett antal bestämmelser som innebär förpliktelser för medlemsstaterna. Dessa överensstämmer i många avseenden med förpliktelserna i dataskyddsdirektivet, som har genomförts i Sverige genom personuppgiftslagen (1998:204). Eftersom man i svensk lagstiftning har valt att genomföra dataskyddsdirektivet generellt, finns det redan författningar som reglerar personuppgiftsbehandlingen inom de verksamhetsområden som berörs av rambeslutets tillämpningsområde.

Något generaliserat kan man uttrycka det så att det rör sig om tre olika typer av författningsreglering; dels sådana lagar som reglerar ett eller flera enskilda register, dels generella författningar för en viss sektor av samhället, som dessutom kan reglera ett eller flera register, och dels personuppgiftslagen som tillämpas helt eller delvis. De författningar som gäller vid sidan av personuppgiftslagen brukar betecknas registerförfattningar. För att förenkla framställningen här används benämningen sektorsförfattningar för de författningar som gäller för ett visst verksamhetsområde, t.ex. polisdatalagen (1998:622). Det finns exempel på verk-

samheter där såväl personuppgiftslagen och en sektorsförfattning som särbestämmelser för ett visst register ska tillämpas samtidigt. Regleringen på området är således mycket komplex.

I detta avsnitt ges en beskrivning av den reglering som styr personuppgiftsbehandlingen på de områden som omfattas av rambeslutet. Beskrivningen tar särskilt sikte på sådana bestämmelser i svensk rätt som har relevans för bedömningen av om svensk rätt uppfyller rambeslutet.

## 4.2 Grundläggande bestämmelser om behandling av personuppgifter

Enligt 2 kap. 3 § regeringsformen får anteckning om medborgare i allmänt register inte utan hans samtycke grundas enbart på hans politiska åskådning. Vidare ska varje medborgare, i den utsträckning som närmare anges i lag, skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling.

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller sedan år 1995 som svensk lag. Två av artiklarna i konventionen, artikel 8 och artikel 13, har betydelse för myndigheters rätt att behandla personuppgifter.

Artikel 8 föreskriver att var och en har rätt till skydd för bl.a. sitt privat- och familjeliv. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Kravet på att inskränkningen ska ha lagstöd anses innebära att inskränkningen måste vara utformad med sådan precision att den är i rimlig utsträckning förutsebar.

I artikel 13 föreskrivs att var och en, vars i konventionen angivna fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet.

## 4.3 Personuppgiftslagen

### 4.3.1 Lagens tillämpningsområde

Personuppgiftslagen är generellt tillämplig och innehåller generella riktlinjer för behandling av personuppgifter, oavsett ändamålet med behandlingen. Lagen ersatte den tidigare datalagen (1973:289) när data-skyddsdirektivet genomfördes i svensk rätt. På polisområdet gäller dock datalagen alltså för vissa register.

Personuppgiftslagen är subsidiär i förhållande till annan författningsreglering (2 §). Samtidigt som personuppgiftslagen infördes tillskapades särskilda lagar och förordningar som reglerar behandlingen av personuppgifter för ett visst verksamhetsområde, för en viss typ av register eller för ett bestämt register. I polisdatalagen och motsvarande författningar för Skatteverkets och Kustbevakningens brottsbekämpande verksamhet

finns särreglering som till stora delar ersätter personuppgiftslagen. Motsvarande gäller för personuppgiftsbehandlingen inom åklagarväsendet, domstolsväsendet och kriminalvården. För Tullverkets del har en annan lagstiftningsmodell valts, men resultatet är detsamma, nämligen att personuppgiftslagen delvis gäller. Utgångspunkten har varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (prop. 1990/91:60 s. 58 och KU 1990/91:11 s. 11).

Personuppgiftslagen reglerar hur personuppgifter får hanteras. Lagen ska tillämpas på all 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 vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen kompletteras av personuppgiftsförordningen (1998: 1191).

### 4.3.2 Grundläggande krav för behandlingen

I 9 § personuppgiftslagen slås fast vissa grundläggande krav för all behandling av personuppgifter. Sådana uppgifter ska alltid behandlas på ett korrekt och lagligt sätt samt i enlighet med god sed. Personuppgifter ska samlas in och behandlas för särskilda, uttryckligt angivna 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 riktiga 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 inte uppfyller dessa krav, 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. Därefter ska de oidentifieras eller förstöras. Behandling som sker för att bevara uppgifter för historiska, statistiska eller vetenskapliga ändamål får dock ske under längre tid än vad som är nödvändigt för de ursprungliga ändamålen. Det möjliggör t.ex. behandling i form av elektronisk arkivering av personuppgifter.

### 4.3.3 Tillåten och otillåten behandling

I lagen finns en uttömmande uppräkningslista av under vilka förutsättningar behandling av personuppgifter är tillåten (10–12 §§). Av särskilt intresse i detta sammanhang är 13 § som förbjuder behandling av känsliga personuppgifter. Känsliga personuppgifter definieras i lagen som uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Förbudet mot behandling av

känsliga uppgifter är inte undantagslöst. Det gäller inte personuppgifter som inte ingår i eller är avsedda att ingå i strukturerat material, dvs. en samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier (5 a §). I 14–19 §§ anges under vilka förutsättningar känsliga uppgifter får behandlas. Undantag från förbudet görs t.ex. för viss nödvändig behandling, bl.a. för att den registrerades eller annans vitala intressen ska kunna skyddas och den registrerade inte kan lämna samtycke till behandlingen. Det finns också utrymme för regeringen, eller den myndighet regeringen bestämmer, att meddela föreskrifter om ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse (20 §). Sådana föreskrifter finns i 8 § personuppgiftsförordningen. Av den bestämmelsen följer att myndigheter generellt även får behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ärendet.

Enligt 21 § personuppgiftslagen är det som huvudregel förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. 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.

#### 4.3.4 Information och rättelse

Personuppgiftslagen innehåller ett flertal bestämmelser som syftar till att genom information trygga den enskildes rätt att kontrollera om behandling av personuppgifter om honom eller henne pågår. Har uppgifterna samlats in från någon annan än den enskilde, ska den registrerade informeras när uppgifterna registreras, eller om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången (24 §). Information behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnande av uppgifterna i lag eller författning eller om det skulle vara omöjligt eller kräva en oproportionerligt stor arbetsinsats. Informationen ska omfatta uppgift om vem som är personuppgiftsansvarig, ändamålet med behandlingen samt all övrig information som den registrerade behöver för att kunna ta tillvara sina rättigheter i samband med behandlingen (25 §). Den personuppgiftsansvarige är vidare skyldig att efter ansökan, en gång per år, gratis informera om huruvida och i så fall vilka uppgifter om sökanden som behandlas, ändamålet med behandlingen, varifrån uppgifterna kommer och till vem de lämnas ut (26 §). Det bör anmärkas att uppgiftsskyldigheten inte omfattar alla uppgifter, bl.a. inte uppgifter som omfattas av sekretess eller tystnadsplikt gentemot den registrerade (27 §).

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen, ska på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgifts-

#### **4.3.5 Säkerhet vid behandlingen**

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 uppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige har ett stort ansvar för säkerheten.

#### **4.3.6 Överföring av personuppgifter till tredjeland**

Enligt 33 § personuppgiftslagen är det förbjudet att föra över personuppgifter under behandling till tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring 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 databehandling av personuppgifter. I 35 § finns vissa bemyndiganden som avser möjligheten att besluta om ytterligare undantag från förbudet i 33 §. I bilagor till personuppgiftsförordningen anges vissa länder som enligt särskilt beslut av Europeiska gemenskapernas kommission anses ha en adekvat skyddsnivå för behandlingen av personuppgifter eller som har slutit avtal med Europeiska unionen om överföring av vissa slags uppgifter om flygpassagerare.

#### **4.3.7 Tillsyn**

Datainspektionen är enligt 2 § personuppgiftsförordningen tillsynsmyndighet enligt personuppgiftslagen. Det kan redan här nämnas att de sektorsförfattningar som gäller utöver personuppgiftslagen som är aktuella i detta sammanhang (se avsnitt 4.4 och 4.5.2–4.6) inte innehåller några avvikande bestämmelser i fråga om tillsynsmyndighet. Datainspektionen har därför ansetts vara tillsynsmyndighet även enligt de särskilda sektorsförfattningarna (se t.ex. prop. 2004/05:164 s. 53 f.). Detsamma gäller för andra särskilda registerförfattningar.

Datainspektionen har enligt 43 § personuppgiftslagen för sin tillsyn rätt att på begäran få tillgång till de personuppgifter som behandlas och upplysningar och dokumentation av behandlingen och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Om tillsynsmyndigheten inte, efter

begäran kan få tillräckligt underlag för att konstatera att behandlingen är laglig, får myndigheten enligt 44 § vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än att lagra dem. Det bör dock framhållas att det anses vara en allmän rättsgrundsats att vite inte bör användas mot statliga myndigheter (prop. 2004/05:164 s. 54 och 2006/07:46 s. 105).

Enligt 45 § ska myndigheten, om den konstaterar att uppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt, eller om saken är brådskande, får myndigheten på motsvarande sätt förbjuda annan behandling än lagring. Tillsynsmyndigheten får också, enligt 47 §, ansöka hos länsrätten om att sådana uppgifter som har behandlats på olagligt sätt ska utplånas.

#### **4.3.8 Sanktioner**

Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada för den registrerade har vederbörande, enligt 48 §, rätt till skadestånd från den personuppgiftsansvarige. Skadeståndsansvaret är i princip strikt. Den registrerade behöver bara visa att det förekommit en felaktig behandling och att denna skadat eller kränkt honom eller henne.

Lagen innehåller också en straffbestämmelse i 49 §. Till böter eller fängelse i högst sex månader döms bl.a. den som uppsåtligen eller av grov oaktsamhet behandlar personuppgifter i strid med bestämmelserna om behandling av känsliga personuppgifter eller för över personuppgifter till tredjeland i strid med bestämmelserna i 33–35 §§.

### **4.4 Behandling av personuppgifter inom polisen**

#### **4.4.1 Allmänt om polisens behandling av personuppgifter**

Polisdatalagen bygger, som har framgått ovan, på personuppgiftslagen och innehåller de särregler som har ansetts nödvändiga i polisens verksamhet. Den kompletteras av polisdataförordningen (1999:81). Personuppgiftslagen gäller i de frågor som inte regleras i polisdatalagen.

Polisdatalagen utgör bara en del av lagstiftningen om polisens register. Polisens register kan i princip delas in i tre kategorier, beroende på vilka bestämmelser som styr behandlingen. Dessa är

- register som förs med stöd av bestämmelser om särskilda register i polisdatalagen eller annan registerlagstiftning,
- register som förs med stöd av allmänna bestämmelser i polisdatalagen och personuppgiftslagen, och
- register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av den numera upphävda datalagen och Datainspektionens tillstånd.

Andra registerförfattningar som är av intresse i detta sammanhang är lagen (1998:620) om belastningsregister och lagen (1998:621) om

misstankeregister. I övrigt kan nämnas lagen (2000:344) om Schengens informationssystem (se avsnitt 4.7.3), lagen (2006:444) om passagerarregister, förordningen (1997:903) om ordningsbottsregister och förordningen (1997:902) om strafförelägganderegister.

Prop. 2008/09:16

#### 4.4.2 Polisdatalagen

##### *Allmänt om regleringen*

Polisdatalagen innehåller både allmänna regler om behandling av personuppgifter i polisiärt arbete och, som nyss nämnts, regler om vissa särskilda register. Behandling av personuppgifter som sker med stöd av lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem eller lagen om passagerarregister har undantagits från lagens tillämpningsområde.

Polisdatalagen gäller, utöver personuppgiftslagen, vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att

- förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
- övervaka den allmänna ordningen och säkerheten,
- hindra störningar av den allmänna ordningen och säkerheten samt ingripa när något sådant inträffat eller
- bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

I polisdatalagen finns vissa allmänna bestämmelser om behandling av personuppgifter. I 5 § regleras tillåtligheten av behandling av känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen). Sådana uppgifter får inte behandlas enbart på grund av vad som är känt om en person om sådana förhållanden. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med känsliga personuppgifter när det är oundgängligen nödvändigt för syftet med behandlingen. Vidare finns bestämmelser om utlämnande av uppgifter (6–8 §§). I detta sammanhang är av särskilt intresse den bestämmelse som reglerar möjligheten att lämna ut uppgifter till utländska myndigheter och mellanfolkliga organisationer (7 §). Huvudregeln är att uppgifter får lämnas ut om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Därutöver finns bestämmelser om rättelse och skadestånd (9 §). De allmänna bestämmelserna gäller även för behandling av personuppgifter i register som inte är automatiserade (se 2 §).

Polisdatalagen innehåller också särskilda bestämmelser om vissa register som förs med hjälp av automatiserad behandling, bl.a. kriminalunderrättelseregister (17–21 §§). Med underrättelseverksamhet avses den polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats, eller kan komma att utövas, och som inte utgör förundersökning enligt 23 kap.

rättegångsbalken. Med kriminalunderrättelseverksamhet avses annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen.

Automatiserad behandling av personuppgifter i kriminalunderrättelseverksamhet får – förutom i kriminalunderrättelseregister – förekomma i s.k. särskilda undersökningar. Sådana får inledas efter särskilt beslut, om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas och har till syfte att ge underlag för beslut om förundersökning eller för beslut om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott (14 §).

#### *Register som regleras särskilt i polisdatalagen*

En typ av register som regleras särskilt i polisdatalagen är, som har nämnts ovan, *kriminalunderrättelseregister*. Sådana får föras för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslig verksamhet eller för att underlätta tillgången till allmänna uppgifter med anknytning till kriminalunderrättelseverksamhet. Ett sådant register får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet har utövats eller kan komma att utövas. Det krävs vidare som huvudregel att den person som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva den allvarliga brottsliga verksamheten.

Register med *uppgifter om DNA-analyser* i brottmål regleras också särskilt, liksom *fingeravtrycksregister* och *signalements- och känneteckensregister* (22–31 §§).

Säkerhetspolisen ska föra ett särskilt register (*SÄPO-registret*) som har till ändamål att underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet och bekämpa terrorism. Registret ska också utgöra underlag för registerkontroll enligt säkerhetsskyddslagen (1996:627). Registret, som regleras i 32–35 §§ polisdatalagen, innehåller endast identifieringsuppgifter, uppgifter om grunden för registrering och hänvisning till de ärenden där uppgifter om den registrerade behandlas. All behandling av personuppgifter av betydelse för verksamheten sker i andra system (för en närmare beskrivning, se Ds 2007:43 s. 295).

#### *Förslag till ny lagstiftning om behandling av personuppgifter i polisens brottsbekämpande verksamhet*

Ett förslag till en ny reglering, som ska ersätta polisdatalagen och polisdataförordningen har presenterats i departementspromemorian *Behandling av personuppgifter i polisens brottsbekämpande verksamhet* (Ds 2007:43). Promemorian har remissbehandlats och en proposition planeras till våren 2009.

### **4.4.3 Andra registerförfattningar**

Som har nämnts inledningsvis i detta avsnitt finns det ett antal registerförfattningar som reglerar register som förs helt eller delvis inom



ramen för polisens brottsbekämpande verksamhet, nämligen lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem, lagen om passagerarregister, förordningen om ordningsbotsregister och förordningen om strafförelägganderegister.

De uppräknade författningarna innehåller bestämmelser om personuppgiftsbehandling när det gäller respektive register. I var och en av dessa författningar regleras bl.a. ändamålet med registret, vilka uppgifter som får finnas i registret och när de ska gallras. Lagen om Schengens informationssystem behandlas kort i avsnitt 4.7.3. För en närmare genomgång av författningarna i övrigt hänvisas till promemorian.

Särskilda bestämmelser om vapenregister finns därutöver i vapenlagen (1996:67).

## 4.5 Andra myndigheters behandling av personuppgifter för brottsbekämpning

### 4.5.1 Tullverket

Tullverkets behandling av personuppgifter regleras i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och i förordningen (2005:791) i samma ämne.

Lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet behandlar i stort sett samma frågor som polisdatalagen men är uppbyggd på ett något annorlunda sätt. Den gäller bl.a., till skillnad från flertalet andra författningar om behandling av personuppgifter, *i stället* för personuppgiftslagen (5 §). I 6 § hänvisas dock till vissa bestämmelser i personuppgiftslagen.

Lagen innehåller dels allmänna regler om behandling av personuppgifter i tullens brottsbekämpande arbete, dels bestämmelser om en särskild databas, tullbrottsdatabasen (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 (1 §). Lagen tillämpas även i viss utsträckning på behandling av uppgifter om juridiska personer.

Personuppgifter får behandlas i Tullverkets brottsbekämpande verksamhet om det behövs för att förhindra eller upptäcka brottslig verksamhet, för att utreda eller beivra visst brott, eller för att fullgöra det arbete som Tullverket är skyldigt att utföra enligt lagen (2000:1219) om internationellt tullsamarbete (7 §). Vidare får personuppgifter behandlas när det är nödvändigt för att tillhandahålla information till andra svenska brottsbekämpande myndigheter (8 §). Uppgifter får enligt 9 § som huvudregel inte behandlas för några andra ändamål än de som anges i 7 och 8 §§ (jfr finalitetsprincipen i 9 § d personuppgiftslagen). Uppgifter får lämnas ut till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till andra.

Känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen), får inte behandlas enbart på grund av vad som är

känt om en person om 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 (11 §).

I 12–15 §§ anges de närmare förutsättningarna för behandling av uppgifter för de tre huvudsyften som anges i 7 §.

För ändamålet att förhindra eller upptäcka brottslig verksamhet får enligt 12 § uppgifter behandlas i följande fall

- om uppgifterna dels ger anledning att anta att brottslig verksamhet, som innefattar brott för vilket är föreskrivet fängelse i minst två år har utövats eller kan komma att utövas, eller som innefattar andra brott, om verksamheten sker systematiskt, dels kan hänföras till en person och gör att personen skäligen kan misstänkas för verksamheten i fråga,
- om uppgifterna avser sådana transportmedel, varor eller hjälpmedel som kan antas ha samband med sådan verksamhet som nyss sagts och inte kan hänföras till en person, eller
- om uppgifterna avser en person som, utan att vara skäligen misstänkt, kan antas ha samband med sådan verksamhet.

Dessutom får uppgifter om passagerare, importörer, exportörer och transportörer samt varor och transportmedel behandlas i syfte att förhindra eller upptäcka brottslig verksamhet (13 §).

För ändamålet att utreda och beivra brott får uppgifter om den som misstänkas för brottet och om andra personer behandlas när det behövs för att utreda eller beivra brottet (14 §).

Som huvudregel ska uppgifter om personer som inte är misstänkta eller kan komma att misstänkas för brott fördes med en särskild upplysning om detta. Uppgifter om en person som kan ha samband med brottslig verksamhet ska fördes med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak (16 §).

I 19 § anges i detalj vilka typer av personuppgifter som får behandlas i tullbrottsdatabasen och i 20–22 §§ anges vilka sökbegrepp som får användas. Lagen innehåller också regler om när gallring av olika uppgifter ska ske (27 och 28 §§). Det bör noteras att 27 § innehåller ett bemyndigande för regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter om att uppgifter ska bevaras under längre tid än de frister som annars gäller. I bestämmelsen anges inte för vilka ändamål det får föreskrivas att uppgifter ska bevaras längre. I 4 § förordningen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet förskrivs att uppgifter och handlingar i ett ärende som avser prövning av om förundersökning skall inledas får bevaras längre än vad som anges 27 § i lagen men att de ska gallras senast vid utgången av det kalenderår då påföljd inte längre kan dömas ut för de brott som omfattades av prövningen av om förundersökning ska inledas.

Slutligen finns bestämmelser om information till den registrerade (29 §) och överklagande (30 §).

Kustbevakningens behandling av personuppgifter regleras i dag av personuppgiftslagen och förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen. Till skillnad från motsvarande författning för Tullverket, som gäller istället för personuppgiftslagen, gäller förordningen alltså utöver personuppgiftslagen (1 §). Förordningen är dock uppbyggd på ungefär samma sätt som Tullverkets författning. Kustbevakningen är personuppgiftsansvarig för behandlingen (8 §). I det följande redovisas endast de regler i förordningen som gäller för den brottsbekämpande verksamheten.

I förordningen finns dels allmänna regler om behandling av personuppgifter i Kustbevakningen brottsbekämpande arbete, dels bestämmelser om ett särskilt register för den verksamhet som förordningen omfattar, kustbevakningsdatabasen. I den brottsbekämpande verksamheten får personuppgifter behandlas om det är nödvändigt för att förhindra eller upptäcka brottslig verksamhet som innefattar brott mot vilka Kustbevakningen har att ingripa, eller för att utreda sådana brott (4 §). Känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen), får inte behandlas enbart på grund av vad som är känt om en person om sådana förhållanden. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med känsliga personuppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen (9 §). I förordningen skiljer man mellan uppgifter som används gemensamt i verksamheten (kustbevakningsdatabasen) och uppgifter som endast enskilda eller begränsade grupper av tjänstemän har tillgång till (11 §). Behandlingen av uppgifter i kustbevakningsdatabasen omgärdas av särskilda regler när det gäller de personer om vilka uppgifter får behandlas, vilka uppgifter som får förekomma och sökbegränsningar. I förordningen finns också bl.a. bestämmelser om sökning och gallring. Personuppgiftslagens bestämmelser om rättelse och skadestånd tillämpas på behandling enligt förordningen (23 §).

Det bör i sammanhanget nämnas att det föreligger ett förslag till ny reglering av behandlingen av personuppgifter inom Kustbevakningen. (se Ds 2007:43 s. 388 ff.). Inom Forsvarsdepartementet förbereds en lagrådsremiss som behandlar ny lagstiftning på området.

#### 4.5.3 Skatteverket

I lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och förordningen (1999:105) i samma ämne regleras behandlingen av personuppgifter i verkets brottsbekämpande verksamhet. Lagen – som gäller dels för spaning och utredning av brott, dels för att förebygga brott – är uppbyggd med polisdatalagen som förebild och gäller utöver personuppgiftslagen. Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om person-

uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

Skatteverkets brottsbekämpande verksamhet avser i första hand sådana brott som anges i 1 § lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar, bl.a. brott enligt skattebrottslagen (1971:69) och lagen (1986:436) om näringsförbud. Eftersom Skatteverket får medverka vid förundersökning i fråga om andra brott, om åklagaren finner särskilda skäl för det (1 § lagen om Skatteverkets medverkan i brottsutredningar), omfattar tillämpningsområdet för de nämnda sektorsförfattningarna avseende Skatteverkets personuppgiftsbehandling även sådana brott.

I lagen regleras underrättelseregister, som får föras dels för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslighet, dels för att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet. Lagen innehåller en uttömmande reglering av vilka typer av personuppgifter som får förekomma i underrättelseregister (10 §). Ett underrättelseregister får som huvudregel innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslighet utövats eller kan komma att utövas och den som avses med uppgifterna skäligen kan misstänkas för denna verksamhet. Känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen), får inte behandlas enbart på grund av vad som är känt om en person om sådana förhållanden (4 §). Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Känsliga personuppgifter får dock aldrig behandlas i underrättelseverksamhet.

Lagen innehåller också uppgifter om utlämnande av uppgifter, bl.a. till utländska myndigheter och organisationer (6 §), och om gallring (15 §). Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt lagen (16 §). Skatteverkets beslut i fråga om rättelse får överklagas (17 §).

#### 4.5.4 Åklagarväsendet

Förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet gäller utöver personuppgiftslagen (1 §). Den är tillämplig på Åklagarmyndighetens och Ekobrottsmyndighetens åklagarverksamhet, om behandlingen av personuppgifter är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Sådan behandling av personuppgifter som regleras i förordningen om register över strafförelägganden har undantagits från tillämpningsområdet.

I förordningen anges uttömmande vilken behandling av personuppgifter som är tillåten. Huvudregeln är att uppgifter om den som kan misstänkas för brott och om andra personer får behandlas, när det behövs för att en åklagare ska kunna utföra de uppgifter som enligt rättegångsbalken eller annan författning ankommer på åklagare (7 §). Vidare får

personuppgifter behandlas för tillsyn, planering, uppföljning eller framställning av statistik. Dessutom får uppgifter behandlas när det är nödvändigt för att tillhandahålla information som behövs i författningsreglerad verksamhet hos en brottsbekämpande eller brottsbeivrande myndighet eller för att lämna uppgifter till andra, om uppgiftsskyldighet följer av lag eller förordning (8 och 9 §§). Känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen), får inte behandlas enbart på grund av vad som är känt om en person om sådana förhållanden (10 §). Om uppgifterna finns i en handling som kommit in till myndigheten får de dock behandlas. Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen.

Inom åklagarväsendet förs en ärendedatabas, vars ändamål och innehåll regleras i förordningen. I 13 § anges vilka personuppgifter som ärendedatabasen får innehålla. Det rör sig bl.a. om uppgifter som behövs för kommunikation med personen, uppgifter om en fysisk eller juridisk persons ställning och koppling till andra personer i ett ärende samt uppgifter om fysiska personernas personliga och ekonomiska förhållanden, om juridiska personers ekonomiska förhållanden, uppgifter om brottshjälpmedel och transportmedel samt om beslut, händelser och åtgärder i ett ärende. Förordningen reglerar också vilka sökbegrepp som får användas vid sökning i ärendedatabasen (14–16 §§) samt gallring (21 §) och utlämnande av uppgifter (17 och 18 §§). Uppgifter får som huvudregel lämnas ut till en utländsk myndighet eller en mellanfolklig organisation, endast om utlämnandet sker inom ramen för ett samarbete som är reglerat i en internationell överenskommelse som är bindande för Sverige. Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt förordningen (19 §).

Åklagarmyndigheten får enligt 3 § förordningen (1997:902) om register över strafförelägganden föra ett centralt register för strafförelägganden. Vidare får Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket enligt 2 § föra lokala register över strafförelägganden. I 9 § finns bestämmelser om vilka uppgifter som registren får innehålla. Det rör sig såvitt gäller strafförelägganderegister bl.a. om uppgifter om den misstänkte och om målsäganden samt om gärningen, påföljden, beslut i ärendet och underrättelser. I 17 och 18 §§ anges vilka sökbegrepp som får användas vid sökning i registren. Förordningen innehåller inga bestämmelser om rättelse av felaktiga uppgifter eller om skadestånd för otillåten behandling av personuppgifter.

Det bör i sammanhanget nämnas att det pågår ett arbete med att utarbeta förslag till en ny reglering avseende den behandling av personuppgifter som sker inom åklagarväsendet och som avser brottsutredning, åtal eller andra åtgärder vid brottsbekämpning. Regeringen beslutade i september 2007 direktiv för en översyn av reglerna om personuppgiftsbehandling inom åklagarväsendet (dir. 2007:126). Utredningsuppdraget ska redovisas senast den 30 september 2008.

## 4.6 Lagstiftning om behandling av personuppgifter inom andra verksamhetsområden som berörs av rambeslutet

Prop. 2008/09:16

### 4.6.1 Allmänna utgångspunkter

Tillämpningsområdet för rambeslutet omfattar även internationellt rättsligt samarbete, bl.a. rättslig hjälp och verkställighet av straffrättsliga påföljder. Eftersom det även omfattar verkställighet av straffpåföljder sträcker det sig alltså utanför de brottsbekämpande myndigheternas krets.

Rättsligt samarbete hanteras till viss del av åklagarväsendet men även domstolsväsendet berörs. Enligt vissa författningar ska nämligen domstol pröva frågor om rättslig hjälp eller meddela beslut som krävs för handläggningen av exempelvis överlämnanden enligt den europeiska arresteringsordern eller ärenden om rättslig hjälp. Vidare ska domstol besluta i vissa frågor som rör övertagande av straffverkställighet. På verkställighetsstadiet berörs framför allt kriminalvården.

Det straffrättsliga samarbetet äger rum genom direkt kommunikation mellan berörda myndigheter eller via respektive stats centralmyndighet. Centralmyndigheten för rättslig hjälp i brottmål (som ingår i Regeringskansliet) har bl.a. till uppgift att motta och överlämna framställningar om rättslig hjälp i de fall där direktkommunikation inte får eller kan användas. Utvecklingen inom Europeiska unionen går dock mot lösningar som bygger på kommunikation direkt mellan berörda myndigheter såsom åklagare, domstolar och de myndigheter som svarar för verkställighet av straffrättsliga påföljder. Centralmyndighetens roll när det gäller internationellt rättsligt samarbete mellan medlemsstaterna i Europeiska unionen är därför numera ytterst begränsad.

När det gäller utlämningsärenden, överlämnande enligt en europeisk arresteringsorder och överförande av straffverkställighet kan följande sägas. Hanteringen av sådana ärenden styrs av särskilda regleringar i lagen (2003:1156) om överlämnande från Sverige enligt en arresteringsorder, lagen (1957:668) om utlämning för brott, lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge samt lagen (1972:260) om internationellt samarbete rörande verkställighet av brottmålsdom. Innehållet i dessa författningar redogörs inte närmare för här eftersom de inte innehåller några särskilda bestämmelser om personuppgiftsbehandling. En redogörelse för innehållet i de aktuella författningarna finns i promemorian (avsnitt 5.4–5.5).

### 4.6.2 Kriminalvården

#### *Allmänt om regleringen*

Kriminalvårdens behandling av personuppgifter regleras i lagen (2001:617) om behandling av personuppgifter inom kriminalvården och förordningen (2001:682) i samma ämne. Regleringen gäller för samtliga myndigheter inom kriminalvården, således inte bara för myndigheten

Kriminalvården utan även för övervakningsnämnderna och Kriminalvårdsnämnden.

Lagen innehåller vissa särbestämmelser i förhållande till personuppgiftslagen, som i övrigt gäller för kriminalvårdens verksamhet (2 §). Lagen innehåller endast övergripande bestämmelser för behandlingen, medan förordningen bl.a. innehåller bestämmelser om de register som ska föras inom kriminalvården (centrala kriminalvårdsregistret och säkerhetsregistret) och detaljerade regler om vilka typer av uppgifter som får behandlas beträffande olika personkategorier.

Lagen gäller 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 utländsk dom ska verkställa en av ovan nämnda påföljder i Sverige,
- har ålagts förvandlingsstraff för böter eller vite,
- på annan grund är intagna i häkte eller kriminalvårdsanstalt, eller
- som annars transporteras av kriminalvårdens transporttjänst.

Enligt 3 § får personuppgifter behandlas bara om det är nödvändigt 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 häktning, verkställighet av påföljd, intagning av annat skäl eller transport.

Känsliga personuppgifter, dvs. uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr 13 § personuppgiftslagen), får inte behandlas enbart på grund av det förhållandet. Om uppgifter om en person behandlas på annan grund får uppgifterna kompletteras med sådana uppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen. Sådana uppgifter får inte användas som sökbegrepp, om inte regeringen har föreskrivit det. Bara de personer som behöver det på grund av sina arbetsuppgifter får ha direktåtkomst till uppgifter (5–6 §§).

Reglerna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt lagen eller enligt föreskrifter som har meddelats med stöd av lagen. Ett beslut om rättelse eller om information enligt 26 § personuppgiftslagen får överklagas hos allmän förvaltningsdomstol (12 §). Beslutet ska dock först omprövas av Kriminalvården (13–15 §§).

#### *Register som regleras särskilt*

Det *centrala kriminalvårdsregistret* regleras i 34–36 §§ i förordningen. Ändamålet med registret är dels att myndigheten ska kunna fullgöra sina

författningenliga uppgifter, dels att underlätta tillgången till sådana uppgifter om verkställighet av påföljd som rättsväsendets myndigheter behöver. Registret omfattar endast personer som har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, eller har ålagts förvandlingsstraff för böter eller vite, eller som på grund av utländsk dom ska verkställa en sådan påföljd i Sverige.

*Säkerhetsregistret* regleras i 39–41 samt i 43–46 §§. Ändamålet med registret är att upprätthålla ordningen och att förebygga brott. Registret omfattar endast personer som är häktade eller intagna i vissa kriminalvårdsanstalter för att avtjäna fängelsestraff eller som ska verkställa en utländsk sådan påföljd. Registrering av uppgifter i registret förutsätter därutöver att vissa särskilda omständigheter föreligger, t.ex. att den som registreringen avser tidigare har rymt eller har gjort sig skyldig till allvarligt hot eller våld mot personal eller mot andra intagna eller att det föreligger 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 bl.a. sådana journaler lämnas ut till den myndighet i den andra staten som är ansvarig för verkställigheten (48 §).

### 4.6.3 Domstolsväsendet

Behandlingen av personuppgifter inom domstolsväsendet regleras, såvitt är av intresse i detta sammanhang, i tre olika förordningar. En av dem innehåller bestämmelser om behandlingen i allmän domstol och de två andra bestämmelser om behandlingen i förvaltningsdomstol.

Förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling gäller vid automatiserad behandling av personuppgifter i Högsta domstolens, hovrätternas och tingsrätternas rättskipande och rättsvårdande verksamhet. Vid de allmänna förvaltningsdomstolarna tillämpas förordningen (2001:641) om registerföring m.m. vid Regeringsrätten och kammarrätterna med hjälp av automatiserad behandling respektive förordningen (2001:640) om registerföring m.m. vid länsrätt med hjälp av automatiserad behandling.

De tre förordningarna är uppbyggda på samma sätt och innehåller i stor utsträckning likalydande bestämmelser. Redogörelsen i det följande omfattar således alla tre förordningarna, om inte annat sägs. Förordningarna gäller utöver personuppgiftslagen, som således i övrigt gäller för personuppgiftsbehandlingen inom domstolsväsendet. Förordningarna innehåller bestämmelser om två typer av register, nämligen verksamhetsregister och rättsfallsregister.

Domstolarna får föra *verksamhetsregister*, vilkas övergripande ändamål är att vara ett hjälpmedel vid handläggningen av mål och ärenden. Enligt förordningarna får registren användas för handläggning av mål och ärenden, planering, uppföljning och utvärdering av verksamheten, och framställning av statistik. För andra domstolar än länsrätter finns ett fjärde ändamål, nämligen att fullgöra författningenlig underrättelse-skyldighet. Ett verksamhetsregister får endast innehålla de uppgifter som



anges i en detaljerad uppräknning i en bilaga till respektive förordning. Det rör sig om uppgifter om bl.a. mål eller ärenden, om parter och andra aktörer, om personer som ska höras eller yttra sig, om förhandling, om handläggningen i övrigt och om rättegångskostnader.

Vid angivande av vad saken gäller (ärendemening) får sådana känsliga personuppgifter som anges i 13 § personuppgiftslagen och uppgifter om lagöverträdelser m.m. som anges i 21 § personuppgiftslagen behandlas endast om det är nödvändigt för att saken ska kunna återges på ett ändamålsenligt sätt. I övrigt får sådana uppgifter behandlas endast om uppgifterna har lämnats i ett mål eller ärende eller om de behövs för handläggningen av målet eller ärendet. Känsliga personuppgifter får inte användas som sökbegrepp. Samtliga förordningar innehåller regler om gallring i verksamhetsregister.

Domstolarna får vidare föra *rättsfallsregister* för återsökning av vägledande avgöranden, rättsutredningar och liknande rättslig information. Ett sådant rättsfallsregister får endast innehålla de uppgifter som anges i en detaljerad uppräknning i en bilaga till respektive förordning. Det rör sig om uppgifter om bl.a. mål- och ärendenummer, avgörandenummer, avgörandedatum, sökord och fullföljd. Personuppgiftslagens regler om gallring tillämpas på registren.

Vid sidan av behandlingen i register innehåller förordningarna också bestämmelser om att domstolarna får behandla personuppgifter automatiserat i löpande text, ljudupptagningar eller ljud- och bildupptagningar. Personuppgifter som behandlas i löpande text eller i ljud- och bildupptagningar bevaras eller gallras enligt bestämmelserna i personuppgiftslagen.

Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt förordningarna. Förordningarna innehåller särskilda regler om överklagande. Beslut i de högsta domstolarna kan inte överklagas. Övriga domstolars beslut överklagas till närmast högre instans inom domstolsväsendet.

Det bör i sammanhanget nämnas att det föreligger förslag till nya regler när det gäller regleringen och användningen av personregister och annan behandling av personuppgifter inom domstolsväsendet. Domstolsdatautredningen har föreslagit att de fyra förordningar som i dag reglerar personuppgiftsbehandlingen inom domstolsväsendet ska ersättas med lagar (se SOU 2001:32 och SOU 2001:100). En departementspromemoria planeras under hösten 2008.

## 4.7 Lagstiftning om internationellt samarbete

### 4.7.1 Inledning

Rambeslutets tillämpningsområde omfattar endast sådana uppgifter som överförs eller görs tillgängliga mellan stater inom Europeiska unionen eller mellan en medlemsstat och ett tredjeland eller ett internationellt organ som sysslar med brottsbekämpning. I detta avsnitt redovisas lagstiftning som särskilt tar sikte på internationellt samarbete inom de verksamhetsområden som berörs av rambeslutet och som innehåller

särreglering när det gäller informationsutbyte och behandling av personuppgifter.

För en mer allmän beskrivning av den lagstiftning som reglerar internationellt samarbete, bl.a. avseende straffverkställighet och verkställighet av icke frihetsberövande påföljder, och det samarbete som sker mellan medlemsstaterna och de viktigaste internationella organ som sysslar med brottsbekämpning hänvisas till promemorians avsnitt 5.

#### **4.7.2 Regler om användningsbegränsningar**

Från slutet av 1980-talet föreslogs allt oftare vid förhandlingar om internationella överenskommelser om rättsligt samarbete och informationsutbyte bestämmelser om begränsningar i fråga om hur överlämnad information får användas. Det väckte så småningom frågan om hur man skulle hantera den typen av bestämmelser i svensk rätt. Genom en bestämmelse i lagen (1991:435) med vissa bestämmelser om internationellt samarbete på brottmålsområdet infördes en generell bestämmelse som gav myndigheterna rätt att, i fall där en främmande stat hade ställt villkor angående användningen av upplysningar eller bevismaterial, följa detta villkor oavsett vad som annars var föreskrivet i lag eller annan författning.

Lagen upphävdes när lagen (2000:562) om internationell rättslig hjälp i brottmål (se avsnitt 4.7.5) infördes. Numera finns det således ingen generell lagstiftning på området utan motsvarande bestämmelser finns i flera olika lagar.

Det förhållandet att en regel om användningsbegränsning finns i en lag som primärt gäller för ett visst verksamhetsområde får inte tolkas så att den bara ska tillämpas i den verksamheten. Tvärtom gäller en användningsbegränsning för alla svenska myndigheter. JO har i ett ärende som berörde flera myndigheter utvecklat detta närmare (se JO 2007/08 s. 57).

#### **4.7.3 Lagstiftning om samarbete i den brottsbekämpande verksamheten**

##### *Lagen om internationellt polisiärt samarbete*

I lagen (2000:343) om internationellt polisiärt samarbete regleras samarbete mellan svenska brottsbekämpande myndigheter och motsvarande myndigheter i andra medlemsstater i Europeiska unionen samt Norge och Island. Lagen reglerar bl.a. Schengensamarbetet men även annat polis-samarbete som är konventionsbundet. I lagen anges vilka svenska tjänstemän som är behöriga att delta i samarbetet, nämligen svenska polismän, tulltjänstemän och kustbevakningstjänstemän, när de enligt lag eller annan författning har polisiära befogenheter.

Det bör påpekas att den viktigaste delen av informationsutbytet inom Schengensamarbetet regleras i lagen om Schengens informationssystem. Den nu aktuella lagen reglerar annat samarbete och informationsutbyte som är mera inriktat på enskilda fall.

I lagen finns en bestämmelse (3 §) om hur uppgifter som har erhållits från andra stater får användas. Bestämmelsen motsvarar i huvudsak 1 § i den upphävda lagen med särskilda bestämmelser om internationellt samarbete på brottmålsområdet. Har en svensk myndighet fått upplysningar eller bevismaterial från en annan stat för att användas i underrättelseverksamhet om brott eller vid utredning av brott, och gäller på grund av överenskommelse med den andra staten villkor som begränsar möjligheten att utnyttja materialet, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. Vad som nu har sagts gäller även för överenskommelser med mellanfolkliga organisationer.

#### *Lagen om vissa former av internationellt samarbete i brottsutredningar*

Lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar innehåller regler om gränsöverskridande samarbete i enskilda brottsutredningar. Syftet är att förbättra det polisiära och det straffrättsliga samarbetet mellan medlemsstaterna i kampen mot den gränsöverskridande brottsligheten. Behöriga myndigheter i två eller flera medlemsstater får genom en överenskommelse inrätta en gemensam utredningsgrupp för brottsutredningar. När det finns en sådan överenskommelse tillämpas lagen. De utredningsgrupper som inrättas med stöd av någon annan internationell överenskommelse omfattas inte av lagen.

Lagen innehåller bl.a. bestämmelser om användningsbegränsningar. Har en svensk myndighet fått uppgifter genom en gemensam utredningsgrupp som inrättats med stöd av lagen och gäller villkor som begränsar möjligheten att använda uppgifterna, ska en svensk myndighet enligt 5 § följa villkoren oavsett vad som annars är föreskrivet i lag eller författning. Enligt 6 § får överlämnandet av uppgifter eller bevismaterial från en svensk myndighet till en sådan utredningsgrupp förenas med villkor som är nödvändiga av hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt.

Den svenska myndighet som har överlämnat material med villkor får enligt 7 § på begäran av en myndighet i en annan stat medge undantag från villkoret.

Lagen innehåller också vissa bestämmelser om s.k. kontrollerade leveranser (10–14 §§) och om brottsutredningar med användning av skyddsidentitet (15–17 §§). Med kontrollerad leverans avses att en viss förbjuden vara, oftast narkotika, tillåts passera gränsen utan att myndigheterna ingriper, i syfte att man ska kunna spåra upp de personer som ligger bakom brottet. Både vid kontrollerade leveranser och vid brottsutredningar med användning av skyddsidentitet ska reglerna om användningsbegränsning i 5–7 §§ tillämpas (13 respektive 16 §).

#### *Lagen om Schengens informationssystem*

I dataregistret Schengens informationssystem (SIS) kan varje medlemsstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersöks med en begäran om att en viss åtgärd ska vidtas om

personen eller föremålet påträffas. I lagen (2000:344) om Schengens informationssystem regleras behandlingen av personuppgifter i den nationella delen av SIS. Lagen, som gäller utöver personuppgiftslagen (prop. 1999/2000:64 s. 135), innehåller bl.a. regler om vilka uppgifter som får registreras och i vilka syften (3 och 4 §§), en särskild bestämmelse om att känsliga uppgifter inte får registreras (7 §), bestämmelser om gallring, rättelse och skadestånd (11–13 §§).

Lagen innehåller också en regel om användningsbegränsning (10 §) enligt vilken en svensk myndighet inte får utnyttja en uppgift i registret för något annat syfte än det som den registrerande staten har angett vid registreringen. Om den registrerande staten har lämnat sitt samtycke, får dock en svensk myndighet använda uppgiften för ett annat ändamål.

#### 4.7.4 Lagen om internationellt tullsamarbete

Syftet med det internationella tullsamarbetet, som regleras i lagen (2000:1219) om internationellt tullsamarbete, är att förhindra, upptäcka, utreda och beivra överträdelse av tullbestämmelser. Tullverket eller annan behörig svensk myndighet ska bistå utländsk myndighet och mellanfolklig organisation. Behöriga myndigheter är, förutom Tullverket, Rikspolisstyrelsen, polismyndigheter, Kustbevakningen och Statens jordbruksverk (1 kap. 5 §). Tullverket har ansvaret för samordningen av samarbetet.

Vid internationellt tullsamarbete kan de svenska myndigheterna agera endast inom ramen för sina befogenheter enligt nationell lagstiftning (1 kap. 3 §). Samarbetet består bl.a. i att länderna självmant eller efter ansökan ska delge varandra uppgifter som behövs för tullsamarbetet.

Bestämmelser om utbyte av uppgifter finns i 2 kap. 6–8 §§. När det är nödvändigt för att genomföra internationellt tullsamarbete, får en svensk behörig myndighet lämna ut uppgifter till behörig utländsk myndighet eller mellanfolklig organisation, även om uppgiften är sekretessbelagd. Endast uppgifter som är tillgängliga för myndigheten inom dess verksamhetsområde omfattas (2 kap. 6 §). Uppgifterna får förenas med villkor för användandet, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt (2 kap. 7 §).

Har en uppgift översänts till en utländsk myndighet, är den svenska myndigheten i princip skyldig att på begäran av den som uppgiften avser underrätta denne om vart uppgiften har sänts och för vilket ändamål (2 kap. 8 §). Detta gäller dock inte om det är uppenbart obehövt eller om det kan befaras att underrättelsen skulle försvåra den utländska utredningen eller beslutet. Gäller sekretess för uppgiften behöver underrättelse inte heller lämnas (2 kap. 8 §).

Om en svensk myndighet har tagit emot uppgifter eller bevisning från en annan stat enligt en internationell överenskommelse om samarbete i fråga om bekämpning av överträdelse av tullbestämmelser som innehåller villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning (4 kap. 2 §). Lagen är dock inte tillämplig på sådant samarbete som avses i lagen (1969:200) om

#### 4.7.5 Lagen om internationell rättslig hjälp i brottmål

I lagen (2000:562) om internationell rättslig hjälp i brottmål finns bestämmelser om skyldighet att på en utländsk myndighets begäran vidta åtgärder som bl.a. förhör under förundersökning, bevisupptagning, telefonförhör, kvarstad, husrannsakan och användning av hemliga tvångsmedel (1 kap. 2 §) och motsvarande bestämmelser om hur Sverige kan begära rättslig hjälp utomlands (3 kap.). Verkställighetsregler finns i förordningen (2000:704) om internationell rättslig hjälp i brottmål.

Lagen är generell, dvs. den gäller i förhållande till alla stater även om dessa inte har tillträtt samma konventioner om rättslig hjälp i brottmål som Sverige. Vissa regler gäller dock bara i förhållande till medlemsstater i Europeiska unionen samt Norge och Island.

En utländsk stats begäran om rättslig hjälp i Sverige handläggs av åklagare och domstol, under förutsättning att åtgärden kan vidtas enligt svensk lag under en förundersökning eller rättegång. I vissa fall får rättslig hjälp beviljas, även om den misstänkta gärningen inte utgör brott enligt svensk lagstiftning (2 kap. 2 §).

I 2 kap. finns allmänna bestämmelser om förfarandet vid en ansökan om rättslig hjälp i Sverige. I princip används samma förfarande som vid motsvarande svensk åtgärd under förundersökning eller rättegång (2 kap. 10 §). Åklagaren kan begära biträde av en polismyndighet, Tullverket eller Kustbevakningen i samma utsträckning som för en motsvarande svensk förundersökningsåtgärd.

Om en svensk myndighet i ett ärende om rättslig hjälp har fått uppgifter eller bevisning från en annan stat för att användas vid utredning av brott eller i ett rättsligt förfarande med anledning av brott, och gäller bindande villkor som begränsar möjligheterna att använda uppgifterna eller bevisningen, ska, enligt 5 kap. 1 §, villkoret följas oavsett vad som annars är föreskrivet i lag eller annan författning. Detsamma gäller beträffande villkor som en stat har ställt upp när den på eget initiativ lämnar sådana uppgifter.

På motsvarande sätt får rättslig hjälp som lämnas av en svensk myndighet i enskilda fall förenas med villkor som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga ur allmän synpunkt (5 kap. 2 §).

## 5 Genomförande av rambeslutet

### 5.1 Inget genomgripande behov av ny lagstiftning

Det har i avsnitt 4.1 konstaterats att – genom att rambeslutet innehåller bestämmelser som i många avseenden liknar de som finns i data-skyddsdirektivet som har genomförts också inom de sektorer som påver-

kas av rambeslutet – det svenska regelverket redan till stora delar är anpassat till de krav på dataskydd som ställs i rambeslutet.

Mot den nu angivna bakgrunden kan det konstateras att det inte krävs någon omfattande lagstiftning för att genomföra rambeslutet.

En fråga av intresse i sammanhanget är om reglering som rör personuppgiftsbehandling bör ha lagform för att skyddet för den enskilde ska kunna anses vara tillfredsställande. Såväl regeringen som riksdagen har framhållit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag (se prop. 1990/91:60 s. 58 och 1997/98:44 s. 41 samt KU 1990/91:11 s. 11.) För närvarande regleras personuppgiftsbehandlingen inom vissa delar av rättsväsendet endast i förordning. Det finns emellertid redan förslag om att betydande delar av personuppgiftsbehandlingen i domstolarna och inom Kustbevakningen ska regleras i lag. För åklagarväsendets del pågår en översyn med samma inriktning. Om dessa förslag genomförs kommer det därefter bara att återstå enstaka register som fortfarande regleras i förordning. Även om det i det fortsatta lagstiftningsarbetet med att genomföra rambeslutet – beroende på vilka förändringar som har hunnit ske – kan vara lämpligt att överväga om viss reglering av personuppgiftsbehandling som finns i förordning bör ges lagform kan det dock inte hävdas att Sverige på den grunden inte uppfyller förpliktelseerna i rambeslutet, så länge författningarna i övrigt uppfyller kraven. Att vissa författningar inte har lagform spelar alltså ingen roll i det avseendet.

I de följande avsnitten görs en översiktlig bedömning av lagstiftningsbehovet utifrån innehållet i rambeslutet. Utgångspunkten är därvid att de skyldigheter som uppställs i rambeslutet endast avser uppgifter som utbyts mellan medlemsstaterna. Frågan om det av andra skäl finns behov av eller är lämpligt att se över den svenska regleringen rörande övrig personuppgiftsbehandling behandlas därför inte i denna proposition. För en mer grundläggande redovisning av även sådana aspekter hänvisas till promemorian.

Som har nämnts pågår det ett omfattande lagstiftningsarbete på flera av de områden som berörs. Det pågår också förhandlingar inom Europeiska unionen om rättsakter som kan komma att beröra polissamarbetet och det straffrättsliga samarbetet. Även i dessa delar hänvisas till nyss nämnda departementspromemoria. Den bedömning av behovet av lagstiftning som görs i denna proposition utgår från det nu aktuella rättsläget.

## 5.2 Rambeslutets syfte och tillämpningsområde

### 5.2.1 Syftet med rambeslutet

Syftet med rambeslutet är enligt *artikel 1 punkten 1* att säkerställa en hög skyddsnivå för fysiska personer när det gäller behandling av personuppgifter. Samma grundläggande syfte gäller för den svenska lagstiftningen som rör personuppgiftsbehandling, även om detta inte uttryckligen framgår av alla aktuella författningar. Det krävs dock inte någon komplettering av lagstiftningen i detta hänseende, eftersom punkten närmast kan ses som en programförklaring.

Det kan noteras att det av *artikel 1 punkten 2* framgår att rambeslutet endast är avsett att skydda fysiska personer, medan den svenska lagstiftningen i viss utsträckning ger motsvarande skydd för juridiska personer, se exempelvis 19 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Detta utgör dock inte något problem, eftersom medlemsstaterna får ha regler som skapar ett starkare skydd nationellt (*artikel 1 punkten 5* och *skäl 8*).

Sammanfattningsvis kräver inte rambeslutets bestämmelser om syftet med beslutet några lagändringar i svensk rätt.

## 5.2.2 Rambeslutets tillämpningsområde

### *Allmänt om tillämpningsområdet*

Enligt *artikel 1* är rambeslutet tillämpligt på behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete enligt avdelning VI i fördraget om Europeiska unionen när personuppgifter överförs eller har överförts eller görs tillgängliga eller har gjorts tillgängliga i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Det innebär att polisiärt eller rättsligt samarbete i annat syfte faller utanför tillämpningsområdet. Rättslig hjälp i civilmål faller också utanför, liksom t.ex. informationsutbyte som rör offer för olyckshändelser även om informationen förmedlas via polisiära kanaler.

Vidare framgår – som har nämnts ovan – att rambeslutet enbart omfattar uppgifter som förs över eller görs tillgängliga, eller har överförts eller gjorts tillgängliga, mellan medlemsstater eller från medlemsstater till tredjeland eller till internationella organisationer som sysslar med brottsbekämpning. Som har nämnts ovan (avsnitt 5.1) är det mot denna bakgrund som analysen av lagstiftningsbehovet i denna proposition ska ses. En klart uttalad målsättning med rambeslutet är dock att även dataskyddet vid nationell behandling ska hålla samma standard som krävs enligt detta, i syfte att underlätta informationsutbytet inom Europeiska unionen (*skäl 8*). Detta förhållande återspeglas i flera av artiklarna i rambeslutet.

Tillämpningsområdet omfattar enligt *punkten 3* behandling av personuppgifter som utförs helt eller delvis automatiserat samt annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Att rambeslutet är tillämpligt på uppgifter som *kommer att ingå* i ett register innebär att det inte bara är tillämpligt på uppgifter som har överförts elektroniskt utan även på uppgifter i mottagna handlingar, om uppgifterna ska registreras. Tillämpningsområdet motsvarar i denna del dataskyddsdirektivet, som har genomförts genom personuppgiftslagen som har varit utgångspunkten när man har utformat den särlagstiftning som gäller utöver eller istället för personuppgiftslagen. Författningarna om personuppgiftsbehandling inom polisen, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendet, domstolsväsendet och kriminalvården har alla samma grundläggande tillämpningsområde som personuppgiftslagen och uppfyller därigenom kraven i rambeslutet. Vidare är dessa författningar inriktade på sådan verksamhet som anges i

punkten 2 (dvs. sådan verksamhet som syftar till att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder). Några förändringar i fråga om tillämpningsområdet för de olika sektorsförfattningarna krävs därför inte.

De särskilda författningarna om enskilda register, exempelvis författningarna om belastningsregister, misstankeregister, strafförelägganderegister och ordningsbotsregister, reglerar behandlingen i ett eller flera register. Uppgifter i dessa register som har sitt ursprung i andra länder faller automatiskt inom rambeslutets tillämpningsområde, eftersom registren i fråga har brottsbekämpning, lagföring eller straffverkställighet som ändamål.

Den personuppgiftsbehandling som träffas av rambeslutets tillämpningsområde är i svensk rätt redan författningsreglerad, främst genom personuppgiftslagen och de sektorsförfattningar som nyss har nämnts. Det krävs alltså inte några lagstiftningsåtgärder på denna grund.

#### *Undantag från tillämpningsområdet*

I artikel 1 punkten 4 görs ett uttryckligt undantag från tillämpningsområdet när det gäller nationella säkerhetsintressen och särskild underrättelseverksamhet som rör nationell säkerhet. Undantaget gäller alltså inte generellt för den myndighet eller organisation som sysslar med frågor rörande nationell säkerhet utan för verksamheten som sådan. Så som undantaget är utformat faller Säkerhetspolisens verksamhet i allt väsentligt utanför tillämpningsområdet. I den utsträckning som Säkerhetspolisen har uppgifter som inte kan sägas röra nationell säkerhet omfattas myndigheten dock av rambeslutets tillämpningsområde. Ett exempel på detta är när Säkerhetspolisen biträder den öppna polisen eller Tullverket med hanteringen av hemliga tvångsmedel i deras verksamhet. Sådant biträde torde dock ofta vara av rent teknisk karaktär och medför då inte något utbyte av uppgifter för Säkerhetspolisens del med andra stater. Däremot torde vissa delar av den verksamhet inom myndigheten som rör t.ex. arbetet mot grov organiserad brottslighet kunna omfattas.

Säkerhetspolisens personuppgiftsbehandling regleras på i huvudsak samma sätt som personuppgiftsbehandling regleras för polisen i övrigt. Polisdatalagen innehåller dock särskilda bestämmelser om Säkerhetspolisens register. Eftersom Säkerhetspolisens personuppgiftsbehandling endast till mindre del avviker från vad som gäller för den övriga polisen, innebär det i allt väsentligt att regleringen i samma utsträckning som för polisen antingen uppfyller kraven eller behöver förändras. I det kommande lagstiftningsarbetet måste dock tydiggöras vilka delar av Säkerhetspolisens personuppgiftsbehandling som faller utanför rambeslutets tillämpningsområde.

Förutom ovan nämnda undantag bör det noteras att det av *skäl 9* följer att rambeslutet inte ska uppfattas som tillämpligt på uppgifter som en medlemsstat har fått från en annan medlemsstat, men som har sitt ursprung i den första staten.

Sammanfattningsvis bedöms rambeslutets bestämmelser om tillämpningsområdet i sig inte kräva några lagändringar.



*Artikel 2* i rambeslutet innehåller vissa definitioner. Flera av dessa har sin motsvarighet i dataskyddsdirektivet. De motsvarar således de definitioner som finns i 3 § personuppgiftslagen, som gäller för den lagstiftning som berörs av rambeslutet. Det kan noteras att begreppet ”blockering” inte definieras i dataskyddsdirektivet men däremot i personuppgiftslagen. I det fortsatta lagstiftningsarbetet bör en närmare analys göras av om personuppgiftslagens definition av begreppet behöver anpassas till definitionen i rambeslutet.

Det finns därutöver även andra definitioner, t.ex. av begreppen ”behöriga myndigheter” och ”avidentifiering”. Dessa definitioner är inte av den arten att de måste införas i svensk lagstiftning.

## 5.3 Huvudregler om tillåtna ändamål för behandling av uppgifter

### 5.3.1 Innehållet i rambeslutet

Enligt *artikel 3* får personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och uppgifterna får som huvudregel endast behandlas för det ändamål som låg till grund för insamlingen av dem. Personuppgifter får dock även vidarebehandlas för andra ändamål om dessa inte är oförenliga med dem för vilka uppgifterna först samlades in, allt under förutsättning att de berörda myndigheterna får behandla uppgifterna för givna ändamål enligt nationell rätt och behandlingen dessutom är nödvändig och står i proportion till de ursprungliga ändamålen. Den tillåtna vidarebehandlingen av uppgifter som har överförs eller gjorts tillgängliga begränsas emellertid även enligt *artikel 11* till vissa särskilt uppräknade ändamål, bl.a. för att förebygga, utreda, avslöja eller lagföra andra brott eller verkställa andra straffrättsliga påföljder än de för vilka uppgifterna överfördes eller gjordes tillgängliga eller för andra rättsliga eller administrativa förfaranden med direkt anknytning till sådan verksamhet. Möjligheterna att vidarebehandla uppgifter för andra särskilda ändamål än det ursprungliga behandlas närmare i avsnitt 5.4.4.

Ett generellt undantag från huvudregeln om att uppgifter bara får behandlas för det ursprungliga ändamålet är att uppgifter alltid får vidarebehandlas för historiska, statistiska eller vetenskapliga ändamål, under förutsättning att medlemsstaterna föreskriver lämpliga skyddsåtgärder, såsom avidentifiering av uppgifterna.

Behandlingen av personuppgifter måste alltid vara lagenlig och adekvat, relevant och inte orimlig i förhållande till det ändamål för vilket uppgifterna samlades in.

*Artikel 15* ålägger mottagaren av uppgifter att på begäran av den myndighet som har överfört uppgifterna ge besked om hur uppgifterna behandlas.

De nu nämnda bestämmelserna i artikel 3 motsvaras delvis av bestämmelserna i 9 § personuppgiftslagen. Den paragrafen innehåller bl.a. en regel om att personuppgifter som huvudregel endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål (första stycket punkten c). Uppgifter får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen, första stycket punkten d). Uppgifterna ska också vara adekvata och relevanta i förhållande till ändamålen med behandlingen (första stycket punkten d).

Personuppgiftslagens regler om grundläggande krav på behandlingen i dessa delar gäller inom de nu aktuella verksamhetsområdena eftersom det inte finns avvikande bestämmelser. För Tullverkets del – där personuppgiftslagen bara gäller om det särskilt anges – finns en direkt hänvisning till de aktuella bestämmelserna i 9 § personuppgiftslagen. Som har framgått ovan (avsnitt 4.4.3) har de författningar som reglerar enskilda register i författningarna särskilt angivna ändamål. Detsamma gäller de flesta av de sektorsförfattningar som berörs av rambeslutet. Rambeslutets bestämmelser i denna del torde därför inte kräva några lagändringar.

Behandling för historiska, statistiska eller vetenskapliga ändamål är, som har framgått ovan generellt tillåten enligt rambeslutet, men bara under förutsättning att medlemsstaterna föreskriver lämpliga skyddsåtgärder. Motsvarande krav ställs i dataskyddsdirektivet. Personuppgifter får enligt 9 § första stycket punkten i personuppgiftslagen inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 9 § tredje stycket får dock personuppgifter bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid. Möjligheten att använda personuppgifter som bevaras för sådana ändamål är dock begränsad. De får användas för att vidta åtgärder mot den registrerade bara om denne har samtyckt till det eller om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. I propositionen till personuppgiftslagen diskuterades ingående huruvida den svenska arkivlagstiftningen uppfyllde kraven i dataskyddsdirektivet i detta avseende. Regeringen ansåg att så var fallet (prop. 1997/98:44 s. 47 f.) och riksdagen anslöt sig till detta.

Det kan i sammanhanget nämnas att sektorsförfattningarna och de olika registerförfattningar innehåller särskilda gallringsregler som utgör särregleringar i förhållande till personuppgiftslagens allmänna bestämmelser. Samtliga dessa uppfyller dock de grundläggande kraven i personuppgiftslagen.

De flesta av sektorsförfattningarna innehåller, som har framgått i avsnitt 4.5 och 4.6, en reglering som motsvarar personuppgiftslagens i fråga om vidarebehandling för historiska, statistiska eller vetenskapliga ändamål. Det finns dock några undantag. Tullverkets författningar lämnar utrymme för att handlingar bevaras i stället för att gallras, men anger inte för vilka ändamål dessa får bevaras (se avsnitt 4.5.1). Dessa bestämmelser kan därför behöva ses över.

Med hänvisning till vad som har anförts ovan bedöms rambeslutet, med något enstaka undantag, inte kräva några lagändringar när det gäller

huvudreglerna om tillåtna ändamål för behandling av uppgifter och om vidarebehandling för historiska, statistiska eller vetenskapliga ändamål. Bestämmelsen om skyldighet att på begäran informera den överförande myndigheten om hur uppgifter behandlas behöver inte lagregleras.

Prop. 2008/09:16

## 5.4 Begränsningar i rätten att behandla uppgifter

### 5.4.1 Inledning

Rambeslutet innehåller flera bestämmelser som syftar till att på olika sätt begränsa rätten att behandla uppgifter. Dessa bestämmelser utgör ett viktigt led i det skydd som rambeslutet är avsett att skapa för de uppgifter som omfattas av beslutet.

En del av dessa bestämmelser gäller generellt för alla uppgifter, t.ex. förbud mot överföring av uppgifter till tredjeland, medan andra avser en viss typ av uppgifter, t.ex. känsliga uppgifter. I detta avsnitt görs en analys av i vilken utsträckning svensk rätt uppfyller rambeslutets krav när det gäller bestämmelser som begränsar rätten att behandla uppgifter.

### 5.4.2 Behandling av känsliga personuppgifter

I *artikel 6* i rambeslutet regleras behandling av vad som brukar kallas känsliga personuppgifter. Med detta avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv (jfr 13 § personuppgiftslagen). Enligt artikeln får sådana uppgifter behandlas – dvs. överföras eller tas emot och användas eller behandlas vidare – endast när det är absolut nödvändigt och om det föreskrivs tillräckliga skyddsåtgärder i den nationella lagstiftningen. Rambeslutets bestämmelser om behandling av känsliga personuppgifter skiljer sig således från de i dataskyddsdirektivet, där det ställs upp andra typer av begränsningar för behandling. Dessa återspeglas i 13–19 §§ personuppgiftslagen.

Som har framgått ovan (avsnitt 4.3.3) innehåller personuppgiftslagen bestämmelser om under vilka förutsättningar känsliga personuppgifter får behandlas. Till skillnad från rambeslutet ställer personuppgiftslagen i vissa fall enbart krav på att behandlingen ska vara nödvändig och inte på att den ska vara absolut nödvändig. Personuppgiftslagen lämnar också ett förhållandevis stort utrymme för behandling av känsliga personuppgifter i olika undantagssituationer. Det kan därför ifrågasättas om personuppgiftslagen kan anses uppfylla rambeslutets krav i denna del. I den utsträckning personuppgiftslagen blir tillämplig på behandling av känsliga personuppgifter som omfattas av rambeslutet bör därför en närmare analys av behovet av författningsändringar göras.

Som har framgått ovan (avsnitt 4.4–4.7) styrs dock behandling av känsliga personuppgifter på det område som berörs av rambeslutet, med något undantag, inte av personuppgiftslagen utan av särskilda bestämmelser i andra författningar. De författningar som innehåller särregler för personuppgiftsbehandlingen hos polisen, Tullverket,

Kustbevakningen, Skatteverket och kriminalvården innehåller samtliga bestämmelser om behandling av känsliga uppgifter som avviker från personuppgiftslagens (se avsnitt 4.5 och 4.6). Bestämmelserna i dessa författningar tillåter visserligen behandling i större utsträckning än personuppgiftslagen, men är utformade så att möjligheten att behandla känsliga uppgifter är mycket begränsad. Bestämmelserna fordrar att behandlingen ska vara absolut nödvändig, vilket står i god överensstämmelse med innehållet i rambeslutet eller ställer motsvarande krav. Reglerna innehåller dessutom andra preciseringar, t.ex. i form av förbud att använda känsliga uppgifter som sökbegrepp. Dessa regler torde därmed anses uppfylla kraven i rambeslutet inom sina respektive tillämpningsområden.

Det kan noteras att det inte finns några särregler för personuppgiftsbehandling av känsliga personuppgifter i de registerförfattningar som reglerar enskilda register. Detta ska ses mot bakgrund av att dessa normalt har preciserade bestämmelser om vilka typer av uppgifter som får finnas i registren och att bestämmelserna om innehållet i praktiken inte tillåter registrering av känsliga uppgifter. Mot den bakgrunden finns det inget behov av att reglera förekomsten av känsliga uppgifter i dessa författningar.

Det kan vidare noteras att de förordningar som i dag reglerar domstolsväsendets personuppgiftsbehandling (se avsnitt 4.6.3) tillåter behandling av känsliga uppgifter när det är nödvändigt för att saken ska kunna återges på ett ändamålsenligt sätt eller uppgifterna har lämnats i ett mål eller ett ärende och behövs för handläggningen. Samma reglering finns när det gäller åklagarsväsendets personuppgiftsbehandling. Enligt förordningen om behandling av personuppgifter inom åklagarsväsendet (se avsnitt 4.5.4) får känsliga personuppgifter behandlas om de förekommer i en handling som har kommit in till Åklagarmyndigheten eller Ekobrottsmyndigheten i ett ärende. Om uppgifter behandlas på en annan grund hos nämnda myndigheter får de kompletteras med känsliga uppgifter om det är absolut nödvändigt för syftet med behandlingen. Som har nämnts pågår arbete med att revidera den svenska regleringen på de nämnda områdena. Frågan om de nu aktuella bestämmelsernas förhållande till rambeslutets krav kräver ytterligare analys – även med beaktande av utgångspunkten att principen om allmänhetens tillgång till offentliga handlingar kan tillgodoses vid tillämpningen (skäl 31). En sådan fördjupad analys bör sker i det fortsatta lagstiftningsärendet för genomförande av rambeslutet.

Sammanfattningsvis finns det i svensk rätt regler som begränsar användningen av känsliga personuppgifter som i huvudsak bedöms uppfylla rambeslutets krav. En närmare analys av behovet av lagändringar bör dock göras i det kommande lagstiftningsarbetet.

### 5.4.3 Behandling av uppgifter för datoriserade beslut

I *artikel 7* finns bestämmelser om vad som benämns datoriserade beslut. Med datoriserade beslut avses sådana beslut som dels har rättsliga följder för någon eller som annars påverkar honom eller henne negativt, dels enbart grundas på en automatisk behandling avsedd att bedöma vissa

personliga egenskaper. I artikeln föreskrivs att sådana beslut endast ska vara tillåtna om de har stöd i lag och det i lagen fastställs skyddsåtgärder för den enskilde. Mot bakgrund av rambeslutets tillämpningsområde torde innebörden av artikeln vara att överförda uppgifter bara får behandlas inom ramen för datoriserade beslutsprocesser om kraven i artikel 7 är uppfyllda.

Bestämmelserna i artikel 7 motsvaras av artikel 15 i dataskyddsdirektivet som har genomförts genom 29 § personuppgiftslagen. Det förtjänar dock att påpekas att det i Sverige inte förekommer något datoriserat beslutsfattande på de områden som omfattas av rambeslutet. Det saknas därför redan av det skälet anledning att göra några lagändringar med anledning av rambeslutets bestämmelser om datoriserade beslut.

#### 5.4.4 Allmänna begränsningar för vidarebehandling

##### *Innehållet i rambeslutet*

Som har nämnts ovan innehåller *artikel 3 punkten 2* begränsningar när det gäller för vilka ändamål andra än det ursprungliga (eller historiska, statistiska eller vetenskapliga ändamål) som uppgifter som omfattas av rambeslutet får behandlas vidare. För det första ska behandlingen inte vara oförenlig med det ändamål för vilket uppgifterna samlades in. I *skäl 6* framhålls att det får avgöras på nationell nivå vilka ändamål som ska anses vara oförenliga med det ändamål för vilket personuppgifterna ursprungligen insamlades. För det andra ska den behandlande myndigheten vara behörig att utföra behandlingen. För det tredje ska behandlingen vara nödvändig och stå i proportion till det andra ändamålet.

*Artikel 11* måste tolkas så att den innehåller mer preciserade begränsningar än nyss nämnda artikel när det gäller vidarebehandling av uppgifter. Uppgifter som omfattas av rambeslutet får vidarebehandlas – i enlighet med kraven i artikel 3 punkten 2 – för andra ändamål än de för vilka de överfördes eller gjordes tillgängliga *endast* för följande syften.

För det första tillåter rambeslutet vidarebehandling för de ändamål som har störst praktisk betydelse från verksamhetssynpunkt, nämligen att förebygga, upptäcka, utreda eller lagföra andra brott än de som föranledde att uppgifterna överfördes eller gjordes tillgängliga samt för verkställighet av annan påföljd (*artikel 11 a*).

För det andra är det tillåtet att vidarebehandla uppgifter för andra rättsliga eller administrativa förfaranden som har direkt anknytning till förebyggande, avslöjande, utredning eller lagföring av brott eller till verkställigheten (*artikel 11 b*). Det torde innebära att uppgifterna exempelvis får användas för indrivningen av skadestånd, företagsbot eller andra ekonomiska åligganden i en brottmålsdom. Vidare bör de kunna användas exempelvis i nådeärenden eller i ärenden som rör ändring av påföljd. Särskild förverkandetalan angående utbyte av brottslig verksamhet kan vara ett annat exempel. Likaså bör de kunna vidarebehandlas för att ta ut skatt, tull eller andra avgifter som är direkt relaterade till det brott för vilket de överfördes.

För det tredje tillåter rambeslutet att uppgifter vidarebehandlas för att avvärja en överhängande och allvarlig fara för allmän säkerhet (*artikel*

11 c). Utrymmet för tillämpningen av denna bestämmelse torde vara begränsat. Det torde komma i fråga framför allt i de fall där man inte hinner kontakta den andra staten därför att behovet av att agera har uppkommit plötsligt.

Slutligen får vidarebehandling ske för vilket annat ändamål som helst, under förutsättning att den överförande staten har lämnat medgivande till det i enlighet med sin nationella lagstiftning (*artikel 11 d*). De grundläggande förutsättningarna i artikel 3 punkten 2 a, bl.a. att behandlingen inte är oförenlig med de ändamål för vilket uppgifterna samlades in, måste dock alltid vara uppfyllda. Det bör noteras att ett medgivande till vidarebehandling av uppgifter som har överförts från en annan stat, beroende på den enskilda statens nationella lagstiftning, kan lämnas i form av ett allmänt samtycke till vidarebehandling av kategorier av information eller för en viss typ av behandling (*skäl 20*).

### *Behovet av lagändringar*

Rambeslutet ställer, som framgått ovan, mer preciserade krav än dataskyddsdirektivet när det gäller annan vidarebehandling än för historiska, statistiska eller vetenskapliga ändamål. Begränsningarna i fråga om vidarebehandling har i huvudsak intresse för situationer där den mottagande myndigheten själv vill vidarebehandla uppgifter för ett helt annat ändamål än brottsbekämpning eller vill lämna uppgifterna vidare till en myndighet som varken sysslar med brottsbekämpning, lagföring eller verkställighet av straff. Begränsningarna torde därför i praktiken inte ha så stor påverkan på de berörda myndigheternas verksamhet.

När det gäller bestämmelserna i artikel 3 kan följande sägas. Finalitetsprincipen i personuppgiftslagen innebär att personuppgifter inte får vidarebehandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (9 § d personuppgiftslagen, se avsnitt 4.3.2). För den brottsbekämpande verksamheten som bedrivs av polisen, åklagarmyndigheterna, Tullverket, Skatteverket och Kustbevakningen, finns, som har framgått ovan, bestämmelser om personuppgiftsbehandling som med endast ett undantag – Tullverkets personuppgiftsbehandling – innebär att bestämmelsen i 9 § första stycket d personuppgiftslagen i princip är tillämplig. För Tullverkets del uttrycks i lagen uttömmande de ändamål för vilka behandling får ske och någon hänvisning till den aktuella bestämmelsen i personuppgiftslagen finns inte. Emellertid är ändamålsbestämmelserna för tullens brottsbekämpande verksamhet angivna på ett sådant sätt att Tullverket i stort sett torde ha samma möjlighet att vidarebehandla och lämna ut uppgifter till andra myndigheter som om verket haft att tillämpa en bestämmelse motsvarande den i 9 § första stycket d personuppgiftslagen. Det kan dock inte uteslutas att det kan uppkomma situationer i vilka ändamålsbestämmelserna inte täcker en upptänklig vidarebehandling, som får ske enligt bestämmelserna i rambeslutet. Det kan därför finnas behov av att se över om ändamålsbestämmelserna för Tullverkets del överensstämmer med rambeslutet.

De villkor för vidarebehandling som uppställs i artikel 3.2 b och c om att de berörda myndigheterna ska ha befogenhet att behandla uppgifterna

för det andra ändamålet enligt nationell rätt och att behandlingen ska vara nödvändig och står i proportion till de ursprungliga ändamålen kan anses uppfyllda genom bestämmelserna i 9 § a respektive e personuppgiftslagen. Dessa bestämmelser gäller även i Tullverkets verksamhet (6 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet).

Mot bakgrund av det anförda är några lagstiftningsåtgärder med anledning av bestämmelserna i artikel 3 om vidarebehandling för andra ändamål än historiska, statistiska eller vetenskapliga ändamål – möjligen med undantag för den reglering som gäller för Tullverket – inte nödvändiga.

I sammanhanget bör utlämnande av uppgifter med stöd av offentlighetsprincipen nämnas. Utlämnande av uppgifter utgör en form av vidarebehandling av uppgifterna. I *skäl 31* anges att rambeslutet gör att principerna om allmänhetens tillgång till offentliga handlingar kan tillgodoses vid tillämpningen av principerna i detta. Skälet är något otydligt uttryckt men det torde inte råda något tvivel om att innebörden av detsamma är att det inte är meningen att rambeslutet ska inskränka den rätt till insyn som allmänheten har genom rätten att ta del av allmänna offentliga handlingar. Sådan vidarebehandling som sker för att uppfylla kraven i den svenska offentlighetsprincipen torde alltså inte anses oförenlig med rambeslutets bestämmelser om begränsningar i rätten att vidarebehandla uppgifter. En annan sak är att allmänhetens möjligheter att få tillgång till sådana uppgifter som omfattas av rambeslutet är tämligen begränsad eftersom uppgifterna i stor utsträckning omfattas av sekretess (se promemorian, avsnitt 4.8). Frågan om rambeslutet kräver en mer omfattande sekretessreglering än den som gäller i dag bör analyseras vidare i det fortsatta lagstiftningsarbetet.

Bestämmelserna i artikel 11 i rambeslutet innebär att vidarebehandling som sker i syfte att förebygga, upptäcka, utreda eller lagföra ett annat brott alltid är tillåten. Vidarebehandling får alltså ske om uppgifterna behövs för att handlägga konkreta brottsmisstankar. Vidarebehandling för att förebygga brott skapar också utrymme för att behandla uppgifter även utan konkreta brottsmisstankar. Likaså måste uppgifter få användas t.ex. för att berika pågående underrättelsearbete eller för att verkställa en existerande påföljd. Det kan också vara nödvändigt för polisen att bevara och behandla information om brott och brottstyper för specifika ändamål, t.ex. att jämföra tillvägagångssättet vid allvarliga brott eller att övervaka seriebrottslingar.

Bestämmelserna i artikel 11 om att all annan vidarebehandling än sådan som faller under a, b eller c förutsätter den överförande statens samtycke kan sägas snäva in bestämmelserna i artikel 3 på så sätt att även om ett ändamål för vidarebehandling inte är oförenligt med de ursprungliga så får vidarebehandling i vissa fall ändå inte ske utan samtycke. Detta innebär att finalitetsprincipen i personuppgiftslagen inte ensam kan anses uppfylla rambeslutets bestämmelser om förutsättningar för vidarebehandling. Frågan är om det finns andra bestämmelser i svensk rätt som uppfyller rambeslutet i denna del.

Som har redogjorts för i avsnitt 4.7 innehåller svensk rätt regler för hantering av information eller bevismaterial som en svensk myndighet får från en utländsk myndighet med villkor för användningen, s.k.

användningsbegränsningar. Principen är att sådana villkor tar över vad som annars gäller enligt svensk rätt. Det innebär t.ex. att åtalsplikten inte gäller. Som har redovisats närmare i nämnda avsnitt finns det bestämmelser om användningsbegränsningar i lagen om internationell rättslig hjälp i brottmål (5 kap. 1 §), lagen om internationellt polisiärt samarbete (3 §), lagen om vissa former av internationellt samarbete i brottsutredningar (5, 13 och 16 §§), lagen om internationellt tullsamarbete (4 kap. 2 §) samt lagen om Schengens informationssystem (10 §). I samtliga lagar föreskrivs att svenska myndigheter är skyldiga att följa de villkor som ställs av en utländsk myndighet eller mellanfolklig organisation.

Den typ av begränsningar som de aktuella artiklarna innebär för vidarebehandlingen av uppgifter torde kunna betraktas som sådana användningsbegränsningar som de nyss nämnda reglerna träffar (jfr prop. 2007/08:83 s. 41 f. avseende artikel 26 i Prümrådsbeslutet). Bestämmelserna i de nämnda författningarna innebär att information som mottas på detta sätt av polisen, åklagare, Tullverket och Kustbevakningen täcks och att de villkor som rambeslutet föreskriver, t.ex. kravet på samtycke, ska följas. Vidare täcks den information som har kommit genom sådana kanaler och som därefter kommer någon av de nämnda myndigheterna eller Skatteverket, domstolsväsendet eller kriminalvården till del (se avsnitt 4.7.2 och JO 2007/08 s. 57). Även om rambeslutet i denna del således inte torde kräva några lagstiftningsåtgärder kan det finnas skäl att i det fortsatta lagstiftningsarbetet överväga om det ändå är lämpligt att införa kompletterande bestämmelser.

I det fortsatta lagstiftningsärendet får vidare närmare övervägas om det finns behov av kompletterande reglering när det gäller information som Skatteverket och Kustbevakningen mottar i sin brottsbekämpande verksamhet från en annan stat (jfr promemorian, s.186 f.). Sådana överväganden kan också behöva göras beträffande sådan information som svenska myndigheter, t.ex. Åklagarmyndigheten och Kriminalvården, mottar inom ramen för sin hantering av utlämningsärenden, överlämnande enligt en europeisk arresteringsorder och överförande av straffverkställighet. Hanteringen av sådana ärenden styrs, som har nämnts i avsnitt 4.6.1, nämligen av särskilda regleringar i lagen om överlämnande från Sverige enligt en arresteringsorder, lagen om utlämning för brott, lagen om utlämning för brott till Danmark, Finland, Island och Norge samt lagen om internationellt samarbete rörande verkställighet av brottmålsdom. Dessa lagar innehåller inte några bestämmelser som begränsar rätten att använda uppgifter.

Det bör i sammanhanget noteras att ett genomförande av rambeslutet kräver att det finns en reglering som säkerställer att svenska myndigheter inte behandlar uppgifter på ett sätt som inte rambeslutet tillåter. Däremot kräver inte rambeslutet att det finns nationella regler som reglerar möjligheten för svenska myndigheter att ställa villkor för användningen av uppgifter som överförs till andra stater och medge undantag från sådana villkor. Frågan om en sådan reglering bör införas behandlas inte i denna proposition. Det kan däremot vara lämpligt att se över denna fråga i det fortsatta lagstiftningsarbetet.



*Innehållet i rambeslutet*

I *artikel 12* föreskrivs att om det gäller särskilda begränsningar i fråga om utbyte av uppgifter mellan nationella myndigheter enligt den överförande statens lagstiftning, så ska den överförande staten underrätta mottagaren om begränsningarna. Mottagaren ska se till att dessa begränsningar för behandling följs. Medlemsstaterna får inte tillämpa några andra begränsningar när det gäller överföring av uppgifter till en annan stat än som gäller motsvarande nationella överföringar.

*Artikel 16 punkten 2* innehåller en liknande bestämmelse om skyldighet att iaktta den överförande statens nationella rätt. I den föreskrivs att om den överförande staten begär det i enlighet med sin nationella lagstiftning, så ska den mottagande staten inte lämna någon information till den registrerade.

*Behovet av lagändringar*

Bestämmelserna i nu aktuella artiklarna har – till skillnad från de mer allmänna begränsningarna för användning av uppgifter som har behandlats i avsnitt 5.4.4 – sitt ursprung i det faktum att det kan finnas begränsningar i rätten till användning av uppgifter på nationell nivå som bör iakttas även efter överföring av uppgifter till en annan stat. Även denna typ av begränsningar torde kunna betraktas som sådana användningsbegränsningar som det finns regler om i svensk rätt (se avsnitt 4.7). Samma resonemang som har förts ovan i avsnitt 5.4.4 kan därför föras när det gäller i vilken utsträckning svensk rätt uppfyller rambeslutet.

Sammanfattningsvis är de befintliga reglerna om användningsbegränsningar i svensk rätt i huvudsak tillräckliga för att uppfylla rambeslutet även i dessa delar. I vissa fall kan dock behovet av lagändringar behöva analyseras närmare (jfr avsnitt 5.4.4).

**5.4.6 Skyldighet att iaktta överförande stats gallringsfrister**

När personuppgifter överförs till eller görs tillgängliga för en annan medlemsstat får, enligt *artikel 9*, den överförande staten underrätta mottagaren om de tidsfrister som gäller för gallring av uppgifterna. Mottagaren är då som huvudregel skyldig att, när fristen löper ut, radera eller blockera uppgifterna eller att göra en bedömning av om uppgifterna fortfarande behövs. Skyldigheten gäller dock inte om uppgifterna vid tidsfristens utgång behövs för en pågående utredning, lagföring av brott eller verkställighet av straffrättsliga påföljder.

Även här är det alltså fråga om bestämmelser i den överförande statens nationella rätt som följer med uppgifter som överförs. Kravet på att den överförande statens gallringsfrister ska iakttas kan innebära en begränsning i rätten att använda eller på annat sätt vidarebehandla uppgifter för ett ändamål som annars skulle ha varit tillåtet, t.ex. för att inleda en brottsutredning. Ett villkor om att en överförd uppgift ska

gallras efter en bestämd tid som uppställs i samband med överförandet skulle därför kunna ses som en sådan användningsbegränsning som anges i de olika författningar som innehåller bestämmelser om användningsbegränsningar (se avsnitt 4.7, jfr avsnitt 5.4.4). Ett sådant synsätt kan emellertid ifrågasättas. Syftet med bestämmelserna om användningsbegränsningar är att begränsa rätten att *använda* uppgifter till vissa bestämda ändamål. Skyldighet att gallra en uppgift sträcker sig längre än så eftersom det innebär ett förbud mot att låta uppgiften finnas kvar tillgängligt efter en viss tid, således även ett förbud mot att använda uppgiften för det ändamål som den överfördes för. Syftet med att underrätta mottagarstaten om en gallringsfrist torde snarare vara att på ett mera allmänt plan upprätthålla ett önskat dataskydd än att styra användningsområdet för den uppgift som överförs. I det fortsatta lagstiftningsarbetet bör därför närmare analyseras om det behövs kompletterande lagstiftning (jfr prop. 2007/08:83 s. 48).

### 5.4.7 Begränsningar i rätten att överföra uppgifter till tredjeland eller till internationella organisationer

#### *Innehållet i rambeslutet*

Överföring av uppgifter till tredjeland eller till internationella organ, eller organisationer som har inrättats genom internationella överenskommelser, regleras i *artikel 13*. Det uppställs krav för att uppgifter som omfattas av rambeslutet ska få föras över eller göras tillgängliga. Sådan överföring får ske endast om

- den är nödvändig för att förebygga, utreda, upptäcka eller lagföra brott eller för verkställighet av en straffrättslig påföljd,
- mottagaren har ansvar för sådan verksamhet,
- den stat från vilken uppgifterna har erhållits har gett samtycke till överföringen, och
- mottagaren har en adekvat skyddsnivå för databehandling.

Samtliga dessa villkor måste alltså som huvudregel vara uppfyllda för att det ska vara tillåtet att föra över uppgifter eller att göra dessa tillgängliga för ett tredjeland eller ett internationellt organ.

Undantag från kraven på förhandsmedgivande till överföring föreskrivs endast om överföringen är absolut nödvändig antingen för att avvärja en omedelbar och allvarlig fara för allmän säkerhet eller för en medlemsstats väsentliga intressen och ett förhandsmedgivande inte hinner utverkas i tid. I sådana fall ska den myndighet som ska medge överföring underrättas utan dröjsmål.

Vissa undantag medges också från kravet på adekvat skyddsnivå hos mottagaren, nämligen om den nationella lagstiftningen hos den medlemsstat som överför uppgifterna föreskriver detta på grund av vissa viktiga intressen eller om mottagaren sörjer för skyddsåtgärder som den överförande staten bedömer vara tillräckliga enligt sin lagstiftning. Vid bedömningen av om skyddsnivån är adekvat ska hänsyn tas till alla relevanta omständigheter, bl.a. uppgifternas art, syftet med behandlingen och varaktigheten av densamma.

I 33 § personuppgiftslagen föreskrivs ett generellt förbud mot överföring av personuppgifter till tredjeland, nämligen om landet inte har en adekvat nivå för skyddet av personuppgifterna (se avsnitt 4.3.6). Personuppgiftslagen innehåller dock inte något generellt förbud mot överföring av personuppgifter till internationella organ.

Flera av de författningar som nu är aktuella innehåller särskilda regler om utlämnande av uppgifter till såväl utländska myndigheter som mellanfolkliga organisationer. Reglerna är i stort sett utformade på samma sätt. De tillåter att uppgifter lämnas ut om detta följer av en internationell överenskommelse som har godkänts av riksdagen eller om en för Sverige bindande överenskommelse har träffats med en annan stat.

De nu nämnda reglerna om förutsättningarna för att överföra uppgifter till tredjeland eller till mellanfolkliga organ innehåller dock inte begränsningar i den utsträckning som artikel 13 kräver.

Bestämmelserna i rambeslutet om förbud mot överföring av uppgifter till tredjeland, internationella organ eller organisationer begränsar rätten att använda uppgifterna. Som har redogjorts för i avsnitt 4.7 innehåller svensk rätt regler för hantering av information eller bevismaterial som en svensk myndighet får från en utländsk myndighet med villkor för användningen, s.k. användningsbegränsningar. Liksom när det gäller allmänna begränsningar i rätten att vidarebehandla uppgifter och sådana begränsningar för behandling som kan härledas från den överförande statens nationella rätt (jfr avsnitt 5.4.4 och 5.4.5) görs bedömningen att de svenska bestämmelserna om användningsbegränsningar i huvudsak uppfyller rambeslutet i denna del men att behovet av lagändringar inom vissa verksamhetsområden kan behöva analyseras närmare (jfr avsnitt 5.4.4).

#### **5.4.8 Begränsningar i rätten att överföra uppgifter till privata parter**

##### *Innehållet i rambeslutet*

*Artikel 14* reglerar vidarebehandling i form av överföring av personuppgifter som har erhållits från en annan medlemsstat till privata parter i medlemsstaterna. För sådan överföring ställs särskilt stränga krav. Överföring är tillåten endast om behörig myndighet i den andra staten har samtyckt till överföring och inga legitima intressen för den registrerade hindrar överföringen samt överföringen i det enskilda fallet är absolut nödvändig av något av de fyra följande skälen:

1. för att utföra en författningsenlig uppgift,
2. för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder,
3. för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten, eller
4. för att förhindra att enskildas rättigheter lider allvarlig skada.

Vid överföringen ska myndigheten underrätta mottagaren om för vilket ändamål uppgifterna uteslutande får användas. Det bör anmärkas att den nu aktuella regleringen dock inte berör personuppgifter som lämnas från

domstolsväsendet, polisen eller tullväsendet till privata parter i brottmål, (*skäl 18*). Som exempel på privata parter nämns försvarsadvokater och brottsoffer.

Som exempel på när det kan vara nödvändigt att lämna uppgifter för att avvärja en omedelbar och allvarlig fara för allmän säkerhet och förhindra att enskilda personers rättigheter lider allvarlig skada nämns varningar till banker eller kreditinstitut om förfalskade värdepapper. Vidare nämns i fråga om fordonsstölder uppgiftslämnande till försäkringsbolag för att hindra olaglig handel med stulna motorfordon och för att återföra stulna motorfordon från utlandet (*skäl 17*).

### *Behovet av lagändringar*

De stränga kraven i artikel 14 för överföring av uppgifter som har överförts från eller gjorts tillgängliga av en annan stat till privata parter har inte någon motsvarighet i svensk lagstiftning. Eftersom undantag från huvudprincipen har gjorts för sådant uppgiftslämnande som utgör ett normalt led i brottmålsprocessen, nämligen uppgifter till parter i brottmål, dit även brottsoffer och försvarare räknas, torde begränsningarna dock inte bli så stora.

Samma resonemang som har förts ovan (avsnitt 5.4.7) när det gäller möjligheten att tillämpa svenska bestämmelser om användningsbegränsningar för att ta om hand rambeslutets begränsningar i rätten att överföra uppgifter till tredje stat eller internationella organ gör sig gällande när det gäller de nu aktuella bestämmelserna. Svensk rätt bedöms därför i huvudsak uppfylla rambeslutet i denna del. I sammanhanget bör utlämnande av uppgifter med stöd av offentlighetsprincipen uppmärksammas. I den delen hänvisas till avsnitt 5.4.4.

### **5.4.9 Sammanfattning**

Rambeslutet innehåller att antal artiklar som på olika sätt begränsar rätten att behandla personuppgifter som omfattas av rambeslutet. I viss utsträckning kräver dessa lagändringar. Det bör dock betonas att rambeslutet endast omfattar uppgifter som en svensk myndighet har fått från en annan medlemsstat eller som har gjorts tillgängliga av en annan medlemsstat. Även om det krävs lagändringar kan regleringen därför utformas så att den inte hämmar det informationsutbyte som äger rum nationellt.

Det som i så fall krävs är någon form av märkning av uppgifter som härrör från en annan medlemsstat, som gör den behandlande myndigheten uppmärksam på att uppgifterna inte får användas fritt. Varje överföring från en annan stat eller tillgängliggörande kommer nämligen att bära med sig begränsningar i fråga om behandling. Om uppgifter som bär med sig en användarbegränsning inte är märkta finns det en uppenbar risk att någon annan än den som tog emot uppgifterna oavsiktligt använder dessa i strid med användningsbegränsningen. I det fortsatta lagstiftningsarbetet bör även denna fråga uppmärksammas.

### 5.5.1 Innehållet i rambeslutet

Enligt *artikel 4 punkten 2* ska personuppgifter, när de inte längre behövs för det ändamål för vilka de samlats in eller vidarebehandlats, raderas eller avidentifieras. Radering kan också ske genom att datamediet förstörs (*skäl 14*). Arkivering i en separat datamiljö i överensstämmelse med nationell rätt påverkas inte av regeln om radering i artikel 4. Arkiveringen behöver inte göras i en särskild databas, men däremot får uppgifterna inte längre användas för att förebygga, utreda, upptäcka eller lagföra brott eller för straffverkställighet (*skäl 13*).

I *artikel 5* i rambeslutet finns bestämmelser om gallringsfrister. Där föreskrivs att det ska fastställas lämpliga tidsfrister för radering av personuppgifter eller för omprövning av behovet att bevara uppgifterna. Medlemsstaterna ska införa förfaranderegler som garanterar att tidsfristerna efterlevs.

### 5.5.2 Behovet av lagändringar

Utgångspunkten i rambeslutet är densamma som i dataskyddsdirektivet, nämligen att personuppgifter av integritetsskäl inte får finnas tillgängliga längre tid än vad som krävs för ändamålet med behandlingen. Av det skälet ska det finnas i förväg bestämda frister för när olika typer av uppgifter ska gallras. Det överläts till medlemsstaterna att avgöra hur långa gallringsfristerna ska vara, men utgångspunkten är att de inte får vara längre än nödvändigt. Huvudregeln är att gallringen ska leda till att uppgifterna raderas eller avidentifieras. Gallring kan också ske genom arkivering av uppgifterna.

De författningar som berörs av rambeslutet innehåller gallringsregler (se avsnitt 4). Dessa är anpassade till de särskilda behoven inom respektive verksamhetsområde eller för det aktuella registret. Gallringsreglerna är därför utformade på olika sätt. Personuppgiftslagens generella föreskrift om att uppgifter som inte längre behövs för sitt ändamål ska gallras återspeglas i vissa författningar (se t.ex. 13 § polisdatlagen), men dessutom innehåller dessa särskilda gallringsregler för vissa register eller vissa typer av uppgifter. Kravet på att det ska finnas särskilt angivna gallringsfrister är således uppfyllt. Sammanfattningsvis får den befintliga lagstiftningen anses uppfylla kraven i rambeslutet när det gäller grundläggande bestämmelser om gallring och krav på att det ska finnas gallringsfrister.

## 5.6 Information till den registrerade

### 5.6.1 Innehållet i rambeslutet

Medlemsstaterna ska enligt *artikel 16* i rambeslutet se till att den registrerade i enlighet med nationell rätt informeras om förekommande insamling eller behandling av personuppgifter. Vilka former informationen ska ha bestäms av medlemsstaterna. Det kan göras t.ex. genom

lagstiftning eller offentliggörande av vilka typer av uppgiftsbehandling som förekommer (*skäl 27*). Medlemsstaterna har dock möjlighet att, i enlighet med sin nationella lagstiftning, begära att en medlemsstat till vilken uppgifter har överförts eller gjorts tillgängliga inte informerar den registrerade utan förhandsmedgivande. Dessa begränsningar i rätten att behandla uppgifter har behandlats i avsnitt 5.4.5.

Enligt *artikel 17 punkten 1* har varje registrerad person rätt att på begäran, med rimliga intervall, utan hinder och utan större tidsutdräkt eller kostnader få åtminstone

- bekräftelse från den registeransvarige eller från den nationella tillsynsmyndigheten på om uppgifter om honom eller henne har överförts till eller gjorts tillgängliga för en annan stat, eller annan mottagare som anges i rambeslutet, samt information om till vilka mottagare eller kategorier av mottagare som uppgifter lämnats och information om vilka uppgifter som behandlas, eller
- bekräftelse från den nationella tillsynsmyndigheten på att alla nödvändiga kontroller har utförts.

Medlemsstaterna har enligt *punkten 2* rätt att begränsa tillgången till information enligt det första alternativet i punkten 1, om begränsningen med beaktande av vederbörandes legitima intressen är en nödvändig och rimlig åtgärd för att

- a) hindra obstruktion mot officiella eller rättsliga utredningar, förundersökningar eller förfaranden,
- b) inte inverka negativt på förebyggande, upptäckt, utredning och lagföring av brott eller verkställighet av straffrättsliga påföljder,
- c) skydda allmän säkerhet,
- d) skydda nationell säkerhet, eller
- e) skydda den registrerades eller andra personers fri- och rättigheter.

En vägran att lämna information ska enligt huvudregeln vara skriftlig och innehålla skälen för vägran. Grundas vägran på någon av punkterna a–e ovan behöver någon underrättelse inte lämnas. Under alla förhållanden ska den registrerade underrättas om att han eller hon kan överklaga till den nationella tillsynsmyndigheten, en rättslig myndighet eller till domstol.

## 5.6.2 Behovet av lagändringar

Personuppgiftslagen innehåller i likhet med rambeslutet bestämmelser om information till den registrerade (se avsnitt 4.3.4). Regleringen i personuppgiftslagen innebär att information ska lämnas i betydligt större omfattning än vad som krävs i rambeslutet. Av 6 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet följer att personuppgiftslagens bestämmelser om information till den registrerade gäller i sådan verksamhet. Varken polisdatlagen eller någon av de övriga sektorsförfattningar som berörs av rambeslutet innehåller särskilda bestämmelser om information till den registrerade, vilket innebär att bestämmelserna i 23–26 §§ personuppgiftslagen om information till den registrerade gäller. Vissa registerförfattningar har inte heller några regler om information till den registrerade. Även i de fallen torde 23–26 §§ gälla. Eftersom artikel 16 enbart innehåller krav på

att det ska finnas nationella regler om information till den registrerade och kraven i artikel 17 är mindre långtgående än personuppgiftslagens bestämmelser uppfyller Sverige kraven i de fall där personuppgiftslagen är tillämplig.

I författningarna om enskilda register finns i vissa fall särskilda regler om information till den registrerade. Enligt 9 § lagen om belastningsregister har en enskild rätt att på begäran skriftligen få del av samtliga uppgifter ur registret om sig själv. Sådana uppgifter ska lämnas på begäran utan avgift en gång per kalenderår. Vidare anges vissa andra situationer där den enskilde har rätt till registerutdrag. Bestämmelsen är något annorlunda utformad än motsvarande regel i personuppgiftslagen, men får anses uppfylla kraven i rambeslutet. Lagen om misstankeregister innehåller också bestämmelser om utlämnande av uppgifter till enskilda. Den registrerade själv tillhör inte dem som har rätt till information. Detta bör ses mot bakgrund av dels att rätten till information för brottsmisstänka regleras i rättegångsbalken (23 kap. 18 och 21 §§), dels att information i många fall skulle skada den brottsbekämpande verksamheten. Att inte lämna information till den registrerade om uppgifter i misstankeregistret är således väl förenligt med de undantag som anges i artikel 17 punkten 2 a–c. Särregleringen torde därför uppfylla kraven i rambeslutet.

Även lagen om internationellt tullsamarbete innehåller en särskild bestämmelse om information (se avsnitt 4.7.4). Enligt 2 kap. 8 § är en svensk myndighet som har sänt över en uppgift till en utländsk myndighet eller mellanfolklig organisation skyldig att, på begäran av den som uppgiften rör, underrätta denne om vilken utländsk myndighet eller organisation som uppgiften översänts till och för vilket ändamål. Under rättelse behöver dock inte lämnas i vissa fall, bl.a. om det är uppenbart obehövligt. Det kan diskuteras om undantaget från skyldigheten att underrätta i det fallet är förenlig med rambeslutet, som inte gör något sådant undantag. Frågan bör uppmärksammas i det fortsatta lagstiftningsarbetet.

Rätten att överklaga beslut i fråga om information behandlas i avsnitt 5.8.

Sammanfattningsvis torde rambeslutets bestämmelser om registrerade personers rätt till information, möjligen med undantag för bestämmelserna om information till enskilda i lagen om internationellt tullsamarbete, inte kräva några lagändringar.

## 5.7 Korrigering av personuppgifter

### 5.7.1 Innehållet i rambeslutet

*Artikel 4* innehåller regler om rättelse, radering och blockering. Syftet med artikeln är att tillgodose kraven på kvaliteten på uppgifterna. Den grundläggande principen, som slås fast i *artikel 4 punkten 1*, är att personuppgifter ska rättas om de är felaktiga samt, om så är möjligt och nödvändigt, kompletteras eller aktualiseras. Om det finns skäl att anta att en radering av personuppgifter skulle påverka den registrerades intressen

ska uppgifterna blockeras i stället. Blockerade uppgifter får endast behandlas för det ändamål som hindrade att de raderades.

Från kravet på radering görs i punkten 4 undantag för personuppgifter som ingår i ett domstolsbeslut eller underlaget för ett sådant beslut. I fråga om sådana uppgifter ska rättelse, radering eller blockering utföras enligt nationell lagstiftning. I skäl 12 framhålls också att kravet på korrekthet måste ses på ett annat sätt när det gäller uppgifter i rättsliga förfaranden. Uppgifterna grundar sig ofta på personers subjektiva uppfattningar och då hänför sig kravet på korrekthet inte till innehållet i utsagan utan till det faktum att en viss utsaga har avgetts.

I *artikel 8* föreskrivs att myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. I görligaste mån ska kvaliteten på uppgifterna kontrolleras innan dessa överförs eller görs tillgängliga. Dessutom ska alltid så långt möjligt annan information bifogas som gör att den mottagande myndigheten kan bedöma om uppgifterna är korrekta, fullständiga, aktuella och tillförlitliga. Om personuppgifter översänds spontant ska den mottagande myndigheten utan dröjsmål bedöma om uppgifterna är nödvändiga för det ändamål för vilka de översändes.

Skulle det visa sig att felaktiga uppgifter har översänts, eller att uppgifter har översänts olovligen, ska mottagaren enligt *artikel 8 punkten 2* omedelbart underrättas om detta. Uppgifterna ska då omgående rättas, raderas eller blockeras i enlighet med *artikel 4*. Det innebär, som nyss nämnts, bl.a. att radering inte behöver ske i domstolsbeslut och underlaget för dem. När det gäller sådana uppgifter ska vidare, enligt skäl 15, rättelse, radering eller blockering ske enligt nationell rätt, om de behandlas av domstolsliknande myndigheter. Med detta avses myndigheter med behörighet att fatta rättsligen bindande beslut.

Enligt *artikel 18* punkten 1 ska medlemsstaterna fastställa om den registrerade har rätt att vända sig direkt till den personuppgiftsansvarige eller till tillsynsmyndigheten för att begära att den personuppgiftsansvarige fullgör sina uppgifter att rätta, radera eller blockera personuppgifter. Vägrar den personuppgiftsansvarige att rätta, radera eller blockera uppgiften, ska beslutet vara skriftligt och innehålla uppgift om hur den berörde kan anföra klagomål eller på annat sätt begära prövning enligt nationell rätt. Den registrerade har rätt att få besked om huruvida behandlingen har varit korrekt eller inte. Medlemsstaterna får dock även föreskriva att den registrerade endast ska informeras av tillsynsmyndigheten om att en kontroll av behandlingen har utförts.

Om den registrerade bestrider att en viss uppgift är korrekt, och det inte kan fastställas om så är fallet, får uppgiften enligt punkten 2 märkas.

### 5.7.2 Behovet av lagändringar

Artiklarna 4 och 8 i rambeslutet motsvarar delvis *artikel 6 d* i dataskyddsdirektivet, som i sin tur återspeglas i *9 §* personuppgiftslagen. Enligt första stycket punkterna g och h i den paragrafen föreskrivs att de uppgifter som behandlas ska vara riktiga och, om det är nödvändigt, aktuella samt att den personuppgiftsansvarige ska se till att alla rimliga



åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. De nu aktuella punkterna i 9 § gäller vid Tullverkets personuppgiftsbehandling. De är också – i avsaknad av särreglering – tillämpliga i polisens, Kustbevakningens, åklagarväsendets, domstolarnas och kriminalvårdens verksamhet.

Artikel 18 motsvarar delvis artikel 12 b i dataskyddsdirektivet, som har genomförts genom regeln i 28 § personuppgiftslagen. Enligt den paragrafen är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna personuppgifter som inte har behandlats korrekt enligt lagen eller föreskrifter som utfärdats med stöd av lagen. En åtgärd av det nu aktuella slaget förutsätter dock att den personuppgiftsansvarige har övertygats om att uppgiften i fråga är felaktig (prop. 1997/98:44 s. 87). Om så inte är fallet kan den registrerade anmäla saken till tillsynsmyndigheten, som, om den delar den registrerades uppfattning och inleder tillsyn, har möjlighet att försöka åstadkomma rättelse på frivillig väg eller förbjuda den personuppgiftsansvarige att behandla personuppgifterna på något annat sätt än genom att lagra dem. Som en sista utväg kan tillsynsmyndigheten föra talan vid domstol om att uppgifterna ska utplånas (47 § personuppgiftslagen). Den registrerade kan också, om det rör sig om en myndighets behandling av personuppgifter, själv överklaga den personuppgiftsansvariga myndighetens beslut angående rättelse (52 § personuppgiftslagen).

När det gäller skyldigheten att på begäran av den registrerade rätta uppgifter är, genom hänvisningar i respektive sektorsförfattning, 28 § personuppgiftslagen tillämplig på personuppgiftsbehandlingen vid de myndigheter som berörs av rambeslutet. I 12 § lagen om Schengens informationssystem finns en särskild rättelseregeln. Där föreskrivs att Rikspolisstyrelsen är skyldig att på begäran av den registrerade, eller om det annars finns anledning till det, snarast rätta, blockera eller utplåna en personuppgift som styrelsen har registrerat, om uppgiften är rättsligt eller sakligt felaktig. Bestämmelsen torde uppfylla kraven i de nu aktuella artiklarna. Förordningen om register över förelägganden av ordningsbot innehåller varken någon regel om rättelse eller någon hänvisning till personuppgiftslagens regel om rättelse. Eventuella behov av författningsändring i den förordningen kan dock tillgodoses genom förändringar på förordningsnivå. Detsamma gäller regleringen i förordningen om register över strafförelägganden. Övriga författningar om enskilda register innehåller samtliga hänvisningar till 28 § personuppgiftslagen som gör rättelseregeln tillämplig.

Från kravet på rättelse görs undantag i artikel 4 punkten 4 i rambeslutet som innebär att felaktiga uppgifter i domstolsbeslut och underlaget för dem inte behöver raderas. Det kan noteras att det inte finns någon motsvarande begränsning i 9 § personuppgiftslagen. Rambeslutet kräver dock inte att de svenska reglerna ändras i denna del.

När det gäller rambeslutets bestämmelser om korrigerig av personuppgifter finns det skäl att beröra den svenska offentlighetsprincipen. Som har nämnts ovan (avsnitt 5.4.4) torde innebörden av skäl 31 vara att det inte är meningen att rambeslutet ska inskränka den rätt till insyn som allmänheten har genom rätten att ta del av allmänna offentliga

handlingar. Det är därför av särskilt intresse att notera att bestämmelserna i rambeslutet om rättelse, blockering och radering, liksom när det gäller dataskyddsdirektivets motsvarande bestämmelser, som huvudregel inte pekar ut vilken metod som ska väljas för korrigerings i olika situationer. Rambeslutet gör undantag endast för situationer då det finns skälig grund att anta att en radering skulle kunna påverka den registrerades legitima intressen varvid det föreskrivs att uppgifter inte ska raderas utan istället blockeras (artikel 4 punkten 3). Det är följaktligen i princip upp till den personuppgiftsansvarige att avgöra med vilken metod en eventuell korrigerings ska göras (se prop. 1997/98:44 s. 87). Detta innebär typiskt sett att myndigheter inte, i strid med offentlighetsprincipen och arkivlagstiftningen, kommer att kunna vidta åtgärder som innebär att uppgifter som ingår i allmänna handlingar raderas. Det vanliga torde i stället vara att en felaktig eller ofullständig uppgift kompletteras med en uppgift som är korrekt. När det gäller motsvarande bestämmelse i dataskyddsdirektivet uttalade Datalagskommittén att det enda kravet är att det i alla sammanhang klart framgår att den felaktiga uppgiften har ersatts av en annan uppgift och vilka de rätta förhållandena är (SOU 1997:39 s. 217 f.). Motsvarande får anses gälla även i fråga rättelse enligt det nu aktuella rambeslutet.

Det kan alltså konstateras att rambeslutets olika förpliktelser när det gäller korrigerings av personuppgifter i huvudsak överensstämmer med den svenska regleringen och att några lagändringar inte torde behövas.

## 5.8 Tillgång till rättsmedel

I *artikel 20* föreskrivs att den registrerade ska ha rätt att, utan att det påverkar möjligheten att utnyttja något administrativt förfarande, inför domstol föra talan mot kränkningar av sådana rättigheter som skyddas av rambeslutet.

I 52 § personuppgiftslagen finns bestämmelser om rätt att överklaga en myndighets beslut i fråga om information och rättelse. Enligt paragrafen får en myndighets beslut om information enligt bl.a. 26 § och om rättelse enligt 28 § överklagas till allmän förvaltningsdomstol. Eftersom varken polisdatalagen eller någon av de andra särskilda författningar som reglerar register i polisverksamheten innehåller några bestämmelser om överklagande gäller 52 § personuppgiftslagen i sådan verksamhet.

I de författningar som gäller för de andra verksamhetsområden som berörs av rambeslutet, bl.a. de författningar som gäller för domstolsväsendet och kriminalvården, finns särskilda bestämmelser om överklagande som med ett undantag i sak ger samma rätt till överklagande som 52 § personuppgiftslagen. I dessa fall uppfyller Sverige alltså redan kraven i rambeslutet. Den författning som gäller för Skatteverkets behandling av personuppgifter vid medverkan i brottsutredningar, innehåller en särskild bestämmelse om överklagande som dock inte omfattar överklagande av bristande information från den personuppgiftsansvarige. Här torde det således krävas lagändring för att Sverige ska uppfylla kraven i rambeslutet.

Lagen om Schengens informationssystem innehåller, som tidigare nämnts, en särskild regel om rättelse men ingen regel om överklagande. Möjlighet att överklaga torde dock i dessa fall följa av allmänna förvaltningsrättsliga principer. I prop. 2006/07:33 s. 32 om godkännande av rådsbeslutet om andra generationen av Schengens informationssystem har dock framhållits att det kan vara lämpligt att se över lagen på denna punkt.

Utöver möjligheten att överklaga beslut av en personuppgiftsansvarig myndighet finns det även andra möjligheter att agera för den som känner sig förfördelad av hur behandlingen av personuppgifter rörande honom eller henne har skötts. I avsnitt 4.3.7 och 5.10.2 behandlas de befogenheter som Datainspektionen och Säkerhets- och Integritets-skyddsnämnden har i egenskap av tillsynsmyndigheter när det gäller klagomål från enskilda. En annan möjlighet är att begära skadestånd av staten för skada som någon anställd har vållat i sin myndighetsutövning. Frågor om skadestånd för felaktig personuppgiftsbehandling behandlas i avsnitt 4.3.8. Om den felaktiga handläggningen utgör en brottslig gärning har även en enskild person – för det fall åklagare har beslutat att inte väcka allmänt åtal – som regel rätt att väcka åtal mot en tjänsteman som han anser gjort sig skyldig till brottsligt handlande (20 kap. 8 § rättegångsbalken). Slutligen kan varje medborgare vända sig till Riksdagens ombudsmän (JO) med klagomål. Om JO finner att fel har begåtts kan han rikta kritik mot myndigheten eller tjänstemannen eller väcka fråga om disciplinärt ansvar. Om det felaktiga handlandet utgör brott kan JO väcka åtal för detta.

Sammanfattningsvis torde rambeslutets bestämmelser om tillgång till rättsmedel inte kräva några lagändringar i svensk rätt.

## 5.9 Säkerhet och skydd vid uppgiftsbehandling

### 5.9.1 Innehållet i rambeslutet

I *artikel 22 punkterna 1, 3 och 4* regleras säkerheten vid behandling av personuppgifter. Artikeln ålägger medlemsstaterna att se till att behöriga myndigheter vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från att avsiktligt eller oavsiktligt utplånas eller gå förlorade samt från ändringar, otillåten spridning och otillåten tillgång till uppgifterna. I *punkten 2* ställs mera konkreta krav på olika typer av åtgärder som dels ska förhindra att uppgifterna hamnar i orätta händer, dels tillförsäkra att det går att i efterhand kontrollera vem som har lagt in uppgifter och att de system som används fungerar tillfredsställande.

I *artikel 21* i rambeslutet föreskrivs att personuppgifter endast får behandlas av anställda vid den behöriga myndigheten eller efter instruktioner från denna, om det inte föreligger rättsliga skyldigheter till annan behandling. Vidare ska den som anlitas för att arbeta för en behörig myndighet vara bunden av alla de bestämmelser om skydd av uppgifter som gäller för respektive myndighet.

Enligt *artikel 25 punkten 4* ska tillsynsmyndighetens ledamöter och personal vara bundna av tystnadsplikt rörande uppgifter de fått del av i tjänsten även sedan anställningen eller uppdraget har upphört.

Enligt *artikel 10 punkten 1* ska varje överföring av personuppgifter registreras eller dokumenteras för att möjliggöra kontroll av behandlingen i efterhand.

### 5.9.2 Behovet av lagändringar

I 30 och 31 §§ personuppgiftslagen finns bestämmelser om säkerhet vid behandlingen av personuppgifter som, även om de är mer generell utformade, motsvarar rambeslutets bestämmelser om säkerhet vid personuppgiftsbehandling. Vidare föreskrivs i 32 § personuppgiftslagen att tillsynsmyndigheten får besluta om säkerhetsåtgärder enligt 31 §. I 6 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns en direkt hänvisning till bestämmelserna i 30–32 §§ personuppgiftslagen. Varken övriga sektorsförfattningar eller de lagar som reglerar enskilda register innehåller några bestämmelser om datasäkerhet, varför 30–32 §§ personuppgiftslagen är tillämpliga på dessa.

När Schengenkonventionen genomfördes i svensk rätt gjordes bedömningen att Sverige genom de allmänna skyddsreglerna i personuppgiftslagen uppfyllde de säkerhetskrav som konventionen ställde (jfr prop. 1999/2000:64 s. 148). Konventionens krav på datasäkerhet har – också i fråga om detaljer rörande vilka enskilda säkerhetsåtgärder som krävs – stora likheter med de krav som ställs i rambeslutet. Även när det gäller motsvarande bestämmelser i det rådsbeslut som kommer att ersätta Schengenkonventionens bestämmelser om Schengens informationssystem har regeringen gjort den preliminära bedömningen att det inte krävs några författningsändringar (prop. 2006/07:33 s. 11 f.). Motsvarande bedömning gjordes i fråga om kraven på datasäkerhet i Europokonventionen (jfr prop. 1996/97:164 s. 46 f.).

Regelverket om arkivering räknas också som bestämmelser om informationssäkerhet (prop. 1997/98:44 s. 92). Som exempel kan nämnas reglerna i 3, 5 och 6 §§ arkivlagen (1990:782) om hur arkivhandlingar och arkiv ska hanteras.

Vidare bör nämnas att regeln i 5 kap. 2 § sekretesslagen (1980:100) andra stycket 1 om sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd med avseende på byggnader eller andra anläggningar, lokaler eller inventarier har ansetts gälla för uppgifter om en tingsrätts datorer och tillhörande utrustning (RÅ 2004:97).

Mot den nu angivna bakgrunden bedöms rambeslutets bestämmelser i fråga om säkerhet vid personuppgiftsbehandling inte kräva några lagändringar.

Artikel 21 har sin motsvarighet i artikel 16 i dataskyddsdirektivet. Den har genomförts genom 30 § i personuppgiftslagen som, något förenklat, föreskriver att den som arbetar med personuppgiftsbehandling ska göra detta i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal som anger detta. Om det i lag eller annan författning finns särskilda bestämmelser om behandling av personuppgifter i det allmänna verksamheten gäller i stället dessa.

I fråga om Tullverkets personuppgiftsbehandling hänvisas till 30 § personuppgiftslagen. Övriga författningar innehåller inte någon särreglering, vilket innebär att personuppgiftslagens bestämmelser gäller.

När det gäller innehållet i artikel 21 bör framhållas att i det allmänna verksamheten kan disciplinärt ansvar utkrävas av en arbetstagare som uppsåtligt eller av oaktsamhet åsidosätter vad som gäller för anställningen; se 14 § lagen (1994:260) om offentlig anställning. Detta torde utgöra en tillräcklig åtgärd för att åstadkomma att anställda följer regelverket vid behandlingen av personuppgifter. Det finns, utöver förbudet i 21 § personuppgiftslagen mot att behandla uppgifter om lagöverträdelse, inte något formellt hinder mot att låta viss behandling av personuppgifter ske utanför en myndighet. Arten av de verksamheter som omfattas av rambeslutet är dock sådan att utrymmet för att låta behandla personuppgifter utanför myndighetssfären torde vara mycket begränsat. Det som möjligen kan komma i fråga torde vara teknisk bearbetning i någon form. Sådan bearbetning måste uppfylla säkerhetskraven i 30 och 31 §§ personuppgiftslagen. Inte heller artikel 21 torde således kräva någon lagstiftningsåtgärd.

När det gäller artikel 25 punkten 4 kan följande sägas. För många av de personuppgifter som behandlas inom ramen för den brottsbekämpande verksamheten gäller sekretess såväl till skydd för det brottsbekämpande verksamheten som till skydd för den registrerade. För en närmare beskrivning av sekretessen hänvisas till promemorian. Av särskilt intresse här är den bestämmelse i 13 kap. 1 § sekretesslagen som föreskriver att om en myndighet i verksamhet som avser tillsyn eller revision från annan myndighet erhåller uppgifter som är sekretessbelagda där så gäller sekretessen också hos den mottagande myndigheten. Att den tystnadsplikt som gäller i fråga om sekretessbelagda uppgifter gäller även efter det att en person har lämnat sin anställning eller sitt uppdrag följer av 1 kap. 6 § sekretesslagen. Några lagändringar bedöms därför inte vara nödvändiga med anledning av artikel 25.

Skyldigheten att dokumentera överföring av personuppgifter torde inte behöva regleras i lag. Sammanfattningsvis kräver rambeslutets bestämmelser i dessa delar inte några lagändringar.

## 5.10 Tillsyn

### 5.10.1 Innehållet i rambeslutet

Enligt *artikel 25* ska varje medlemsstat utse en eller flera tillsynsmyndigheter som ska övervaka tillämpningen av de bestämmelser som antas i enlighet med rambeslutet. En sådan myndighet ska vara oberoende när de fullgör sina åligganden och ha vissa befogenheter, nämligen utredningsbefogenheter, faktiska befogenheter att ingripa, samt befogenhet att inleda rättsliga förfaranden. Var och en ska ha rätt att vända sig till tillsynsmyndigheten i frågor som rör behandling av personuppgifter.

I *artikel 10 punkten 2* föreskrivs att den nationella tillsynsmyndigheten ska få tillgång till registrering och dokumentation som rör behandlingen av personuppgifter.

Vidare föreskrivs i *artikel 23* att den nationella tillsynsmyndigheten ska rådfrågas innan behandling av personuppgifter i nya register påbörjas, dels om känsliga personuppgifter kommer att behandlas, dels om typen av behandling, särskilt användning av nya teknik eller nya förfaranden som innebär speciella risker för registrerades grundläggande fri- och rättigheter och deras rätt till privatliv.

Artikel 23 innehåller således inte, som artikel 20 i dataskyddsdirektivet, något uttryckligt krav på anmälan av särskilt integritetskänsliga behandlingar för förhandskontroll av tillsynsmyndigheten. Under förhandlingsarbetet har också gjorts klart att artikel 23 endast innebär förpliktelser av det slag som anges i artikel 28 punkten 2 i dataskyddsdirektivet. Tolkad på detta sätt ålägger den alltså inte medlemsstaterna att ha ett system med obligatorisk förhandskontroll av enskilda register utan tillsynsmyndighetens möjlighet att påverka kan tillgodoses på annat sätt, t.ex. genom att myndigheten får möjlighet att yttra sig i ett lagstiftningsärende. Eftersom medlemsstaterna har rätt att föreskriva strängare regler hindrar artikeln å andra sidan dem inte från att ha ett system med kontroll på förhand i fråga om enskilda register eller liknande.

### 5.10.2 Behovet av lagändringar

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (2 § personuppgiftsförordningen, se avsnitt 4.3.7). Det innebär att inspektionen kommer att utöva tillsyn även över behandlingen av sådana uppgifter som omfattas av rambeslutet.

När det gäller tillsynsmyndighetens befogenheter innehåller rambeslutet inte några krav på andra befogenheter än de som dataskyddsdirektivet förutsätter. Innehållet i de ovan refererade artiklarna motsvarar i sak vad som gäller enligt artikel 28 punkterna 1 och 2 samt del av punkten 3 i dataskyddsdirektivet. Dessa har genomförts i svensk rätt genom 43–47 §§ personuppgiftslagen. Enligt 43 § 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 denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. I 44–46 §§ personuppgiftslagen regleras tillsynsmyndighetens rätt att meddela förelägganden för att framtvinga rättelse. Enligt 47 § får tillsynsmyndigheten ansöka hos allmän förvaltningsdomstol om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas. I allt väsentligt gäller personuppgiftslagens bestämmelser för de verksamheter som omfattas av rambeslutets tillämpningsområde.

Det bör också nämnas att den nyinrättade Säkerhets- och integritetsskyddsnämnden (se prop. 2006/07:133 och lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet) har vissa tillsynsuppgifter vid sidan om Datainspektionen när det gäller Säkerhetspolisens personuppgiftsbehandling, bl.a. avseende Säkerhetspolisens behandling av uppgifter enligt polisdatalagen. Enskilda kan vända sig till nämnden och begära särskild kontroll. Säkerhets- och integritetsskyddsnämndens befogenheter regleras i lagen om tillsyn över viss brottsbekämpande

verksamhet. Enligt 4 § har nämnden rätt att av förvaltningsmyndigheter få de uppgifter och det biträde som nämnden begär. Även domstolar och förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter den begär. Av förarbetena framgår att nämnden ska utöva sin tillsyn bl.a. genom inspektioner (prop. 2006/07:133 s. 68 f.). Nämndens tillsyn kan utmynna i uttalanden till regeringen, till den granskade myndigheten eller underrättelser till en enskild, i det sistnämnda fallet antingen om nämnden har granskat ett särskilt förhållande på eget initiativ eller om den enskilde har utnyttjat sin rätt att begära särskild kontroll.

Sammanfattningsvis innehåller svensk rätt bestämmelser om tillsyn som i huvudsak motsvarar rambeslutets krav. Huruvida de befogenheter som tillsynsmyndigheterna har i dag bör utökas får analyseras närmare i det kommande lagstiftningsarbetet.

## 5.11 Skadestånd

Enligt *artikel 19* i rambeslutet har den som har lidit skada till följd av en otillåten behandling av personuppgifter eller någon annan åtgärd som är oförenlig med nationell lagstiftning rätt till ersättning av den registeransvarige, eller av en annan myndighet, för den skada som han eller hon har lidit. I fråga om översända uppgifter kan mottagaren inte åberopa att dessa var felaktiga för att undgå ansvar. Däremot kan mottagaren i vissa fall ha regressrätt mot den översändande för det skadestånd som har betalats ut.

En delvis motsvarande reglering som den i rambeslutet finns i artikel 23 punkten 1 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 48 § personuppgiftslagen. Skadeståndsansvaret enligt den paragrafen omfattar varje typ av skada eller kränkning som en behandling i strid med reglerna i personuppgiftslagen, eller föreskrifter som har meddelats med stöd av den lagen, har orsakat. Ersättningskyldigheten kan dock jämkas, i den utsträckning det är skäligt, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

Samtliga författningar som berörs av rambeslutet, med undantag av förordningarna om strafförelägganderegister respektive ordningsbetsregister, innehåller hänvisningar som gör 48 § personuppgiftslagen tillämplig på behandling som sker i strid med reglerna i respektive författning.

Det kan noteras att dataskyddsdirektivet – som ju reglerar förhållandet mellan det allmänna och enskilda – inte innehåller några bestämmelser motsvarande dem i artikel 19 punkten 2 i rambeslutet som reglerar regressrätt mellan stater. Några sådana bestämmelser finns inte heller i personuppgiftslagen. Staternas skyldighet beträffande regressanspråk är att se som ett folkrättsligt åtagande och kräver inte några lagstiftningsåtgärder. Det kan emellertid finnas anledning att i ett lämpligt sammanhang överväga en reglering av formerna för handläggningen av sådana regresskrav.

När det gäller möjligheterna till jämkning av skadeståndsansvar enligt personuppgiftslagen blir vad som är skäligt en fråga för domstol i varje

enskilt fall att bedöma. Den omständigheten att en myndighet i en sådan situation kan göra gällande regressansvar mot en utländsk myndighet torde regelmässigt medföra att jämkning inte kommer ifråga. I det fortsatta lagstiftningsarbetet bör dock närmare utredas om det finns andra situationer i vilka jämkning skulle kunna aktualiseras på ett sätt som inte är förenligt med rambeslutet.

När det gäller förordningarna om strafförelägganderegister respektive ordningsbottsregister torde bestämmelserna om skadestånd i respektive sektorslag inte vara tillämpliga, eftersom de bestämmelserna tar sikte på behandling i strid med bestämmelser i *respektive lag*. Det kan också ifrågasättas om statens allmänna skadeståndsansvar enligt skadeståndslagen är tillräckligt. Om uppgifter som finns i registret eller tillförs registret kan förväntas överföras eller göras tillgängliga på det sätt som avses i rambeslutet kan det alltså finnas anledning att överväga behovet av författningsändringar. Med hänsyn till att regleringen finns i förordning torde dock eventuella kompletteringar kunna göras på förordningsnivå.

Sammanfattningsvis bedöms svensk lagstiftning i huvudsak motsvara rambeslutets bestämmelser om skadeståndsansvar. Det bör dock i det fortsatta lagstiftningsarbetet närmare utredas om möjligheterna till jämkning av skadeståndsansvar i svensk rätt till fullo är förenliga med rambeslutet.

## 5.12 Sanktioner

### 5.12.1 Innehållet i rambeslutet

Rambeslutet ställer i *artikel 24* krav på effektiva, proportionella och avskräckande påföljder för överträdelser av bestämmelser som antagits i enlighet med rambeslutet. Det står medlemsstaterna fritt att avgöra vilka medel som ska användas (se *skäl 30*).

### 5.12.2 Behovet av lagändringar

Sanktioner för överträdelser av bestämmelser kan vara av olika slag beroende på vad bestämmelserna rör och i vilket sammanhang de finns. De kan vara av straffrättslig karaktär eller av administrativ karaktär, t.ex. disciplinära åtgärder, vite eller skadestånd.

När dataskyddsdirektivet – som också förutsätter sanktioner – genomfördes framhöll regeringen att de huvudsakliga sanktionerna var möjligheterna att utdöma skadestånd och använda vite. Dessa sanktioner ansågs som effektiva och i stort sett tillräckliga (prop. 1997/98:44 s. 108). Viss kriminalisering ansågs dock nödvändig, men den begränsades till några få områden (se 49 § personuppgiftslagen).

I 44–46 §§ personuppgiftslagen finns således bestämmelser som ger Datainspektionen möjlighet att förelägga vite i en rad situationer. Det bör dock framhållas att det anses vara en allmän rättsgrundsats att vite inte bör användas mot statliga myndigheter (prop. 2004/05:164 s. 54 och 2006/07:46 s. 105). Även om 44 § personuppgiftslagen i och för sig



skulle vara tillämplig på en viss myndighets verksamhet torde alltså inte vitessanktionen kunna användas.

De i detta ärende aktuella författningarna med särbestämmelser om personuppgiftsbehandling innehåller varken några särskilda straffbestämmelser eller någon hänvisning till 49 § personuppgiftslagen. Detta gäller såväl sektorsförfattningarna som de författningar som reglerar enskilda register. Det förhållandet att vissa författningar gäller utöver personuppgiftslagen skulle kunna tolkas så att 49 § personuppgiftslagen därmed skulle vara tillämplig. Lagrådet har dock i ett tidigare lagstiftningsärende (prop. 2000/01:33 s. 346) ansett att legalitetsprincipen medför att 49 § personuppgiftslagen inte kan ges motsvarande tillämpning på bestämmelser som avviker från personuppgiftslagen och som har tagits in i särlagstiftning. Nämnade bestämmelse torde därför inte kunna tillämpas på överträdelse av bestämmelser som har antagits i enlighet med rambeslutet. Frågan är då om det finns andra straffrättsliga bestämmelser som kan anses uppfylla rambeslutets krav på sanktioner.

En typ av straffansvarsbestämmelser som kan bli aktuella är bestämmelserna om dataintrång i 4 kap. 9 c § brottsbalken. Bestämmelserna får anses väl uppfylla kravet vad gäller otillåten behandling i form av ändring, radering, förstörande och liknande åtgärder. De täcker likaså varje handlande som innebär att någon skaffar sig tillgång till personuppgifter i strid med regelverket. Straffbestämmelserna om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken fyller också en viktig funktion i sammanhanget, eftersom de straffbelägger såväl oaktsamt som uppsåtligt röjande av uppgifter som någon är skyldig att hemlighålla.

Överträdelse av bestämmelser som har antagits i enlighet med rambeslutet torde också kunna komma att bedömas som tjänstefel (20 kap. 1 § brottsbalken) förutsatt att de i straffbestämmelsen angivna förutsättningarna är uppfyllda, t.ex. att åtgärden vidtas vid myndighetsutövning.

I promemorian görs emellertid bedömningen att det är tveksamt om det, vid sidan av straffansvaret för dataintrång och brott mot tystnadsplikt, finns någon straffbestämmelse som täcker rambeslutets krav på sanktioner för överträdelse och att det därför kan finnas skäl att närmare överväga behovet av straffbestämmelser i det fortsatta arbetet. Liknande frågor har tidigare varit föremål för regeringens bedömning.

I rådets beslut 2007/533 av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) finns bestämmelser om sanktioner. Enligt artikel 65 i beslutet ska medlemsstaterna se till att effektiva, proportionella och avskräckande sanktioner utdöms i enlighet med nationell lag, bl.a. om uppgifter i SIS II missbrukas eller om utbyte av viss information sker i strid med beslutet. I prop. 2006/07:33 (s. 33) har beträffande nämnda bestämmelse i det aktuella rådsbeslutet (som då återfanns i artikel 55) gjorts bedömningen att förekomsten av relevanta straffbestämmelser i svensk rätt är tillräckligt för att uppfylla rådsbeslutets krav på sanktioner.

Även rådets beslut 2008/633/RIF av den 23 juni 2008 om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Europol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott innehåller bestämmelser om krav på sanktioner. I artikel 12 föreskrivs att

medlemsstaterna ska vidta nödvändiga åtgärder för att se till att all användning av VIS-uppgifter som strider mot bestämmelserna i beslutet är straffbar genom sanktioner, inklusive administrativa och/eller straffrättsliga sanktioner, vilka ska vara effektiva, proportionella och avskräckande. Även i detta fall har regeringen gjort bedömningen (prop. 2007/08:132 s. 18) att svensk rätt torde uppfylla kravet på sanktioner och därvid hänvisat till bestämmelserna om tjänstefel, dataintrång och brott mot tystnadsplikt.

Det kan konstateras att de nämnda EG-rättsakternas bestämmelser om sanktioner har samma syfte och uppvisar stora likheter med kraven på sanktioner i rambeslutet. Regeringen har gjort bedömningen att svensk rätt torde anses uppfylla kraven på sanktioner i de två rättsakterna. Samma slutsats torde kunna dras när det gäller rambeslutet.

Sammanfattningsvis torde rambeslutets bestämmelser om sanktioner inte kräva några lagändringar.

### 5.13 Övriga frågor

Enligt *artikel 26* påverkar rambeslutet inte sådana avtal som medlemsstaterna eller Europeiska unionen har ingått innan rambeslutet antogs. Vid tillämpningen av sådana avtal ska dock överföring av uppgifter till tredjeland ske med respekt för bestämmelserna i artikel 13 punkten 1 c och punkten 2 om förhandsmedgivande.

*Artikel 28* reglerar förhållandet till tidigare antagna unionsakter. Om dessa reglerar utbyte av personuppgifter eller tillgång till informationssystem som inrättats enligt fördraget om Europeiska unionen och innehåller särskilda villkor för mottagarens användning av uppgifterna ska sådana villkor ha företräde framför reglerna i rambeslutet. Som exempel kan nämnas Schengens informationssystem.

Av *artikel 27* följer att rambeslutet ska utvärderas efter fem år, särskilt med avseende på konsekvenserna av att tillämpningsområdet har begränsats till uppgifter som har överförts eller gjorts tillgängliga.

Rambeslutet ska enligt genomföras inom två år efter antagandet. (*artikel 29*). Det träder i kraft den tjugonde dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning (*artikel 30*).

De nu redovisade artiklarna kräver inte några lagstiftningsåtgärder.

## 6 Godkännande av rambeslutet

**Regeringens förslag:** Riksdagen godkänner det inom Europeiska unionen upprättade utkastet till Dataskyddsrambeslut.

**Promemorians förslag:** Överensstämmer med regeringens förslag.

**Remissinstanserna:** Det övervägande antalet remissinstanser som har yttrat sig har tillstyrkt förslaget eller lämnat det utan erinran.

*Juridiska fakulteten vid Lunds universitet* och *Svenska Journalistförbundet* har avstyrkt förslaget på den grunden att konsekvenserna av nödvändiga lagändringar inte är tillräckligt utredda.

*Justitieombudsmannen*, *Säkerhets- och integritetsskyddsnämnden*, *Datainspektionen* och *Riksarkivet* har framfört synpunkter på utformningen av rambeslutet och det svenska genomförandet av rambeslutet, men har inte angivit sin inställning till förslaget att godkänna beslutet.

Ett antal remissinstanser, däribland *Hovrätten för Nedre Norrland* och *Säkerhetspolisen*, har motiverat sin positiva inställning till rambeslutet med att beslutet kan förväntas förstärka skyddet för den enskilde när det gäller behandling av personuppgifter. *Åklagarmyndigheten* har framhållit att det är angeläget att stödja en förbättring av det gränsöverskridande utbytet av sådan information som kan effektivisera brottsbekämpningen. Enligt myndigheten får rambeslutet antas stödja en sådan utveckling genom det grundläggande skydd för behandling av personuppgifter det innebär. *Rikspolisstyrelsen* har uttalat att ett utökat internationellt informationsutbyte på de aktuella områdena förutsätter gemensamma riktlinjer vid behandling av personuppgifter för att åstadkomma såväl ett skydd för den personliga integriteten som för informationen och för att säkerställa att informationen är av god kvalitet. *Kustbevakningen* har framfört liknande synpunkter.

## Skälen för regeringens förslag

### *Godkännandeproposition eller proposition med lagförslag?*

Innan Sverige röstar för ett antagande av ett rambeslut i ministerrådet, måste riksdagens godkännande inhämtas, om beslutet – som i detta fall – förutsätter lagändringar eller annars bedöms vara av större vikt.

I denna proposition redovisas innehållet i utkastet till rambeslut och hur rambeslutet förhåller sig till svensk rätt. Propositionen utmynnar i förslaget att riksdagen ska godkänna utkastet till rambeslut, men några lagförslag presenteras inte. Däremot lämnas en allmän beskrivning av i vilka avseenden rambeslutet bedöms kräva lagändringar. Avsikten är att lämna förslag till lagändringar på grundval av en särskild proposition under förutsättning att riksdagen har godkänt utkastet till rambeslut.

Regeringen vill inledningsvis uttrycka sin förståelse för de synpunkter *Juridiska fakulteten vid Lunds universitet* och *Svenska Journalistförbundet* har framfört när det gäller svårigheterna att bedöma konsekvenserna av ett antagande av rambeslutet när frågan om godkännande av detsamma och frågan om vilka konkreta lagändringar som det föranleder inte behandlas i ett sammanhang. Regeringen delar *Hovrätten för Nedre Norrlands* uppfattning att det hade varit att föredra att frågan om godkännande av rambeslutet hade kunnat avvakta till dess att det finns slutliga förslag till de lagändringar som rambeslutet nödvändiggör. Det är, som riksdagen har framhållit vid flera tillfällen, givetvis önskvärt att i samband med att ett utkast till rambeslut läggs fram för riksdagens godkännande även presentera de lagändringar som behövs för att genomföra beslutet. Riksdagen har emellertid ansett att det är möjligt att godkänna ett utkast till råds- eller rambeslut och först därefter fatta beslut om aktuella lagstiftningsåtgärder. Att avvakta med följdlagstiftning på

detta sätt bör enligt riksdagens uttalanden emellertid endast ske när det är nödvändigt på grund av de tidsramar som gäller för antagandet av beslutet (bet. 1999/2000:JuU20 s. 6). Utgångspunkten bör därför vara att riksdagen, när den beslutar i fråga om godkännande av en överenskommelse, också har möjlighet att ta ställning till de lagändringar som blir aktuella till följd av överenskommelsen.

Beträffande det nu aktuella utkastet till rambeslut har det inom rådet träffats en principöverenskommelse om beslutets innehåll. Sverige kan lyfta sin parlamentariska granskningsreservation först efter det att riksdagens godkännande har inhämtats. Rambeslutet har ett mycket brett tillämpningsområde och berör lagstiftning om behandling av personuppgifter inom såväl polisväsendet som Tullverket, Kustbevakningen, åklagarväsendet, Skatteverket, domstolsväsendet och kriminalvården. Inom flera av dessa områden pågår reformarbete. Polisdatalagen, som har en central roll i sammanhanget, är som har framgått av avsnitt 4.4.2 för närvarande under omarbetning. Ny lagstiftning kan förväntas träda i kraft tidigast under 2009. Personuppgiftsbehandlingen inom både Kustbevakningen och domstolsväsendet är också föremål för översyn. Vidare har regeringen tillsatt en utredare som ska se över åklagarväsendets behandling av personuppgifter. Den utredningen ska presentera sitt arbete under hösten 2008. Vidare pågår arbete inom Justitiedepartementet med anledning av ett flertal andra rättsakter som rör brottsbekämpande myndigheters personuppgiftsbehandling. Till detta kommer att det pågår förhandlingar inom Europeiska unionen om ytterligare instrument som också berörs av rambeslutets tillämpningsområde.

Det pågår alltså reformarbete både i Sverige och inom Europeiska unionen på de områden som berörs av rambeslutet. Det innebär att det är nära nog omöjligt att i nuläget redovisa vilka lagstiftningsändringar som slutligen kan komma att krävas. I avsnitt 5 har emellertid redovisats i huvuddrag vilka lagändringar i förhållande till gällande rätt som rambeslutet kan väntas föranleda.

Vidare finns det skäl att erinra om att rambeslutet i många avseenden innehåller bestämmelser som liknar de som finns i dataskyddsdirektivet som har genomförts i svensk rätt samt att det svenska regelverket i stora delar är anpassat till det krav på dataskydd som ställs i rambeslutet. Det torde därför inte krävas några genomgripande lagstiftningsåtgärder för att genomföra rambeslutets krav.

Om Sverige skulle avvakta med att godkänna utkastet till rambeslut till dess att det finns ett tillfredsställande beredningsunderlag i fråga om behovet av lagändringar och den närmare utformningen av dessa, skulle det innebära en avsevärd försening av antagandet av rambeslutet. En sådan fördröjning kan ibland accepteras, men vore i detta fall särskilt olycklig eftersom rambeslutet dels syftar till att stärka enskildas rättigheter vid personuppgiftsbehandling, dels har stor betydelse för utvecklingen av andra instrument. Mot den bakgrunden finns det i detta fall starka skäl för regeringen att föreslå riksdagen att godkänna utkastet till rambeslut utan att regeringen samtidigt lägger fram de förslag till lagändringar som bedöms vara nödvändiga.

Både den ökade gränsöverskridande brottsligheten och den större rörligheten för personer skapar behov av ett tätare samarbete mellan de brottsbekämpande myndigheterna i olika länder och utökade möjligheter till rättslig hjälp i brottmål. Europol fyller en viktig funktion i samarbetet mellan brottsbekämpande myndigheter, samtidigt som Eurojust och det europeiska rättsliga nätverket har fått allt viktigare roller i arbetet med att förbättra det straffrättsliga samarbetet. Under senare år har dessutom en rad olika instrument förhandlats fram inom Europeiska unionen som ger medlemsstaterna större möjligheter att på ett enkelt sätt utbyta information med varandra, att verkställa påföljder beslutade i andra medlemsstater och att arbeta tillsammans med brottsbekämpande uppgifter.

Beräffande samarbetet mellan brottsbekämpande myndigheter kan Prümrådsbeslutet (se prop. 2007/08:83) och VIS-rådsbeslutet (se prop. 2007/08:132) nämnas som exempel på den pågående utvecklingen.

Det pågår också ett intensivt arbete med att utveckla det straffrättsliga samarbetet. Efter de redan genomförda rambesluten om en europeisk arresteringsorder och om frysning av egendom och bevismaterial är bl.a. ett rambeslut om en europeisk bevisinhämtningsorder (prop. 2007/08:141) nu aktuellt. När det gäller straffverkställighet kan nämnas rambesluten om tillämpning av principen om ömsesidigt erkännande på bötesstraff respektiver förverkande (se Ds 2007:18) samt rambeslutet om överförande av frihetsberövande påföljder inom Europeiska unionen (prop. 2007/08:84). Det finns också ett rambeslut som rör erkännande och övervakning av vissa icke frihetsberövande påföljder (se Ds 2008:42).

Det ökade samarbetet gynnar framför allt effektiviteten i brottsbekämpning och lagföring och skapar betydligt bättre förutsättningar att angripa allvarlig och gränsöverskridande brottslighet. Det är viktigt att den information som finns om allvarliga hot mot samhället kan utnyttjas, oavsett var den finns, och att brottsligheten i största möjliga utsträckning kan förhindras.

Det ökade informationsflödet kan emellertid också innebära nackdelar. Det kan leda till att myndigheterna samlar på sig stora mängder information om enskilda individer. Ett utökat informationsutbyte ställer därför krav på ett gott skydd för den enskildes personliga integritet. Eftersom dataskyddsdirektivet inte omfattar verksamhet på det polisiära och straffrättsliga området är behovet av bestämmelser om dataskydd på dessa områden stort. Dataskyddsrambeslutet kan sägas utgöra en betydelsefull skyddsreglering när informationsutbytet ökar och skapa balans när det gäller personlig integritet och samhällets intresse av att utreda och lagföra brott. Rambeslutet har tillkommit i det uttalade syftet att öka den enskildes skydd mot felaktig eller otillbörlig behandling av personuppgifter vid polisiärt och straffrättsligt samarbete över gränserna.

*Datainspektionen* har framhållit att det hade varit önskvärt att kraven i rambeslutet hade varit mer långtgående. Inspektionen har i det sammanhanget anfört att det bör finnas harmoniserade regler som anger en miniminivå i fråga om dataskydd också för den behandling av personuppgifter på detta område som sker nationellt. Enligt regeringens

mening är det positivt att man nu har förhandlat fram harmoniserade regler för behandlingen av sådana personuppgifter som utbyts mellan medlemsstaterna och vissa organ och informationssystem. Frågan om harmoniserade regler vad gäller personuppgiftsbehandling generellt på polis- och straffrättsområdet kan eventuellt bli föremål för diskussioner längre fram. Avsaknaden av sådana regler i detta rambeslut utgör dock enligt regeringens mening inte skäl att avstå från att godkänna beslutet.

Flera remissinstanser har framfört att rambeslutet kan komma att medföra praktiska komplikationer vid hanteringen av uppgifterna. *Datainspektionen* har påtalat att det förhållandet att rambeslutet endast är tillämpligt på personuppgifter som utbyts och inte på den behandling av uppgifter som sker nationellt medför att olika regler ska tillämpas för uppgifter i en och samma databas beroende på varifrån uppgifterna härrör. Detta kan enligt Datainspektionens mening komma att innebära tillämpningssvårigheter. *Hovrätten för Nedre Norrland* har påtalat att nödvändigheten av att särbehandla uppgifter som har överförts från annat land ställer särskilda krav på märkning av uppgifterna. *Kustbevakningen* har framfört liknande synpunkter och pekat på att det är resurskrävande. *Säkerhetspolisen* har konstaterat att rambeslutet kan komma att innebära att myndighetens hantering av personuppgifter kommer att styras av olika regelverk. *Åklagarmyndigheten* har ifrågasatt om det är lämpligt, eller ens tekniskt möjligt, att med rimliga insatser förverkliga ambitionen att förena alla ”importerade” uppgifter med en uppgift om att de emanerar från ett annat medlemsland.

Oavsett om man i det fortsatta lagstiftningsärendet väljer en minimalistisk väg och enbart genomför de författningsändringar som rambeslutet kräver eller om man går längre så torde det finnas behov av att på något sätt tekniskt märka uppgifter som kommer från andra stater för vilka det gäller olika typer av begränsningar i rätten att behandla dem. Det gäller nämligen så länge inte regleringen avseende behandlingen av uppgifter är helt harmoniserad inom Europeiska unionen, något som rambeslutet alltså inte kräver. Behovet av att märka uppgifter kommer att gälla för alla myndigheter som får uppgifter som omfattas av rambeslutet överförda till sig. Regeringen instämmer i att detta kan innebära tekniska utmaningar. Det kan inte heller uteslutas att det på andra sätt komplicerar myndigheternas hantering av uppgifterna. Sådana problem torde dock inte vara något nytt eftersom många av de berörda myndigheterna redan i dag erhåller uppgifter från andra stater för vilka det gäller användningsbegränsningar och som av det skälet måste hanteras annorlunda än andra uppgifter som myndigheterna behandlar. Detta i sig kan, mot bakgrund av syftet med rambeslutet, enligt regeringens mening inte heller utgöra skäl att inte godkänna beslutet.

Några remissinstanser har framfört att beslutet i vissa avseenden ger utrymme för olika tolkningar och därmed kan vålla tillämpningssvårigheter.

Enligt *Säkerhetspolisens* mening ger formuleringen av undantaget för viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet upphov till frågor då den kan tolkas som att det finns områden som berör nationell säkerhet som faller inom tillämpningsområdet. Säkerhetspolisen har också pekat på att viss del av myndighetens verksamhet inte kan sägas röra nationell säkerhet och

därmed kan komma att omfattas av regelverket i rambeslutet. Såväl Säkerhetspolisen som *Skatteverket* har understrukit vikten av att det i det kommande lagstiftningsarbetet klagörs i vilka avseenden respektive myndighet omfattas av rambeslutet.

När det gäller undantaget för viktiga nationella säkerhetsintressen kan regeringen dela Säkerhetspolisens synpunkt att rambeslutet ger utrymme för tolkning när det gäller vad som ska anses vara ett viktigt nationellt intresse och vad som inte når upp till den graden. Enligt regeringens mening torde – med hänsyn till hur arbetet är fördelat mellan Säkerhetspolisen och den öppna polisen i Sverige – den slutsatsen dock kunna dras att all verksamhet som Säkerhetspolisen bedriver som rör nationell säkerhet faller utanför rambeslutets tillämpningsområde. Som har framgått ovan (avsnitt 5.2.2) torde emellertid viss verksamhet som Säkerhetspolisen bedriver falla utanför begreppet nationell säkerhet och därför omfattas av rambeslutet. När det gäller samtliga berörda myndigheter får det i det fortsatta lagstiftningsärendet närmare utredas hur tillämpningsområdet för de författningsbestämmelser som föranleds av rambeslutet bör avgränsas.

*Datainspektionen* har vidare anfört att rambeslutet inte uppfyller de krav på tydlighet och förutsebarhet som bör ställas när det gäller tillåtna ändamål för vidarebehandling av uppgifter. *Datainspektionen* har anfört att möjligheten enligt artikel 11 d att behandla uppgifter för vilket annat ändamål som helst om det föreligger samtycke knappast är förenlig med kravet i artikel 3 punkt 2 på att det nya ändamålet ska vara förenligt med det ursprungliga. Enligt regeringens uppfattning måste dessa bestämmelser, vilket har anförts i avsnitt 5.4.2, på grund av hänvisningen i inledningen i artikel 11 till artikel 3 punkten 2, tolkas så att de grundläggande kraven i artikel 3 punkten 2 alltid gäller för vidarebehandling av uppgifter. Bestämmelserna i rambeslutet i denna del torde därför inte ge upphov till några tolkningsproblem.

*JO* har ifrågasatt hur den svenska offentlighetsprincipen står sig i förhållande till rambeslutets bestämmelser. *JO* har därvid uttryckt tveksamhet när det gäller promemorians tolkning av innebörden av skäl 31 och ifrågasatt om den verkligen kan tolkas så att Sverige har möjlighet att med hänvisning till den svenska offentlighetsprincipen underlåta att genomföra rambeslutets bestämmelser. *JO* har vidare gjort bedömningen att rambeslutets bestämmelser om radering av personuppgifter inte i alla delar är förenliga med den svenska offentlighetsprincipen.

Som har framgått ovan (avsnitt 5.4.2) kan regeringen instämma i att skäl 31 är något otydligt uttryckt. Enligt regeringens mening måste innebörden av detsamma vara att det inte är meningen att rambeslutet ska inskränka den rätt till insyn som allmänheten har genom rätten att ta del av allmänna offentliga handlingar. Regeringen gör också den reflektionen att skyldigheten att radera eller blockera uppgifter som har överförts olovligen i viss mening kan sägas påverka den rätt till insyn i allmänna handlingar som offentlighetsprincipen innebär. Enligt regeringens mening måste man dock, mot bakgrund av att skyldigheten avser uppgifter som har erhållits felaktigt, ha förståelse för att det från integritetssynpunkt för vissa stater är viktigt att sådana uppgifter ska kunna raderas eller blockeras så snart som möjligt.

Angående rambeslutets bestämmelser om tillsyn har *Säkerhets- och Integritetsskyddsnämnden* anført att förhållandet mellan å ena sidan rambeslutets krav på att en nationell tillsynsmyndighet ska ha befogenheter att inleda rättsliga förfaranden och å andra sidan den skyldighet som åligger nämnden att lämna resultatet av sin tillsyn när det gäller personuppgiftsbehandling vidare till annan myndighet för åtgärd måste tydliggöras. Som har anförts i avsnitt 5.10 anser regeringen att – även om svensk rätt i huvudsak uppfyller rambeslutets krav på tillsyn – frågan om tillsynsmyndigheternas befogenheter bör analyseras närmare i det kommande lagstiftningsarbetet.

Vad gäller bestämmelserna i utkastet till rambeslut om skadestånd har *Datainspektionen* anført att det förhållandet att en person, för att tillvarata sin rätt, kan tvingas vända sig till en annan medlemsstat med krav på ersättning kan medföra betydande praktiska problem för denne. Problemen blir enligt inspektionen än större då skadeståndsanspråk enligt utkastet till rambeslut ska regleras av den nationella lagstiftningen i den medlemsstat som är svarande. Att en person får vända sig till den stat som åsamkat skadan samt att den statens nationella skadeståndsregler tillämpas är dock inte unikt för det nu aktuella samarbetet. Enligt regeringens mening är den valda lösningen också den som bäst garanterar en korrekt behandling av skadeståndsfrågan.

### *Sammanfattande bedömning*

Rambeslutet innehåller bestämmelser som är ägnade att kompensera det effektivare uppgiftsutbytet på de områden som omfattas av beslutet med ett starkt dataskydd. Antagandet av rambeslutet är en högt prioriterad fråga inom Europeiska unionen, för att nå den önskade balansen mellan å ena sidan effektiv brottsbekämpning och å andra sidan nödvändigt integritetsskydd. Det är självfallet viktigt att den enskilde har ett bra skydd mot felaktig behandling av personuppgifter inom detta viktiga område.

Den remisskritik som har framförts när det gäller tydligheten i rambeslutet och de praktiska svårigheter som i viss mån måste sägas vara förenade med ett antagande av beslutet kan enligt regeringens mening inte anses väga upp den förbättring för skyddet av enskildas integritet som rambeslutet avgjort kommer att medföra.

Sverige har under lång tid varit drivande både i fråga om ett ökat informationsutbyte och i fråga om skydd för den enskildes integritet mot alltför extensiv behandling av personuppgifter. Rambeslutet är ett stort steg framåt i detta avseende. Sverige bör därför medverka till att rambeslutet antas. Mot den bakgrunden är det angeläget att Sverige så snart som möjligt kan lyfta sin parlamentariska reservation, så att rambeslutet kan träda i kraft.

Mot denna bakgrund föreslår regeringen att riksdagen godkänner utkastet till rambeslut.



*Rikspolisstyrelsen* har i sitt remissvar framfört att ett genomförande av rambeslutet kan komma att medföra behov av ökade resurser. I det sammanhanget har styrelsen påpekat att rambeslutet bara är en av flera olika rättsakter som måste genomföras ungefär samtidigt och att även om promemorians bedömning att genomförandet kan ske inom polisväsendets nuvarande budgetram är rimlig om den ses isolerad så framstår det vid en helhetsbedömning som klart att de nödvändiga resurserna för ett framgångsrikt genomförande av rambeslutet, och övriga åtaganden inom ramen för samarbetet inom Europeiska unionen, inte ryms inom polisväsendets nuvarande budgetram. Även *Kustbevakningen*, *Säkerhetspolisen* och *Säkerhets- och Integritetsskyddsnämnden* har påtalat att ett genomförande av rambeslutet kan medföra ekonomiska konsekvenser för respektive myndighet.

Det har i avsnitt 6 konstaterats att det på sistone har förhandlats och alltjämt pågår ett intensivt arbete inom Europeiska unionen med att förhandla rättsakter som på olika sätt rör samarbetet mellan brottsbekämpande myndigheter och det straffrättsliga samarbetet. Flera av dessa rättsakter rör helt eller delvis informationsutbyte och därmed personuppgiftsbehandling. Som konstateras i promemorian har det vid översyner av personuppgiftsbehandlingen inom polisen, tullväsendet, Kustbevakningen, domstolarna och kriminalvården genomgående gjorts bedömningen att sådana reformer inte medför några mer påtagliga kostnadsökningar. Flera av de reformer som har genomförts eller kommer att genomföras syftar till att effektivisera brottsbekämpningen och kan därmed på sikt väntas medföra ett effektivare resursutnyttjande.

Ett beslut om godkännande av rambeslutet föranleder i sig inte några kostnadskonsekvenser. På ett par års sikt, vid genomförandet av rambeslutet, som kommer att ske delvis genom lagstiftning och redovisas i en kommande proposition till riksdagen, kan däremot kostnadskonsekvenser uppstå. Det är dock svårt att med säkerhet bedöma om, och i så fall vilka kostnader det nämnda pågående arbetet inom Europeiska unionen kommer att medföra för berörda myndigheter. I dagsläget görs bedömningen att dessa kostnader ryms inom befintliga ramar på statsbudgeten.

Utkast till rambeslut om skydd av personuppgifter  
som behandlas inom ramen för polissamarbete och  
straffrättsligt samarbete

Prop. 2008/09:16  
Bilaga 1



**EUROPEISKA  
UNIONENS RÅD**

**Bryssel den 24 juni 2008  
(OR. en)**

**9260/08**

**Interinstitutionellt ärende:  
2005/0202 (CNS)**

**CRIMORG 71  
DROIPEN 43  
ENFOPOL 89  
DATAPROTECT 23  
ENFOCUSTOM 55  
COMIX 370**

**RÄTTSAKTER OCH ANDRA INSTRUMENT**

---

Ärende: RÅDETS RAMBESLUT om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete

---

# RÅDETS RAMBESLUT

av den

**om skydd av personuppgifter som behandlas inom ramen för polissamarbete  
och straffrättsligt samarbete**

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionen, särskilt artiklarna 30, 31 och 34.2 b,

med beaktande av kommissionens förslag,

med beaktande av Europaparlamentets yttrande<sup>1</sup>, och

---

<sup>1</sup> EUT C 125 E, 22.5.2008, s. 154.

av följande skäl:

- (1) Europeiska unionen har som mål att bevara och utveckla unionen som ett område med frihet, säkerhet och rättvisa inom vilket en hög säkerhetsnivå ska uppnås genom gemensamma insatser från medlemsstaternas sida när det gäller polissamarbete och straffrättsligt samarbete.
- (2) Gemensamma insatser på polissamarbetets område i enlighet med artikel 30.1 b i fördraget om Europeiska unionen och gemensamma insatser rörande straffrättsligt samarbete i enlighet med artikel 31.1 a i samma fördrag innebär att det blir nödvändigt att behandla relevant information, vilket bör omfattas av lämpliga bestämmelser om skydd av personuppgifter.
- (3) Lagstiftning som omfattas av avdelning VI i fördraget om Europeiska unionen syftar till att främja polissamarbete och rättsligt samarbete med avseende på såväl samarbetets effektivitet som dess lagenlighet och överensstämmelse med grundläggande rättigheter, särskilt rätten till ett privatliv och rätten till skydd av personuppgifter. Gemensamma normer för behandling och skydd av personuppgifter i syfte att förebygga och bekämpa brott kan bidra till att uppnå dessa båda mål.

- (4) I Haagprogrammet för ett stärkt område med frihet, säkerhet och rättvisa i Europeiska unionen, som antogs av Europeiska rådet den 4 november 2004, understryks behovet av en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning, under noggrant iakttagande av centrala villkor på området skydd av personuppgifter. Kommissionen uppmanades att senast i slutet av 2005 lägga fram förslag om detta. Detta återspeglas i rådets och kommissionens handlingsplan för genomförande av Haagprogrammet för ett stärkt område med frihet, säkerhet och rättvisa<sup>1</sup>.
- (5) Utbytet av personuppgifter inom ramen för polissamarbetet och det straffrättsliga samarbetet, särskilt enligt den princip om tillgänglighet som tas upp i Haagprogrammet, bör bygga på klara regler som stärker det ömsesidiga förtroendet mellan behöriga myndigheter och garanterar att den relevanta informationen skyddas på ett sätt som utesluter all diskriminering med avseende på sådant samarbete mellan medlemsstaterna samtidigt som enskildas grundläggande rättigheter respekteras fullt ut. Befintliga instrument på europeisk nivå är inte tillräckliga; 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<sup>2</sup> är inte tillämpligt i fråga om behandling av personuppgifter i samband med verksamheter som faller utanför gemenskapsrättens tillämpningsområde, till exempel sådana som anges i avdelning VI i fördraget om Europeiska unionen, och under inga omständigheter på uppgiftsbehandling som rör allmän säkerhet, försvar, nationell säkerhet eller statlig verksamhet på det straffrättsliga området.

---

<sup>1</sup> EUT C 198, 12.8.2005, s. 1.

<sup>2</sup> EGT L 281, 23.11.1995, s. 31. Direktivet ändrat genom förordning (EG) nr 1882/2003 (EUT L 284, 31.10.2003, s.1).

- (6) Detta rambeslut är endast tillämpligt på uppgifter som de behöriga myndigheterna samlar in eller behandlar för att kunna förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. I detta rambeslut bör det överlåtas till medlemsstaterna att på nationell nivå mer exakt besluta vilka andra ändamål som ska anses oförenliga med det ändamål för vilket personuppgifterna ursprungligen insamlades. I allmänhet bör vidarebehandling för historiska, statistiska eller vetenskapliga ändamål inte anses vara oförenlig med det ursprungliga ändamålet för behandlingen.
- (7) Tillämpningsområdet för detta rambeslut begränsas till behandlingen av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna. Inga slutsatser bör dras av denna begränsning beträffande unionens behörighet att anta rättsakter om insamling och behandling av personuppgifter på nationell nivå eller det lämpliga i att unionen gör detta i framtiden.
- (8) I syfte att underlätta informationsutbytet inom unionen vill medlemsstaterna säkerställa att den standard i fråga om dataskydd som fastställs inom nationell databehandling ska motsvara den som föreskrivs i rambeslutet. När det gäller nationell databehandling hindrar detta rambeslut inte medlemsstaterna från att föreskriva garantier för skydd av personuppgifter högre än dem som fastställs i detta rambeslut.

- (9) Detta rambeslut bör inte tillämpas på personuppgifter som en medlemsstat erhållit inom tillämpningsområdet för detta rambeslut och som härrör från denna medlemsstat.
- (10) Tillnärmningen av medlemsstaternas lagstiftningar bör inte leda till några försämringar i det dataskydd de ger utan i stället syfta till att garantera en hög skyddsnivå inom unionen.
- (11) Det är nödvändigt att precisera målen med skyddet av personuppgifter inom ramen för polisens och rättsväsendets verksamheter och att införa bestämmelser om vilken behandling av personuppgifter som är tillåten i syfte att säkerställa att uppgifter som kan komma att utbytas har behandlats på lagligt sätt och i enlighet med grundläggande principer i fråga om uppgifters kvalitet. Samtidigt är det viktigt att inte polisens, tullens, domstolarnas eller andra behöriga myndigheters legitima verksamheter äventyras.
- (12) Principen om uppgifters korrekthet ska tillämpas med beaktande av den aktuella behandlingens art och syfte. Så grundar sig exempelvis uppgifterna inom framför allt rättsliga förfaranden på enskilda personers subjektiva uppfattning och kan i vissa fall omöjligen kontrolleras. Följaktligen kan inte korrekthetskravet röra korrektheten i ett uttalande utan blott och bart det faktum att ett visst uttalande har gjorts.



- (13) Arkivering i ett separat dataset bör tillåtas endast om uppgifterna inte längre krävs eller används för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder. Arkivering i ett separat dataset bör även tillåtas om de arkiverade uppgifterna lagras i en databas tillsammans med andra uppgifter på ett sådant sätt att de inte längre kan användas för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder. Lämplig längd av arkiveringsperioden bör vara avhängig av syftet med arkiveringen och de registrerade personernas legitima intressen. I fråga om arkivering för historiska ändamål kan man fastställa en mycket lång period.
- (14) Uppgifter får också raderas genom att datamediet förstörs.
- (15) När det gäller icke korrekta, ofullständiga eller inte längre aktuella uppgifter som överförs eller gjorts tillgängliga för en annan medlemsstat och vidarebehandlas av domstolsliknande myndigheter, med vilket avses myndigheter med behörighet att fatta rättsligen bindande beslut, bör rättelse, strykning eller blockerande utföras enligt nationell lagstiftning.

- (16) För att kunna garantera en hög skyddsnivå för personuppgifter om enskilda personer krävs det gemensamma bestämmelser för att fastställa om de uppgifter som behandlas av behöriga myndigheter i medlemsstaterna uppfyller laglighets- och kvalitetskraven.
- (17) Därför bör man på europeisk nivå fastställa de villkor som ska vara uppfyllda för att medlemsstaternas behöriga myndigheter ska ha rätt att till myndigheter och privata parter i medlemsstater överföra och göra tillgängliga personuppgifter som erhållits från andra medlemsstater. I många fall är överföring av personuppgifter från domstolsväsendet, polisen eller tullen till privata parter nödvändig för att lagföra brott eller för att avvärja en omedelbar och allvarlig fara för allmän säkerhet eller förhindra att enskilda personers rättigheter lider allvarlig skada, till exempel genom att utfärda varningar avseende förfalskningar av värdepapper till banker och kreditinstitut eller, i fråga om fordonsstölder, genom att överföra personuppgifter till försäkringsbolag för att förhindra olaglig handel med stulna motorfordon eller för att förbättra villkoren för återförande av stulna motorfordon från utlandet. Detta innebär inte överföring av arbetsuppgifter från polis och domstolar till privata parter.
- (18) Reglerna i detta rambeslut avseende överföring av personuppgifter från domstolsväsendet, polisen eller tullen till privata parter tillämpas inte på utlämnandet av uppgifter till privata parter (såsom försvarsadvokater och brottsoffer) i samband med brottmål.

- (19) Den vidare behandlingen av personuppgifter som erhållits från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat, särskilt det att vidarebefordra sådana uppgifter eller göra dem tillgängliga på nytt, bör omfattas av gemensamma bestämmelser på europeisk nivå.
- (20) När personuppgifter får vidarebehandlas efter det att den medlemsstat från vilken uppgifterna erhållits har givit sitt samtycke bör varje medlemsstat ha möjlighet att fastställa de närmare villkoren för att ge sådant samtycke, inbegripet exempelvis allmänt samtycke för kategorier av information och kategorier av ytterligare behandling.
- (21) När personuppgifter får vidarebehandlas för administrativa förfaranden inbegriper dessa förfaranden också åtgärder av reglerings- och tillsynsorgan.
- (22) Polisens, tullens, domstolarnas eller andra behöriga myndigheters legitima verksamheter kan kräva att uppgifter sänds till myndigheter i tredjestater eller internationella organ som har skyldigheter i fråga om att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.
- (23) Om uppgifter överförs från en medlemsstat till tredjestater eller internationella organ ska uppgifterna i princip omfattas av ett adekvat skydd.

- (24) Om personuppgifter överförs från en medlemsstat till tredjestater eller internationella organ bör en sådan överföring i princip ske först efter det att den medlemsstat som har lämnat uppgifterna har gett sitt samtycke till överföringen. Varje medlemsstat bör få bestämma de närmare villkoren för att ge sådant samtycke, till exempel genom ett generellt samtycke för kategorier av uppgifter eller för vissa angivna tredjestater.
- (25) För ett effektivt samarbete i fråga om brottsbekämpning krävs att om ett hot mot en medlemsstats eller en tredjestats allmänna säkerhet är så överhängande att det är omöjligt att i tid inhämta ett förhandsmedgivande bör den behöriga myndigheten få överföra de relevanta personuppgifterna till den berörda tredjestaten utan sådant förhandsmedgivande. Detsamma kan gälla om andra väsentliga, lika betydelsefulla, intressen i en medlemsstat står på spel, exempelvis om en medlemsstats kritiska infrastruktur kan bli föremål för ett överhängande hot eller om en medlemsstats finansiella system kan drabbas av allvarliga störningar.
- (26) För att tillförsäkra den registrerade personen ett effektivt rättsskydd kan det bli nödvändigt att informera denne om behandlingen av dennes personuppgifter, särskilt vid synnerligen allvarlig kränkning av dennes rättigheter som ett resultat av hemlig insamling av uppgifter.

- (27) Medlemsstaterna bör se till att den registrerade personen informeras om att personuppgifter kan eller håller på att samlas in, behandlas eller överförs till en annan medlemsstat för att förebygga, utreda, avslöja och lagföra brott eller verkställa straffrättsliga påföljder. De närmare villkoren för den registrerade personens rätt att bli informerad och undantag från denna rätt bör fastställas i den nationella lagstiftningen. Detta kan genomföras på ett generellt sätt, t.ex. genom lagstiftning eller offentliggörande av en förteckning över olika typer av uppgiftsbehandling.
- (28) För att kunna garantera skyddet av personuppgifter utan att äventyra ändamålet med brottsutredningar måste man fastställa den registrerades rättigheter.
- (29) Några medlemsstater har gett den berörda personen rätt till tillgång till uppgifter i brottmål genom ett system där det nationella tillsynsorganet, i den berörda personens ställe, utan någon restriktion har tillgång till alla personuppgifter som rör den berörda personen och även får rätta, stryka eller uppdatera icke korrekta uppgifter. I sådana fall med indirekt tillgång får det i den nationella lagstiftningen i dessa medlemsstater föreskrivas att det nationella tillsynsorganet endast kommer att informera den berörda personen om att alla nödvändiga kontroller har utförts. Dessa medlemsstater tillhandahåller emellertid i särskilda fall även möjligheter till direkt tillgång för den berörda personen, såsom tillgång till rättsliga register för att erhålla kopior av egna kriminalregisteruppgifter eller handlingar avseende egna förhör hos polismyndigheterna.

- (30) Det bör införas gemensamma bestämmelser om konfidentiell och säker uppgiftsbehandling, om ansvar och påföljder när uppgifterna används på otillåtet sätt av de behöriga myndigheterna samt om möjligheter för den registrerade till rättslig prövning. Det ankommer dock på varje medlemsstat att själv fastställa utformningen av bestämmelserna om skadeståndsgrundande överträdelser och om vilka påföljder som ska tillämpas vid överträdelse av de nationella dataskyddsbestämmelserna.
- (31) Detta rambeslut gör att principen om allmänhetens tillgång till offentliga handlingar kan tillgodoses vid tillämpningen av principerna i detta.
- (32) När så behövs för att skydda personuppgifter med avseende på behandling som genom sin omfattning eller typ innebär särskilda risker för grundläggande rättigheter och friheter, till exempel behandling med ny teknik, nya mekanismer eller förfaranden, bör man säkerställa att den behöriga nationella tillsynsmyndigheten rådfrågas före upprättandet av behandlingssystem för dessa uppgifter.
- (33) Inrättandet i medlemsstaterna av tillsynsmyndigheter, som fullständigt oberoende genomför sina åligganden, är en mycket viktig del av skyddet av personuppgifter som behandlas inom ramen för polissamarbetet och det straffrättsliga samarbetet mellan medlemsstaterna.

- (34) De tillsynsmyndigheter som redan inrättats i medlemsstaterna i enlighet med direktiv 95/46/EG bör också kunna axla ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta rambeslut.
- (35) Dessa tillsynsmyndigheter bör ha nödvändiga resurser för att kunna genomföra sina uppgifter, inklusive befogenhet att – särskilt när det gäller klagomål från enskilda personer – undersöka och ingripa eller befogenhet att inleda rättsliga förfaranden. Dessa tillsynsmyndigheter bör även bidra till att sörja för insyn i behandlingen av uppgifter i sina respektive medlemsstater. Emellertid bör deras befogenheter inte inkräkta på särskilda regler som fastställts för brottmål eller domstolsväsendets oberoende.
- (36) I artikel 47 i fördraget om Europeiska unionen föreskrivs det att ingenting i det fördraget ska inverka på fördragen om upprättandet av Europeiska gemenskaperna eller på senare fördrag och rättsakter om ändring eller komplettering av dessa. Följaktligen påverkar detta rambeslut inte skyddet av personuppgifter enligt gemenskapsrätten, särskilt inte det skydd som föreskrivs i direktiv 95/46/EG, 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<sup>1</sup> och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)<sup>2</sup>.

---

<sup>1</sup> EGT L 8, 12.1.2001, s. 1.

<sup>2</sup> EGT L 201, 31.7.2002, s. 37. Direktivet ändrat genom direktiv 2004/24/EG (EUT L 105, 13.4.2006, s. 54).

- (37) Detta rambeslut påverkar inte bestämmelserna om sådan olaglig tillgång till uppgifter som avses i rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem<sup>1</sup>.
- (38) Detta rambeslut påverkar inte medlemsstaternas eller unionens gällande skyldigheter och åtaganden enligt bilaterala och/eller multilaterala avtal med tredjestater. Framtida avtal bör följa bestämmelserna om utbyte med tredjestater.
- (39) Flera rättsakter som antagits på grundval av avdelning VI i fördraget om Europeiska unionen innehåller särskilda bestämmelser om skydd av personuppgifter som överförs eller på något annat sätt behandlas i enlighet med de rättsakterna. I några fall utgör dessa bestämmelser en komplett och enhetlig uppsättning regler som omfattar alla relevanta aspekter av dataskydd (principer om uppgifternas kvalitet, regler om datasäkerhet, reglering av de registrerades rättigheter och skydd, organisation av tillsyn och ansvar) och i dessa regleras frågor mer detaljerat än i detta rambeslut. De tillämpliga dataskyddsbestämmelserna i dessa rättsakter, särskilt de som reglerar funktionssättet för Europol, Eurojust, Schengens informationssystem (SIS) och tullinformationssystemet (TIS) samt de rättsakter genom vilka medlemsstaternas myndigheter ges direkt tillgång till vissa datasystem i andra medlemsstater, bör inte påverkas av detta rambeslut. Detsamma gäller de dataskyddsbestämmelser som reglerar automatisk överföring av DNA-profiler, fingeravtrycksuppgifter och uppgifter ur nationella fordonsregister i enlighet med rådets beslut 2008/.../RIF av den...<sup>\*</sup> om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet<sup>2</sup>.

---

<sup>1</sup> EUT L 69, 16.3.2005, s. 67.

<sup>\*</sup> EUT: Vänligen för in nummer, datum och uppgifter avseende offentliggörandet av beslutet i dok. 11896/07.

<sup>2</sup> EUT L



- (40) I andra fall är räckvidden för dataskyddsbestämmelser i rättsakter som antagits i enlighet med avdelning VI i fördraget om Europeiska unionen mer begränsade. Ofta fastställs det i dessa rättsakter särskilda villkor för den medlemsstat som från en annan medlemsstat tar emot information innehållande personuppgifter i fråga om de ändamål för vilka mottagaren kan använda uppgifterna, medan det i fråga om övriga dataskyddsaspekter hänvisas till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981 eller till nationell lagstiftning. I den mån det i bestämmelserna i dessa rättsakter fastställs villkor för mottagande medlemsstater för användning eller vidare överföring av personuppgifter vilka är strängare än villkoren i motsvarande bestämmelser i detta rambeslut, ska dessa förstnämnda inte heller påverkas. I alla övriga avseenden ska de regler som fastställs i detta rambeslut gälla.
- (41) Detta rambeslut påverkar inte Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter eller tilläggsprotokollet av den 8 november 2001 till denna konvention eller Europarådets konventioner om straffrättsligt samarbete.

- (42) Eftersom målet för detta rambeslut, nämligen att fastställa gemensamma bestämmelser om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och det därför, på grund av åtgärdens omfattning och verkningar, bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om upprättandet av Europeiska gemenskapen, till vilken det hänvisas i artikel 2 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i artikel 5 i fördraget om upprättandet av Europeiska gemenskapen går detta rambeslut inte utöver vad som är nödvändigt för att uppnå detta mål.
- (43) Förenade kungariket deltar i detta rambeslut i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, fogat till fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, och i enlighet med artikel 8.2 i rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket<sup>1</sup>.

---

<sup>1</sup> EGT L 131, 1.6.2000, s. 43.

- (44) Irland deltar i detta rambeslut i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, fogat till fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, och i enlighet med artikel 6.2 i rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket<sup>1</sup>.
- (45) När det gäller Island och Norge utgör detta rambeslut, 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, en utveckling av bestämmelser i Schengenregelverket<sup>2</sup> vilka rör det område som avses i artikel 1.H och 1.I i rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtalet<sup>3</sup>.

---

<sup>1</sup> EGT L 64, 7.3.2002, s. 20.

<sup>2</sup> EGT L 176, 10.7.1999, s. 36.

<sup>3</sup> EGT L 176, 10.7.1999, s. 31.

- (46) När det gäller Schweiz utgör detta rambeslut, 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 de bestämmelser i Schengenregelverket<sup>1</sup> vilka rör det område som avses i artikel 1.H och 1.I i rådets beslut 1999/437/EG av den 17 maj 1999 jämförd med artikel 3 i rådets beslut 2008/149/EG<sup>2</sup> av den 28 januari 2008 om ingående av det avtalet på Europeiska unionens vägnar.
- (47) När det gäller Liechtenstein utgör detta rambeslut, 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, en utveckling av bestämmelser i Schengenregelverket vilka omfattas av det område som avses i artikel 1 punkt H och I i beslut 1999/437/EG, jämförd med artikel 3 i rådets beslut 2008/262/EG av den 28 februari 2008 om undertecknande av det protokollet på Europeiska unionens vägnar<sup>3</sup>.

---

<sup>1</sup> EUT L 53, 27.2.2008, s. 52.

<sup>2</sup> EUT L 53, 27.2.2008, s. 50.

<sup>3</sup> EUT L 83, 26.3.2008, s. 5.

- (48) Detta rambeslut står i överensstämmelse med de grundläggande rättigheter och principer som erkänns framför allt i Europeiska unionens stadga om de grundläggande rättigheterna<sup>1</sup>. Detta rambeslut syftar till att garantera full respekt för rätten till det skydd för privatlivet och det skydd av personuppgifter som kommer till uttryck i artiklarna 7 och 8 i stadgan.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

*Artikel 1*

*Syfte och tillämpningsområde*

1. Syftet med detta rambeslut är att säkerställa en hög skyddsnivå för fysiska personers grundläggande fri- och rättigheter, särskilt när det gäller deras rätt till privatliv, med avseende på behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete enligt avdelning VI i fördraget om Europeiska unionen och samtidigt garantera en allmän säkerhet på hög nivå.
2. I enlighet med detta rambeslut ska medlemsstaterna skydda fysiska personers grundläggande fri- och rättigheter, och särskilt deras rätt till privatliv, när personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder
  - a) överförs, har överförts, görs eller har gjorts tillgängliga mellan medlemsstaterna,
  - b) överförs, har överförts, görs eller har gjorts tillgängliga av medlemsstaterna till myndigheter eller informationssystem som inrättats i enlighet med avdelning VI i fördraget om Europeiska unionen, eller

---

<sup>1</sup> EUT C 303, 14.12.2007, s. 1.

- c) överförs, har överförts, görs eller har gjorts tillgängliga för medlemsstaternas behöriga myndigheter av myndigheter eller informationssystem som inrättats i enlighet med fördraget om Europeiska unionen eller fördraget om upprättandet av Europeiska gemenskapen.
3. Detta rambeslut gäller för sådan behandling av personuppgifter som helt eller delvis utförs automatiskt samt för annan behandling än automatisk av sådana personuppgifter som ingår i eller kommer att ingå i ett register.
4. Detta rambeslut påverkar inte viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet.
5. Detta rambeslut hindrar inte medlemsstaterna från att föreskriva strängare säkerhetsåtgärder för skydd av personuppgifter som samlas in eller behandlas på nationell nivå än de som fastställs i detta rambeslut.

*Artikel 2*  
*Definitioner*

I detta rambeslut gäller följande definitioner:

- a) personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifieringsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.
- b) behandling av personuppgifter och behandling: varje åtgärd eller serie av åtgärder som vidtas med personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, hämtning, läsning, användning, utlämnande genom överföring, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, radering eller förstöring.
- c) blockering: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.
- d) register med personuppgifter och register: varje 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.

- e) registerförare: varje organ som behandlar personuppgifter för den registeransvariges räkning.
- f) mottagare: varje organ till vilken uppgifterna utlämnas.
- g) den registrerades samtycke: varje slag av frivillig, uttrycklig och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom.
- h) behöriga myndigheter: byråer eller organ som inrättats genom rättsakter antagna av rådet enligt avdelning VI i fördraget om Europeiska unionen, samt polismyndigheter, tullmyndigheter, domstolar eller andra behöriga myndigheter i medlemsstaterna som genom nationell lagstiftning är bemyndigade att behandla personuppgifter inom tillämpningsområdet för detta rambeslut.
- i) registeransvarig: en fysisk eller en juridisk person, en myndighet, en byrå eller varje annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
- j) markering: markering av lagrade personuppgifter utan syfte att begränsa behandlingen av dessa i framtiden.
- k) avidentifiering: att ändra personuppgifter på ett sådant sätt att detaljerna beträffande personliga eller sakliga förhållanden inte längre eller endast med oproportionerligt stor insats i fråga om tid, kostnader och arbete kan tillskrivas en identifierad eller identifierbar fysisk person.



### *Artikel 3*

#### *Principerna om lagenlighet, proportionalitet och ändamål*

1. De behöriga myndigheterna får inom ramen för sina uppgifter samla in personuppgifter endast för särskilda, uttryckligt angivna och berättigade ändamål och uppgifterna får endast behandlas för det ändamål som låg till grund för insamlingen av dem. Behandlingen av uppgifterna ska vara lagenlig och adekvat, relevant och inte orimlig i förhållande till det ändamål för vilket de samlades in.
  
2. Vidare behandling för ett annat ändamål är tillåten om
  - a) denna vidare behandling inte är oförenlig med de ändamål för vilket uppgifterna samlades in,
  - b) de behöriga myndigheterna i enlighet med tillämpliga rättsliga bestämmelser är bemyndigade att behandla sådana uppgifter för ett sådant annat ändamål, och
  - c) denna behandling är nödvändig och står i proportion till det andra ändamålet.

Dessutom får de överförda personuppgifterna behandlas vidare av den behöriga myndigheten för historiska, statistiska eller vetenskapliga ändamål, under förutsättning att medlemsstaterna föreskriver lämpliga säkerhetsåtgärder, som avidentifiering av uppgifterna.

#### *Artikel 4*

##### *Rättelse, radering och blockering*

1. Personuppgifter ska rättas om de är felaktiga samt, om så är möjligt och nödvändigt, kompletteras eller aktualiseras.
2. Personuppgifter ska raderas eller avidentifieras när dessa inte längre behövs för de ändamål för vilka de lagligen insamlades eller lagligen vidare bearbetas. Arkivering av de uppgifter som införts i ett separat dataset under en lämplig period i överensstämmelse med national lagstiftning ska inte påverkas av denna bestämmelse.
3. Personuppgifter ska inte raderas utan blockeras, om det finns skälig grund att anta att en radering skulle kunna påverka den registrerades legitima intressen. Blockerade uppgifter får endast behandlas för det ändamål som hindrade att de raderades.
4. Om personuppgifterna ingår i ett domstolsbeslut eller akten i samband med utfärdandet av ett rättsligt beslut ska rättelse, radering eller blockering utföras i enlighet med nationella bestämmelser om rättsliga förfaranden.

## *Artikel 5*

### *Fastställande av tidsfrister för radering och kontroll*

För radering av personuppgifter eller en regelbunden kontroll av nödvändigheten av lagringen av uppgifterna ska lämpliga tidsfrister fastställas. Genom föreskrifter om förfarandena ska det garanteras att tidsfristerna efterlevs.

## *Artikel 6*

### *Behandling av särskilda kategorier av uppgifter*

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv får endast förekomma när detta är absolut nödvändigt och om det i den nationella lagstiftningen tillhandahålls tillräckliga skyddsåtgärder.

## *Artikel 7*

### *Datoriserade beslut*

Ett beslut som har negativa rättsliga följder för den registrerade eller som väsentligt berör honom eller henne och som enbart grundas på en automatisk behandling av uppgifter avsedd att bedöma vissa personliga egenskaper hos den registrerade ska endast vara tillåtet om detta föreskrivs i en lag där det även föreskrivs bestämmelser till skydd för den registrerades legitima intressen.

## *Artikel 8*

### *Kontroll av kvaliteten på de uppgifter som överförs eller görs tillgängliga*

1. 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. De behöriga myndigheterna ska därför i görligaste mån kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga. Vid all överföring av uppgifter ska, så långt detta är möjligt, sådan tillgänglig information läggas till som gör att den mottagande medlemsstaten kan bedöma graden av korrekthet, fullständighet, aktualitet och tillförlitlighet. Om personuppgifter överförs utan att någon begäran har gjorts ska den mottagande myndigheten utan dröjsmål bedöma huruvida dessa uppgifter är nödvändiga för det ändamål som låg till grund för överföringen.
2. Om det visar sig att felaktiga uppgifter har överförts eller att uppgifter olovligen har överförts ska mottagaren omedelbart underrättas om detta. Uppgifterna måste ofördröjligen rättas, raderas eller blockeras i enlighet med artikel 4.

## *Artikel 9*

### *Tidsfrister*

1. När den överförande myndigheten överför uppgifter eller gör dessa tillgängliga, får den enligt nationell lagstiftning och i enlighet med artiklarna 4 och 5 meddela de tidsfrister för lagring av uppgifterna efter vilka mottagaren ska radera eller blockera uppgifterna eller kontrollera om dessa fortfarande behövs. Denna skyldighet ska inte tillämpas, om dessa uppgifter vid utgången av tidsfristerna krävs för en pågående utredning, lagföring av brott eller verkställighet av straffrättsliga påföljder.
2. Om den överförande myndigheten inte har angivit en tidsfrist enligt punkt 1 ska de tidsfrister som avses i artiklarna 4 och 5 för lagring av uppgifterna enligt de mottagande medlemsstaternas nationella lagstiftning tillämpas.

## *Artikel 10*

### *Registrering och dokumentation*

1. Varje överföring av personuppgifter ska registreras eller dokumenteras för att man ska kunna kontrollera om behandlingen av uppgifterna är lagenlig, utföra egenkontroll samt garantera integritet och säkerhet för uppgifterna.

2. Registrering och dokumentation enligt punkt 1 ska på begäran översändas till den för skydd av uppgifter behöriga tillsynsmyndigheten. Den behöriga tillsynsmyndigheten får använda dessa uppgifter endast för att kontrollera skyddet av personuppgifter, för att se till att behandlingen fungerar tillfredsställande och för att sörja för uppgifternas integritet och säker uppgiftsbehandling.

*Artikel 11*

*Behandling av personuppgifter som överförs från  
eller gjorts tillgängliga av en annan medlemsstat*

Personuppgifter som överförs från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat får, i enlighet med kraven i artikel 3.2, endast vidarebehandlas för följande ändamål, utöver dem för vilka de överfördes eller gjordes tillgängliga:

- a) För att förebygga, utreda, avslöja eller lagföra andra brott eller verkställa andra straffrättsliga påföljder än de för vilka uppgifterna överfördes eller gjordes tillgängliga.
- b) För andra rättsliga eller administrativa förfaranden med direkt anknytning till förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder.

- c) För att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten.
- d) För varje annat syfte endast med förhandsmedgivande från den överförande medlemsstaten eller med den registrerades samtycke givet i överensstämmelse med nationell lagstiftning.

Dessutom får de överförda personuppgifterna behandlas vidare av de behöriga myndigheterna för historiska, statistiska eller vetenskapliga ändamål under förutsättning att medlemsstaterna föreskriver lämpliga säkerhetsåtgärder som exempelvis avidentifiering av uppgifterna.

### *Artikel 12*

#### *Iakttagande av nationella restriktioner för behandling av uppgifter*

1. Om det, enligt den överförande medlemsstatens nationella lagstiftning, under särskilda omständigheter gäller särskilda begränsningar i fråga om utbyte av uppgifter mellan behöriga myndigheter inom den medlemsstaten, ska den överförande myndigheten informera mottagaren om dessa begränsningar. Mottagaren ska se till att dessa begränsningar för behandlingen följs.
2. Vid tillämpning av punkt 1 ska medlemsstaterna inte tillämpa några andra begränsningar när det gäller överföringen av uppgifter till andra medlemsstater eller till byråer eller organ som inrättats i enlighet med avdelning VI i fördraget om Europeiska unionen än de som gäller motsvarande nationella överföringar av uppgifter.

*Artikel 13*

*Överföring till behöriga myndigheter i tredjestater  
eller till internationella organ*

1. Medlemsstaterna ska föreskriva att personuppgifter som överförts eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat får överföras till tredjestater eller internationella organ endast om
  - a) detta är nödvändigt för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
  - b) den mottagande myndigheten i tredjestaten eller det mottagande internationella organet har ansvar för förebyggande, utredning, avslöjande eller lagföring av brott eller för verkställigheten av straffrättsliga påföljder,
  - c) den medlemsstat från vilken uppgifterna erhöles har gett sitt samtycke till överföringen i enlighet med sin nationella lagstiftning, och om
  - d) berörd tredjestat eller internationellt organ sörjer för en adekvat skyddsnivå för den avsedda databehandlingen.



2. Överföring utan förhandsmedgivande enligt punkt 1 c ska tillåtas endast om överföringen av uppgifter är absolut nödvändig för att kunna avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller en tredjestat eller för en medlemsstat väsentliga intressen och ett förhandsmedgivande inte kan erhållas i tid. Den myndighet som ansvarar för att bevilja medgivandet ska informeras utan dröjsmål.
3. Med avvikelse från punkt 1 d får personuppgifter överföras om
  - a) den nationella lagstiftningen i den medlemsstat som överför uppgifterna föreskriver detta på grund av
    - i) den registrerades legitima specifika intressen, eller
    - ii) legitima faktiska intressen, främst viktiga allmänna intressen, eller
  - b) tredjestaten eller mottagande internationella organ sörjer för skyddsåtgärder som av den berörda medlemsstaten bedöms som adekvata i enlighet med dennas nationella lagstiftning.
4. Bedömningen av om den skyddsnivå som avses i punkt 1 d är adekvat ska ske på grundval av alla de förhållanden som har samband med en eller flera överföringar av personuppgifter. Särskild hänsyn ska tas till uppgifternas art, den föreslagna behandlingens eller behandlingarnas ändamål och varaktighet, ursprungsstaten och den stat eller internationella organ som utgör slutdestination för uppgifterna, den lagstiftning, både allmän och sektoriell, som gäller i den berörda tredjestaten eller för det berörda internationella organet samt de yrkesregler och säkerhetsbestämmelser som ska tillämpas.

## Artikel 14

### Överföring till privata parter i medlemsstaterna

1. Medlemsstaterna ska föreskriva att personuppgifter som överförts från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat endast får överföras till privata parter om
  - a) den behöriga myndigheten i den medlemsstat från vilken uppgifterna erhållits har samtyckt till överföring i enlighet med sin nationella lagstiftning,
  - b) inga legitima specifika intressen för den registrerade personen hindrar överföringen, och om
  - c) överföringen i särskilda fall är absolut nödvändig för att den behöriga myndighet som överför uppgifterna till en privat part ska kunna
    - i) utföra en uppgift den lagenligen tilldelats,
    - ii) förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder,
    - iii) avvärja en omedelbar och allvarlig fara för den allmänna säkerheten, eller
    - iv) förhindra att enskilda personers rättigheter lider allvarlig skada.
2. Den behöriga myndighet som överför uppgifterna till en privat part ska underrätta denna om för vilka ändamål uppgifterna uteslutande får användas.

*Artikel 15*

*Information på begäran av den behöriga myndigheten*

Mottagaren ska på begäran informera den behöriga myndighet som har överfört uppgifter eller gjort dem tillgängliga om hur dessa behandlas.

*Artikel 16*

*Information till den registrerade*

1. Medlemsstaterna ska se till att den registrerade informeras om insamling eller behandling av personuppgifter av deras behöriga myndigheter i enlighet med nationell lagstiftning.
2. Om personuppgifter har överförts eller gjorts tillgängliga mellan medlemsstaterna, får varje medlemsstat i enlighet med bestämmelserna i sin nationella lagstiftning enligt punkt 1, begära att den andra medlemsstaten inte informerar den registrerade. I sådana fall ska den senare medlemsstaten inte informera den registrerade utan förhandsmedgivande från den andra medlemsstaten.

*Artikel 17*  
*Rätt till tillgång*

1. Varje registrerad ska ha rätt att på begäran, med rimliga intervall, utan hinder och utan större tidsutdräkt eller kostnader erhålla
  - a) åtminstone en bekräftelse från den registeransvarige eller från den behöriga nationella tillsynsmyndigheten på huruvida uppgifter som rör honom eller henne har överförts eller gjorts tillgängliga samt information om till vilka mottagare eller mottagarkategorier uppgifterna har lämnats ut och information om vilka uppgifter som behandlas, eller
  - b) åtminstone en bekräftelse från den behöriga nationella tillsynsmyndigheten på att alla nödvändiga kontroller har utförts.
  
2. Medlemsstaterna får anta lagstiftning som begränsar tillgången till information enligt punkt 1 a, om denna begränsning med vederbörligt beaktande av vederbörandes legitima intressen är en nödvändig och rimlig åtgärd för att
  - a) hindra obstruktion mot officiella eller rättsliga utredningar, förundersökningar eller förfaranden,
  - b) inte inverka menligt på förebyggande, upptäckt, utredning och lagföring av brott eller verkställighet av straffrättsliga påföljder,
  - c) skydda allmän säkerhet,
  - d) skydda nationell säkerhet,
  - e) skydda den registrerade eller andra personers fri- och rättigheter.

3. Varje vägran till tillgång eller begränsning av denna ska skriftligen meddelas den registrerade. De sakliga och rättsliga skäl som beslutet grundar sig på ska därvid också meddelas. Det sistnämnda meddelandet kan underlåtas om skäl enligt punkt 2 a–e föreligger. I samtliga dessa fall ska den registrerade meddelas att han eller hon kan överklaga till den behöriga nationella tillsynsmyndigheten, en rättslig myndighet eller domstol.

### *Artikel 18*

#### *Rätt till rättelse, radering eller blockering av uppgifter*

1. Den registrerade ska ha rätt att förvänta sig att den registeransvarige fullgör sin skyldighet enligt artiklarna 4, 8 och 9 att rätta, radera eller blockera personuppgifter som registrerats inom ramen för detta rambeslut. Medlemsstaterna ska fastställa huruvida den registrerade får göra anspråk på denna rättighet direkt gentemot den registeransvarige eller via den behöriga nationella tillsynsmyndigheten. Om den registeransvarige vägrar att rätta, radera eller blockera måste vägran meddelas skriftligen och den registrerade måste informeras om de möjligheter som tillhandahålls inom den nationella lagstiftningen att anföra klagomål eller begära prövning. När klagomålet eller begäran om prövning behandlats ska den registrerade informeras om huruvida den registeransvarige handlat korrekt eller ej. Medlemsstaterna får även föreskriva att den registrerade ska informeras av den behöriga nationella tillsynsmyndigheten om att en översyn har utförts.

2. Om den registrerade bestrider korrektheten av en personuppgift och det inte kan fastställas huruvida denna är korrekt får denna uppgift markeras.

#### *Artikel 19*

##### *Rätt till ersättning*

1. Var och en som lidit skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av detta rambeslut ska ha rätt till ersättning för den skada han lidit av den registeransvarige eller av en annan ansvarig myndighet enligt nationell lagstiftning.
2. Om den behöriga myndigheten i en medlemsstat överför personuppgifter kan mottagaren inte åberopa det faktum att de överförda uppgifterna varit felaktiga för att undgå det ansvar som denne i enlighet med den nationella lagstiftningen har gentemot den skadelidande. Om mottagaren utbetalar skadestånd för en skada som vållats av att felaktigt överförda uppgifter kommit till användning ska den överförande behöriga myndigheten ersätta mottagaren det skadestånd som utbetalats men därvid ta med i beräkningen eventuella felaktigheter som kan ha begåtts av mottagaren.

#### *Artikel 20*

##### *Rättsmedel*

Utan att det påverkar något administrativt förfarande som kan användas innan ett ärende anhängiggörs vid en rättslig instans ska den registrerade ha rätt att inför domstol föra talan mot kränkningar av sådana rättigheter som skyddas av den tillämpliga nationella lagstiftningen.

## *Artikel 21*

### *Sekretess i samband med behandlingen av uppgifter*

1. Var och en som får tillgång till personuppgifter som faller under tillämpningsområdet för detta rambeslut får endast behandla dessa i sin egenskap av anställd vid den behöriga myndigheten eller efter instruktioner från denna, såvida det inte föreligger rättsliga skyldigheter till annan behandling.
2. Var och en som arbetar för en behörig myndighet i en medlemsstat ska vara bunden av samtliga dataskyddsbestämmelser som gäller för respektive behörig myndighet.

## *Artikel 22*

### *Säkerhet i samband med behandlingen av uppgifter*

1. Medlemsstaterna ska se till att de behöriga myndigheterna vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från att utplånas genom olyckshändelse eller otillåtna handlingar och från att gå förlorade genom olyckshändelse samt från ändringar, otillåten spridning av eller otillåten tillgång till uppgifter, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk och eller om uppgifterna gjorts tillgängliga genom direkt automatisk åtkomst, samt mot varje annat slag av otillåten behandling, varvid hänsyn särskilt ska tas till de risker som behandlingen innebär och arten av de uppgifter som ska skyddas. Dessa åtgärder ska med beaktande av den befintliga tekniska nivån och de kostnader som är förenade med åtgärdernas genomförande leda till att en lämplig säkerhetsnivå uppnås i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som ska skyddas.

2. När det gäller automatisk databehandling ska varje medlemsstat vidta lämpliga åtgärder för att
- a) förhindra att obehöriga kommer åt datorutrustning som används för behandling av personuppgifter (åtkomstskydd för utrustning),
  - b) förhindra att databärare läses, kopieras, ändras eller avlägsnas av obehöriga (databärarkontroll),
  - c) förhindra obehörig införing av uppgifter och obehörig granskning, ändring eller radering av lagrade personuppgifter (lagringskontroll),
  - d) förhindra att obehöriga kan använda system för automatisk databehandling med hjälp av utrustning för dataöverföring (användarkontroll),
  - e) se till att personer som är behöriga att använda ett system för automatisk databehandling endast har tillgång till uppgifter som omfattas av deras behörighet (åtkomstkontroll),
  - f) se till 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) se till att det finns möjlighet att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiskt databehandlingssystem, samt när och av vem uppgifterna 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) se till att de system som används kan återställas vid störningar (återställande),
  - j) se till att system fungerar, att funktionsfel rapporteras (driftsäkerhet) och att de lagrade uppgifterna inte kan förvanskas genom funktionsfel i systemet (dataintegritet).
3. Medlemsstaternas ska sörja för att endast sådana personer får utses till registerförare som kan ge garantier för att vidta de nödvändiga tekniska och organisatoriska åtgärderna enligt punkt 1 och beaktar anvisningarna i artikel 21. Den behöriga myndigheten ska övervaka registerföraren i dessa avseenden.
4. Personuppgifter får endast behandlas av en registerförare på grundval av en rättsakt eller ett skriftligt avtal.

### *Artikel 23*

#### *Föregående samråd*

Medlemsstaterna ska sörja för att de behöriga nationella tillsynsmyndigheterna rådfrågas före behandling av personuppgifter när nya behandlingssystem inrättas om

- a) särskilda uppgiftskategorier enligt artikel 6 behandlas, eller om

- b) behandlingens typ, särskilt användning av ny teknik, nya mekanismer eller förfaranden, i övrigt innebär särskilda risker för registrerades grundläggande fri- och rättigheter och framför allt deras rätt till privatliv.

*Artikel 24*

*Påföljder*

Medlemsstaterna ska anta lämpliga bestämmelser för att säkerställa att detta rambeslut genomförs fullt ut och framför allt föreskriva effektiva, proportionella och avskräckande påföljder för överträdelse av bestämmelser som antagits i enlighet med detta rambeslut.

*Artikel 25*

*Nationella tillsynsmyndigheter*

1. Varje medlemsstat ska se till att det utses en eller flera myndigheter med uppgift att inom dess territorium vägleda och övervaka tillämpningen av de bestämmelser som medlemsstaterna antagit i enlighet med detta rambeslut. Dessa myndigheter ska vara fullt oberoende när de fullgör sina åligganden.
2. Varje tillsynsmyndighet ska framför allt ha
  - a) utredande befogenheter, som befogenhet att få tillgång till uppgifter som blir föremål för behandling och befogenhet att samla in all information som är nödvändig för att utföra tillsynen,

- b) faktisk befogenhet att ingripa, som till exempel att kunna avge yttranden innan en behandling äger rum, att se till att sådana yttranden i lämplig omfattning offentliggörs, att kunna besluta om blockering, radering eller förstöring av uppgifter, att kunna besluta om tillfälligt eller definitivt förbud mot behandling, att kunna ge den registeransvarige en varning eller tillrättavisning eller att kunna hänskjuta frågor till nationella parlament eller andra politiska institutioner,
  - c) befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av detta rambeslut har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser. Beslut av tillsynsmyndigheten, som ger upphov till klagomål bör kunna överklagas till domstol.
3. Var och en ska kunna vända sig till tillsynsmyndigheten med en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter. Den berörda personen ska informeras om vilka följder hans begäran har fått.
4. Medlemsstaterna ska föreskriva att tillsynsmyndighetens ledamöter och personal ska vara bundna av de för respektive behörig myndighet gällande dataskyddsbestämmelserna och ha tystnadsplikt med avseende på konfidentiell information som de har tillgång till även sedan deras uppdrag eller anställning upphört.

#### *Artikel 26*

#### *Förhållande till avtal med tredjestater*

Detta rambeslut ska inte påverka medlemsstaternas eller unionens skyldigheter och åtaganden enligt de bilaterala och/eller multilaterala avtal med tredjestater som förelåg när detta rambeslut antogs.

När dessa avtal tillämpas ska överföringen till en tredjestat av personuppgifter som erhållits från en annan medlemsstat genomföras med respekt för artikel 13.1 c eller 13.2, i tillämpliga fall.

### *Artikel 27*

#### *Utvärdering*

1. Medlemsstaterna ska senast den ... \* rapportera till kommissionen om de nationella åtgärder som de har vidtagit för att säkerställa fullständig efterlevnad av detta rambeslut, framför allt när det gäller de bestämmelser som redan ska följas när uppgifter samlas in. Kommissionen ska särskilt undersöka konsekvenserna av dessa bestämmelser för tillämpningsområdet för detta rambeslut i enlighet med i artikel 1.2.
2. Kommissionen ska inom ett år lämna rapport till Europaparlamentet och rådet om resultatet av den utvärdering som avses i punkt 1 och tillsammans med rapporten lämna lämpliga förslag till ändringar av detta rambeslut.

---

\* EUT: Vänligen för in datumet fem år efter antagandet av detta rambeslut.

## *Artikel 28*

### *Förhållande till tidigare antagna unionsakter*

Om rättsakter som antagits enligt avdelning VI i fördraget om Europeiska unionen före den dag då detta rambeslut träder i kraft och som reglerar utbytet av personuppgifter mellan medlemsstaterna eller tillgång för medlemsstaternas utsedda myndigheter till informationssystem som inrättats enligt fördraget om upprättandet av Europeiska gemenskapen innehåller särskilda villkor för den mottagande medlemsstatens användning av sådana uppgifter, ska dessa villkor ha företräde framför bestämmelserna i rambeslutet när det gäller användning av uppgifter som tagits emot eller gjorts tillgängliga av en annan medlemsstat.

## *Artikel 29*

### *Genomförande*

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta rambeslut före den ...\*.
2. Senast vid denna tidpunkt ska medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till de bestämmelser genom vilka skyldigheterna enligt detta rambeslut införlivas med deras nationella lagstiftning samt upplysningar om de tillsynsmyndigheter som avses i artikel 25. På grundval av denna information och en skriftlig rapport som kommissionen utarbetar med hjälp av denna information ska rådet före den ...\*\* bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i detta rambeslut.

---

\*\* EUT: Vänligen för in datumet tre år efter antagandet av detta rambeslut.



## UTKAST TILL UTTALANDE FRÅN RÅDET

"Rådet kommer att undersöka hur i framtiden de uppgifter som fullgörs av de befintliga gemensamma dataskyddsmyndigheter som var för sig inrättats för Schengens informationssystem, Europol, Eurojust och tullinformationssystemet, i enlighet med tillämpliga rättsliga grunder skulle kunna kombineras inom en enda dataskyddsmyndighet, vilket inbegriper den rådgivande funktionen, samtidigt som man beaktar dessa systems och organs specifika särart.

Rådet anser att detta är ett sätt att ytterligare förbättra organisationen av dataskyddet på området polissamarbete och straffrättsligt samarbete."

---

I promemorian föreslås att riksdagen ska godkänna ett inom Europeiska unionen upprättat utkast till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Utkastet till rambeslut innehåller bestämmelser som syftar till att förstärka skyddet för behandling av personuppgifter inom nu nämnda områden, i det vidare syftet att kunna förbättra det gränsöverskridande utbytet av information om brottsbekämpning mellan medlemsstaterna. Rambeslutet utgör ett viktigt komplement till andra instrument om polisiärt och straffrättsligt samarbete.

Utkastet innehåller bestämmelser om allmänna principer för behandlingen av personuppgifter, behandling av känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. I stora delar motsvarar utkastet till rambeslutet innehållet i det s.k. dataskyddsdirektivet, som har genomförts i svensk rätt genom personuppgiftslagen.

I promemorian övervägs, på ett mera allmänt plan, vilka lagändringar som kan bli nödvändiga med anledning av rambeslutet.

Promemorian innehåller inga lagförslag.



## Förteckning över remissinstanserna

Prop. 2008/09:16  
Bilaga 4

1. Riksdagens ombudsmän
2. Riksrevisionen
3. Hovrätten för Nedre Norrland
4. Falu tingsrätt
5. Malmö tingsrätt
6. Kamrarrätten i Stockholm
7. Länsrätten i Stockholms län
8. Länsrätten i Östergötlands län
9. Justitiekanslern
10. Domstolsverket
11. Åklagarmyndigheten
12. Ekobrottsmyndigheten
13. Rikspolisstyrelsen
14. Säkerhetspolisen
15. Säkerhets- och integritetsskyddsnämnden
16. Kriminalvården
17. Brottsförebyggande rådet
18. Brottsoffermyndigheten
19. Kustbevakningen
20. Tullverket
21. Skatteverket
22. Datainspektionen
23. Statskontoret
24. Juridiska fakulteten vid Uppsala universitet
25. Juridiska fakulteten vid Lunds universitet
26. Riksarkivet
27. Sveriges advokatsamfund
28. Facket för Service och Kommunikation (SEKO)
29. ST-Polisväsendet
30. Svenska Avdelningen av internationella Juristkommissionen
31. Svenska Helsingforskommittén för Mänskliga Rättigheter
32. Svenska Journalistförbundet
33. Svenska polisförbundet
34. Sveriges Akademikers Centralorganisation (SACO)
35. Sveriges Domareförbund
36. Sveriges Kommuner och Landsting
37. Tidningsutgivarna
38. Tull-Kust

Utdrag ur protokoll vid regeringssammanträde den 18 september 2008

Närvarande: Statsministern Reinfeldt, ordförande, och statsråden Olofsson, Odell, Ask, Husmark Pehrsson, Leijonborg, Larsson, Erlandsson, Torstensson, Björklund, Carlsson, Littorin, Borg, Malmström, Sabuni, Billström, Adelsohn Liljeroth, Tolgfors

Föredragande: Statsrådet Ask

---

Regeringen beslutar proposition 2008/09:16 Godkännande av  
Dataskyddsrambeslutet