Regeringens proposition 2020/21:186

Kompletterande bestämmelser till EU:s cybersäkerhetsakt

Prop. 2020/21:186

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 29 april 2021

Stefan Löfven

Peter Hultqvist
(Försvarsdepartementet)

Propositionens huvudsakliga innehåll

I propositionen föreslås en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I den föreslagna lagen finns kompletterande bestämmelser till EU:s cybersäkerhetsakt om bland annat nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Den nya lagen föreslås träda i kraft den 28 juni 2021.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringens förslag:

1. Riksdagen antar regeringens förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Förordningen (EU) 2019/881 benämns i denna lag EU:s cybersäkerhetsakt.

Ord och uttryck i denna lag har samma betydelse som i EU:s cybersäkerhetsakt.

Nationell myndighet för cybersäkerhetscertifiering

2 § Den myndighet som regeringen bestämmer

1. är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt, och
2. utövar tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Ackreditering av organ för bedömning av överenstämmelse

3 § I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

Tillsynsbefogenheter

4 § Vid tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs har den nationella myndigheten för

cybersäkerhetscertifiering de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt.

5 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för tillsynen och för att EU:s cybersäkerhetsakt, genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

6 § Den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Vid handräckning tillämpas bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Om den nationella myndigheten för cybersäkerhetscertifiering begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.

7 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering.

Administrativa sanktionsavgifter

8 § Den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift av den som

1. har utfärdat en EU-försäkran om överenstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,
2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. har utfärdat en EU-försäkran om överensstämmelse eller innehar ett cybersäkerhetscertifikat och inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering,

6. överträder ett beslut om föreläggande enligt 5 § som innebär ett förbud, eller

7. använder ett europeiskt cybersäkerhetscertifikat som har återkallats enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

9 § En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

10 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppkommit till följd av överträdelsen,

2. om den som har begått överträdelsen tidigare begått en överträdelse, och

3. den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

11 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

12 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

13 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

14 § Sanktionsavgiften tillfaller staten.

15 § En sanktionsavgift ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

16 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Tystnadsplikt

17 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).

Avgifter

18 § Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana avgifter.

Ändring av beslut av privata organ för bedömning av överensstämmelse

19 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och
2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Överklagande

20 § Beslut enligt EU:s cybersäkerhetsakt och enligt denna lag av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 28 juni 2021.

2.2 Förslag till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs att 3 § lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska ha följande lydelse.

Lydelse enligt förslaget i 2.1	*Föreslagen lydelse*
3 §	
I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.	
I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering *och marknadskontroll i samband med saluföring av produkter* och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.	I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.	

Denna lag träder i kraft den 16 juli 2021.

3 Ärendet och dess beredning

Den 17 april 2019 beslutade Europaparlamentet och rådet att anta förordningen (EU) 2019/881 om Enisa (Europeiska unionens säkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). EU-förordningen, här kallad EU:s cybersäkerhetsakt, i dess svenska lydelse finns i *bilaga 1*. EU:s cybersäkerhetsakt trädde i kraft den 27 juni 2019. Vissa bestämmelser om cybersäkerhetscertifiering som kräver kompletterande nationella bestämmelser ska tillämpas från och med den 28 juni 2021.

Regeringen beslutade den 31 oktober 2019 att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande bestämmelser som EU:s cybersäkerhetsakt ger anledning till och överväga om det finns anledning att införa ytterligare krav för att skydda verksamhet som är av betydelse för Sveriges säkerhet (dir. 2019:73).

Utredningen, som tog namnet Cybersäkerhetsutredningen (Fö 2019:01), överlämnade den 30 september 2020 delbetänkandet EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58).

En sammanfattning av delbetänkandet finns i *bilaga 2*. Delbetänkandets lagförslag finns i *bilaga 3*.

Delbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissvaren finns tillgängliga på regeringens webbplats (www.regeringen.se) och i Försvarsdepartementet (Fö2020/00954).

Lagrådet

Regeringen beslutade den 24 mars 2021 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 5*. Lagrådets yttrande finns i *bilaga 6*. Regeringen följer delvis Lagrådets förslag. Lagrådets synpunkter och förslag behandlas i avsnitten 7.2, 8.3, 8.6, 8.7, 9.2.4 och i författningskommentaren.

I förhållande till lagrådsremissen har dessutom vissa språkliga och redaktionella ändringar gjorts.

4 EU:s cybersäkerhetsakt

4.1 Syfte och huvudsakligt innehåll

Syftet med EU:s cybersäkerhetsakt är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen.

EU:s cybersäkerhetsakt reglerar dels Europeiska unionens cybersäkerhetsbyrå (Enisa), dels ett ramverk för cybersäkerhetscertifiering.

I fråga om Enisa regleras mål, uppgifter och organisatoriska frågor. Enisa ska främja spridningen av cybersäkerhetscertifiering i unionen, bl.a.

genom att bidra till inrättandet och underhållandet av ramverket för cybersäkerhetscertifiering på unionsnivå. Bestämmelserna i den delen trädde i kraft den 27 juni 2019.

Europeiska kommissionen ska utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. Enisa ska med hjälp av expertråd och i nära samarbete med Europeiska gruppen för cybersäkerhetscertifiering (ECCG) lämna förslag på europeiska certifieringsordningar. Syftet är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering medför att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater.

Genom ramverket möjliggörs en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering, vilket skapar en digital inre marknad för IKT-produkter, IKT-tjänster och IKT-processer.

4.2 Det europeiska ramverket för cybersäkerhetscertifiering

4.2.1 Allmänt om det europeiska ramverket för cybersäkerhetscertifiering

Det europeiska ramverket för cybersäkerhetscertifiering innebär en möjlighet för tillverkare och leverantörer att upprätta en s.k. EU-försäkran om överensstämmelse eller ansöka om ett europeiskt cybersäkerhetscertifikat som intygar att en viss IKT-produkt, IKT-tjänst eller IKT-process uppfyller kraven enligt en europeisk ordning för cybersäkerhetscertifiering.

En EU-försäkran om överenstämmelse eller ett europeiskt cybersäkerhetscertifikat ska intyga att en produkt, tjänst eller process uppfyller angivna säkerhetskrav när det gäller att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via produkten, tjänsten eller processen.

EU-försäkringar om överenstämmelse och europeiska cybersäkerhetscertifikat syftar även till att hjälpa slutanvändarna att göra informerade val och bidra till att harmonisera cybersäkerhetsrutinerna inom unionen.

I skäl 71 i EU:s cybersäkerhetsakt anges att de europeiska ordningarna för cybersäkerhetscertifiering bör bygga på vad som redan existerar på internationell och nationell nivå och, om så krävs, på tekniska specifikationer från forum och konsortier.

Vidare anges att certifieringsordningar som drivs av industrin eller andra privata organisationer inte bör ingå i cybersäkerhetsaktens tillämpningsområde.

Cybersäkerhetsakten ska inte påverka tillämpningen av unionsrätt som innehåller särskilda bestämmelser om certifiering av IKT-produkter, IKT-

tjänster och IKT-processer, t.ex. Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (den allmänna dataskyddsförordningen).

EU:s cybersäkerhetsakt ska inte heller påverka medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område (artikel 2).

Cybersäkerhetscertifiering kan vara en kostsam process, vilket i sin tur kan leda till högre priser för kunder och konsumenter. Behovet av certifiering kan också variera beroende på i vilket sammanhang produkterna och tjänsterna ska användas och den snabba tekniska utvecklingen. Därför bör det – enligt EU:s cybersäkerhetsakt – vara frivilligt att använda en europeisk cybersäkerhetscertifiering, om inte annat föreskrivs i unionsrätten eller medlemsstaternas nationella rätt som antagits i enlighet med unionsrätten. På vissa områden kan det bli nödvändigt att i framtiden införa särskilda krav på cybersäkerhet och göra cybersäkerhetscertifiering obligatorisk för vissa IKT-produkter, IKT-tjänster och IKT-processer för att förbättra cybersäkerheten i unionen.

Kommissionen ska regelbundet följa upp vilka effekter antagna europeiska ordningar för cybersäkerhetscertifiering har på tillgången till säkra IKT-produkter, IKT-tjänster och IKT-processer på den inre marknaden och bör också regelbundet bedöma i hur hög utsträckning tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer i unionen använder certifieringsordningarna, effektiviteten hos de europeiska ordningarna för cybersäkerhetscertifiering och om bestämda ordningar bör göras obligatoriska. Bedömningen bör göras mot bakgrund av unionens lagstiftning med koppling till cybersäkerhet, särskilt direktiv (EU) 2016/1148, med beaktande av säkerheten i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster.

I avsaknad av harmoniserad unionsrätt får medlemsstaterna införa nationella tekniska föreskrifter som föreskriver obligatorisk certifiering inom ramen för en europeisk ordning för cybersäkerhetscertifiering i enlighet med Europaparlamentets och rådets direktiv (EU) 2015/1535 om ett informationsförfarande när det gäller tekniska föreskrifter och i fråga om föreskrifter för informationssamhällets tjänster.

Medlemsstaterna får även använda europeisk cybersäkerhetscertifiering i samband med offentlig upphandling och inom ramen för Europaparlamentets och rådets direktiv 2014/24/EU om offentlig upphandling.

I syfte att säkerställa en harmonisering och undvika fragmentering upphör nationella ordningar eller förfaranden för certifiering av IKT-produkter, IKT-tjänster eller IKT-processer som omfattas av en europeisk ordning för cybersäkerhetscertifiering att gälla från och med den dag som fastställs av kommissionen genom en sådan ordning (genomförandeakt). Medlemsstaterna får inte heller införa nya nationella ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster eller IKT-processer som redan omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering. Medlemsstaterna är dock inte förhindrade att anta eller behålla nationella ordningar för cybersäkerhetscertifiering för att skydda den nationella säkerheten.

4.2.2 Artiklar i EU:s cybersäkerhetsakt

Ett europeiskt ramverk för cybersäkerhetscertifiering

I artikel 46 i EU:s cybersäkerhetsakt anges att ett europeiskt ramverk för cybersäkerhetscertifiering ska inrättas för att förbättra förutsättningarna för den inre marknadens funktion genom att höja cybersäkerhetsnivån i unionen och möjliggöra en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering i syfte att skapa en digital inre marknad för IKT-produkter, IKT-tjänster och IKT-processer.

Unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering

I artikel 47 anges att kommissionen ska offentliggöra unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering (nedan kallat unionens löpande arbetsprogram) i vilket strategiska prioriteringar ska fastställas för framtida europeiska ordningar för cybersäkerhetscertifiering. I unionens löpande arbetsprogram ska det särskilt ingå en förteckning över IKT-produkter, IKT-tjänster och IKT-processer eller kategorier av sådana som kan gagnas av att omfattas av en europeisk ordning för cybersäkerhetscertifiering. Inkludering av specifika IKT-produkter, IKT-tjänster och IKT-processer eller kategorier av sådana i unionens löpande arbetsprogram ska motiveras av ett eller flera av de skäl som anges i artikeln, t.ex. efterfrågan på marknaden.

Begäran om en europeisk ordning för cybersäkerhetscertifiering

Enligt artikel 48 får kommissionen begära att Enisa utarbetar ett förslag till certifieringsordning eller ser över en befintlig europeisk ordning för cybersäkerhetscertifiering på grundval av unionens löpande arbetsprogram. I vederbörligen motiverade fall får kommissionen eller europeiska gruppen för cybersäkerhetscertifiering begära att Enisa utarbetar ett förslag till certifieringsordning eller ser över en befintlig europeisk ordning för cybersäkerhetscertifiering som inte ingår i unionens löpande arbetsprogram.

Utarbetande, antagande och översyn av en europeisk ordning för cybersäkerhetscertifiering

I artikel 49 anges att efter en begäran från kommissionen i enlighet med artikel 48, ska Enisa utarbeta ett förslag till certifieringsordning som uppfyller de krav som anges i artiklarna 51, 52 och 54. Efter en begäran från europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 48.2 får Enisa utarbeta ett förslag till certifieringsordning som uppfyller de krav som anges i artiklarna 51, 52 och 54. Vid utarbetande av ett förslag till certifieringsordning ska Enisa samråda med alla berörda intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess. För varje förslag till certifieringsordning ska Enisa inrätta en för ändamålet särskilt tillsatt arbetsgrupp i enlighet med artikel 20.4 i syfte att tillhandahålla Enisa särskild rådgivning och sakkunskap. Enisa ska ha ett nära samarbete med europeiska gruppen för cybersäkerhetscertifiering. Europeiska gruppen för cybersäkerhetscertifiering ska ge Enisa bistånd och expertråd vid utarbetandet av förslagen till certifierings-

ordning och ska anta ett yttrande om förslaget till certifieringsordning. Med utgångspunkt i förslaget till certifieringsordning som Enisa lagt fram, får kommissionen anta genomförandeakter för europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer. Enisa ska åtminstone vart femte år utvärdera varje antagen europeisk ordning för cybersäkerhetscertifiering och därvid beakta synpunkter från berörda intressenter.

Webbplats om europeiska ordningar för cybersäkerhetscertifiering

I artikel 50 anges att Enisa ska underhålla en särskild webbplats med information om och offentliggörande av europeiska ordningar för cybersäkerhetscertifiering, europeiska cybersäkerhetscertifikat och EU-intyg om överensstämmelse, även information med avseende på europeiska ordningar för cybersäkerhetscertifiering som inte längre är giltiga, på indragna och utgångna europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, och på förteckningen över länkar till cybersäkerhetsinformation som tillhandahålls i enlighet med artikel 55. I tillämpliga fall ska det på webbplatsen också anges vilka nationella ordningar för cybercertifiering som har ersatts av en europeisk ordning för cybersäkerhetscertifiering.

Säkerhetsmålsättningarna för europeiska ordningar för cybersäkerhetscertifiering

Enligt artikel 51 ska en europeisk ordning för cybersäkerhetscertifiering vara utformad för att, i tillämpliga fall, uppnå minst de säkerhetsmålsättningar som anges i artikeln.

Assuransnivåer för europeiska ordningar för cybersäkerhetscertifiering

I artikel 52 anges att en europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av assuransnivåerna ”grundläggande”, ”betydande” och ”hög” för IKT- produkter, IKT-tjänster och IKT-processer.

Assuransnivån för en europeisk certifieringsordning utgör förtroendegrunden för att en IKT-produkt, IKT-tjänst eller IKT-process uppfyller säkerhetskraven i en särskild europeisk ordning för cybersäkerhetscertifiering. I syfte att säkerställa konsekvens i den europeiska ramen för cybersäkerhetscertifiering ska en europeisk ordning för cybersäkerhetscertifiering kunna specificera assuransnivån för EU-försäkringar om överensstämmelse och europeiska cybersäkerhetscertifikat som har utfärdats inom ramen för den ordningen. En EU-försäkran om överensstämmelse kan endast avse assuransnivån grundläggande medan ett europeiskt cybersäkerhetscertifikat kan avse någon av assuransnivåerna grundläggande, betydande eller hög.

Assuransnivåerna avspeglar motsvarande stringens och djup i fråga om utvärdering av IKT-produkten, IKT-tjänsten och IKT-processen och fastställs genom hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska mildra eller förhindra incidenter. Varje assuransnivå bör vara konsekvent inom de olika sektoriella områden där certifiering tillämpas.

En europeisk ordning för cybersäkerhetscertifiering kan ha flera utvärderingsnivåer beroende på hur stringent och djupgående utvärderingsmetoden är. Utvärderingsnivåer ska motsvara en av assuransnivåerna och vara kopplad till en lämplig kombination av assuranskomponenter. För samtliga assuransnivåer bör IKT-produkten, IKT-tjänsten eller IKT-processen omfatta en rad säkra funktioner som fastställs i ordningen.

Självbedömning av överensstämmelse

I artikel 53 anges att en europeisk ordning för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer möjlighet att göra en självbedömning av överensstämmelse, dvs. en EU-försäkran om överensstämmelse. En självbedömning av överensstämmelse ska dock endast tillåtas i förhållande till IKT-produkter, IKT-tjänster och IKT-processer med låg risk som motsvarar assuransnivån grundläggande. Denna typ av bedömning av överensstämmelse bedöms lämplig för IKT-produkter och IKT-tjänster med lägre komplexitet som inte utgör en stor risk för det allmänna samhällsintresset (skäl 79). Genom att utfärda en EU-försäkran om överensstämmelse tar tillverkaren eller leverantören ansvar för att IKT-produkten, IKT-tjänsten eller IKT-processen överensstämmer med de krav som anges i certifieringsordningen. Det är frivilligt att utfärda en EU-försäkran om överensstämmelse om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt. En EU-försäkran om överensstämmelse ska erkännas i alla medlemsstater.

Komponenter i europeiska ordningar för cybersäkerhetscertifiering

I artikel 54 anges de komponenter som en europeisk ordning för cybersäkerhetscertifiering åtminstone ska innehålla. Av artikeln följer att föremålet och tillämpningsområdet för certifieringsordningen, inbegripet typen eller kategorierna av de IKT-produkter, IKT-tjänster och IKT-processer som omfattas av certifieringsordningen och en tydlig beskrivning av syftet med ordningen och hur de valda standarderna, utvärderingsmetoderna och assuransnivåerna överensstämmer med behoven hos ordningens avsedda användare ska anges. Om självbedömning av överensstämmelse är tillåtet inom ramen för ordningen ska också anges samt, i tillämpliga fall, särskilda eller ytterligare krav som gäller för organ för bedömning av överensstämmelse för att garantera deras tekniska kompetens att utvärdera cybersäkerhetskraven. Vidare ska, i tillämpliga fall, anges vilka uppgifter som är nödvändiga för certifieringen och som en sökande ska lämna till eller på annat sätt göra tillgängliga för organ för bedömning av överensstämmelse och regler för övervakning av efterlevnaden av IKT-produkter, IKT-tjänster och IKT-processer vad gäller kraven i europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven. Härutöver anges i artikeln ytterligare komponenter som en europeisk ordning för cybersäkerhetscertifiering ska innehålla.

I artikel 55 anges att tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse har utfärdats eller som är certifierade ska lämna kompletterande cybersäkerhetsinformation enligt vad som anges i artikeln.

Cybersäkerhetscertifiering

I artikel 56 anges att IKT-produkter, IKT-tjänster och IKT-processer som har certifierats enligt en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49, ska förutsättas överensstämma med kraven i en sådan ordning. Vidare anges att cybersäkerhetscertifieringen ska vara frivillig, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

I artikel 56.4 anges att de organ för bedömning av överensstämmelse som avses i artikel 60 ska utfärda europeiska cybersäkerhetscertifikat i enlighet med artikeln som avser assuransnivå grundläggande eller betydande på grundval av de kriterier som ingår i den europeiska ordningen för cybersäkerhetscertifiering, som antagits av kommissionen i enlighet med artikel 49.

I artikel 56.5 anges att genom undantag från punkten 4, och i motiverade fall, får en europeisk ordning för cybersäkerhetscertifiering föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen får utfärdas endast av ett offentligt organ. Ett sådant organ ska vara en nationell myndighet för cybersäkerhetscertifiering som avses i artikel 58.1 eller ett offentligt organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 60.1.

Av artikel 56.6 framgår att om en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 kräver assuransnivån hög, ska det europeiska cybersäkerhetscertifikatet enligt den ordningen endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller, i följande fall, av ett organ för bedömning av överensstämmelse:

– Efter förhandsgodkännande av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse.
– Efter allmän delegering på förhand av uppgiften att utfärda ett sådant europeiskt cybersäkerhetscertifikat till ett organ för bedömning av överensstämmelse från den nationella myndigheten för cybersäkerhetscertifiering.

I artikel 56.9 anges att ett europeiskt cybersäkerhetscertifikat ska utfärdas för den period som fastställs i den europeiska ordningen för cybersäkerhetscertifiering och får förnyas under förutsättning att de relevanta kraven alltjämt uppfylls.

Av artikel 56.10 framgår att ett europeiskt cybersäkerhetscertifikat som utfärdats i enlighet med denna artikel ska erkännas i alla medlemsstater.

I artikel 57.1 anges att de nationella ordningarna för cybersäkerhetscertifiering och därtill hörande förfaranden, för IKT-produkter, IKT-tjänster och IKT-processer som omfattas av en europeisk ordning för cybersäkerhetscertifiering, ska upphöra att ha verkan från och med den dag som anges i den genomförandeakt som antagits i enlighet med artikel 49.7. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster och IKT-processer som inte omfattas av en europeisk ordning för cybersäkerhetscertifiering får kvarstå.

Av artikel 57.2 framgår att medlemsstaterna inte får införa nya nationella ordningar för cybersäkerhetscertifiering av de IKT-produkter, IKT-tjänster och IKT-processer som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.

Av artikel 57.3 framgår att befintliga certifikat som har utfärdats enligt nationella ordningar för cybersäkerhetscertifiering och som omfattas av en europeisk ordning för cybersäkerhetscertifiering ska förbli giltiga tills de löper ut.

Hänvisningar i nationell lagstiftning till nationella standarder som har upphört att ha verkan i och med att en europeisk ordning för cybersäkerhetscertifiering har trätt i kraft kan orsaka förvirring. Medlemsstaterna bör därför se till att antagandet av en europeisk ordning för cybersäkerhetscertifiering avspeglas i deras nationella lagstiftning (skäl 98).

Nationella myndigheter för cybersäkerhetscertifiering

I artikel 58.1 anges att varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium eller, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i denna andra medlemsstat som ansvariga för tillsynsuppgifterna i den utseende medlemsstaten.

Av artikel 58.2 följer att medlemsstaten ska underrätta kommissionen om vilka nationella myndigheter för cybersäkerhetscertifiering som utsetts. Om en medlemsstat utser mer än en myndighet ska den också informera kommissionen om vilka uppgifter som var och en av dessa myndigheter tilldelats.

Av artikel 58.3 följer att varje nationell myndighet för cybersäkerhetscertifiering ska, utan att det påverkar tillämpningen av artikel 56.5 a och 56.6, vara oberoende av de enheter som den utövar tillsyn över vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande.

Av artikel 58.4 följer att medlemsstaterna ska säkerställa att den verksamhet som bedrivs av den nationella myndigheten för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat som avses i artiklarna 56.5 a och 56.6 är strikt avskild från deras uppgifter och ansvarsområden i förhållande till tillsynsverksamheten och att dessa verksamheter utförs oberoende av varandra.

Av artikel 58.7 framgår att nationella myndigheter för cybersäkerhetscertifiering bl.a. ska

- övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering,
- övervaka IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med kraven i de europeiska cybersäkerhetscertifikat som har utfärdats inom deras respektive territorier, i samarbete med andra berörda marknadsövervakningsmyndigheter,
- kontrollera att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer som är etablerade inom deras respektive territorier fullgör sina skyldigheter när de genomför självbedömning av överensstämmelse enligt artiklarna 53.2 och 53.3 och motsvarande europeisk ordning för cybersäkerhetscertifiering,
- aktivt bistå och stödja de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning,
- övervaka och kontrollera den verksamhet som bedrivs av de offentliga organ som avses i artikel 56.5,
- i tillämpliga fall utfärda bemyndiganden för organ för bedömning av överensstämmelse i enlighet med artikel 60.3 och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organen för bedömning av överensstämmelse inte uppfyller kraven i cybersäkerhetsakten,
- behandla klagomål från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av nationella myndigheter för cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 56.6, eller avseende en EU-försäkran av överensstämmelse som utfärdats enligt artikel 53,
- lämna en årlig sammanfattande rapport om den verksamhet som bedrivits enligt leden b, c och d i denna punkt eller enligt punkt 8 till Enisa och europeiska gruppen för cybersäkerhetscertifiering,
- samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, bl.a. genom att utbyta information om IKT-produkter, IKT-tjänster och IKT-processer som eventuellt avviker från kraven i cybersäkerhetsakten eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och
- övervaka relevant utveckling på området cybersäkerhetscertifiering.

I artikel 58.8 anges de minimibefogenheter som varje nationell myndighet för cybersäkerhetscertifiering ska ha för att kunna fullgöra tillsyn över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering.

Av artikel 58.9 framgår att nationella myndigheter för cybersäkerhetscertifiering ska samarbeta med varandra och med kommissionen, bl.a. genom att utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer.

Inbördes granskning

I artikel 59.1 anges att de nationella myndigheterna för cybersäkerhetscertifiering omfattas av inbördes granskning i syfte att uppnå likvärdiga standarder i hela unionen för EU-försäkringar om överensstämmelse och europeiska cybersäkerhetscertifikat.

Av artikel 59.4 framgår att den inbördes granskningen ska utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och kommissionen och ska utföras minst vart femte år. Enisa får delta i den inbördes granskningen.

Organen för bedömning av överensstämmelse

Av artikel 60.1 framgår att organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008. Sådan ackreditering ska endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till EU:s cybersäkerhetsakt.

I artikel 60.2 anges att om ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a och 56.6 ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som ett organ för bedömning av överensstämmelse enligt punkten 1.

Av artikel 60.3 framgår att om de europeiska ordningarna för cybersäkerhetscertifiering innehåller särskilda eller ytterligare krav enligt artikel 54.1 f ska endast organ för bedömning av överensstämmelse som uppfyller dessa krav bemyndigas av den nationella myndigheten för cybersäkerhetscertifiering att utföra uppgifter inom ramen för sådana ordningar.

Av artikel 60.4 framgår att ackrediteringen som avses i punkten 1 ska utfärdas till organen för bedömning av överensstämmelse för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse fortfarande uppfyller kraven i denna artikel. Nationella ackrediteringsorgan ska vidta alla lämpliga åtgärder inom en rimlig tidsram för att begränsa, tillfälligt upphäva eller återkalla ackrediteringen av ett organ för bedömning av överensstämmelse som har utfärdats i enlighet med punkten 1 om villkoren för ackrediteringen inte har uppfyllts, eller inte längre uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot bestämmelserna i cybersäkerhetsakten.

Anmälan till kommissionen

I artikel 61.1 anges att de nationella myndigheterna för cybersäkerhetscertifiering till kommissionen ska anmäla de organ som har ackrediterats och, i tillämpliga fall, bemyndigade i enlighet med artikel 60.3 att utfärda europeiska cybersäkerhetscertifikat på angivna assuransnivåer enligt artikel 52.

Av artikel 61.2 följer att kommissionen, ett år efter ikraftträdandet av en europeisk ordning för cybersäkerhetscertifiering, ska offentliggöra en förteckning över de organ för bedömning av överensstämmelse som har anmälts.

Av artikel 61.4 följer att en nationell myndighet för cybersäkerhetscertifiering får lämna in en begäran till kommissionen om att stryka ett organ för bedömning av överensstämmelse, som anmälts av den myndigheten, från den förteckning som avses i punkten 2.

Europeiska gruppen för cybersäkerhetscertifiering

Av artikel 62 följer att en europeisk grupp för cybersäkerhetscertifiering ska bildas. Gruppen ska bestå av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller företrädare för andra berörda nationella myndigheter. Gruppen ska ha i uppgift att bl.a. ge råd till och bistå kommissionen i dess arbete för att säkerställa ett konsekvent genomförande och en konsekvent tillämpning av det europeiska ramverket för cybersäkerhetscertifiering, särskilt när det gäller frågor som rör unionens löpande arbetsprogram, cybersäkerhetscertifiering, strategisamordning och utarbetandet av de europeiska ordningarna för cybersäkerhetscertifiering.

Rätt att lämna in klagomål

I artikel 63.1 anges att fysiska och juridiska personer ska ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller, när klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse som handlar i enlighet med artikel 56.6, till den berörda nationella myndigheten för cybersäkerhetscertifiering.

Rätt till ett effektivt rättsmedel

I artikel 64.1 anges att fysiska och juridiska personer ska ha rätt till effektiva rättsmedel avseende beslut fattade av den myndighet eller det organ som avses i artikel 63.1, och avseende underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till den myndighet eller det organ som avses i artikel 63.1.

Sanktioner

I artikel 65 anges att medlemsstaterna ska fastställa regler om sanktioner vid överträdelser av det europeiska ramverket för cybersäkerhetscertifiering och europeiska certifieringsordningar, och ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

5 En ny lag införs

Regeringens förslag: En ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt införs.

Ord och uttryck i den nya lagen ska ha samma betydelse som i EU:s cybersäkerhetsakt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Sveriges advokatsamfund* ifrågasätter att ytterligare en fristående författning på informationssäkerhetsområdet införs. Övriga remissinstanser tillstyrker eller yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: EU:s cybersäkerhetsakt är bindande i sin helhet och direkt tillämplig i varje medlemsstat. Den ger medlemsstaterna rätt, men föreskriver även en skyldighet för dem, att vidta åtgärder för att säkerställa att regelverket i det europeiska ramverket för cybersäkerhetscertifiering införs och tillämpas på ett ändamålsenligt och effektivt sätt. En medlemsstat får dock inte vidta några åtgärder för att införliva de materiella bestämmelserna i det europeiska ramverket med nationell rätt. Det är endast om nationell rätt kan anses strida mot cybersäkerhetsakten, i de fall akten ger möjlighet eller föreskriver en skyldighet att vidta lagstiftningsåtgärder nationellt och om det behövs nationella åtgärder till stöd för regelverkets syfte, som ändringar i nationell rätt aktualiseras. Flera av artiklarna i EU:s cybersäkerhetsakt förutsätter att nationella kompletterande bestämmelser införs, bl.a. i fråga om utseende av nationell myndighet för cybersäkerhetscertifiering (artikel 58), rätten till ett effektivt rättsmedel (artikel 64) och sanktioner (artikel 65).

Vissa av de kompletterande nationella bestämmelser som behöver införas, t.ex. de om sanktionsavgifter, förutsätter lagstöd. Genom EU:s cybersäkerhetsakt införs ett nytt regelverk för cybersäkerhetscertifiering. Något motsvarande regelverk på nationell nivå finns för närvarande inte. Regeringen anser därför, till skillnad mot *Sveriges Advokatsamfund*, att en ny lag bör införas. Som utredningen föreslår bör den nya lagen benämnas lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Vissa av de bestämmelser som föreslås i den nya lagen bör hänvisa till artiklar i EU:s cybersäkerhetsakt, till exempel till artikel 58 som anger vilka befogenheter som den nationella myndigheten för cybersäkerhetscertifiering har. Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. För att eventuella ändringar i EU:s cybersäkerhetsakt ska få omedelbart genomslag i Sverige är det lämpligt att hänvisningarna i den nya lagen är dynamiska.

Flera av de ord och uttryck som används i EU:s cybersäkerhetsakt definieras i artikel 2 i cybersäkerhetsakten. Ord och uttryck som används i den nya lagen bör därför ha samma betydelse som i EU:s cybersäkerhetsakt.

6 Nationell myndighet för cybersäkerhetscertifiering

6.1 Regeringen ska utse den nationella myndigheten för cybersäkerhetscertifiering

Regeringens förslag: Den myndighet som regeringen bestämmer ska vara nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering att utföra de uppgifter som anges i EU:s cybersäkerhetsakt. Det är därmed upp till varje medlemsstat att bestämma om en eller flera myndigheter ska utses. Som utredningen föreslår bör det i den nya lagen därför införas en bestämmelse som anger att den myndighet som regeringen bestämmer ska vara nationell myndighet för cybersäkerhetscertifiering.

6.2 Försvarets materielverk bör vara nationell myndighet för cybersäkerhetscertifiering

Regeringens bedömning: Försvarets materielverk bör vara nationell myndighet för cybersäkerhetscertifiering.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker eller invänder inte mot utredningens bedömning. Några remissinstanser, däribland *Skatteverket*, anser att Myndigheten för samhällsskydd och beredskap bör vara nationell myndighet för cybersäkerhetscertifiering.

Skälen för regeringens bedömning: En viktig utgångspunkt vid inrättandet av den nationella myndigheten för cybersäkerhetscertifiering är att, som utredningen och flera remissinstanser framhåller, beakta de krav på oberoende som EU:s cybersäkerhetsakt ställer. Det gäller verksamhet som avser utfärdande av cybersäkerhetscertifikat och verksamhet som innefattar tillsyn. Under förutsättning att kravet på oberoende uppfylls finns inget hinder enligt EU:s cybersäkerhetsakt mot att utse en myndighet att utföra samtliga uppgifter som åligger den nationella myndigheten för cybersäkerhetscertifiering.

De uppgifter som den nationella myndigheten för cybersäkerhetscertifiering ska ha innefattar sammantaget omvärldsbevakning av frågor som rör cybersäkerhet och cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer, samverkan med nationella och internationella aktörer på området, ansvar för viss cybersäkerhetscertifieringsverksamhet, främst på högsta assuransnivån och tillsynsansvar över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering.

Försvarets materielverk bedriver verksamhet som kräver bred och djup kunskap och teknisk kompetens inom ramen för verksamhet som Sveriges nationella certifieringsorgan för IT-säkerhet i produkter och system (CSEC). Erfarenhet från certifieringsverksamhet och den tekniska kunskapen som Försvarets materielverk har är också en fördel vid uppbyggnaden av ett system för en effektiv tillsyn över regelverket för cybersäkerhetscertifiering. Till detta kommer att Försvarets materielverk bedöms ha goda förutsättningar att hantera den i vissa fall känsliga information som kommer att behöva tillgängliggöras både vid cybersäkerhetscertifiering på högsta assuransnivån och inom ramen för tillsynsverksamheten.

Regeringen bedömer, i likhet med utredningen, att Försvarets materielverk är den myndighet som är bäst lämpad och bör utses att utföra de uppgifter som åligger den nationella myndigheten för cybersäkerhetscertifiering.

För att säkerställa de krav på oberoende som EU:s säkerhetsakt ställer behöver vissa frågor om bl.a. myndighetens organisation och beslutsförfarande regleras. Detta kan lämpligen göras genom förordning.

6.3 Avgiftsfinansierad verksamhet

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och den nya lagen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om sådana avgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering kommer att utfärda cybersäkerhetscertifikat efter ansökan från den tillverkare eller leverantör som exempelvis vill få en produkt certifierad enligt det europeiska ramverket för cybersäkerhetscertifiering. Kostnader i den verksamheten bör bekostas av de tillverkare och leverantörer som ansöker om ett europeiskt cybersäkerhetscertifikat.

I fråga om avgiftsfinansiering av kostnader för tillsyn har regeringen tidigare uttalat att det bör beaktas att sådana avgifter ska motsvaras av en tydlig motprestation från tillsynsorganets sida, stödja syftet med tillsynen och ge incitament till avsedda beteenden hos tillsynsorganet och objektansvariga samt vara enkla, lättbegripliga och förutsägbara för de objektansvariga, se bl.a. propositionen Lag om sprängämnesprekursorer och redovisning av krisberedskapens utveckling (prop. 2013/14:144 s. 94).

Regeringen bedömer att detta är uppfyllt i fråga om tillsynen över regelverket om cybersäkerhetscertifiering. Tillsynsavgiften bör tas ut av de aktörer vars verksamhet prövas eller är föremål för tillsynsåtgärd. Möjligheten för den nationella myndigheten för cybersäkerhetscertifiering att ta ut avgifter bör således omfatta alla berörda organ för bedömning av överensstämmelse och innehavare av europeiska cybersäkerhetscertifikat eller utfärdare av EU-försäkringar om överensstämmelse. Den nationella myndigheten för cybersäkerhetscertifiering bör även få ta ut avgift för

tillsynsverksamhet enligt den nya lagen och föreskrifter som har meddelats i anslutning till lagen.

Som utredningen föreslår bör det i den nya lagen också införas ett bemyndigande för regeringen eller den myndighet regeringen bestämmer att få meddela föreskrifter om sådana avgifter.

Regeringen anser i likhet med utredningen att det inte bör införas någon författningsreglerad avgiftsfinansiering för verksamhet som bedrivs av privata organ för bedömning av överensstämmelse. Dessa organ bedriver verksamhet på en marknad och avgiften för utfärdande av ett cybersäkerhetscertifikat bör bestämmas i konkurrens mellan berörda aktörer.

7 Tillsynsbefogenheter

7.1 Rätt att få tillträde till lokaler och handräckning av Kronofogdemyndigheten

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Vid handräckning ska bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande tillämpas. Om den nationella myndigheten för cybersäkerhetscertifiering begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Kronofogdemyndigheten* och *Transportstyrelsen* anser att utredningens lagförslag bör förtydligas så att det framgår med stöd av vilka bestämmelser som Kronofogdemyndighetens biträde ska lämnas. Transportstyrelsen anser också att det i bestämmelsen bör anges att rätten till tillträde till lokal av integritetsskäl inte bör gälla om lokalen utgör en bostad. S*katteverket* ifrågasätter nödvändigheten att ge rätt till tillträde med hjälp av Kronofogdemyndigheten i alla förekommande fall. *Svenska journalistförbundet* anser att det bör införas en bestämmelse om begränsning av den nationella myndigheten för cybersäkerhetscertifierings rätt till tillgång till uppgifter som omfattas av journalisters tystnadsplikt motsvarande det beslagsförbud som finns i 27 kap. 2 § rättegångsbalken.

Skälen för regeringens förslag: Av artikel 58.8 d i EU:s cybersäkerhetsakt följer att den nationella myndigheten för cybersäkerhetscertifiering ska ha rätt att få tillgång till alla lokaler hos organ för bedömning av överensstämmelse eller innehavare av ett europeiskt cybersäkerhetscertifikat i syfte att genomföra utredningar i enlighet med unionsrätten eller medlemsstaternas processrätt.

Tillsynsobjekten är tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som är innehavare av cybersäkerhetscertifikat samt organ för bedömning av överensstämmelse. För att tillsyn ska kunna

bedrivas på ett effektivt sätt är det nödvändigt att den nationella myndigheten för cybersäkerhetscertifiering får vidta vissa undersökningar av de lokaler som de får tillträde till och till det som påträffas där. Alla sådana undersökningar måste dock begränsas till det som är nödvändigt för att tillsynen ska kunna genomföras och måste vara inriktade enbart på sådant som har relevans för tillsynen av efterlevnaden av bestämmelserna i EU:s cybersäkerhetsakt. Proportionalitetsprincipen ska beaktas innan myndigheten begär tillträde och gör undersökningar.

Om verksamhetsutövaren vägrar att ge den nationella myndigheten för cybersäkerhetscertifiering tillträde till en lokal för bör den nationella myndigheten för cybersäkerhetscertifiering kunna begära biträde av Kronofogdemyndigheten för att få tillgång till en lokal för att kunna kontrollera handlingar, utrustning och verksamheten på plats.

Som *Kronofogdemyndigheten* och *Transportstyrelsen* uppmärksammar bör det tydligt anges med stöd av vilka bestämmelser Kronofogdemyndighetens biträde ska lämnas och att rätten till tillträde till lokal av integritetsskäl inte bör gälla om lokalen utgör en bostad. Regeringen föreslår att lagtexten utformas i enlighet med detta.

Skatteverket ifrågasätter nödvändigheten att ge rätt till tillträde med hjälp av Kronofogdemyndigheten i alla förekommande fall.

Den nationella myndigheten för cybersäkerhetscertifiering måste i sin tillsynsverksamhet beakta proportionalitetsprincipen, som kommer till uttryck i bl.a. 5 § tredje stycket förvaltningslagen (2017:900). Det innebär att de åtgärder som myndigheten vidtar aldrig får vara mer långtgående än vad som behövs och får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot. Regeringen anser därför inte att det finns anledning att i den föreslagna bestämmelsen införa ytterligare begränsningar i rätten att få tillträde till lokaler med biträde av Kronofogdemyndigheten.

Svenska journalistförbundet anser att det bör införas en bestämmelse om begränsning av den nationella myndigheten för cybersäkerhetscertifierings rätt till tillgång till uppgifter som omfattas av journalisters tystnadsplikt motsvarande det beslagsförbud som finns i 27 kap. 2 § rättegångsbalken.

Bestämmelser om s.k. källskydd i journalistisk verksamhet finns i bl.a. tryckfrihetsförordningen. Enligt 1 kap. 1 § tredje stycket tryckfrihetsförordningen står det var och en fritt att meddela uppgifter och underrättelser i vilket ämne som helst till bl.a. journalister och tidningsredaktioner för offentliggörande i tryckta skrifter m.m. En meddelare har rätt att vara anonym (3 kap. 1 § tryckfrihetsförordningen). Den som har tagit emot en uppgift för publicering har, med vissa undantag, tystnadsplikt beträffande meddelarens identitet (3 kap. 3 § tryckfrihetsförordningen). Den nationella myndigheten för cybersäkerhetscertifierings befogenheter avgränsas av att de endast får utövas för fullgörandet av de uppgifter som myndigheten har enligt EU:s cybersäkerhetsakt och den nya lagen.

Regeringen anser att det inte finns något hinder mot att beakta nationella bestämmelser om t.ex. anonymitetsskydd, efterforskningsförbud och tystnadsplikt inom ramen för det europeiska systemet för cybersäkerhetscertifiering. Skyldigheten att tillhandahålla den nationella myndigheten för cybersäkerhetscertifiering information begränsas således av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Eftersom det

följer redan av principen om att grundlag har företräde framför vanlig lag, behöver detta inte anges särskilt i den nya lagen.

7.2 Befogenhet att besluta om förelägganden som får förenas med vite

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för att EU:s cybersäkerhetsakt, de genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, den nya lagen och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Enligt artikel 58.8 c i EU:s cybersäkerhetsakt ska varje nationell myndighet för cybersäkerhetscertifiering ha rätt att vidta lämpliga åtgärder, i enlighet med nationell rätt, för att säkerställa att den som utfärdar en EU-försäkran om överensstämmelse eller utfärdar eller innehar ett europeiskt cybersäkerhetscertifikat uppfyller kraven i EU:s cybersäkerhetsakt eller en europeisk ordning för cybersäkerhetscertifiering.

Regeringen anser i likhet med utredningen att detta bör säkerställas genom att det i den nya lagen införs en ordning som innebär att den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för att EU:s cybersäkerhetsakt, de genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, den nya lagen och föreskrifter som har meddelats i anslutning till lagen ska följas. Vidare föreslås att sådana beslut om föreläggande ska få förenas med vite.

Enligt *Lagrådet* bör det klargöras om avsikten är att ett föreläggande ska kunna riktas mot någon som saluför en produkt som certifierad, trots att något certifikat inte finns. Regeringen konstaterar att artikel 58.8 c i EU:s cybersäkerhetsakt, som bestämmelsen i den nya lagen genomför, inte uttryckligen tar sikte på den situationen. Det bör lämpligen överlämnas till rättstillämpningen att avgöra om frågan faller inom tillämpningsområdet för den nu aktuella regleringen eller om det finns annan lagstiftning, t.ex. på konsumentskyddsområdet, som kan vara tillämplig.

7.3 Omedelbar verkställighet och inhibition

Regeringens bedömning: Det behövs inte några särskilda bestämmelser om att beslut av den nationella myndigheten för cybersäkerhetcertifiering får verkställas omedelbart eller om inhibition av sådana beslut.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Förvaltningsrätten i Stockholm* anser att det av effektivitetsskäl bör övervägas att i den nya lagen införa en särskild

bestämmelse om att tillsynsmyndigheten får bestämma att ett beslut om föreläggande ska gälla omedelbart. Övriga remissinstanser yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning: Om den nationella myndigheten för cybersäkerhetscertifiering konstaterar att det finns skäl att ingripa genom beslut om föreläggande kan det finnas behov att beslutet ska kunna verkställas omedelbart. Så kan exempelvis vara fallet om myndigheten beslutar att ett förfarande eller en verksamhet inte får fortsätta. Omedelbar verkställighet av ett sådant beslut kan förhindra eller minska sårbarheter och risken för skador. Även andra beslut av myndigheten kan behöva verkställas omedelbart. Skälet för detta kan vara att det annars finns en risk för att syftet med beslutet inte uppnås. Det gäller till exempel beslut som rör tillträde till lokaler för att genomföra undersökningar.

I 35 § förvaltningslagen finns bestämmelser om när en myndighets beslut får verkställas. Utgångspunkten är att ett beslut som får överklagas inom en viss tid får verkställas när överklagandetiden har gått ut, om beslutet inte har överklagats. Ett beslut får dock i vissa fall verkställas omedelbart. Det gäller till exempel om ett väsentligt allmänt eller enskilt intresse kräver det. Myndigheten ska dock först noga överväga om det finns skäl att avvakta med att verkställa beslutet på grund av att beslutet medför mycket ingripande verkningar för någon enskild, att verkställigheten inte kan återgå om ett överklagande av beslutet leder till att det upphävs, eller någon annan omständighet.

Regeringen anser att detta är en lämplig och effektiv ordning även i fråga om den nationella myndigheten för cybersäkerhetscertifierings beslut. Någon särskild bestämmelse av det slag som *Förvaltningsrätten i Stockholm* efterfrågar bör därför inte införas.

En domstol som ska pröva ett överklagande av ett förvaltningsbeslut som gäller omedelbart kan förordna att det överklagade beslutet tills vidare inte ska gälla, s.k. inhibition. Möjligheten till inhibition innebär att risken för att en aktör drabbas av skada på grund av ett felaktigt beslut av den nationella myndigheten för cybersäkerhetscertifiering minimeras. Bestämmelser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291). Någon särskild bestämmelse om inhibition behöver därför inte tas in i den nya lagen.

7.4 Tillsynsbefogenheter i övrigt

Regeringens bedömning: Kompletterande bestämmelser om tillsynsbefogenheter i övrigt behöver inte regleras i lag.

Utredningens bedömning överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Enligt artikel 58.8 i EU:s cybersäkerhetsakt kan den nationella myndigheten för cybersäkerhetscertifiering begära att utfärdare av en EU-försäkran om överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och organ för bedömning av överensstämmelse ska lägga fram alla uppgifter som myndigheten behöver för att kunna fullgöra sin uppgift (punkten a). Myndigheten har också befogenhet att genomföra undersökningar, i form

av kontroller, av utfärdare av en EU-försäkran om överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och organ för bedömning av överensstämmelse för att kunna verifiera överensstämmelse med bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering (punkten b).

Regeringen instämmer i utredningens bedömning att det inte behöver införas några kompletterande bestämmelser i lag om den nationella myndigheten för cybersäkerhetscertifierings befogenheter enligt bestämmelserna i artikel 58.8 a och b.

7.5 Samma tillsynsbefogenheter med stöd av den nya lagen som enligt EU:s cybersäkerhetsakt

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering ska ha de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt även vid tillsynen över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Ett fungerande europeiskt system för cybersäkerhetscertifiering förutsätter att nationella bestämmelser införs som kompletterar EU:s cybersäkerhetsakt. Tillsynen över regelverket bör lämpligen omfatta att såväl bestämmelserna i EU:s cybersäkerhetsakt som de kompletterande nationella bestämmelserna följs. För att tillsynsverksamheten ska kunna bedrivas på ett effektivt och ändamålsenligt sätt bör de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering har enligt artikel 58.8 i EU:s cybersäkerhetsakt gälla även vid tillsyn enligt den nya lagen och föreskrifter som har meddelats i anslutning till lagen.

Regeringen föreslår i likhet med utredningen att en bestämmelse om detta förs in i den nya lagen.

7.6 Återkallelse av europeiska cybersäkerhetscertifikat

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i akten eller en europeisk ordning för cybersäkerhetscertifiering.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Enligt artikel 58.8 e i EU:s cybersäkerhetsakt får en nationell myndighet för cybersäkerhetscertifiering, i enlighet med nationell rätt, återkalla europeiska cybersäker-

hetscertifikat som har utfärdats av den myndigheten eller organ för bedömning av överensstämmelse i enlighet med artikel 56.6, om sådana certifikat inte uppfyller kraven i akten eller en europeisk ordning för cybersäkerhetscertifiering. IKT-produkter, IKT-tjänster och IKT-processer som har certifierats enligt en europeisk ordning för cybersäkerhetscertifiering, som antagits enligt artikel 49, ska förutsättas överensstämma med kraven i en sådan ordning (artikel 56.1).

Av artikel 56.4 framgår att de organ för bedömning av överensstämmelse som avses i artikel 60 får utfärda europeiska cybersäkerhetscertifikat i enlighet med vad som anges i artikeln och som avser assuransnivå ”grundläggande” eller ”betydande” Genom undantag från punkten 4, och när en europeisk ordning för cybersäkerhetscertifiering föreskriver det, får ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen utfärdas endast av ett offentligt organ. Ett sådant organ ska antingen vara en nationell myndighet för cybersäkerhetscertifiering som avses i artikel 58.1 eller ett offentligt organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 60.1 (artikel 56.5).

Om en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 kräver assuransnivå ”hög” ska det europeiska cybersäkerhetscertifikatet endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller, efter bemyndigande av den myndigheten, av ett organ för bedömning av överensstämmelse. Detta får ske först efter antingen ett förhandsgodkännande av myndigheten för varje enskilt europeiskt cybersäkerhetscertifikat eller efter en allmän delegering på förhand av uppgiften att utfärda ett sådant europeiskt cybersäkerhetscertifikat till organet för bedömning av överensstämmelse (artikel 56.6).

Som utredningen föreslår bör det i den nya lagen införas en bestämmelse som ger den nationella myndigheten för cybersäkerhetscertifiering rätt att återkalla cybersäkerhetscertifikat som myndigheten eller ett organ för bedömning av överensstämmelse som ackrediterats enligt artikel 60.1 har utfärdat och som inte längre uppfyller kraven i EU:s cybersäkerhetsakt eller en europeisk ordning för cybersäkerhetscertifiering.

Regeringen anser att det bör överlämnas till rättstillämpningen att utveckla närmare praxis i fråga om sådan återkallelse.

8 Sanktioner

8.1 Straffrättsliga sanktioner bör inte införas

Regeringens bedömning: Det bör inte införas straffrättsliga sanktioner för överträdelser av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Transportstyrelsen* är tveksam till bedömningen att det inte finns tillräckliga skäl att införa straffrättsliga sanktioner med hänsyn till att de produkter, tjänster och processer som omfattas av

cybersäkerhetscertifiering kan förväntas utgöra kritiska komponenter för landets försvars- och krishanteringsförmåga. Övriga remissinstanser yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning: I artikel 58.8 f i EU:s cybersäkerhetsakt anges att varje nationell myndighet för cybersäkerhetscertifiering ska utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör. Vidare föreskrivs i artikel 65 att medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla reglerna och åtgärderna samt ändringar av dessa utan dröjsmål till kommissionen.

EU:s cybersäkerhetsakt reglerar inte frågan om vilka typer av sanktioner som bör finnas eller i vilka fall som en sanktionsavgift bör tas ut av den som inte följer bestämmelserna i ramverket för cybersäkerhetscertifiering.

Kriminalisering som metod att förhindra överträdelse av olika normer i samhället bör användas med försiktighet och bör inte komma i fråga om det finns någon alternativ metod som är tillräckligt effektiv för att komma till rätta med det oönskade beteendet.

Regeringens förslag om den nationella myndigheten för cybersäkerhetscertifierings ansvar för tillsyn och befogenheter innebär att myndigheten får effektiva verktyg i arbetet med att motverka brister i fråga om cybersäkerhetscertifiering.

Mot den bakgrunden, och med hänsyn till möjligheten att införa administrativa sanktioner, anser regeringen – i likhet med utredningen – att det inte bör införas några bestämmelser som innebär straffrättsliga sanktioner vid överträdelser av det europeiska ramverket för cybersäkerhetscertifiering.

8.2 Ett system med administrativa sanktionsavgifter

Regeringens förslag: Den nationella myndigheten för cybersäkerhetscertifiering ska kunna besluta om sanktionsavgifter för vissa överträdelser av EU:s cybersäkerhetsakt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Ett system med administrativa sanktionsavgifter används ofta för att enkelt och snabbt beivra regelöverträdelser. Sanktionsavgifter bör tas ut endast när det gäller lätt konstaterbara överträdelser för vilka utredningsinslaget är begränsat. Ansvaret är således vanligtvis strikt i dessa fall. Sanktionsavgifter bör drabba alla som överträder reglerna lika och avgiften bör vara anpassad till överträdelsen enligt schabloner.

Regeringen anser att införandet av en ordning med administrativa sanktionsavgifter för vissa överträdelser av EU:s cybersäkerhetsakt är såväl lämpligt som ändamålsenligt. Som utredningen framhåller kan en

sådan ordning antas medföra såväl ökad följsamhet till som färre överträdelser av regelverket. En annan konsekvens av införandet av ett sanktionssystem bör också bli att konsumenternas förtroende för branschen på sikt kan öka, vilket ligger i det allmännas intresse.

En sådan ordning utgör också ett lämpligt komplement till den möjlighet att få besluta förelägganden, som får förenas med vite, som behandlas i avsnitt 7.2.

Regeringen föreslår därför, i likhet med utredningen, att det i den nya lagen införs bestämmelser om att den nationella myndigheten för cybersäkerhetscertifiering ska kunna besluta om sanktionsavgifter för vissa överträdelser av EU:s cybersäkerhetsakt.

8.3 Överträdelser som ska leda till sanktionsavgift

Regeringens förslag: Sanktionsavgift ska tas ut av den som

1. har utfärdat en EU-försäkran om överensstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,
2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. har utfärdat en EU-försäkran om överensstämmelse eller innehar ett cybersäkerhetscertifikat och inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering,
6. överträder ett beslut av den nationella myndigheten för cybersäkerhetscertifiering om föreläggande som innebär ett förbud, eller
7. använder ett europeiskt cybersäkerhetscertifikat som blivit återkallat enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Kammarrätten i Stockholm* och *Transportstyrelsen* anser att utredningens förslag i denna del är delvis oklart och bör förtydligas.

Skälen för regeringens förslag

Utgångspunkter

Det europeiska ramverket för cybersäkerhetscertifiering utgörs av EU:s cybersäkerhetsakt och de europeiska ordningar för cybersäkerhetscertifiering som kommer att utfärdas med stöd av akten. Det är ett

omfattade och komplext regelsystem. Som utredningen anför bör endast mer allvarliga, tydliga och avgränsade överträdelser leda till att den nationella myndigheten för cybersäkerhetscertifiering beslutar om sanktionsavgift. Utgångspunkterna vid övervägande av vilka överträdelser bör omfattas av sanktionsavgift bör i första hand vara syftet med regleringen, vikten av att bestämmelserna efterlevs och de skador som kan bedömas uppkomma vid överträdelser. Flertalet aktörer som kommer att vara verksamma på marknaden för cybersäkerhetscertifiering är vinstdrivande företag som verkar i konkurrens med varandra. Sanktionssystemet behöver därför också utformas på ett sätt som kan antas ge aktörerna tillräckliga skäl att följa de krav som uppställs och därmed undvika risken att drabbas av sanktionsavgift.

Regeringen delar utredningens bedömning att överträdelser av EU:s cybersäkerhetsakt och de skyldigheter som följer av en europeisk ordning för cybersäkerhetscertifiering ska – oavsett om det är fråga om en frivillig eller obligatorisk certifiering – kunna föranleda att en sanktionsavgift beslutas.

När det gäller frågan om vilka överträdelser som bör kunna föranleda beslut om sanktionsavgift, är det viktigt att det är tydligt vilka överträdelser som avses och vem en sanktionsavgift ska kunna tas ut av. Det europeiska ramverket för cybersäkerhetscertifiering innebär att det i de europeiska ordningarna för cyberhetsäkerhetscertifiering kommer att införas ytterligare och mer specifika bestämmelser som gäller vid certifiering av en produkt, tjänst eller process enligt den aktuella ordningen. De europeiska ordningarna för cybersäkerhetscertifiering kan därför förväntas bidra till en ökad tydlighet i fråga om de överträdelser som kan föranleda beslut om sanktionsavgift.

Regeringen anser därför inte att det finns skäl att justera utredningens lagförslag i denna del på det sätt som *Kammarrätten i Stockholm* och *Transportstyrelsen* efterfrågar.

Utfärdande av en EU-försäkran om överensstämmelse i strid med villkor i en europeisk ordning för cybersäkerhetscertifiering

Tillverkaren eller leverantören av en IKT-produkt, IKT-tjänst eller IKT-process får under vissa förutsättningar utfärda en EU-försäkran om överensstämmelse. Genom att upprätta en sådan försäkran tar tillverkaren eller leverantören ansvar för att produkten, tjänsten eller processen överensstämmer med den tillämpliga europeiska ordningen för cybersäkerhetscertifiering (artikel 53.2). I dessa fall görs det alltså inte någon oberoende prövning av om IKT-produkten, IKT-tjänsten eller IKT-processen i fråga uppfyller de krav som anges i den tillämpliga europeiska ordningen för cybersäkerhetscertifiering. Det är viktigt att ansvarig tillverkare eller leverantör ges tydliga incitament att säkerställa att de villkor som gäller är uppfyllda. I annat fall finns det en risk att IKT-produkter, IKT-tjänster och IKT-processer marknadsförs under angivande att de uppfyller vissa säkerhetskrav som de inte uppfyller. Det kan i sin tur medföra säkerhetsrisker och orsaka skador i de verksamheter som IKT-produkten, IKT-tjänsten eller IKT-processen används i. Det riskerar också äventyra tilliten till det europeiska systemet för cybersäkerhetscertifiering. Som utredningen föreslår bör en sanktionsavgift därför kunna tas ut av en

tillverkare eller leverantör som har utfärdat en EU-försäkran om överenstämmelse trots att kraven enligt den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-produkten inte är uppfyllda.

Enligt lagrådsremissens förslag skulle sanktionsavgift även tas ut om kraven enligt EU:s cybersäkerhetsakt inte är uppfyllda. Som *Lagrådet* påpekar motsvarar detta dock inte innehållet i artikel 53.2 i EU:s cybersäkerhetsakt. Lagtexten bör därför förtydligas och även justeras i sak i enlighet med Lagrådets förslag.

Bristande fullgörelse av uppgiftsskyldigheten

Den fysiska eller juridiska person som ansöker om att få sin produkt, tjänst eller process certifierad av ett organ för bedömning av överensstämmelse är skyldig att göra all information som krävs för att genomföra certifieringen tillgänglig (artikel 56.7). De uppgifter som tillverkaren eller leverantören lämnar ligger till grund för bedömningen om ett cybersäkerhetscertifikat ska utfärdas eller inte. Det förutsätts att de uppgifter som lämnas är korrekta. Felaktiga uppgifter eller underlåtelse att lämna uppgifter kan medföra att certifikat utfärdas på felaktiga grunder. De konsekvenser och risker som felaktigt utfärdade certifikat medför är desamma som vid felaktigt utfärdande av en EU-försäkran om överensstämmelse. En överträdelse som innebär att någon har lämnat oriktiga eller ofullständiga uppgifter vid ansökan om certifiering bör därför medföra att en sanktionsavgift får tas ut. Som *Kammarrätten i Stockholm* anför bör det av bestämmelsen framgå att sanktionsavgift endast får beslutas om uppgifterna som har lämnats är av betydelse.

Förslaget i lagrådsremissen innehöll en hänvisning till artikel 56.7 i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering. *Lagrådet*, som uppmärksammar bl.a. att det i artikel 56.7 inte finns någon reglering av ansökan, anser att det saknas skäl att i aktuell bestämmelse föreskriva var ansökan om cybersäkerhetscertifiering regleras och lämnar ett förslag på justering av lagtexten. Regeringen följer Lagrådets förslag.

Innehavare av ett europeiskt cybersäkerhetscertifikat har vidare en skyldighet att informera den myndighet eller det organ som avses artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen (artikel 56.8). Om uppgiftsskyldigheten inte fullgörs bör en sanktionsavgift kunna tas ut av innehavaren av certifikatet.

Även en tillverkare eller leverantör som har utfärdat en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt bör betala en sanktionsavgift. I likhet med *Kammarrätten i Stockholm* anser regeringen att det av lagtexten bör framgå att sanktionsavgift endast bör kunna beslutas om denna brist medför en ökad risk för sårbarhet eller skada.

Överträdelse av villkor

För att säkerställa ett enhetligt europeiskt system för cybersäkerhetscertifiering och uppnå syftet med en hög nivå av cybersäkerhet i unionen är det av avgörande betydelse att de villkor som uppställs enligt ramverket efterlevs, såsom villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat samt villkor för utvidgning eller inskränkning av tillämpningsområdet för certifiering. De europeiska ordningarna för cybersäkerhetscertifiering som kommer att beslutas med stöd av EU:s cybersäkerhetsakt kan förväntas innehålla sådana villkor. En sanktionsavgift bör därför, som *Lagrådet* föreslår, kunna tas ut av den som bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat samt villkor för utvidgning eller inskränkning av tillämpningsområdet för certifiering.

Överträdelse av förbud

Enligt regeringens förslag ska den nationella myndigheten för cybersäkerhetscertifiering ha möjlighet att besluta förelägganden, som får förenas med vite (avsnitt 7.2). Sådana beslut om förelägganden kan riktas mot tillverkare, leverantörer och organ för bedömning av överensstämmelse.

Ett beslut om föreläggande som innebär ett förbud kan antas typiskt sett komma i fråga vid de allvarligaste fallen av bristande följsamhet av regelverket för cybersäkerhetscertifiering eller vid upprepade överträdelser. En sanktionsavgift bör därför kunna tas ut av den som överträder ett beslut om ett sådant förbud. En sanktionsavgift bör dock inte få beslutas om överträdelsen omfattas av ett föreläggande, som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet. Lagtexten bör utformas i enlighet med detta.

Användande av cybersäkerhetscertifikat som har återkallats

Den nationella myndigheten för cybersäkerhetscertifiering ska ha befogenhet att, i enlighet med nationell rätt, besluta att återkalla ett cybersäkerhetscertifikat som har utfärdats av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överenstämmelse i enlighet med artikel 56.6 om sådana certifikat inte uppfyller kraven EU:s cybersäkerhetsakt eller en europeisk ordning för cybersäkerhetscertifiering (artikel 58.8 e). Regeringens förslag innebär att den nationella myndigheten för cybersäkerhetscertifiering ska ha den befogenheten.

De cybersäkerhetscertifikat som får återkallas med stöd av bestämmelserna är sådana som har utfärdats av den nationella myndigheten för cybersäkerhetscertifiering eller av ett organ för bedömning av överensstämmelse med stöd av en europisk ordning för cybersäkerhetscertifiering som kräver assuransnivå hög. Det är angeläget att certifikat för varor, tjänster och processer som har återkallats inte fortsatt används på marknaden. Detta gör sig särskilt gällande i fråga om varor, tjänster och processer som har certifierats på assuransnivå hög eftersom det kan antas att sådana varor, tjänster och processer används i säkerhetskänslig verksamhet. En sanktionsavgift bör därför kunna tas ut

av en tillverkare eller leverantör som använder ett cybersäkerhetscertifikat som har återkallats.

Som *Lagrådet* anför bygger certifieringen inom unionen på att ett certifikat som har utfärdats av en behörig myndighet inom unionen gäller inom den inre marknaden. Därmed följer också att en återkallelse som en sådan myndighet beslutar innebär att certifikatet inte längre gäller inom denna marknad. Regeringen gör bedömningen att en sanktionsavgift enligt den nya lagen därför bör kunna tas ut av den som i Sverige använder ett certifikat som har återkallats av en nationell myndighet för cybersäkerhetscertifiering i en annan medlemsstat. Det bör överlämnas till rättstillämpningen att utveckla närmare praxis i fråga om återkallelse i en sådan situation.

Vem ska sanktionsavgiften tas ut av?

I EU:s cybersäkerhetsakt regleras inte närmare vilka som ska kunna drabbas av sanktioner. Sanktionsavgifter kan användas både mot juridiska och fysiska personer. Sanktionsavgift ska tas ut av den som gör sig skyldig till någon av de överträdelser som anges i lagen. En avgift kan därför tas ut av den som utfärdar en EU-försäkran eller den som utfärdar eller innehar ett europeiskt cybersäkerhetscertifikat och gör sig skyldig till en överträdelse på sätt som anges i bestämmelsen. En sanktionsavgift kan även tas ut av en statlig myndighet, vars verksamhet omfattas av regleringen.

8.4 Beslut om sanktionsavgift i samtliga fall

Regeringens förslag: Det ska vara obligatoriskt att besluta om sanktionsavgift vid överträdelser av regelverket. Det ska gälla strikt ansvar vid sådana överträdelser.

Den nationella myndigheten för cybersäkerhetscertifiering ska besluta om sanktionsavgift.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Sveriges advokatsamfund* anser att det inte finns skäl att införa en ordning med strikt ansvar. Övriga remissinstanser instämmer i utredningens förslag eller yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Det ska gälla strikt ansvar för överträdelser

System med sanktionsavgifter bygger typiskt sett på principen om strikt ansvar. Strikt ansvar innebär att varken uppsåt eller oaktsamhet är ett krav för att ta ut sanktionsavgift. Det räcker att en bestämmelse har överträtts. Regeringen håller med utredningen om att det inte finns skäl att avvika från grundprincipen för sanktionsavgifter att ansvaret ska vara strikt. Det är framförallt den omständigheten att det inte behöver bevisas att ett visst handlande har varit avsiktligt eller avgöras hur oaktsamt handlandet varit som gör en sådan ordning effektiv. Det är också svårt att se att överträdelser i normalfallet kan bero på annat än uppsåt eller oaktsamhet.

Regeringen anser alltså, i likhet med utredningen, men till skillnad från *Sveriges advokatsamfund*, att en ordning ska införas som innebär att överträdelser av det europeiska ramverket för cybersäkerhetscertifiering bygger på strikt ansvar.

Det ska vara obligatoriskt att ta ut sanktionsavgift

En fråga är om det bör vara obligatoriskt att ta ut sanktionsavgift när en viss bestämmelse har överträtts. Sanktionsavgifter bör, som anförs ovan, tas ut endast till följd av lätt konstaterbara överträdelser för vilka utredningsinslaget är begränsat. Ansvaret är således vanligtvis strikt i dessa fall, men andra varianter förekommer. Som regeringen anför i propositionen Informationssäkerhet för samhällsviktiga och digitala tjänster bör tillsynsmyndighetens möjligheter till mer skönsmässiga bedömningar som utgångspunkt vara begränsade med hänsyn till behovet av likabehandling, objektivitet och proportionalitet (prop. 2017/18:205 s. 69 och 70). Regelverket om cybersäkerhetscertifiering kan dock vara komplext, och innebära en resurskrävande hantering för tillsynsmyndigheten. Regeringen anser i likhet med utredningen att övervägande skäl talar för att det på det nu aktuella området bör vara obligatoriskt att besluta om sanktionsavgift när förutsättningarna för detta är uppfyllda. Detta minskar utrymmet för skönsmässiga bedömningar av den nationella myndigheten för cybersäkerhetscertifiering och framstår även som mest ändamålsenligt vid mer allvarliga överträdelser av regelverket.

Den nationella myndigheten för cybersäkerhetscertifiering ska besluta om sanktionsavgift

Regeringen anser i likhet med utredningen att såväl ändamålsskäl som effektivitetsskäl talar för att det bör vara den nationella myndigheten för cybersäkerhetscertifiering som ska besluta om sanktionsavgift. Regeringen föreslår att bestämmelser om detta införs i den nya lagen.

8.5 Ramarna för sanktionsavgiftens storlek

Regeringens förslag: En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Skatteverket* anser att sanktionsavgiftens storlek bör baseras på aktörens förutsättningar i likhet med vad som gäller enligt EU:s dataskyddsförordning. Övriga remissinstanser yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Sanktionsavgifter ska vara effektiva, proportionerliga och avskräckande. Det finns flera tänkbara alternativ i fråga om utformningen. Det kan t.ex. vara fråga om på förhand bestämda belopp eller beloppsintervall, som gäller oavsett vem som begått överträdelsen, eller som är kopplade till t.ex. årsomsättning i näringsverksamhet.

Överträdelser av det europeiska ramverket för cybersäkerhetscertifiering bedöms kunna påverka samhällsviktig verksamhet och även

leda till allvarlig skada för Sveriges säkerhet. Därför bör maximibeloppet sättas så högt att det får en tillräckligt avskräckande effekt.

Bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering kommer att omfatta såväl myndigheter som företag. Aktörerna kommer dock att skilja sig mycket från varandra vad gäller t.ex. storlek och ekonomiska förutsättningar. Detta innebär att vad som upplevs som en avhållande avgift av en aktör med måttliga ekonomiska resurser kan framstå som i det närmaste obetydlig för en aktör med stora resurser. Skillnaderna kommer att finnas mellan olika aktörer, när det gäller företag, i olika branscher och mellan företag inom samma bransch.

De aktörer som omfattas av bestämmelserna är både myndigheter, företag och enskilda. Regeringen anser därför inte att det är lämpligt att koppla sanktionsavgiften till aktörens förutsättningar såsom *Skatteverket* föreslår. Ett system med bestämda beloppsintervall är i stället att föredra (jfr bedömningen i prop. 2017/18:205 s. 70 och 71).

För att sanktionsavgifterna ska vara effektiva, proportionerliga och avskräckande bör intervallet för sanktionsavgiften vara förhållandevis stort. Den nationella myndigheten för cybersäkerhetscertifiering får då möjlighet att göra en nyanserad bedömning när avgiftens storlek ska bestämmas.

När det gäller bestämmandet av ett lämpligt beloppsintervall kan en jämförelse göras med de belopp som kan komma ifråga vid allvarliga överträdelser av bl.a. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, dvs. högst tio miljoner kronor. En sådan avgift har av regeringen bedömts utgöra en effektiv, proportionell och avskräckande sanktion mot allvarliga överträdelser (se prop. 2017/18:205 s. 71).

Mot denna bakgrund, och med beaktande av förekomsten av stora globala aktörer på IKT-marknaden, anser regeringen, i likhet med utredningen, att det högsta beloppet för en sanktionsavgift enligt den föreslagna lagen bör bestämmas till 15 000 000 kronor. Det lägsta beloppet bör lämpligen bestämmas till 10 000 kronor då bl.a. fysiska personer kan vara innehavare av europeiska cybersäkerhetscertifikat. Det breda intervallet motiveras också av det kan röra sig om vitt skilda typer av överträdelser. Om exempelvis en enskild lämnar bristfälliga eller ofullständiga uppgifter vid ansökan om cybersäkerhetscertifiering bör detta i många fall kunna bedömas som mindre allvarligt, medan allvarliga brister i cybersäkerhetskrav i produkter, tjänster och processer som kan skada samhällsviktig verksamhet bör bedömas strängare.

8.6 Sanktionsavgiftens storlek i det enskilda fallet

Regeringens förslag: När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas dels till den skada eller risk för skada som har uppkommit till följd av överträdelsen, dels till om den som har begått överträdelsen tidigare begått en överträdelse och dels till den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens förslag innebär att särskild hänsyn ska tas till de kostnader som har undvikits och inte, som regeringen föreslår, till den vinst som har gjorts.

Remissinstanserna: *Trafikverket* anser att det bör förtydligas i vilken utsträckning sanktionsavgifter kan åläggas vid upprepade förseelser. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: När storleken på sanktionsavgiften ska bestämmas i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. Som utredningen anför är det inte möjligt att i den nya lagen ange samtliga relevanta omständigheter som kan behöva beaktas i enskilda fall. Den nya lagen bör i stället innehålla en bestämmelse som anger sådana omständigheter som särskilt bör beaktas.

Regeringen instämmer i utredningens bedömning att särskild hänsyn bör tas till den skada eller risk för skada som uppstått till följd av överträdelsen och om den avgiftsskyldige tidigare begått en överträdelse. Utredningen föreslår att särskild hänsyn också ska tas till de kostnader som har undvikits till följd av överträdelsen. Regeringen anser dock att det är lämpligare att i stället ta särskild hänsyn till den ekonomiska fördel som överträdelsen har inneburit för den avgiftsskyldige. Liksom i lagen (2007:528) om värdepappersmarknaden kan detta i lagtexten uttryckas så att särskild hänsyn ska tas till den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

En försvårande omständighet som bör beaktas särskilt vid bedömningen av skadan eller risken för skada är om överträdelsen medför sårbarhet eller risk för skada på bl.a. samhällsviktig verksamhet eller säkerhetskänslig verksamhet. Värt att beakta särskilt är också om större konsumentskaror drabbats av överträdelsen. Exempel på omständigheter som kan komma att påverka beloppets storlek men inte behöver tas in i lagen är även hur länge överträdelsen pågått. Om den avgiftsskyldige tidigare gjort sig skyldig till överträdelse av lagen kan det bli aktuellt att beakta om överträdelserna är likartade samt den tid som har gått mellan de olika överträdelserna. Regeringen anser inte att det finns skäl att införa någon begränsning i fråga om antalet sanktionsavgifter som får beslutas i fråga om en viss aktör. Någon sådan bestämmelse som *Trafikverket* efterfrågar föreslås därför inte.

Vissa omständigheter kan det finnas anledning att beakta i mildrande riktning. I propositionen Effektiv bekämpning av marknadsmissbruk gjordes exempelvis bedömningen att det förhållandet att en aktör aktivt

samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelser kan vara en sådan omständighet samt om aktören snabbt har vidtagit rättelse (prop. 2016/17:22 s. 220 och 221).

Att avgiftsskyldigheten bygger på strikt ansvar innebär att det bör finnas en möjlighet för den nationella myndigheten för cybersäkerhetscertifiering att kunna besluta om jämkning av sanktionsavgift. En bestämmelse som ger myndigheten utrymme att i vissa fall sätta ned eller helt avstå från att ta ut någon sanktionsavgift bör därför införas. Regeringen anser att jämkning bör kunna ske om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Det kan exempelvis vara oskäligt att över huvud taget ta ut en avgift om den avgiftsskyldige redan har drabbats av en sanktionsavgift enligt något annat regelverk för i princip samma brist. Att regelverket har överträtts på ett sådant sätt att det varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller överträdelsen på annat sätt varit utom den avgiftsskyldiges kontroll, kan i undantagsfall göra överträdelsen ursäktlig och därför utgöra särskilda skäl för jämkning. Det kan också finnas grund för nedsättning när det rör sig om en bedömningsfråga, t.ex. vilka certifieringsåtgärder som är nödvändiga i ett visst sammanhang och berörd aktör trots en ingående granskning gjort en felaktig bedömning. Enligt regeringen kan det däremot inte anses oskäligt att ta ut en sanktionsavgift om överträdelsen exempelvis beror på att en aktör inte har känt till gällande rätt eller om överträdelsen har orsakats av försämrad ekonomi, tidsbrist eller bristande rutiner. Det bör överlämnas till rättstillämpningen att utveckla närmare praxis kring grunderna för jämkning.

Lagrådet anser att den föreslagna bestämmelsen om jämkning av sanktionsavgift i praktiken inte innebär något annat än ett integrerat moment i den bedömning som ligger till grund för ett beslut enligt bestämmelsen om sanktionsavgiftens storlek. Lagrådet lämnar därför ett förslag till justering av lagtexten i denna del, för att tydliggöra att det inte är fråga om ett särskilt beslut om nedsättning. Regeringen kan inte instämma i Lagrådets förslag, bl.a. eftersom det enligt regeringens mening skulle innebära en ändring i sak som inte är lämplig. Vidare finns det flera exempel på befintlig lagstiftning som har utformats på liknande sätt som enligt lagrådsremissens förslag utan att – såvitt känt – ha förorsakat tillämpningssvårigheter. Det framstår därför inte som ändamålsenligt att justera paragrafen med den förebild i fråga om utformningen som Lagrådet föreslår som alternativ.

Regeringen väljer därför att behålla lagrådsremissens förslag.

8.7 Hinder mot sanktionsavgift

Regeringens förslag: En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: I det sjunde tilläggsprotokollet till den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga) finns bestämmelser om rätten att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. dubbelbestraffningsförbudet. Begreppet straff i den mening som avses i Europakonventionen och EU:s rättighetsstadga anses omfatta vite, se propositionen Administrativa sanktioner på yrkesfiskets område (prop. 2007/08:107 s. 24) och propositionen Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna (prop. 2012/13:143 s. 69).

Om ett vite har dömts ut bör det därför inte vara möjligt att besluta om en sanktion – administrativ eller straffrättslig – för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer har ansetts vara när det inleds en domstolsprocess angående frågan om utdömande av vite (se prop. 2016/17:22 s. 228).

Ett beslut om föreläggande som har förenats vite bör därför inte hindra ett senare beslut om ingripande med sanktionsavgift så länge som den nationella myndigheten för cybersäkerhetscertifiering inte har ansökt om utdömande av vitet. När den nationella myndigheten för cybersäkerhetscertifiering har ansökt om utdömande av vitet bör myndigheten dock vara förhindrad att besluta om sanktionsavgift för en överträdelse som omfattas av vitesföreläggandet. En bestämmelse om detta bör tas in i den nya lagen.

Lagrådet väcker den mer principiella frågan om regleringen inte borde täcka också den situationen att frågan om vitesföreläggande aktualiseras efter ett beslut om att ta ut sanktionsavgift. Enligt regeringens mening motiverar den eventuella risken för en sådan tillämpning av det nu aktuella regelverket inte att innebörden av dubbelbestraffningsförbudet enligt Europakonventionen i en sådan situation behöver komma till särskilt uttryck i lagtexten.

8.8 Förfarandet vid beslut om sanktionsavgift

Regeringens förslag: En sanktionsavgift ska endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom denna tid, ska myndigheten lämna den obetalda avgiften för indrivning. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Sanktionsavgiften tillfaller staten.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Skatteverket* anser att preskriptionstiden bör räknas från identifikationstillfället med hänsyn till att det kan ta tid innan överträdelser upptäcks eller identifieras. Övriga remissinstanser yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Beslut om administrativa sanktionsavgifter är en ingripande åtgärd. I likhet med vad som gäller enligt bl.a. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster bör sådana beslut därför delges den betalningsskyldige enligt delgivningslagen (2010:1932). Som utredningen föreslår bör en bestämmelse om detta tas in i den nya lagen.

Enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster får sanktionsavgift inte beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom två år från överträdelsen. I förarbetena till lagen angav regeringen att en sådan gräns bör finnas på grund av sanktionsavgiftens ingripande natur (prop. 2017/18:205 s. 74). En motsvarande reglering finns i 5 kap. 14 § lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning Samma skäl gör sig gällande i fråga om sanktionsavgift för överträdelser av det europeiska ramverket för cybersäkerhetscertifiering.

En bortre tidsgräns för när en sanktionsavgift får beslutas bör finnas och regeringen anser att två år är en rimlig sådan gräns. Som *Skatteverket* anför kan det ta viss tid innan överträdelser av det europeiska regelverket för cybersäkerhetscertifiering upptäcks. Regeringen anser dock inte att det finns skäl att i det här fallet göra en annan bedömning i fråga om från vilken tidpunkt preskriptionstiden ska börja löpa än den som lagstiftaren har gjort på andra liknande områden. En bestämmelse med motsvarande innebörd som i de nyss nämnda lagarna bör därför införas i den föreslagna lagen. Liksom i andra liknande fall bör bevisbördan för att kommunikation har genomförts ligga på tillsynsmyndigheten (se prop. 2017/18:205 s. 74).

För att regleringen om sanktionsavgifter ska bli tillräckligt handlingsdirigerande och effektiv bör en sanktionsavgift som den nationella myndigheten för cybersäkerhetscertifiering har beslutat kunna drivas in utan att det krävs något domstolsavgörande (3 kap. 1 § första stycket 6 utsökningsbalken). Det bör i den nya lagen införas bestämmelser om att betalning av sanktionsavgift ska ske till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om sanktionsavgift vann laga kraft eller annars inom den längre tid som anges i beslutet. I lagen bör också regleras att myndigheten ska lämna den obetalda avgiften för indrivning om avgiften inte betalas inom denna tid.

Som utredningen föreslår bör en sanktionsavgift preskriberas i den utsträckning verkställighet inte har skett inom fem år.

Sanktionsavgiften bör tillfalla staten.

9 Organ för bedömning av överensstämmelse

9.1 Bestämmelser i EU:s cybersäkerhetsakt

Cybersäkerhetscertifikat enligt EU:s cybersäkerhetsakt kan utfärdas av privata och offentliga organ för bedömning av överensstämmelse samt av den nationella myndigheten för cybersäkerhetscertifiering. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008. En sådan ackreditering ska endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till EU:s cybersäkerhetsakt. Av bilagan framgår bl.a. att ett organ för bedömning av överensstämmelse ska vara en juridisk person.

Utgångspunkten är att de organ för bedömning av överensstämmelse som avses i artikel 60 i EU:s cybersäkerhetsakt ska utfärda europeiska cybersäkerhetscertifikat som avser assuransnivå ”grundläggande” eller ”betydande” på grundval av de kriterier som ingår i en europeisk ordning för cybersäkerhetscertifiering (artikel 56.4). Genom undantag från den bestämmelsen, och i vederbörligen motiverade fall, får en europeisk ordning för cybersäkerhetscertifiering föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen endast kan utfärdas av ett offentligt organ för bedömning av överensstämmelse. Ett sådant organ ska vara nationell myndighet för cybersäkerhetscertifiering eller ett offentligt organ som är ackrediterat som ett organ för bedömning av överensstämmelse enligt artikel 60.1.

Om en europeisk ordning för cybersäkerhetscertifiering kräver assuransnivå ”hög” ska europeiska cybersäkerhetscertifikat enligt den ordningen endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller, i följande fall, av ett organ för bedömning av överensstämmelse (artikel 56.6):

– Efter förhandsgodkännande av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse (artikel 56.6 a).
– Efter allmän delegering på förhand av uppgiften att utfärda ett sådant europeiskt cybersäkerhetscertifikat till ett organ för bedömning av överensstämmelse från den nationella myndigheten för cybersäkerhetscertifiering (artikel 56.6 b).

Om ett europeiskt cybersäkerhetscertifikat utfärdas av den nationella myndigheten för cybersäkerhetscertifiering enligt artiklarna 56.5 a och 56.6 ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som ett organ för bedömning av överensstämmelse (artikel 60.2).

Om de europeiska ordningarna för cybersäkerhetscertifiering innehåller särskilda eller ytterligare krav enligt artikel 54.1 f ska endast organ för bedömning av överensstämmelse som uppfyller dessa krav bemyndigas av

den nationella myndigheten för cybersäkerhetscertifiering att utföra uppgifter inom ramen för sådana ordningar (artikel 58.7 e och 60.3).

9.2 Ackreditering av organ för bedömning av överensstämmelse

9.2.1 Bestämmelser i EU:s cybersäkerhetsakt

Enligt artikel 60.1 ska organen för bedömning av överensstämmelse ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008. En sådan ackreditering ska endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till EU:s cybersäkerhetsakt. Ackrediteringen ska utfärdas till organen för bedömning av överensstämmelse för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse fortfarande uppfyller kraven som anges i artikel 60.

I bilagan till EU:s cybersäkerhetsakt framgår de krav ska organen för bedömning av överensstämmelse ska uppfylla. Bland annat uppställs följande krav:

- Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell rätt och vara en juridisk person.
- Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller de IKT-produkter, IKT-tjänster eller IKT-processer som det bedömer.
- Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för att utföra bedömningen av överensstämmelse får inte utgöras av den som konstruerar, tillverkar, levererar, installerar, köper, äger, använder eller underhåller den IKT-produkt, IKT-tjänst eller IKT-process som bedöms, eller de som företräder någon av dessa parter.
- Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får varken delta direkt i konstruktionen, tillverkningen, marknadsföringen, installationen, användningen eller underhållet av dessa IKT-produkter, IKT-tjänster eller IKT-processer som bedöms, eller företräda de parter som bedriver denna verksamhet.
- Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömningen av överensstämmelse. Det förbudet ska framför allt gälla konsulttjänster.
- Organen för bedömning av överensstämmelse ska också uppfylla de krav som anges i relevant standard som harmoniserats enligt förordning (EG) nr 765/2008 för ackreditering av organ för bedömning av överensstämmelse som utför certifiering av IKT-produkter, IKT-tjänster eller IKT-processer.

Det ställs också krav på bl.a. kompetens och teknisk expertis hos organen för bedömning av överensstämmelse (se bilagan till EU:s cybersäkerhetsakt).

9.2.2 Gällande regelverk om ackreditering

Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning nr 339/93 trädde i kraft den 1 januari 2010. EU-förordningen syftar till att underlätta den fria rörligheten för varor på EU:s inre marknad och samtidigt säkerställa en hög skyddsnivå för allmänna intressen som hälsa och säkerhet i allmänhet, hälsa och säkerhet på arbetsplatser, konsumentskydd och miljöskydd. Genom EU-förordningen har gemensamma bestämmelser och principer om ackreditering av organ för bedömning av överensstämmelse, t.ex. laboratorier, kontrollorgan och certifieringsorgan införts. EU-förordningen innehåller även regler om marknadskontroll, kontroll av produkter från tredje länder och CE-märkning. Genom lagen (2011:791) om ackreditering och teknisk kontroll har svensk rätt anpassats till EU-förordningen. Lagen och tillhörande förordning (2011:811) om ackreditering och teknisk kontroll uppställer krav för bl.a. ackreditering av organ för bedömning av överensstämmelse och hur bedömningar av överensstämmelse och rapportering av sådana ska göras. Den innehåller även bestämmelser om certifiering av anordningar, tillsyn och avgifter. Styrelsen för ackreditering och teknisk kontroll (Swedac) ansvarar, som nationellt ackrediteringsorgan, för ackreditering enligt EU-förordningen och ansvarar för övrig ackreditering av organ för bedömning av överensstämmelse. Swedac fattar beslut att utse anmälda organ för bedömning av överensstämmelse och fattar beslut att begränsa eller återkalla en sådan anmälan. Swedac utövar tillsyn över organ som avses i lagen samt har rätt att ta ut avgifter för att täcka kostnader för ackreditering, tillsyn och bedömning.

Bestämmelsen i artikel 60.1 i EU:s cybersäkerhetsakt om att organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008 innebär alltså att Swedac är den myndighet som ska ackreditera organ för bedömning av överenstämmelse enligt EU:s cybersäkerhetsakt.

9.2.3 Kompletterande bestämmelser om ackreditering

Regeringens förslag: I den nya lagen ska det upplysningsvis anges att bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering finns i artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till cybersäkerhetsakten samt att det i förordning (EG) nr 765/2008 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om krav för ackreditering av sådana organ.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: De flesta remissinstanser yttrar sig inte särskilt över förslaget. *Styrelsen för ackreditering och teknisk kontroll* (*Swedac)* anser att utredningens förslag innebär att Swedac och den nationella myndigheten för cybersäkerhetscertifiering kommer att ha tillsynsuppdrag som är delvis överlappande. Enligt Swedac bör förhållandet mellan tillsynsrollerna klargöras i det fortsatta arbetet.

Skälen för regeringens förslag

En upplysningsbestämmelse om vissa bestämmelser om ackreditering

I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till cybersäkerhetsakten finns det bestämmelser om krav på ackreditering och att organen för bedömning av överensstämmelse ska vara ackrediterade enligt förordning (EG) nr 765/2008. Även de europeiska ordningarna för cybersäkerhetscertifiering som kommer att utfärdas som genomförande akter kan komma att innehålla bestämmelser om ackreditering. I förordningen (EG) nr 765/2008 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse. Detta innebär att det vid cybersäkerhetscertifiering enligt det europeiska ramverket kommer att finnas bestämmelser om ackreditering i flera EU-rättsakter och på nationell nivå. I den nya lagen bör det införas en upplysningsbestämmelse som tydliggör det. Regeringen föreslår att utredningens lagtextförslag justeras i enlighet med detta.

Ett normgivningsbemyndigande om krav för ackreditering

Det kan finnas behov av kompletterande bestämmelser avseende ackreditering enligt det europeiska ramverket för cybersäkerhets-certifiering. Som utredningen föreslår bör regeringen eller den myndighet som regeringen bestämmer därför få meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse. Lagtexten bör utformas i enlighet med detta.

Gränsdragningen mellan tillsynsmyndigheternas ansvarsområden

Den nationella myndigheten för cybersäkerhetscertifiering har i uppgift att utöva tillsyn över efterlevnaden av regelverket för det europeiska systemet för cybersäkerhet. Uppgiften att utöva tillsyn omfattar även organen för bedömning av överensstämmelse. Den nationella myndigheten för cybersäkerhetscertifiering har t.ex. befogenhet att genomföra undersökningar, i form av kontroller, av organen för bedömning av överensstämmelse. Även Styrelsen för ackreditering och teknisk kontroll (Swedac) har i uppgift att bedriva tillsyn. Swedacs uppgifter och ansvar för såväl ackreditering som tillsyn av organ för bedömning av överensstämmelse framgår av gällande reglering om ackreditering i förening med de ytterligare krav som anges i EU:s cybersäkerhetsakt och kommande europeiska ordningar för cybersäkerhetscertifiering. Som *Swedac* uppmärksammar kan Swedacs och den nationella myndigheten för cybersäkerhetscertifierings tillsynsverksamhet i viss utsträckning komma att överlappa varandra. Myndigheterna behöver därför samverka och

samråda vid bedrivande av tillsyn. Detta framgår också delvis redan av EU:s cybersäkerhetsakt. I artikel 58.7 punkten e framgår nämligen att den nationella myndigheten för cybersäkerhetscertifiering aktivt ska bistå och stödja det nationella ackrediteringsorganet med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse. Det europeiska regelverket är därmed utformat med beaktande av de båda organens till del överlappande uppgifter i det här avseendet. Det finns också bestämmelser om samverkan i förvaltningslagen (8 §) och i myndighetsförordningen (2007:515).

Regeringen ser därför, till skillnad från Swedac, inte något behov av att reglera detta särskilt. Genom nära och effektiv samverkan mellan den nationella myndigheten för cybersäkerhetscertifiering och det nationella ackrediteringsorganet bör eventuella oklarheter i fråga om t.ex. gränsdragning mellan myndigheternas tillsynsområden kunna undvikas.

9.2.4 EU-förordningen (EG) nr 765/2008 byter titel

Regeringens förslag: Den nya lagen ändras så att upplysningsbestämmelsen i lagen om EU-förordningen (EG) nr 765/2008 anger den lydelse av förordningens titel som träder i kraft den 16 juli 2021.

Utredningen lämnar inte något förslag i denna del.

Skälen för regeringens förslag: Regeringens förslag som behandlas i avsnitt 9.2.3 innebär att det i den nya lagen upplysningsvis ska anges att bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering finns i EU-förordningen (EG) nr 765/2008.

I artikel 39.1 i förordningen (EU) 2019/1020 om marknadskontroll och överensstämmelse för produkter anges att titeln till förordningen (EG) nr 765/2008 ska ersättas. Ändringen gäller från och med den 16 juli 2021. Anledningen är att bestämmelser om marknadskontroll i förordningen (EG) nr 765/2008 upphävs den 16 juli 2021 i samband med att förordningen (EU) 2019/1020 om marknadskontroll och överensstämmelse blir fullt tillämplig.

I lagrådsremissen föreslås att det görs en ändring i den nya lagen, så att EU-förordningen (EG) nr 765/2008 anges med dess nya titel. Enligt *Lagrådet* skulle en mer ändamålsenlig ordning kunna vara att ändringen i stället genomförs i form av en övergångsbestämmelse till den nya lagen. Lagrådet lämnar också ett förslag på hur detta kan genomföras. Regeringen, som bl.a. noterar att Lagrådets förslag avviker från vad som är författningstekniskt brukligt för ändringar av nu aktuellt slag, anser dock att utformningen enligt lagrådsremissens förslag är såväl lämpligare som tydligare från bl.a. ett rättstillämpningsperspektiv och därför bör stå kvar.

9.3 Överlämnande av förvaltningsuppgifter till organ för bedömning av överensstämmelse

Regeringens bedömning: I EU:s cybersäkerhetsakt finns bestämmelser som innebär att förvaltningsuppgifter, innefattande myndighetsutövning, överlämnas till privata organ för bedömning av överensstämmelse.

Det behövs inte några motsvarande bestämmelser i den nya lagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser yttrar sig inte särskilt över utredningens bedömning i denna del. *Tullverket* anser dock att överlämnandet av förvaltningsuppgift till privata organ för bedömning av överensstämmelse uttryckligen bör regleras i den nya lagen.

Skälen för regeringens bedömning: Enligt 12 kap. 4 § andra stycket regeringsformen kan förvaltningsuppgifter överlämnas till juridiska personer och enskilda individer. Om förvaltningsuppgiften innefattar myndighetsutövning, får ett överlämnande göras endast med stöd av lag

I EU:s cybersäkerhetsakt finns bestämmelser om att de organ för bedömning av bestämmelse som avses i artikel 60 ska utfärda cybersäkerhetscertifikat på assuransnivå ”grundläggande” och ”betydande” (artikel 56.4). Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorganet under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till cybersäkerhetsakten (artikel. 60.1). Av bilagan framgår att ett organ för bedömning av överensstämmelse ska vara en juridisk person. Ett organ för bedömning av överensstämmelse kan alltså vara såväl en offentligrättslig som privaträttslig aktör.

Om det i en europeisk ordning för cybersäkerhetscertifiering ställs krav på assuransnivå ”hög”, ska den nationella myndigheten för cybersäkerhetscertifiering utfärda cybersäkerhetscertifikat enligt den ordningen (artikel 56.6). Den nationella myndigheten för cybersäkerhetscertifiering kan dock på förhand delegera uppgiften till ett organ för bedömning av överensstämmelse. Vidare kan en europeisk ordning för cybersäkerhetscertifiering innehålla särskilda eller ytterligare krav (artikel 54.1 f). I de fallen ska endast organ för bedömning av överensstämmelse som uppfyller dessa krav bemyndigas av den nationella myndigheten för cybersäkerhetscertifiering att utföra uppgifter inom ramen för sådana ordningar (artikel 60.3). Enligt artikel 58.7 e får en nationell myndighet för cybersäkerhetscertifiering i tillämpliga fall utfärda bemyndiganden enligt artikel 60.3 för organ för bedömning av överensstämmelse att utföra certifieringsuppgifter och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organet inte uppfyller kraven enligt EU:s cybersäkerhetsakt.

Som utredningen anför utgör ett cybersäkerhetscertifikat, särskilt när det är fråga om obligatorisk cybersäkerhetscertifiering, en förutsättning för att en tillverkare eller leverantör ska kunna tillhandahålla IKT-produkten, IKT-tjänsten eller IKT-processen på den inre marknaden. Uppgiften att utfärda cybersäkerhetscertifikat utgör en förvaltningsuppgift som innefattar myndighetsutövning.

Uppgiften för såväl privata som offentliga organ för bedömning av överensstämmelse att utfärda europeiska cybersäkerhetscertifikat regleras i EU:s cybersäkerhetsakt. Regeringen anser i likhet med utredningen att artiklarna 56.4, 56.6, 58.7 e och 60.3 i EU:s cybersäkerhetsakt ger tillräckligt lagstöd för det överlämnande av förvaltningsuppgifter till privata organ för bedömning av överensstämmelse som regleringen i cybersäkerhetsakten innebär. Det finns därför inte något behov av motsvarande bestämmelser i den nya lagen.

10 Handläggning och rättsmedel

10.1 Myndigheternas handläggning av ärenden

Regeringens bedömning: I den mån det europeiska ramverket för cybersäkerhetscertifiering inte innehåller avvikande bestämmelser är förvaltningslagen tillämplig på berörda myndigheters handläggning av ärenden. Det behövs inga kompletterande nationella regler om ärendehandläggningen hos myndigheterna.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning: Förvaltningslagen gäller för handläggning av ärenden hos förvaltningsmyndigheterna (1 §). Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från förvaltningslagen, tillämpas den bestämmelsen (4 §). När det gäller det europeiska ramverket för cybersäkerhetscertifiering innebär detta att förvaltningslagen ska tillämpas om det inte finns avvikande bestämmelser i EU:s cybersäkerhetsakt och de genomförandeakter som beslutas med stöd av akten.

Regeringen anser i likhet med utredningen att det inte finns behov av kompletterande nationella bestämmelser om handläggningen av ärenden hos den nationella myndigheten för cybersäkerhetscertifiering eller ett offentligt organ för bedömning av överensstämmelse.

Frågan om vilka regler för handläggning som bör gälla i samband med klagomål enligt artiklarna 58.7 f och 63 behandlas i avsnitt 10.3.1.

10.2 Ärendehandläggning hos privata organ för bedömning av överensstämmelse

Regeringens förslag: Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Organ för bedömning av överensstämmelse ska vara juridiska personer, t.ex. aktiebolag. En förutsättning för att en privat aktör ska få vara organ för bedömning av överensstämmelse är att organet ackrediteras av det nationella ackrediteringsorganet. De aktörer som önskar bli ackrediterade ska uppfylla flera krav, bl.a. krav på opartiskhet, tillhandahållande av beskrivningar av de förfaranden enligt vilka organen utför sina bedömningar i syfte att säkerställa insyn samt uppfylla de krav som anges i relevanta standarder enligt förordning (EG) nr 765 (se bilagan till EU:s cybersäkerhetsakt). De europeiska ordningarna för cybersäkerhetscertifiering ska vidare innehålla en rad komponenter som bl.a. kan förväntas ha inverkan på handläggningen av ärenden om cybersäkerhetscertifiering (se artikel 54 i EU:s cybersäkerhetsakt). Det finns vidare en möjlighet för en tillverkare eller leverantör att lämna in klagomål till organet för bedömning av överensstämmelse (se nedan). Det europeiska ramverket för cybersäkerhetscertifiering innehåller således en viss ordning för ärendehandläggning.

I artikel 41 i Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg, förkortad rättighetsstadgan, slås vidare fast att var och en har rätt till god förvaltning. Denna rättighet omfattar bl.a. rätten till kommunikation, aktinsyn och motivering av beslut. Rätten till god förvaltning gäller enligt rättighetsstadgan bara i förhållande till unionens institutioner, organ och byråer. Som regeringen anför i propositionen En modern och rättssäker förvaltning – ny förvaltningslag framstår det som naturligt att utgå från att de allmänna unionsrättsliga principer som gäller i ärenden som handläggs av unionens institutioner och organ också gäller för medlemsstaternas myndigheter, när de handlägger ärenden på unionsrättens område (prop. 2016/17:180 s. 44).

De privata organen för bedömning av överensstämmelse utgör inte myndigheter i förvaltningslagens mening. Förvaltningslagen är därför inte tillämplig på organens handläggning av ärenden.

De privata organen för bedömning av överensstämmelse ska i utövandet av den verksamheten beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet (jfr 1 kap. 9 § regeringsformen). Härutöver bör, som utredningen föreslår, organen för bedömning av överensstämmelse ha en skyldighet att i vissa fall ompröva ett tidigare beslut i ett ärende om certifiering. Det bör i den nya lagen införas en särskild bestämmelse om detta. En lämplig förebild för bestämmelsen kan vara 38 § förvaltningslagen om när en myndighet ska ändra ett beslut.

Regeringen föreslår därför att ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat, om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

10.3 Effektiva rättsmedel

10.3.1 Rätten till klagomål

Regeringens bedömning: Det behövs inga särskilda bestämmelser om den enskildes rätt att ge in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller den nationella myndigheten för cybersäkerhetscertifiering. Det behövs inte heller några särskilda bestämmelser om certifieringsorganens och myndighetens handläggning av sådana klagomål.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning: Klagomål som rör EU-försäkringar av överensstämmelse, europeiska cybersäkerhetscertifikat utfärdade av nationella myndigheter för cybersäkerhetscertifiering och sådana certifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 56.6 (dvs. certifikat som avser högsta assuransnivån) ska ges in till den berörda nationella myndigheten för cybersäkerhetscertifiering. Klagomål ska i övriga fall lämnas till det organ för bedömning av överensstämmelse som har utfärdat det europeiska cybersäkerhetscertifikat som klagomålet avser (artikel 63.1).

Den nationella myndigheten för cybersäkerhetscertifiering eller det organ för bedömning av överensstämmelse som klagomålet lämnats till ska underrätta den klagande om hur förfarandet fortskrider och vilket beslut som fattats, och ska informera den klagande om effektiva rättsmedel enligt artikel 64 (artikel 63.2). Den nationella myndighetens uppgift att behandla klagomål regleras även i artikel 58.7 f. Av bestämmelsen följer att myndigheten i lämplig utsträckning ska undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen.

När den nationella myndigheten för cybersäkerhetscertifiering handlägger klagomålsärenden är förvaltningslagen tillämplig, i den mån det europeiska ramverket inte innehåller avvikande bestämmelser. Som redogörs för ovan innehåller EU:s cybersäkerhetsakt vissa handläggningsregler som ska följas av såväl den nationella myndigheten för cybersäkerhetscertifiering som offentliga och privata organ för bedömning av överensstämmelse. Ytterligare förfaranderegler kan också tillkomma genom de europeiska ordningarna för cybersäkerhetscertifiering. Handläggningsförfarandet enligt cybersäkerhetsakten uppvisar likheter med bestämmelser i förvaltningslagen, t.ex. i fråga om utredningsansvar, skyndsamhetskrav och underrättelseskyldighet (jfr artiklarna 58.7 f och 63.2). Cybersäkerhetsakten ger också enskilda rätt till effektiva rättsmedel även avseende underlåtenhet att vidta åtgärder med anledning av ett klagomål (artikel 64.1 b). Frågan om överklagande behandlas närmare i nästa avsnitt.

Sammantaget gör regeringen i likhet med utredningen bedömningen att det inte finns behov av att införa kompletterande nationella bestämmelser om den nationella myndigheten för cybersäkerhetscertifierings eller ett

organ för bedömning av överensstämmelses handläggning av klagomål enligt EU:s cybersäkerhetsakt.

10.3.2 Överklagande

Regeringens förslag: Beslut enligt EU:s cybersäkerhetsakt och den nya lagen av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse ska få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Domstolsverket* och *Förvaltningsrätten i Stockholm* anser att frågan om forum vid överklagande av beslut bör övervägas ytterligare. Förvaltningsrätten i Stockholm uppmärksammar även frågan om partsställning vid överklagande av beslut som fattas av privaträttsliga subjekt. *Lunds universitet* anser att det bör framgå av lagtexten att det är den nationella myndighetens och organen för bedömning av överensstämmelses beslut som får överklagas.

Skälen för regeringens förslag: Enligt artikel 64.1 a i EU:s cybersäkerhetsakt ska enskilda ha rätt till effektiva rättsmedel avseende beslut som har fattats av den nationella myndigheten för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse.

Enligt artikel 6.1 i Europakonventionen, som gäller som lag, gäller att var och en vid prövningen av hans eller hennes civila rättigheter ska vara berättigad till en rättvis och offentlig förhandling inom skälig tid och inför en opartisk domstol som har upprättats enligt lag.

Beslut om bl.a. cybersäkerhetscertifiering och sanktionsavgifter enligt EU:s cybersäkerhetsakt och den föreslagna lagen innefattar prövningar som faller inom tillämpningsområdet för artikel 6.1. En överprövning av sådana beslut måste därför vara förenlig med konventionens krav i fråga om domstolsprövning. Regeringen föreslår därför, i linje med *Lunds universitets* synpunkter, att det i lagen införs bestämmelser om överklagande som innebär att beslut enligt EU:s cybersäkerhetsakt och den nya lagen av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse ska få överklagas till allmän förvaltningsdomstol.

I likhet med vad som allmänt gäller i fråga om överklagande av förvaltningsbeslut bör det krävas prövningstillstånd vid överklagande till kammarrätten. Detta bör anges i lagtexten.

Domstolsverket uppmärksammar att det kan förekomma uppgifter som är säkerhetsklassificerade enligt säkerhetsskyddslagen (2018:585) i ett överklagat ärende. Regeringen anser dock inte att de praktiska och ekonomiska skäl som myndigheten pekar på ger anledning att i detta lagstiftningsärende överväga särskilda forumregler för mål i domstol enligt det aktuella regelverket.

Utredningens lagförslag reglerar inte frågan om vilken ställning ett privat organ har vid ett överklagande till domstol. Som *Förvaltningsrätten i Stockholm* uppmärksammar finns det dock rättspraxis som ger stöd för att ett enskilt rättssubjekt i vissa fall kan ges motpartsställning även utanför

tillämpningsområdet för 7 a § förvaltningsprocesslagen (1971:291). Regeringen konstaterar att det inte finns beredningsunderlag för att överväga en eventuell sådan reglering.

11 Offentlighet och sekretess

11.1 Utgångspunkter

Det europeiska ramverket för cybersäkerhetscertifiering ger möjlighet för tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer att antingen utfärda en EU-försäkran om överensstämmelse eller ansöka om ett europeiskt cybersäkerhetscertifikat. Såväl en EU-försäkran om överensstämmelse som ett europeiskt cybersäkerhetscertifikat grundas på information om den aktuella produktens, tjänstens eller processens konstruktion och funktionalitet. Vidare inbegriper IKT-produkter, IKT-tjänster och IKT-processer ofta en eller flera komponenter eller annan teknik från tredje part, som är nödvändiga för produkten, tjänsten, eller processen, t.ex. programmoduler, bibliotek eller programmerings-gränssnitt. Detta kan innebära cybersäkerhetsrisker eftersom sårbarheter i sådana tredjepartskomponenter även kan påverka IKT-produkternas, IKT-tjänsternas och IKT-processernas säkerhet. Det finns därför ett behov av att informationen och uppgifterna skyddas, bl.a. av konkurrens- och säkerhetsskäl. Bestämmelser som rör skydd för uppgifter finns i EU:s cybersäkerhetsakt och i offentlighets- och sekretesslagen (2009:400), förkortad OSL.

11.2 Bestämmelser i EU:s cybersäkerhetsakt

Uppgiftsskyldighet

Av artikel 56.7 i EU:s cybersäkerhetsakt följer att den fysiska eller juridiska person som lämnar in sina IKT-produkter, IKT-tjänster eller IKT-processer för certifiering ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndigheten för cybersäkerhetscertifiering, om myndigheten utfärdar certifikatet, eller för det aktuella organet för bedömning av överensstämmelse. Uppgifter som är nödvändiga och som en sökande ska lämna till eller på annat sätt göra tillgängliga för organ för bedömning av överensstämmelse kommer att anges i de europeiska ordningarna för cybersäkerhetscertifiering (artikel 54.1 h).

Innehavare av europeiska cybersäkerhetscertifikat är vidare skyldiga att rapportera nyupptäckta sårbarheter eller oriktigheter vilka rör säkerheten för cybersäkerhetscertifierad IKT till en nationell myndighet för cybersäkerhetscertifiering eller ett organ för bedömning av överensstämmelse. Myndigheten eller organet ska i sin tur överlämna mottagen information till den berörda nationella myndigheten för cybersäkerhetscertifiering (artikel 56.8).

En tillverkare eller leverantör ska också lämna kompletterande cybersäkerhetsinformation om en IKT-produkt, IKT-tjänst eller IKT-process som är certifierad eller för vilken en EU-försäkran om överensstämmelse har utfärdats enligt cybersäkerhetsakten. Den kompletterande säkerhetsinformationen ska tillgängliggöras i elektroniskt format och finnas tillgänglig och vid behov uppdateras åtminstone fram till dess att motsvarande europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse löper ut (artikel 55).

Utfärdare av EU-försäkringar om överensstämmelse, certifikatinnehavare och privata organ för bedömning av överensstämmelse, ska dessutom lämna uppgifter som är nödvändiga för den tillsyn som utförs av den nationella myndigheten för cybersäkerhetscertifiering enligt artiklarna 58.7 och 58.8.

Följaktligen kommer både den nationella myndigheten för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse att i sina verksamheter hantera uppgifter om certifikatsökande, certifikatinnehavare och utfärdare av EU-försäkringar om överensstämmelse och information om IKT-produkter, IKT-tjänster och IKT-processer.

Vidare har den nationella myndigheten för cybersäkerhetscertifiering en skyldighet att lämna uppgifter till andra nationella myndigheter för cybersäkerhetscertifiering, andra myndigheter och till kommissionen. Det följer av bestämmelserna i artiklarna 58.7–58.9 i EU:s cybersäkerhetsakt. Enligt de bestämmelserna ska nationella myndigheter för cybersäkerhetscertifiering övervaka relevant utveckling på området cybersäkerhetscertifiering, samarbeta med varandra och med kommissionen genom att utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer, samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, bl.a. genom att utbyta information om IKT-produkter, IKT-tjänster och IKT-processer som avviker från kraven i cybersäkerhetsakten eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och lämna en årlig sammanfattande rapport om den verksamhet som bedrivits enligt punkten 7 b, c och d eller enligt punkten 8 till Enisa och den europeiska gruppen för cybersäkerhetscertifiering.

Genom artikel 59 inrättas ett system för inbördes granskning i syfte att uppnå likvärdiga standarder i hela unionen för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse. Den inbördes granskningen ska utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsländer och EU-kommissionen och ska utföras minst var femte år. Enisa får delta i den inbördes granskningen. Inom ramen för den inbördes granskningen kommer den nationella myndigheten för cybersäkerhetscertifiering att behöva såväl lämna uppgifter till som ta emot uppgifter från andra nationella myndigheter för cybersäkerhetscertifiering, EU-kommissionen och Enisa.

Konfidentialitet och tystnadsplikt

Bestämmelser om skydd för uppgifter hos organ för bedömning av överensstämmelse finns i punkten 16 i bilagan till EU:s cybersäkerhetsakt.

I denna punkt anges att ett organ som önskar bli ackrediterat ska bevara konfidentialitet och iaktta tystnadsplikt avseende all den information som organen erhåller vid utförandet av bedömning av överensstämmelse i enlighet med det europeiska ramverket för cybersäkerhetscertifiering eller kompletterande nationella bestämmelser, utom i de fall då uppgifter måste lämnas enligt unionsrätten eller medlemsstaternas nationella rätt. Det ställs även krav på att organ för bedömning av överensstämmelse ska ha dokumenterade förfaranden som möter kraven på konfidentialitet och tystnadsplikt. Vidare anges att immateriella rättigheter ska skyddas.

I artikel 54.1 n i EU:s cybersäkerhetsakt anges också att en europeisk ordning för cybersäkerhetscertifiering ska innehålla bestämmelser om hur organ för bedömning av överensstämmelse i tillämpliga fall ska bevara sina uppgifter.

11.3 Inget behov av ändringar i offentlighets- och sekretesslagen

Regeringens bedömning: Det finns inte något behov av ändringar i offentlighets- och sekretesslagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Förvaltningsrätten i Stockholm* anser att det kan finnas behov av att införa en uttrycklig bestämmelse om uppgiftsskyldighet som möjliggör ett utlämnande enligt 10 kap. 28 § offentlighets- och sekretesslagen. Även *Skatteverket* är inne på en liknande linje. Övriga remissinstanser yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning

Utgångspunkter

Till följd av bestämmelserna om uppgiftsskyldighet i EU:s cybersäkerhetsakt kommer organ för bedömning av överensstämmelse och den nationella myndigheten för cybersäkerhetscertifiering att få tillgång till skyddsvärda uppgifter om såväl tillverkare och leverantörer som IKT-produkter, IKT-tjänster och IKT-processer. Det kan t.ex. vara fråga om nyupptäckta cybersäkerhetssårbarheter i certifierad IKT som används i samhällsviktig verksamhet. Den nationella myndigheten för cybersäkerhetscertifiering kommer också att förfoga över ytterligare skyddsvärd information inom ramen för tillsynsverksamheten, t.ex. avseende tester och underlag för provning samt certifieringsorganets bedömning av dessa underlag.

Det finns ett behov av att säkerställa att dessa uppgifter åtnjuter ett fullgott skydd inom det europeiska systemet för cybersäkerhetscertifiering. Som redogörs för ovan finns bestämmelser om konfidentialitet och tystnadsplikt i EU:s cybersäkerhetsakt. I offentlighets- och sekretesslagen finns det ett flertal bestämmelser som kan vara tillämpliga på uppgifter hos ett offentligt organ för bedömning av överensstämmelse eller den nationella myndigheten för cybersäkerhets-

certifiering. Skyddet för uppgifter i de privata organen för överensstämmelses verksamhet behandlas i avsnitt 11.4.

Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden

Enligt 30 kap. 23 § OSL gäller sekretess, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt

1. för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs, och
2. för uppgift om andra ekonomiska eller personliga förhållanden än som avses i 1 för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Som utredningen uppmärksammar kan behov av sådan sekretess komma att aktualiseras i fråga om uppgifter som förekommer i övervaknings-, kontroll- och tillsynsverksamheten hos den nationella myndigheten för cybersäkerhetscertifiering. Regeringen kan i sådant fall besluta om en ändring i offentlighets- och sekretessförordningen (2009:641).

Enligt 31 kap. 12 § OSL gäller sekretess för vissa uppgifter i uppdragsverksamhet för enskilds räkning. Bestämmelsen kan vara tillämplig på uppgifter som ett offentligt organ för bedömning av överensstämmelse eller den nationella myndigheten för cybersäkerhetscertifiering får tillgång till när organet eller myndigheten utfärdar cybersäkerhetscertifikat efter ansökan från t.ex. ett aktiebolag.

Sekretess till skydd för allmänna intressen

Enligt 15 kap. 1 § OSL gäller sekretess för uppgifter som angår Sveriges förbindelser med en annan stat eller i övrigt rör en annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det skulle störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet om uppgifterna röjs.

Enligt 15 kap. 1 a § första stycket OSL gäller sekretess för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs. Motsvarande sekretess gäller enligt paragrafens andra stycke för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal som avses i första stycket. EU:s cybersäkerhetsakt är en sådan bindande EU-rättsakt som avses i 15 kap. 1 a § OSL.

Enligt regeringens bedömning kan bestämmelserna om utrikessekretess aktualiseras i fråga om uppgifter hos den nationella myndigheten för cybersäkerhetscertifiering som ska lämnas till eller som inkommit från andra medlemsstaters nationella myndigheter för cybersäkerhetscertifiering, EU-kommissionen eller Enisa med stöd av bestämmelserna i artiklarna 58.7–9 och 59 i EU:s cybersäkerhetsakt.

Enligt 15 kap. 2 § OSL gäller sekretess för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Så kallad försvarssekretess kan exempelvis aktualiseras hos de offentliga organen för bedömning av överensstämmelse och hos den nationella myndigheten för cybersäkerhetscertifiering i den mån det förekommer uppgifter vars röjande medför att kritiska samhällsfunktioner äventyras och att verksamheter av betydelse för Sveriges säkerhet hotas.

Enligt 17 kap. 1 § OSL gäller sekretess för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjas. Bestämmelsen kan t.ex. aktualiseras i den nationella myndigheten för cybersäkerhetscertifierings tillsynsverksamhet.

Enligt utredningen kan det bli aktuellt för ett organ för bedömning av överensstämmelse att använda tester och prov för att bedöma kunskapsnivå och tilldela status som evaluerare eller certifierare. I en sådan situation bör 17 kap. 4 § OSL kunna bli tillämplig. Enligt den bestämmelsen gäller sekretess för uppgift som ingår i eller utgör underlag för kunskapsprov eller psykologiskt prov under en myndighets överseende, om det kan antas att syftet med provet motverkas om uppgiften röjs.

Sekretessbrytande bestämmelser

Den nationella myndigheten för cybersäkerhetscertifiering, offentliga organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet behöver kunna lämna sekretessbelagda uppgifter som myndigheterna hanterar i certifierings-, tillsyns- eller ackrediteringsverksamhet till varandra. Ett organ för bedömning av överenstämmelse har t.ex. en skyldighet att till den nationella myndigheten för cybersäkerhetscertifiering vidarebefordra information om sårbarheter eller oriktigheter som rör säkerheten för en cybersäkerhetscertifierad IKT-produkt, IKT-tjänst eller IKT-process (artikel 56.8). Vidare har den nationella myndigheten för cybersäkerhetscertifiering en skyldighet att bistå det nationella ackrediteringsorganet med övervakning och kontroll av verksamhet som bedrivs enligt EU:s cybersäkerhetsakt av organen för bedömning av överensstämmelse (artikel 58.7 b). I den verksamheten kan uppgifter som kan omfattas av sekretess behöva lämnas mellan myndigheterna. Den nationella myndigheten för cybersäkerhetscertifiering ska också samarbeta med andra berörda marknadsövervakningsmyndigheter (se artikel 58.7 a).

En uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen får som utgångspunkt inte röjas för enskilda eller andra myndigheter (8 kap. 1 § OSL). För att tillgodose myndigheters behov av information och informationsutbyte i sin verksamhet finns flera undantag från huvudregeln om sekretess mellan myndigheter. Sådana sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns huvudsakligen i 10 kap. OSL.

Enligt 10 kap 2 § OSL hindrar sekretess inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen kan vara tillämplig i fall där någon av de övriga sekretessbrytande reglerna inte gäller, men ska tillämpas restriktivt (se prop. 1979/80:2 Del A s. 465 och 494).

Enligt 10 kap. 17 § OSL hindrar sekretess inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för tillsyn över eller revision hos den myndighet där uppgiften förekommer. Får en myndighet i verksamhet som avser tillsyn eller revision en sekretessreglerad uppgift överförs sekretessen till den mottagande myndigheten om uppgiften inte ingår i ett beslut hos den mottagande myndigheten (11 kap. 1 § OSL). Det är inte bara uppgifter hos den kontrollerade myndigheten som skyddas. Om tillsyns- eller kontrollmyndigheten inhämtar sekretessbelagda uppgifter från någon annan myndighet än den som är föremål för tillsyn eller revision blir också dessa uppgifter sekretesskyddade. Bestämmelsen i 10 kap. 17 § OSL kan bli tillämplig som ett led i tillsynsverksamheten hos den nationella myndigheten för cybersäkerhetscertifiering i fråga om tillsyn över ett offentligt organ för bedömning av överensstämmelse.

Enligt den s.k. generalklausulen i 10 kap. 27 § OSL får en uppgift som omfattas av sekretess lämnas till en annan myndighet om det är uppenbart att intresset av att lämna uppgiften har företräde framför det intresse som sekretessen har att skydda. Generalklausulen kan inte tillämpas om utlämnandet strider mot lag eller förordning. Bestämmelsen är subsidiär i förhållande till andra sekretessbrytande bestämmelser och ska alltså inte tillämpas om någon annan sekretessbrytande bestämmelse kan tillämpas.

Enligt 10 kap. 28 § OSL hindrar inte sekretess att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Som redogörs för ovan innebär EU:s cybersäkerhetsakt, som ska jämställas med lag, en skyldighet för bl.a. offentliga organ för bedömning av överensstämmelse att lämna uppgifter till den nationella myndigheten för cybersäkerhetscertifiering. Regeringen anser därför, till skillnad från *Förvaltningsrätten i Stockholm* och *Skatteverket*, inte att det finns behov av att införa en bestämmelse om uppgiftsskyldighet för att möjliggöra utlämnande av uppgifter enligt 10 kap. 28 §.

Det finns således flera sekretessbrytande bestämmelser som kan tillämpas för att uppgifter som omfattas av sekretess ska kunna lämnas mellan myndigheter i samband med tillsyn och rapportering av sårbarheter. Bestämmelserna kan också vara tillämpliga i den nationella ackrediteringsorganets tillsynsverksamhet över offentliga organ för bedömning av överensstämmelse respektive när myndigheten får uppgifter i samband med ansökan om ackreditering.

De sekretessbrytande bestämmelserna i 10 kap. 15–27 §§ och 28 § första stycket OSL får inte tillämpas om sekretess gäller för uppgiften enligt 15 kap. 1 a §. I sammanhanget kan nämnas att en uppgift för vilken sekretess gäller får röjas för en utländsk myndighet eller en mellanfolklig organisation, om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § OSL). Det innebär att sekretess inte hindrar det informationsutbyte som enligt artiklarna 58.7–9 och 59 i cybersäkerhetsakten ska ske mellan de nationella myndigheterna för cybersäkerhetscertifiering.

Regeringen gör sammantaget bedömningen att det inte finns något behov av att införa nya sekretessbrytande bestämmelser.

Det finns inte behov av några ändringar i offentlighets- och sekretesslagen

Sammanfattningsvis finns det flera sekretessbestämmelser i offentlighets- och sekretesslagen som kan aktualiseras i verksamheten hos offentliga organ för bedömning av överensstämmelse och den nationella myndigheten för cybersäkerhetscertifiering. Det har inte framkommit att det finns behov av att göra några ändringar i offentlighets- och sekretesslagen med anledning av EU:s cybersäkerhetsakt.

11.4 En bestämmelse om tystnadsplikt ska införas

Regeringens förslag: Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att det även ska införas en upplysningsbestämmelse om att den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Bestämmelserna om konfidentialitet och tystnadsplikt i bilagan till EU:s cybersäkerhetsakt gäller för privata organ för bedömning av överensstämmelse. Till skillnad mot offentliga organ för bedömning av överensstämmelse och den nationella myndigheten för cybersäkerhetscertifiering omfattas inte de privata organens hantering av uppgifter av offentlighets- och sekretesslagen, eftersom den lagen, med vissa undantag, endast är tillämplig vid myndigheters hantering av handlingar.

Bestämmelser om tystnadsplikt för privata aktörer finns dock i vissa specialförfattningar. Tystnadsplikten är då ofta reglerad som ett förbud mot att obehörigen röja vissa uppgifter. En sådan bestämmelse finns t.ex. i 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse.

Författningsreglerad tystnadsplikt, oavsett om den följer av bestämmelser i offentlighets- och sekretesslagen eller av annan lag, utgör en inskränkning av yttrandefriheten enligt regeringsformen. Den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Som utredningen föreslår bör det i den nya lagen införas en bestämmelse om tystnadsplikt som innebär att den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt inte obehörigen får röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

En möjlighet för de privata organen för bedömning av överensstämmelse att bryta sekretessen i förhållande till behöriga nationella myndigheter, och då författning kräver att uppgifter lämnas, har intagits i bilagan till EU:s cybersäkerhetsakt. Detta undantag möjliggör nödvändigt informationsutbyte mellan organet i fråga och den nationella myndigheten för cybersäkerhetscertifiering. Att den föreslagna tystnadsplikten avgränsas med ett obehörighetsrekvisit innebär bl.a. att uppgifter kan lämnas ut med samtycke, till den nationella myndigheten för cybersäkerhetscertifiering eller annars som en följd av en skyldighet i lag eller författning.

Det bör också framgå av lagtexten att offentlighets- och sekretesslagen är tillämplig i det allmännas verksamhet. Till skillnad mot utredningen anser regeringen inte att det av lagtexten behöver framgå att den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken. Utformningen av paragrafen i den här delen överensstämmer med motsvarande bestämmelse i 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

12 Behandling av personuppgifter

Regeringens bedömning: Befintlig reglering på personuppgiftsområdet är tillräcklig för den personuppgiftsbehandling som kan komma att utföras av den nationella myndigheten för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet.

Det behöver inte införas nya bestämmelser om behandling av personuppgifter med anledning av EU:s cybersäkerhetsakt.

Utredningens bedömning överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens bedömning.

Skälen för regeringens bedömning: I den verksamhet som den nationella myndigheten för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet bedriver med stöd av EU:s cybersäkerhetsakt och den nya lagen kommer myndigheterna och organen att behöva behandla personuppgifter. Den nationella myndigheten för cybersäkerhetscertifiering kommer t.ex. att behöva behandla organisationsnummer för enskild näringsverksamhet, namn på fysiska företrädare och adress- och kontaktuppgifter inom ramen för sin tillsyns- och certifieringsverksamhet. Organen för bedömning av överensstämmelse kommer att behöva behandla motsvarande uppgifter vid utfärdande av certifikat enligt det nya regelverket. Detsamma gäller när ackrediteringsorganet beslutar om ackreditering av organ för bedömning av överensstämmelse.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om

upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i det följande EU:s dataskyddsförordning, utgör grunden för generell personuppgiftsbehandling inom EU. EU:s cybersäkerhetsakt ska inte påverka tillämpningen av EU:s dataskyddsförordning (skäl 74).

Det innebär att EU:s dataskyddsförordning ska tillämpas i verksamhet hos den nationella myndigheten för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet. I svensk rätt kompletteras EU:s dataskyddsförordning av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Enligt EU:s cybersäkerhetsakt ska den fysiska eller juridiska person som lämnar in en IKT-produkt, IKT-tjänst, eller IKT-process för certifiering göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndigheten för cybersäkerhetscertifiering, om denna myndighet utfärdar certifikatet eller för ett organ för bedömning av överensstämmelse (artikel 56.7). Ett utfärdande av ett cybersäkerhetscertifikat ska gälla inom hela unionen och förutsätter att information om den som ansöker om certifikat, såsom personnummer eller kontaktuppgifter registreras. Tillgången till sådana uppgifter är också en förutsättning för att den nationella myndigheten för cybersäkerhetscertifiering ska kunna utöva tillsyn över t.ex. en innehavare av ett cybersäkerhetscertifikat. Även det nationella ackrediteringsorganet verksamhet finns det ett behov av tillgång till kontaktuppgifter till de organ för bedömning av överensstämmelse som är föremål för ackreditering, bl.a. för att kunna utöva tillsyn över organen.

När det gäller frågan om rättslig grund för personuppgiftsbehandlingen bedömer regeringen att behandlingen är nödvändig för att dels utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (artikel 6.1 e i EU:s dataskyddsförordning), dels fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c i EU:s dataskyddsförordning). De rättsliga grunderna är fastställda i EU:s cybersäkerhetsakt och den föreslagna lagen. De aktuella grunderna för behandlingen är således fastställda i unionsrätten och i den nationella rätten på det sätt som krävs enligt artikel 6.3 i EU:s dataskyddsförordning (jfr prop. 2017/18:105 s. 56–57). EU:s cybersäkerhetsakt och den föreslagna lagen uppfyller kravet i artikel 6.3 i EU:s cybersäkerhetsakt om att unionsrätten och den nationella rätten ska uppfylla ett mål av allmänt intresse och vara proportionella mot det legitima mål som eftersträvas.

Vad gäller frågan om personuppgiftsbehandlingen är proportionerlig bör beaktas att de tillverkare och leverantörer som ansöker om cybersäkerhetscertifikat agerar yrkesmässigt. De uppgifter som kommer att behandlas är inte sådana känsliga personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning eller uppgifter om lagöverträdelser (artikel 10 i EU:s dataskyddsförordning). Det kommer främst vara fråga om kontaktuppgifter till företrädare för juridiska personer. Intrånget i de registrerades personliga integritet bedöms därför vara förhållandevis litet. Vid en avvägning mellan den registrerades personliga integritet och behovet av att personuppgiften behandlas framstår behandlingen som proportionerlig.

Regeringen bedömer att befintlig reglering i EU:s dataskyddsförordning, lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning är tillräcklig för den personuppgiftsreglering som kan komma att utföras av den nationella myndigheten för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet. Det behöver således inte införas några nya bestämmelser om behandling av personuppgifter med anledning av EU:s cybersäkerhetsakt.

13 Ikraftträdande- och övergångsbestämmelser

13.1 Förslaget till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Regeringens förslag: Den nya lagen ska träda i kraft den 28 juni 2021.
Regeringens bedömning: Det behövs inga övergångsbestämmelser.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag och bedömning.

Skälen för regeringens förslag och bedömning: Lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt bör träda i kraft samtidigt som bestämmelserna i EU:s cybersäkerhetsakt om cybersäkerhetscertifiering ska börja tillämpas, dvs. den 28 juni 2021.

Det finns inte behov av några övergångsbestämmelser.

13.2 Förslaget till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Regeringens förslag: Lagen om ändring i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska träda i kraft den 16 juli 2021.
Regeringens bedömning: Det behövs inga övergångsbestämmelser.

Utredningen lämnar inte något förslag i denna del.

Skälen för regeringens förslag och bedömning: Ändringen av titeln till EU-förordningen (EG) nr 765/2008 ska börja tillämpas den 16 juli 2021. Lagen om ändring i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt bör träda i kraft samtidigt.

Det finns inte behov av några övergångsbestämmelser.

Regeringens bedömning: Förslagen innebär att Försvarets materielverk får nya uppgifter, vilket bedöms innebära ökade kostnader för myndigheten.

Förslagen innebär att Kronofogdemyndigheten och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter. De kostnadsökningarna bedöms inte bli större än att de ryms inom befintliga anslag.

Förslagen medför vissa kostnader för företag och enskilda.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Några remissinstanser efterfrågar en utförligare konsekvensanalys. *Domstolsverket* bedömer att kostnadsökningen för domstolarna inte kan hanteras inom befintliga ekonomiska ramar.

Skälen för regeringens bedömning

Konsekvenser för Försvarets materielverk

Regeringen gör bedömningen att Försvarets materielverk (FMV) bör utses till nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. Det innebär att myndigheten får nya ansvarsområden och flera nya uppgifter.

Uppgiften som nationell myndighet för cybersäkerhetscertifiering kommer att medföra behov av resursförstärkning vid myndigheten, främst i form av personalförstärkning. De nya ansvarsområdena och uppgifterna medför ett ökat personalbehov inom FMV som beräknas uppgå till femton årsarbetskrafter samt kostnader för bl.a. utbildning, resor, it och övrig administration. De beräknade utgifterna för den nya verksamheten kan i nuläget uppskattas till 20 000 000 kronor för 2022 och 30 000 000 kronor för 2023 och framåt.

Myndighetens certifieringsverksamhet är för närvarande både anslags- och avgiftsfinansierad. Motsvarande system bör införas när det gäller finansieringen av den certifieringsverksamhet som ska bedrivas enligt EU:s cybersäkerhetsakt. Möjligheten att ta ut avgifter ska avse kostnaden för utfärdande av certifikat.

Myndighetens tillsynsverksamhet ska enligt regeringens förslag avgiftsfinansieras genom att en tillsynsavgift tas ut av de aktörer vars verksamhet prövas eller är föremål för en tillsynsåtgärd. Möjligheten för FMV att ta ut tillsynsavgifter ska omfatta alla utfärdare av EU-försäkringar om överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat, och organ för bedömning av överensstämmelse.

Regeringen avser att vid behov återkomma till riksdagen med förslag om ökade medel för kommande år.

Konsekvenser för Styrelsen för ackreditering och teknisk kontroll (Swedac)

Styrelsen för ackreditering och teknisk kontroll (Swedac) är nationellt ackrediteringsorgan. Jämfört med de uppgifter myndigheten för närvarande utför skiljer sig ansvaret enligt EU:s cybersäkerhetsakt åt endast i mindre omfattning. Ackrediteringsverksamheten vid Swedac

finansieras av kundernas avgifter, som ska täcka samtliga kostnader för ackrediteringen. Eftersom verksamheten när det gäller ackreditering är avgiftsfinansierad bör denna verksamhet inte kräva ytterligare finansiella resurser.

Konsekvenser för Kronofogdemyndigheten

Bestämmelserna om sanktionsavgifter kan komma att öka antalet ärenden hos Kronofogdemyndigheten något. Även förslaget om att den nationella myndigheten för cybersäkerhetscertifiering ska få vända sig till Kronofogdemyndigheten och begära handräckning på plats vid vissa inspektioner kan leda till att Kronofogdemyndighetens hjälp behövs vid ett antal tillfällen men ökningen bedöms dock inte bli särskilt stor och förväntas inte påverka Kronofogdemyndighetens verksamhet mer än att konsekvenserna kan hanteras inom befintliga anslag för myndigheten.

Konsekvenser för domstolarna

Utredningens förslag om möjligheten att överklaga beslut som meddelas av organ för bedömning av överensstämmelse och av myndigheten för cybersäkerhetscertifiering innebär en ny reglering. En viss måltillströmning till allmän förvaltningsdomstol kan därför väntas. Det kan dock antas att överklaganden av beslut av organ för bedömning av överensstämmelse och den nationella myndigheten för cybersäkerhetscertifiering i frågor som avser certifiering inledningsvis kommer ske i begränsad omfattning.

Regeringen anser därför till skillnad från *Domstolsverket* att domstolarnas kostnadsökningar bör rymmas inom de befintliga anslagen.

Konsekvenser för näringslivet och företag

Införandet av det europeiska ramverket för cybersäkerhetscertifiering bedöms komma att påverka såväl företag som tillverkar och levererar angivna IKT-produkter, IKT-tjänster och IKT-processer som företag som använder sig av dessa.

Innehållet i de europeiska certifieringsordningarna, och hur väl svenska företagsprodukter m.m. motsvarar kraven i dessa ordningar, kan dock antas komma att påverka svenska företags konkurrenskraft.

Det nya regelverket förväntas på sikt bidra till ökad cybersäkerhet och en bättre fungerande marknad, vilket i förlängningen är till fördel för både ekonomiska aktörer och unionsmarknadens funktion. En effektiv tillsyn ökar även förutsättningarna för att företagare ska kunna konkurrera på lika villkor.

Konsekvenser för konsumenter och andra användare

Cybersäkerhetscertifiering är förenat med kostnader, vilket innebär att cybersäkerhetscertifierade konsumentprodukter och konsumenttjänster kan antas komma att avspegla sig i priset på sådana produkter och tjänster.

Konsekvenser för samhället

Syftet med det europeiska ramverket för cybersäkerhetscertifiering är att förbättra medborgarnas och företagens cybersäker-

hetsakt kan anses ha positiva konsekvenser för hela samhället, eftersom syftet med certifieringsverksamheten enligt cybersäkerhetsakten är att höja cybersäkerhetsnivån inom unionen och harmonisera europeiska system för cybersäkerhetscertifiering på unionsnivån.

Övriga konsekvenser

Förslagen bedöms inte påverka
- den kommunala självstyrelsen,
- brottsligheten och det brottsförebyggande arbetet,
- sysselsättning och offentlig service i olika delar av landet,
- jämställdheten mellan kvinnor och män, eller
- möjligheterna att nå de integrationspolitiska målen.

Förslagen bedöms inte heller i övrigt medföra några konsekvenser av betydelse.

15 Författningskommentar

15.1 Förslaget till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Förordningen (EU) 2019/881 benämns i denna lag EU:s cybersäkerhetsakt.

Ord och uttryck i denna lag har samma betydelse som i EU:s cybersäkerhetsakt.

I paragrafen anges lagens innehåll. Övervägandena finns i avsnitt 5.

Av *första stycket* framgår att syftet med lagen är att komplettera EU:s förordning om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten). Lagen kompletterar EU:s cybersäkerhetsakt och kan därför inte tillämpas fristående från den. Hänvisningen till EU:s cybersäkerhetsakt är dynamisk. Det innebär att hänvisningen avser cybersäkerhetsakten i den vid varje tidpunkt gällande lydelsen.

Av *andra stycket* framgår att förordningen (EU) 2019/881 i lagen benämns EU:s cybersäkerhetsakt.

Tredje stycket innehåller en upplysning om att ord och uttryck i lagen har samma betydelse som i EU:s cybersäkerhetsakt. I artikel 2 i cybersäkerhetsakten finns definitioner.

Nationell myndighet för cybersäkerhetscertifiering

2 § Den myndighet som regeringen bestämmer

1. är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt, och

2. utövar tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Paragrafen reglerar nationell myndighet för cybersäkerhetscertifiering. Övervägandena finns i avsnitt 6.1, 6.2 och 7.5.

Enligt *punkten 1* är den myndighet som regeringen bestämmer nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Av *punkten 2* framgår att den nationella myndigheten även utövar tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Ackreditering av organ för bedömning av överensstämmelse

3 § I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

I paragrafen finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse. Övervägandena finns i avsnitt 9.2.

Första stycket innehåller en upplysning om att det i artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

Andra stycket innehåller en upplysning om att ackreditering sker enligt förordning (EG) nr 765/2008 och lagen (2011:791) om ackreditering och teknisk kontroll, som kompletterar den förordningen.

Ackrediteringen ska enligt artikel 60.4 i EU:s cybersäkerhetsakt utfärdas till organen för bedömning av överensstämmelse för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse fortfarande uppfyller kraven i artikel 60 och i bilagan till EU:s cybersäkerhetsakt.

I 33 § lagen (2011:791) om ackreditering och teknisk kontroll finns bestämmelser om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om själva ackrediteringen.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt. Bestämmelsen ger stöd för att meddela de kompletterande föreskrifter som kan behövas för ackreditering av organ för bedömning av överensstämmelse enligt cybersäkerhetsaktens bestämmelser respektive kompletterande krav för att organen ska ackrediteras.

4 § Vid tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs har den nationella myndigheten för cybersäkerhetscertifiering de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt.

I paragrafen regleras de befogenheter den nationella myndigheten för cybersäkerhetscertifiering har vid tillsyn enligt lagen och föreskrifter som har meddelats i anslutning till lagen. Övervägandena finns i avsnitt 7.5.

Av paragrafen framgår att de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering har enligt artikel 58.8 i EU:s cybersäkerhetsakt även gäller vid tillsyn över att bestämmelserna i den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs. I artikel 58.8 anges den nationella myndighetens tillsynsbefogenheter, t.ex. befogenheten att genomföra kontroller av innehavare av ett europeiskt cybersäkerhetscertifikat.

5 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för tillsynen och för att EU:s cybersäkerhetsakt, genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

I paragrafen regleras vissa tillsynsbefogenheter enligt lagen. Övervägandena finns i avsnitt 7.2.

I *första stycket* anges att den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för tillsynen och för att EU:s cybersäkerhetsakt, genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Den nationella myndigheten för cybersäkerhetscertifierings möjlighet att besluta om föreläggande med vite utgör en sådan lämplig nationell åtgärd för att säkerställa efterlevnad av regelverket som avses i artikel 58.8 c i EU:s cybersäkerhetsakt. Utfärdare av EU-försäkringar om överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och organ för bedömning av överensstämmelse kan således åläggas att åtgärda brister och uppfylla kraven i EU:s cybersäkerhetsakt eller en europeisk ordning för cybersäkerhetscertifiering. Motsvarande gäller för de krav som följer av den nya lagen och föreskrifter som meddelas i anslutning till lagen. Den nationella myndigheten för cybersäkerhetscertifiering bör dock i första hand försöka få den det gäller att frivilligt lämna information eller rätta till bristerna och således efterkomma myndighetens påpekanden. Befogenheten att besluta förelägganden innefattar även förelägganden som innebär förbud.

I *andra stycket* anges att ett beslut om föreläggande får förenas med vite. Allmänna bestämmelser om vite finns i lagen (1985:206) om viten. Det är den nationella myndigheten för cybersäkerhetscertifiering som i varje enskilt fall ska bedöma om det är lämpligt att förena ett beslut om föreläggande med vite.

6 § Den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än

bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Vid handräckning tillämpas bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Om den nationella myndigheten för cybersäkerhetscertifiering begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.

I paragrafen finns bestämmelser om handräckning. Övervägandena finns i avsnitt 7.1.

I *första stycket* anges att den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillgång till andra lokaler än bostäder och där genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Av artikel 58.8 d i EU:s cybersäkerhetsakt följer att rätten för den nationella myndigheten för cybersäkerhetscertifiering att få tillgång till lokaler omfattar lokaler hos ett organ för bedömning av överensstämmelse och innehavare av ett europeiskt cybersäkerhetscertifikat. För det fall den nationella myndigheten för cybersäkerhetscertifiering vägras tillträde till en lokal för att genomföra utredningar i enlighet med EU:s cybersäkerhetsakt får myndigheten begära handräckning av Kronofogdemyndigheten. Begäran om handräckning får inte avse en lokal som utgör bostad. Rätten till tillträde till lokaler enligt artikel 58.8 d i EU:s cybersäkerhetsakt omfattar inte lokaler hos en utfärdare av en EU-försäkran om överensstämmelse. Begäran om handräckning av Kronofogdemyndigheten får inte avse sådana lokaler.

I *andra stycket* anges att bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande tillämpas vid handräckning. Vidare anges att Kronofogdemyndigheten inte i förväg ska underrätta den som utredningen ska genomföras hos, om den nationella myndigheten för cybersäkerhetscertifiering begär det.

7 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering.

Paragrafen reglerar återkallelse av europeiska cybersäkerhetscertifikat. Övervägandena finns i avsnitt 7.6.

Av paragrafen följer att den nationella myndigheten för cybersäkerhetscertifiering får återkalla europeiska cybersäkerhetscertifikat när de förutsättningar som anges i artikel 58.8 e föreligger.

Ett beslut om återkallelse innebär att IKT-produkten, IKT-tjänsten eller IKT-processen inte längre får tillhandahållas på den inre marknaden som en cybersäkerhetscertifierad IKT-produkt, IKT-tjänst eller IKT-process enligt EU:s cybersäkerhetsakt. En tillverkare eller leverantör som i strid mot angivna bestämmelser ändå tillhandahåller en sådan IKT-produkt, IKT-tjänst eller IKT-process kan göra sig skyldig till överträdelse av regelverket som utgör grund för den nationella myndigheten för cybersäkerhetscertifiering att besluta om sanktionsavgift enligt 8 §.

Som *Lagrådet* uppmärksammar kan tänkbara grunder för ett beslut om återkallelse av ett europeiskt cybersäkerhetscertifikat med stöd av paragrafen vara att det har tillkommit nya normer på EU-nivå som innebär nya krav vilka certifikatet inte uppfyller, eller att certifikatet på något sätt har varit felaktigt redan när det utfärdades. Närmare praxis kring detta får utvecklas i rättstillämpningen.

Administrativa sanktionsavgifter

8 § Den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift av den som

1. har utfärdat en EU-försäkran om överensstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,
2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. har utfärdat en EU-försäkran om överensstämmelse eller innehar ett cybersäkerhetscertifikat och inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering,
6. överträder ett beslut om föreläggande enligt 5 § som innebär ett förbud, eller
7. använder ett europeiskt cybersäkerhetscertifikat som har återkallats enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

I paragrafen, som utformas enligt *Lagrådets* förslag, regleras sanktionsavgifter. Övervägandena finns i avsnitt 8.3.

I paragrafen anges de överträdelser av regelverket som kan föranleda att en sanktionsavgift ska tas ut av den som har gjort sig skyldig till överträdelsen. Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen. Av 10 § framgår att den nationella myndigheten för cybersäkerhetscertifiering ska beakta olika försvårande och förmildrande omständigheter vid prövningen av avgiftens storlek.

Enligt *punkten 1* ska den nationella myndigheten för cybersäkerhetscertifiering besluta att ta ut en sanktionsavgift av den som har utfärdat en EU-försäkran om överensstämmelse enligt artikel 53.2 trots att kraven i den europeiska ordning för cybersäkerhetscertifiering som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda.

Av *punkten 2* följer att en sanktionsavgift ska tas ut av den som har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering. En förutsättning för att sanktionsavgift ska beslutas är att de uppgifter som har lämnats är av betydelse för prövningen och bedömningen av överensstämmelse.

Av *punkten 3* följer att en sanktionsavgift ska tas ut av den som innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen. Sådan information ska delges skyndsamt i de fall en sårbarhet kan drabba tredje part.

Av *punkten 4* följer att en sanktionsavgift ska tas ut av den som har utfärdat en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada. Cybersäkerhetscertifiering syftar bl.a. till att höja säkerheten i IKT-produkter, IKT-tjänster och IKT-processer och på så sätt minska risken för sårbarheter och skador i system och i produkter. En sanktionsavgift ska därför endast kunna beslutas med stöd av punkten 4 om underlåtenheten att lämna information har medfört en sådan ökad risk för sårbarhet eller skada.

Av *punkten 5* följer att en sanktionsavgift ska tas ut av den som bryter mot villkor för utfärdande, bibehållande, fortsättande eller förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering.

Av *punkten 6* följer att en sanktionsavgift ska tas ut av den som överträder ett beslut om föreläggande enligt 5 § som innebär ett förbud.

Av *punkten 7* följer att en sanktionsavgift ska tas ut av den som använder ett europeiskt cybersäkerhetscertifikat som har återkallats enligt artikel 58.8 e.

9 § En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

I paragrafen regleras sanktionsavgifternas storlek. Övervägandena finns i avsnitt 8.5.

Enligt paragrafen ska en sanktionsavgift bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor. Hur avgiften ska bestämmas i det enskilda fallet regleras i 10 §. Det är den nationella myndigheten för cybersäkerhetscertifiering som beslutar om sanktionsavgiftens storlek.

10 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till
1. den skada eller risk för skada som har uppkommit till följd av överträdelsen,
2. om den som har begått överträdelsen tidigare begått en överträdelse, och
3. den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

I paragrafen regleras vilka omständigheter som särskilt ska beaktas när den nationella myndigheten för cybersäkerhetscertifiering bestämmer sanktionsavgiftens storlek. Övervägandena finns i avsnitt 8.6.

Av paragrafen framgår att särskild hänsyn ska tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den som har begått överträdelsen tidigare begått en överträdelse och den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

Vid bestämmande av storleken på sanktionsavgiften i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. I paragrafen anges sådana omständigheter som särskilt bör beaktas.

11 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

I paragrafen regleras jämkning av sanktionsavgift. Övervägandena finns i avsnitt 8.6.

Av paragrafen följer att den nationella myndigheten för cybersäkerhetscertifiering kan sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Det kan exempelvis vara oskäligt att ta ut en avgift om den avgiftsskyldige redan har drabbats av en sanktionsavgift enligt något annat regelverk för i princip samma brist. Att regelverket har överträtts på ett sådant sätt att det varit närmast omöjligt för den avgiftsskyldige att upptäcka överträdelsen eller överträdelsen på annat sätt varit utom den avgiftsskyldiges kontroll, kan i undantagsfall göra överträdelsen ursäktlig och därför utgöra grund för jämkning. Det kan också finnas grund för jämkning när det rör sig om en bedömningsfråga, t.ex. vilka certifieringsåtgärder som är nödvändiga i ett visst sammanhang – och berörd aktör trots en gedigen granskning gjort en felaktig bedömning. Andra omständigheter att beakta i mildrande riktning kan vara att den avgiftsskyldige har samarbetat med den nationella myndigheten för cybersäkerhetscertifiering för att komma till rätta med överträdelsen eller skyndsamt har vidtagit rättelse för att minska skadan eller risken för skada.

Regleringen i 9 § om sanktionsavgifternas storlek hindrar inte ett beslut om jämkning som innebär att sanktionsavgift tas ut med ett belopp som är lägre än 10 000 kronor.

12 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

I paragrafen regleras ett förbud mot beslut om sanktionsavgifter i vissa fall. Övervägandena finns i avsnitt 8.7.

Enligt paragrafen får en sanktionsavgift inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet. Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner.

Om ett beslut om vitesföreläggande har meddelats och en domstolsprocess inletts om utdömande av vitet är den nationella myndigheten för cybersäkerhetscertifiering enligt bestämmelsen förhindrad att besluta om sanktionsavgift för samma överträdelse. Bestämmelsen hindrar inte att en överträdelse först kan bli föremål för ett vitesföreläggande och i ett senare skede beslut om sanktionsavgift, under förutsättning att någon ansökan om utdömande av vitet inte har gjorts.

13 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

I paragrafen regleras när en sanktionsavgift får beslutas och krav på delgivning. Övervägandena finns i avsnitt 8.8.

Första stycket innebär att om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har gjorts inom två år från den dag då överträdelsen ägde rum, får en sanktionsavgift inte tas ut. Bevisbördan för att kommunikation har genomförts ligger på den nationella myndigheten för cybersäkerhetscertifiering.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen.

14 § Sanktionsavgiften tillfaller staten.

I paragrafen anges att en sanktionsavgift tillfaller staten. Övervägandena finns i avsnitt 8.8.

15 § En sanktionsavgift ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Paragrafen reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 8.8.

16 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen reglerar preskription av sanktionsavgifter. Övervägandena finns i avsnitt 8.8.

Bestämmelsen innebär att betalning av beslutad avgift inte kan krävas efter det att fem år gått sedan beslutet fick laga kraft.

Tystnadsplikt

17 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).

I paragrafen finns bestämmelser om tystnadsplikt. Övervägandena finns i avsnitt 11.4.

Enligt *första stycket* får den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s

cybersäkerhetsakt inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes. Organ för bedömning av överensstämmelse kan vara privaträttsliga aktörer, t.ex. ett aktiebolag. Tystnadsplikten innebär att personer som deltar i organet för bedömning av överensstämmelses verksamhet inte får avslöja eller utnyttja det han eller hon fått kännedom om under det att uppgifterna utfördes. Tystnadsplikten gäller såväl under som efter någons deltagande i verksamhet som omfattas av bestämmelsens tillämpningsområde. Den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

I *andra stycket* finns en upplysning om att offentlighets- och sekretesslagen tillämpas i det allmännas verksamhet. Det allmännas verksamhet innefattar t.ex. den verksamhet som den nationella myndigheten för cybersäkerhetscertifiering och offentliga organ för bedömning av överensstämmelse bedriver.

Avgifter

18 § Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana avgifter.

I paragrafen finns bestämmelser om avgifter. Övervägandena finns i avsnitt 6.3.

I *första stycket* anges att den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och den kompletterande lagen. Paragrafen innebär att tillsyns- och certifieringsverksamheterna vid den nationella myndigheten för cybersäkerhetscertifiering kan finansieras genom att avgifter tas ut av de aktörer som orsakar kostnaderna. Den nationella myndigheten för cybersäkerhetscertifiering bör kunna ta ut avgifter av utfärdare av EU-försäkran om överensstämmelse, organ för bedömning av överensstämmelse samt innehavare av europeiska cybersäkerhetscertifikat.

Enligt *andra stycket* får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om sådana avgifter.

Ändring av beslut av privata organ för bedömning av överensstämmelse

19 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och
2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Paragrafen reglerar ändring av beslut av privata organ för bedömning av överensstämmelse. Övervägandena finns i avsnitt 10.2.

Av paragrafen följer att privata organ för bedömning av överensstämmelse har en skyldighet att ändra ett beslut när beslutet är uppenbart

felaktigt på grund av nya omständigheter eller av någon annan anledning och beslutet kan ändras snabbt och enkelt utan att det blir till nackdel för någon enskild. Paragrafen har sin redaktionella förebild i 38 § förvaltningslagen.

Överklagande

20 § Beslut enligt EU:s cybersäkerhetsakt och denna lag av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen, som utformas enligt *Lagrådets* förslag, regleras överklagande av beslut. Övervägandena finns i avsnitt 10.3.

I *första stycket* anges att beslut av den nationella myndigheten för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt och denna lag får överklagas till allmän förvaltningsdomstol.

I fråga om förfarandet vid överklagande av beslut av organ för bedömning av överensstämmelse finns bestämmelser i lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter.

Enligt *andra stycket* krävs det prövningstillstånd vid överklagande till kammarrätten.

15.2 Förslaget till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

3 § I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

I paragrafen finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse. Övervägandena finns i avsnitt 9.2.4.

Andra stycket ändras på så sätt att Europaparlamentets och rådets förordning (EG) nr 765/2008 anges med dess nya titel.

7.6.2019 SV Europeiska unionens officiella tidning L 151/15

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/881

av den 17 april 2019

om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

med beaktande av Regionkommitténs yttrande [2],

i enlighet med det ordinarie lagstiftningsförfarandet [3], och

av följande skäl:

(1) Nätverks- och informationssystem samt elektroniska kommunikationsnät och kommunikationstjänster har en avgörande betydelse för samhället och har blivit själva ryggraden för ekonomisk tillväxt. Informations- och kommunikationsteknik (IKT) är grunden för komplexa system som stöder dagliga samhälleliga verksamheter, håller våra ekonomier igång inom viktiga sektorer som hälso- och sjukvård, energi, finans och transporter, och framför allt bidrar till den inre marknadens funktion.

(2) Användningen av nätverks- och informationssystem bland privatpersoner, organisationer och företag i hela unionen genomsyrar nu hela samhället. Digitalisering och konnektivitet är på väg att bli centrala inslag i ett allt större antal produkter och tjänster, och med tillkomsten av sakernas internet väntas ett extremt högt antal uppkopplade digitala enheter tas i bruk inom unionen under det kommande årtiondet. Trots att allt fler enheter är uppkopplade till internet, är säkerhet och resiliens inte tillräckligt integrerade i konstruktionen, vilket leder till otillräcklig cybersäkerhet. I detta sammanhang leder den begränsade användningen av certifiering till att enskilda användare, organisationsanvändare och företagsanvändare har otillräcklig information om cybersäkerheten hos IKT-produkter, IKT-tjänster och IKT-processer, vilket undergräver förtroendet för digitala lösningar. Nätverks- och informationssystem kan stödja alla aspekter av våra liv och bli en drivkraft för unionens ekonomiska tillväxt. De utgör grunden för uppnåendet av en digital inre marknad.

(3) Ökad digitalisering och konnektivitet leder till ökade cybersäkerhetsrisker, vilket gör samhället som helhet mer sårbart för cyberhot och ökar farorna för enskilda individer, inbegripet sårbara grupper som barn. För att minska dessa risker måste alla nödvändiga åtgärder vidtas för att stärka cybersäkerheten i unionen så att nätverks- och informationssystem, kommunikationsnät, digitala produkter, tjänster och enheter som används av privatpersoner, organisationer och företag – från små och medelstora företag enligt definitionen i kommissionens rekommendation 2003/361/EG [4], till operatörer av kritisk infrastruktur – skyddas bättre mot cyberhot.

[1] EUT C 227, 28.6.2018, s. 86.
[2] EUT C 176, 23.5.2018, s. 29.
[3] Europaparlamentets ståndpunkt av den 12 mars 2019 (ännu ej offentliggjord i EUT) och rådets beslut av den 9 april 2019.
[4] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

(4) Genom att tillgängliggöra relevant information för allmänheten bidrar Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), som inrättats genom Europaparlamentets och rådets förordning (EU) nr 526/2013 ([5]), till utvecklingen av cybersäkerhetsbranschen i unionen, särskilt små och medelstora företag och nystartade företag. Enisa bör sträva efter ett närmare samarbete med universitet och forskningsenheter för att bidra till en minskning av beroendet av cybersäkerhetsprodukter och -tjänster från länder utanför unionen och att förstärka distributionskedjor inom unionen.

(5) Cyberangreppen ökar och en uppkopplad ekonomi och ett uppkopplat samhälle som är mer utsatta för cyberhot och -angrepp kräver starkare skydd. Även om cyberangrepp ofta är gränsöverskridande, är dock behörigheten för, och de politiska insatserna från, cybersäkerhetsmyndigheter och brottsbekämpande organ till övervägande del nationella. Storskaliga incidenter kan störa tillhandahållandet av grundläggande tjänster i hela unionen. Detta kräver en effektiv och samordnad respons och krishantering på unionsnivå som bygger på särskilt utformade strategier och bredare instrument för europeisk solidaritet och ömsesidigt stöd. För beslutsfattare, näringsliv och användare är det också viktigt att det görs regelbundna bedömningar av situationen när det gäller cybersäkerhet och resiliens i unionen, på grundval av tillförlitliga unionsdata, samt systematiska prognoser för framtida utveckling, utmaningar och hot på unionsnivå och global nivå.

(6) Mot bakgrund av de allt större cybersäkerhetsutmaningar som unionen står inför behövs en omfattande uppsättning åtgärder som bygger vidare på tidigare unionsåtgärder och främjar mål som stärker varandra inbördes. Dessa mål innefattar att ytterligare öka medlemsstaternas och företagens kapacitet och beredskap samt att förbättra samarbete, informationsutbyte, och samordning mellan medlemsstaterna och unionens institutioner, organ och byråer. Med tanke på cyberhotens gränsöverskridande karaktär finns det dessutom ett behov av att öka kapaciteten på unionsnivå som ett komplement till medlemsstaternas insatser, särskilt när det gäller storskaliga gränsöverskridande incidenter och -kriser, samtidigt som man beaktar vikten av att underhålla och ytterligare stärka den nationella kapaciteten att bemöta cyberhot av alla storlekar.

(7) Ytterligare insatser behövs också för att öka privatpersoners, organisationers och företagens medvetenhet om cybersäkerhetsfrågor. Dessutom bör, med tanke på att incidenter skadar förtroendet för leverantörerna av digitala tjänster och den digitala marknaden i sig, inte minst bland konsumenter, förtroendet stärkas ytterligare genom att information tillhandahålls på ett transparent sätt om säkerhetsnivån för IKT-produkter, IKT-tjänster och IKT-processer, samtidigt som det understryks att inte ens en hög nivå av cybersäkerhetscertifiering kan garantera att en IKT-produkt, IKT-tjänst eller IKT-process är helt säker. Ett ökat förtroende kan underlättas genom unionsomfattande certifiering som erbjuder gemensamma cybersäkerhetskrav och utvärderingskriterier för olika nationella marknader och sektorer.

(8) Cybersäkerhet är inte bara en fråga kopplad till teknik, utan en fråga där mänskligt beteende är lika viktigt. Därför bör *it-hygien*, det vill säga enkla rutinåtgärder som, när de genomförs och utförs regelbundet av medborgare, organisationer och företag, minimerar deras exponering för risker från cyberhot, starkt främjas.

(9) I syfte att stärka unionens cyberförsvarsstrukturer är det viktigt att underhålla och utveckla medlemsstaternas förmåga att bemöta cyberhot, inbegripet gränsöverskridande incidenter, på ett övergripande sätt.

(10) Företag och enskilda konsumenter bör få korrekt information om säkerhetscertifieringsnivån för deras IKT-produkter, IKT-tjänster och IKT-processer. Samtidigt är ingen produkt helt cybersäker och grundläggande regler för it-hygien måste främjas och prioriteras. Med tanke på den ökande tillgången till uppkopplade apparater finns det en rad frivilliga åtgärder som den privata sektorn kan vidta för att stärka förtroendet för IKT-produkters, IKT-tjänsters och IKT-processers säkerhet.

(11) Moderna IKT-produkter och IKT-system inbegriper ofta, och förlitar sig på, en eller flera komponenter liksom teknik från tredje part, som är nödvändiga för produkten eller tjänsten, t.ex. programmoduler, bibliotek eller programmeringsgränssnitt. Detta beroende skulle kunna innebära extra cybersäkerhetsrisker eftersom sårbarheter i sådana tredjepartskomponenter även kan påverka IKT-produkternas, IKT-tjänsternas och IKT-processernas säkerhet. Om sådana beroendeförhållanden identifieras och dokumenteras kan användare av IKT-produkter, IKT-tjänster och IKT-processer ofta förbättra sin cybersäkerhetsriskhantering genom att exempelvis förbättra sina förfaranden för att hantera och avhjälpa sårbarheter.

([5]) Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004 (EUT L 165, 18.6.2013, s. 41).

(12) Organisationer, tillverkare och leverantörer som är inblandade i utformningen och utvecklingen av IKT-produkter, IKT-tjänster och IKT-processer bör uppmuntras att, i ett tidigt skede av utformningen och utvecklingen, genomföra åtgärder på ett sätt så att säkerheten för dessa produkter, tjänster och processer skyddas i högsta möjliga grad, så att förekomsten av cyberattacker tas med i beräkningen och att de eventuella konsekvenserna av dem förutses och minimeras (nedan kallad *inbyggd säkerhet*). Säkerhetsaspekten bör säkerställas under IKT-produktens, IKT-tjänstens och IKT-processens hela livstid genom att man kontinuerligt utvecklar utformnings- och utvecklingsprocesserna för att minska risken för skada från skadlig användning.

(13) Företag, organisationer och den offentliga sektorn bör konfigurera IKT-produkter, IKT-tjänster och IKT-processer som de utformar på ett sätt som säkerställer en högre grad av säkerhet, som gör att den första användaren kan få den förvalda konfigurationen med de säkraste inställningarna (nedan kallad *säkerhet som standard*) och därmed minska användarnas börda av att behöva konfigurera en IKT-produkt, IKT-tjänst eller IKT-process på lämpligt vis. Säkerhet som standard bör inte kräva omfattande konfigurering eller specifika tekniska kunskaper eller icke-intuitivt handlande från användarens sida som inte känns naturliga, och bör fungera enkelt och tillförlitligt när den tillämpas. Om en riskanalys och en användbarhetsanalys från fall till fall leder till slutsatsen att det inte är möjligt att göra en sådan förvald inställning, bör användarna uppmanas att välja den säkraste inställningen.

(14) Europaparlamentet och rådets förordning (EG) nr 460/2004 ([6]) inrättande Enisa med syftet att bidra till målet att säkerställa en hög och effektiv nivå på nätverks- och informationssäkerheten i unionen och utveckla en kultur av nätverks- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga administrationen. Europaparlamentet och rådets förordning (EG) nr 1007/2008 ([7]) som förlängde Enisas mandat till mars 2012. Genom Europaparlamentets och rådets förordning (EU) nr 580/2011 ([8]) förlängdes Enisas mandat ytterligare till den 13 september 2013. Förordning (EU) nr 526/2013 förlängde Enisas mandat till den 19 juni 2020.

(15) Unionen har redan vidtagit viktiga åtgärder för att säkerställa cybersäkerhet och öka förtroendet för digital teknik. År 2013 antogs EU:s strategi för cybersäkerhet för att vägleda EU:s politiska åtgärder för cyberhot och -risker. I en satsning för att bättre skydda invånarna på nätet antogs unionens första rättsakt på cybersäkerhetsområdet 2016 i form av Europaparlamentets och rådets direktiv (EU) 2016/1148 ([9]). Direktiv (EU) 2016/1148 införde krav om nationell kapacitet på cybersäkerhetsområdet, inrättade de första mekanismerna för att stärka det strategiska och operativa samarbetet mellan medlemsstaterna och införde skyldigheter avseende säkerhetsåtgärder och incidentrapportering inom sektorer som är centrala för ekonomin och samhället, såsom energi, transporter, leverans och distribution av dricksvatten, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, digital infrastruktur samt leverantörer av viktiga digitala tjänster (sökmotorer, molntjänster och elektroniska marknadsplatser).

Enisa fick en viktig roll när det gällde att stödja genomförandet av det direktivet. Dessutom är en effektiv kamp mot it-brottslighet en viktig prioritering i den europeiska säkerhetsagendan, som bidrar till det övergripande målet att uppnå en hög nivå av cybersäkerhet. Andra rättsakter såsom Europaparlamentets och rådets förordning (EU) 2016/679 ([10]) och Europaparlamentets och rådets direktiv 2002/58/EG ([11]) och (EU) 2018/1972 ([12]) kan också bidra till en hög cybersäkerhetsnivå på den digitala inre marknaden.

([6]) Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet (EUT L 77, 13.3.2004, s. 1).
([7]) Europaparlamentets och rådets förordning (EG) nr 1007/2008 av den 24 september 2008 om ändring av förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet i fråga om dess mandatperiod (EUT L 293, 31.10.2008, s. 1).
([8]) Europaparlamentets och rådets förordning (EU) nr 580/2011 av den 8 juni 2011 om ändring av förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet vad gäller dess varaktighet (EUT L 165, 24.6.2011, s. 3).
([9]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).
([10]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).
([11]) 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) (EGT L 201, 31.7.2002, s. 37).
([12]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

(16) Sedan antagandet av EU:s strategi för cybersäkerhet 2013 och den senaste översynen av Enisas uppdrag, har den övergripande politiska ramen förändrats avsevärt eftersom den globala miljön har blivit mer oviss och mindre säker. Mot denna bakgrund och mot bakgrund av den positiva utvecklingen av Enisas roll till en referenspunkt för rådgivning och expertis, som en kontaktpunkt för samarbete och kapacitetsuppbyggnad, samt inom ramen för unionens nya cybersäkerhetsstrategi är det nödvändigt att se över Enisas mandat för att definiera dess roll i det förändrade cybersäkerhetsekosystemet och säkerställa att Enisa bidrar effektivt till unionens reaktion på cybersäkerhetsutmaningar som härrör från den radikalt förändrade hotbilden inom cyberområdet, för vilket det nuvarande mandatet är inte tillräckligt, vilket också medges i utvärderingen av Enisa.

(17) Enisa som inrättas genom denna förordning bör efterträda Enisa, som inrättades genom förordning (EU) nr 526/2013. Enisa bör utföra de uppgifter som den tilldelas genom den här förordningen och andra unionsrättsakter på cybersäkerhetsområdet genom att bland annat tillhandahålla rådgivning och expertis och fungera som unionens informations- och kunskapscentrum. Kommissionen bör främja utbyte av bästa praxis mellan medlemsstaterna och privata aktörer, lägga fram strategiförslag för kommissionen och medlemsstaterna som kan användas som utgångspunkt för unionens sektorsvisa politiska initiativ när det gäller cybersäkerhet och för att främja praktiskt samarbete både medlemsstaterna emellan och mellan medlemsstaterna och unionens institutioner, organ och byråer.

(18) Inom ramen för beslut 2004/97/EG, Euratom antaget i samförstånd mellan medlemsstaternas företrädare, församlade på stats- eller regeringschefsnivå ([13]), beslutade medlemsstaternas företrädare att Enisa skulle ha sitt säte i en stad i Grekland som skulle fastställas av den grekiska regeringen. Enisas värdmedlemsstat bör säkerställa bästa möjliga förutsättningar för en smidig och effektiv drift av Enisa. Det är mycket viktigt att Enisa är förlagd till en lämplig plats, där det bland annat finns lämpliga transportförbindelser och faciliteter för makar och barn som medföljer Enisas personal, för att Enisa ska kunna utföra sina uppgifter väl och effektivt samt för möjligheterna att rekrytera och behålla personal och för en effektivare nätverksverksamhet. De nödvändiga arrangemangen bör efter godkännande av Enisas styrelse fastställas i ett avtal mellan Enisa och värdmedlemsstaten.

(19) Med tanke på de ökande cybersäkerhetsrisker och cybersäkerhetsutmaningar som unionen står inför bör de ekonomiska och personella resurser som anslagits för Enisa ökas för att återspegla dess förstärkta roll och arbetsuppgifter och dess centrala position i ekosystemet av organisationer som försvarar unionens digitala ekosystem, så att Enisa effektivt kan utföra de uppgifter som Enisa tilldelas genom denna förordning.

(20) Enisa bör utveckla och underhålla en hög nivå av expertis och fungera som en referenspunkt och skapa förtroende och tillit för den inre marknaden genom sin opartiskhet, kvaliteten på de råd och den information den tillhandahåller, öppenheten i dess förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter. Enisa bör aktivt stödja nationella ansträngningar och bör aktivt bidra till unionsinsatser och utföra sina uppgifter i fullt samarbete med unionens institutioner, organ och byråer samt med medlemsstaterna, och därigenom undvika dubbelarbete och främja synergier. Enisa bör också stödja sig på synpunkter från och samarbete med den privata sektorn och andra berörda aktörer. Genom en uppsättning uppgifter bör det fastställas hur Enisa ska uppnå sina mål samtidigt som flexibilitet i verksamheten möjliggörs.

(21) För att kunna ge lämpligt stöd till det operativa samarbetet mellan medlemsstaterna bör Enisa ytterligare stärka sin tekniska och mänskliga kapacitet och kompetens. Enisa bör öka sitt kunnande och sin kapacitet. Enisa och medlemsstaterna kan (på frivillig basis) ta fram program för utstationering av nationella experter till Enisa, skapande av expertpooler och utbytesprogram för de anställda.

(22) Enisa bör bistå kommissionen med råd, yttranden och analyser i alla unionsfrågor som rör utveckling, uppdatering och översyn av politik och lagstiftning på cybersäkerhetsområdet och dess sektorsspecifika aspekter för att öka relevansen av unionens politik och lagstiftning med en cybersäkerhetsdimension och möjliggöra konsekvens i genomförandet av denna politik och lagstiftning på nationell nivå. Enisa bör fungera som en referenspunkt för rådgivning och expertis för unionens sektorsspecifika politik och lagstiftningsinitiativ i frågor som rör cybersäkerhet. Enisa bör regelbundet informera Europaparlamentet om sin verksamhet till.

([13]) Beslut 2004/97/EG, Euratom antaget i samförstånd mellan medlemsstaternas företrädare, församlade på stats- eller regeringschefsnivå av den 13 december 2003 om lokaliseringen av sätena för vissa av Europeiska unionens myndigheter och byråer (EUT L 29, 3.2.2004, s. 15).

(23) Den offentliga kärnan av ett öppet internet, nämligen dess huvudsakliga protokoll och infrastruktur utgör globala allmänna nyttigheter, ger internet dess viktiga funktioner som en helhet och underbygger dess normala funktion. Enisa bör stödja säkerheten för den offentliga kärnan av ett öppet internet och stabiliteten för dess funktionssätt och bland annat, men inte begränsat till, nyckelprotokollen (framför allt DNS, BGP och IPv6), driften av domännamnssystemet (till exempel driften av alla toppdomäner) och driften av rotzonen.

(24) Den underliggande uppgiften för Enisa är att främja ett konsekvent genomförande av den gällande rättsliga ramen, i synnerhet ett effektivt genomförande av direktiv (EU) 2016/1148 och andra relevanta rättsliga instrument som avser cybersäkerhetsaspekter, vilket är viktigt för att öka cyberresiliensen. Mot bakgrund av den snabbt föränderliga hotbilden inom cyberområdet på cyberområdet är det uppenbart att medlemsstaterna måste stödjas genom en mer omfattande tvärpolitisk strategi för att bygga upp cyberresiliens.

(25) Enisa bör bistå medlemsstaterna och unionens institutioner, organ och byråer i deras arbete för att bygga upp och förbättra kapacitet och beredskap för att förebygga, upptäcka och reagera på cyberhot och cyberincidenter samt i fråga om säkerhet i nätverks- och informationssystem. Enisa bör särskilt stödja utvecklingen och stärkandet av nationella och unionens enheter för hantering av it-säkerhetsincidenter (Computer Security Incident Response Teams, nedan kallade *CSIRT-enheter*) enligt direktiv (EU) 2016/1148, i syfte att uppnå en hög gemensam mognadsnivå för dem i unionen. Den verksamhet som bedrivs av Enisa avseende medlemsstaternas operativa kapacitet bör aktivt stödja medlemsstaternas åtgärder för att fullgöra sina skyldigheter enligt direktiv (EU) 2016/1148 och bör därför inte ersätta dem.

(26) Enisa bör också bistå med utveckling och uppdatering av strategier för säkerhet i nätverks- och informationssystem på unionsnivå och, på begäran, på medlemsstatsnivå, särskilt för cybersäkerhet, och bör främja spridningen av sådana strategier och följa upp framstegen med deras genomförande. Enisa bör också bidra till uppfyllandet av behoven av utbildning och utbildningsmaterial, däribland offentliga organs behov, och i lämpliga fall huvudsakligen ”utbilda utbildarna” baserat på den europeiska ramen för utveckling av digital kompetens bland medborgarna, för att bistå medlemsstaterna och unionens institutioner, organ och byråer när de utvecklar sin egen utbildningskapacitet.

(27) Enisa bör stödja medlemsstaterna på området medvetenhet och utbildning om cybersäkerhet genom att främja närmare samarbete och utbyte av bästa praxis bland medlemsstaterna. Sådant stöd skulle bland annat kunna bestå i utveckling av ett nätverk av nationella utbildningskontaktpunkter och utvecklingen av en utbildningsplattform för cybersäkerhet. Nätverket av nationella utbildningskontaktpunkter skulle kunna verka inom ramen för nätverket för nationella kontaktpersoner och vara en startpunkt för framtida samordning inom medlemsstaterna.

(28) Enisa bör bistå den samarbetsgrupp som inrättats genom direktiv (EU) 2016/1148 vid utförandet av dess uppgifter, särskilt genom att tillhandahålla expertis och rådgivning och underlätta utbytet av bästa praxis, bland annat vad gäller medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, även i samband med gränsöverskridande beroenden, vad gäller risker och incidenter.

(29) I syfte att stimulera samarbete mellan offentlig och privat sektor samt inom den privata sektorn, särskilt för att stödja skyddet av kritisk infrastruktur, bör Enisa stödja informationsutbyte inom och mellan sektorer, i synnerhet de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148, genom att tillhandahålla bästa praxis och vägledning i fråga om tillgängliga verktyg och förfaranden samt om hur regleringsfrågor som rör informationsutbyte ska hanteras, exempelvis genom att underlätta inrättandet av sektorsvisa centrum för informationsutbyte och analys.

(30) De potentiella negativa effekterna av sårbarheter hos IKT-produkter, IKT-tjänster och IKT-processer ökar ständigt och det är viktigt att upptäcka och åtgärda sådana sårbarheter för att minska den samlade cybersäkerhetsrisken. Det har visat sig att samarbete mellan organisationer, tillverkare eller leverantörer av sårbara IKT-produkter, IKT-tjänster och IKT-processer, personer som sysslar med cybersäkerhetsforskning och regeringar som upptäcker sårbarheter avsevärt ökar både upptäckterna och åtgärdandet av sårbarheter hos IKT-produkter, IKT-tjänster och IKT-processer. Samordnad information om sårbarheter utgör en strukturerad samarbetsprocess där sårbarheter rapporteras till ägaren av ett informationssystem vilket möjliggör för organisationen att diagnostisera och åtgärda sårbarheten innan detaljer om sårbarheten blir kända för tredje parter eller allmänheten. Processen möjliggör också samordning mellan den som upptäckt sådana sårbarheter och organisationen vad gäller offentliggörande av dessa sårbarheter. Samordnade riktlinjer för att offentliggöra sårbarheter skulle kunna spela en viktig roll i medlemsstaternas insatser för att stärka cybersäkerheten.

(31) Enisa bör sammanställa och analysera nationella rapporter som delats på frivillig grund från CSIRT-enheter och den interinstitutionella incidenthanteringsorganisationen för unionens institutioner och byråer (nedan kallad *CERT-EU*) som inrättats genom avtalet mellan Europaparlamentet, Europeiska rådet, Europeiska unionens råd, Europeiska kommissionen, Europeiska unionens domstol, Europeiska centralbanken, Europeiska revisionsrätten, Europeiska utrikestjänsten, Europeiska ekonomiska och sociala kommittén, Europeiska regionkommittén och Europeiska investeringsbanken om organiseringen och driften av incidenthanteringsorganisationen för unionens institutioner och byråer (CERT-EU) ([14]) för att bidra till upprättandet av gemensamma förfaranden, gemensamt språk och gemensam terminologi för utbyte av information. Enisa bör även i detta sammanhang engagera den privata sektorn, inom ramen för direktiv (EU) 2016/1148 som lade grunden för frivilligt utbyte av teknisk information på operativ nivå, i nätverket för enheter för hantering av it-säkerhetsincidenter (nedan kallat *CSIRT-nätverket*) som inrättats genom det direktivet.

(32) Enisa bör bidra till insatser på unionsnivå i samband med storskaliga gränsöverskridande incidenter och -kriser avseende cybersäkerhet. Denna uppgift bör utföras i enlighet med Enisas mandat enligt denna förordning och en metod som medlemsstaterna enats om inom ramen för kommissionens rekommendation (EU) 2017/1584 ([15]) och rådets slutsatser av den 26 juni 2018 om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser. Den uppgiften skulle kunna omfatta insamling av relevant information och att fungera som kontaktpunkt mellan CSIRT-nätverket och såväl tekniska aktörer som beslutsfattare med ansvar för krishantering. Vidare bör Enisa stödja det operativa samarbetet mellan medlemsstater, på begäran av en eller flera medlemsstater, i hanteringen av incidenter ur ett tekniskt perspektiv och underlätta utbyte av relevanta tekniska lösningar mellan medlemsstaterna och genom att ge input till kommunikation med allmänheten. Enisa bör stödja det operativa samarbetet genom att granska formerna för sådant samarbete genom regelbundna cybersäkerhetsövningar.

(33) Till stöd för det operativa samarbetet bör Enisa använda tillgänglig teknisk och operativ expertis från CERT-EU genom ett strukturerat samarbete. Det strukturerade samarbetet skulle kunna förstärka Enisas expertis. Vid behov bör särskilda arrangemang mellan de båda enheterna inrättas för att definiera det praktiska genomförandet av detta samarbete och undvika dubbelarbete.

(34) I fullgörandet av sina uppgifter till stöd för det operativa samarbetet inom CSIRT-nätverket bör Enisa kunna tillhandahålla stöd till medlemsstaterna om de begär det, till exempel genom att ge råd om hur de ska förbättra sin förmåga att förebygga, upptäcka och reagera på incidenter, genom att underlätta den tekniska hanteringen av incidenter som har en betydande eller avsevärd inverkan, eller genom att säkerställa att hot och incidenter analyseras. Enisa bör underlätta den tekniska hanteringen av incidenter som har en betydande eller avsevärd inverkan framför allt genom att stödja frivilligt utbyte av tekniska lösningar mellan medlemsstater eller genom att ta fram kombinerad teknisk information (t.ex. tekniska lösningar som medlemsstaterna delar på frivillig grund). I rekommendation (EU) 2017/1584 rekommenderas medlemsstaterna att samarbeta i god tro och utbyta information sinsemellan och med Enisa om storskaliga incidenter och kriser avseende cybersäkerhet utan onödigt dröjsmål. Sådan information skulle kunna hjälpa Enisa att utföra sin uppgift att stödja det operativa samarbetet.

(35) Som en del av det löpande samarbetet på teknisk nivå för att stödja en gemensam situationsmedvetenhet i unionen bör Enisa, i nära samarbete med medlemsstaterna, ta fram en regelbunden och fördjupad teknisk EU-lägesrapport om cyberincidenter och cyberhot, baserad på allmänt tillgänglig information, sin egen analys och rapporter som Enisa får från medlemsstaternas CSIRT-enheter eller de nationella gemensamma kontaktpunkterna för säkerhet i nätverks- och informationssystem enligt direktiv (EU) 2016/1148, båda på frivillig grund, Europeiska it-brottscentrumet (EC3) vid Europol, CERT-EU och, i tillämpliga fall, Europeiska unionens underrättelseanalyscentrum (EU Intcen) vid Europeiska utrikestjänsten. Rapporten bör göras tillgänglig för rådet, kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik samt CSIRT-nätverket.

(36) Enisas stöd till tekniska efterhandsundersökningar av incidenter med betydande eller avsevärda konsekvenser som inletts på begäran av de berörda medlemsstaterna bör inriktas på att förhindra framtida incidenter. De berörda medlemsstaterna bör tillhandahålla den information och assistans som behövs för att göra det möjligt för Enisa att på ett ändamålsenligt sätt stödja den tekniska efterhandsundersökningen.

([14]) EUT C 12, 13.1.2018, s. 1.
([15]) Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

(37) Medlemsstaterna får uppmana företag som berörs av incidenten att samarbeta genom att tillhandahålla nödvändig information och assistans till Enisa utan att det påverkar deras rätt att skydda kommersiellt känslig information och information som är relevant för allmän säkerhet.

(38) För att bättre förstå utmaningarna inom cybersäkerhetsområdet, och i syfte att tillhandahålla strategisk långsiktig rådgivning till medlemsstaterna och unionens institutioner, organ och byråer, behöver Enisa analysera nuvarande och framväxande cybersäkerhetsrisker. För detta ändamål bör Enisa i samarbete med medlemsstaterna och, om lämpligt, med statistikorgan och andra organ samla in relevant information som är offentligt tillgänglig eller som delats på frivillig grund och utföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om förväntade samhälleliga, rättsliga, ekonomiska och regleringsmässiga konsekvenser av tekniska innovationer inom området nätverks- och informationssäkerhet, i synnerhet cybersäkerhet. Enisa bör också hjälpa medlemsstaterna och unionens institutioner, organ och byråer att identifiera framväxande cybersäkerhetsrisker och förebygga incidenter, genom att utföra analyser av cyberhot, sårbarheter och incidenter.

(39) För att stärka unionens resiliens bör Enisa utveckla expertis på området cybersäkerhet i infrastrukturer, särskilt inom de sektorer som anges i bilaga II till direktiv (EU) 2016/1148 och de som används av de leverantörer av digitala tjänster som förtecknas i bilaga III till det direktivet genom att tillhandahålla rådgivning, vägledning och bästa praxis. För att säkerställa enklare tillgång till bättre strukturerad information om cybersäkerhetsrisker och möjliga motåtgärder bör Enisa utarbeta och underhålla unionens *informationsnav*, en gemensam webbportal som förser allmänheten med information om cybersäkerhet från unionens och medlemsstaternas institutioner, organ och byråer. Att underlätta tillgången till bättre strukturerad information om cybersäkerhetsrisker och möjliga motåtgärder skulle också kunna hjälpa medlemsstaterna att stärka sin kapacitet och anpassa sin praxis, och därmed att bättre stå emot cyberattacker i allmänhet.

(40) Enisa bör bidra till att öka allmänhetens medvetenhet om cybersäkerhetsrisker, bland annat genom en EU-omfattande informationskampanj, genom att främja utbildning och ge vägledning om god praxis för enskilda användare riktad till privatpersoner, organisationer och företag. Enisa bör även bidra till att främja bästa praxis och lösningar, bland annat it-hygien och it-kompetens, för privatpersoner, organisationer och företag genom att samla in och analysera offentligt tillgänglig information om betydande incidenter och genom att sammanställa och offentliggöra rapporter och handböcker i syfte att ge vägledning till privatpersoner, organisationer och företag och att höja den allmänna beredskaps- och resiliensnivån. Enisa bör även sträva efter att förse konsumenter med relevant information om gällande certifieringsordning, t.ex. genom att tillhandahålla riktlinjer och rekommendationer. Enisa bör vidare, i enlighet med handlingsplanen för digital utbildning som fastställdes i kommissionens meddelande av den 17 januari 2018 och i samarbete med medlemsstaterna och unionens institutioner, organ och byråer, organisera regelbundna informations- och folkbildningskampanjer riktade till slutanvändare, i syfte att främja ett säkrare beteende bland enskilda internetanvändare och digital kompetens, för att höja medvetenheten om de potentiella hoten i cyberrymden, bland annat it-brottslighet såsom phishingattacker, botnät, ekonomiska bedrägerier och bankbedrägerier, incidenter rörande databedrägeri, samt att främja grundläggande rådgivning om flerfaktorautentisering, programkorrigeringar, kryptering, anonymisering och dataskydd.

(41) Enisa bör spela en central roll när det gäller att höja slutanvändarnas medvetenhet om enheters säkerhet och säker användning av tjänster, och bör främja inbyggd säkerhet och inbyggt integritetsskydd på unionsnivå. För att uppnå detta mål bör Enisa på lämpligaste sätt använda tillgänglig bästa praxis och erfarenhet, framför allt bästa praxis och erfarenhet från akademiska institutioner och it-säkerhetsforskare.

(42) För att stödja både de företag som verkar inom den europeiska cybersäkerhetssektorn och användarna av cybersäkerhetslösningar bör Enisa utveckla och underhålla ett ”marknadsobservatorium” genom att utföra regelbundna analyser och spridning av information om de viktigaste trenderna på cybersäkerhetsmarknaden, både på tillgångs- och efterfrågesidan.

(43) Enisa bör bidra till unionens insatser för samarbete med internationella organisationer och inom ramarna för relevant internationellt samarbete på cybersäkerhetsområdet. Enisa bör framför allt, där så är lämpligt, bidra till samarbetet med organisationer som OECD, OSSE och Nato. Sådant samarbete kan omfatta gemensamma cybersäkerhetsövningar och gemensam samordning av insatser vid incidenter. Denna verksamhet ska utövas med full respekt för principerna om delaktighet, ömsesidighet och unionens beslutsautonomi, utan att det påverkar den särskilda karaktären hos någon medlemsstats säkerhets- och försvarspolitik.

(44) För att se till att Enisa fullt ut uppnår sina mål bör den samarbeta med berörda EU-tillsynsmyndigheter och andra behöriga myndigheter i unionen, EU-institutioner, -byråer och -organ, däribland CERT-EU, EC3, Europeiska försvarsbyrån (EDA), Europeiska byrån för GNSS (GSA), Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec), Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA), Europeiska centralbanken (ECB), Europeiska bankmyndigheten (EBA), Europeiska dataskyddsstyrelsen, Byrån för samarbete mellan energitillsynsmyndigheter (Acer), Europeiska unionens byrå för luftfartssäkerhet (Easa) och andra unionsorgan som arbetar med cybersäkerhet. Enisa bör också samverka med myndigheter som hanterar dataskydd för att utbyta sakkunskap och bästa praxis samt ge råd om cybersäkerhetsaspekter som kan påverka deras arbete. Företrädare för medlemsstaternas och unionens rättsvårdande myndigheter och dataskyddsmyndigheter bör ha rätt att företrädas i Enisas rådgivande grupp. I samarbetet med rättsvårdande myndigheter om nätverks- och informationssäkerhetsaspekter som kan påverka deras arbete bör Enisa använda existerande informationskanaler och etablerade nätverk.

(45) Samarbete kan upprättas med akademiska institutioner med forskningsinitiativ inom berörda områden och det bör finnas lämpliga kanaler för konsumentorganisationer och andra organisationer att framföra sina synpunkter, vilka bör beaktas.

(46) Enisa bör i sin funktion som sekretariat åt CSIRT-nätverket stödja medlemsstaternas CSIRT-enheter och CERT-EU i det operativa samarbetet avseende alla relevanta uppgifter för CSIRT-nätverket som avses i direktiv (EU) 2016/1148. Enisa bör dessutom främja och stödja samarbete mellan de berörda CSIRT-enheterna i händelse av incidenter, attacker mot eller störningar i de nät eller den infrastruktur som förvaltas eller skyddas av dem och som berör eller kan beröra minst två CSIRT-enheter, och därvid beakta CSIRT-nätverkets operationella standardförfaranden.

(47) För att öka unionens beredskap att hantera incidenter bör Enisa regelbundet organisera cybersäkerhetsövningar på unionsnivå och, på deras begäran, bistå medlemsstaterna och unionens institutioner, organ och byråer med att organisera sådana övningar. En gång vartannat år bör en storskalig heltäckande övning med tekniska, operativa och strategiska inslag organiseras. Enisa bör därutöver regelbundet kunna organisera mindre omfattande övningar med samma mål, att öka unionens beredskap att hantera incidenter.

(48) Enisa bör vidareutveckla och underhålla sina kunskaper om cybersäkerhetscertifiering för att stödja unionens politik på detta område. Enisa bör bygga vidare på befintlig bästa praxis och främja spridningen av cybersäkerhetscertifiering i unionen, bland annat genom att bidra till inrättandet och underhållandet av ett ramverk för cybersäkerhetscertifiering på unionsnivå (europeiskt ramverk för cybersäkerhetscertifiering), i syfte att öka öppenheten i fråga om assuransnivån för cybersäkerhet hos IKT-produkter, IKT-tjänster IKT-processer genom att stärka förtroendet för den digitala inre marknaden och dess konkurrenskraft.

(49) Effektiva cybersäkerhetsstrategier bör bygga på välutvecklade metoder för riskbedömning, både inom den offentliga och inom den privata sektorn. Riskbedömningsmetoder används på olika nivåer, men det saknas gemensam praxis för hur de ska tillämpas på ett effektivt sätt. Främjande och utveckling av bästa praxis för riskbedömning och för interoperabla lösningar för riskhantering inom organisationer i den offentliga och privata sektorn kommer att höja cybersäkerhetsnivån i unionen. Därför bör Enisa stödja samarbete mellan intressenter på unionsnivå och främja deras insatser för upprättande och tillämpning av europeiska och internationella standarder för riskhantering och mätbar säkerhet för elektroniska produkter, system, nät och tjänster som tillsammans med programvara utgör nätverks- och informationssystemen.

(50) Enisa bör uppmuntra medlemsstaterna, tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer att höja sina allmänna säkerhetsstandarder så att alla internetanvändare kan vidta de åtgärder som krävs för att trygga sin egen cybersäkerhet och bör ha incitament att göra detta. I synnerhet bör tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer tillhandahålla nödvändiga uppdateringar och bör återkalla, dra tillbaka eller återvinna IKT-produkter, IKT-tjänster eller IKT-processer som inte uppfyller cybersäkerhetsstandarderna, medan importörer och distributörer bör säkerställa att IKT-produkter, IKT-tjänster och IKT-processer som de släpper ut på unionsmarknaden uppfyller gällande krav och inte utgör en risk för unionens konsumenter.

(51) I samarbete med de behöriga myndigheterna bör Enisa kunna sprida uppgifter om cybersäkerhetsnivån för de IKT-produkter, IKT-tjänster och IKT-processer som erbjuds på den inre marknaden, och utfärda varningar riktade till tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer och ålägga dem att förbättra sina IKT-produkters, IKT-tjänsters och IKT-processers säkerhet, inbegripet cybersäkerhet.

(52) Enisa bör i sitt arbete fullt ut beakta pågående forskning, utveckling och tekniska bedömningar, i synnerhet sådan verksamhet som bedrivs inom unionens olika forskningsinitiativ för att ge råd till unionens institutioner, organ och byråer och, i tillämpliga fall, till medlemsstaterna på deras begäran om forskningsbehoven och prioriteringarna på området cybersäkerhet. För att identifiera behov och prioriteringar för forskningen bör Enisa även rådfråga berörda användargrupper. Mer specifikt skulle ett samarbete kunna upprättas med Europeiska forskningsrådet, Europeiska institutet för innovation och teknik och Europeiska unionens institut för säkerhetsstudier.

(53) Vid utarbetandet av de europeiska ordningarna för cybersäkerhetscertifiering bör Enisa regelbundet samråda med standardiseringsorganisationerna, i synnerhet de europeiska standardiseringsorganisationerna.

(54) Cyberhot är en global fråga. Det behövs ett tätare internationellt samarbete för att förbättra cybersäkerhetsstandarder, bland annat genom att fastställa gemensamma beteendenormer och anta uppförandekoder, användning av internationella standarder, och informationsutbyte, och på så vis främja snabbare internationellt samarbete som svar på nätverks- och informationssäkerhetsproblem och främja en gemensam global syn på sådana problem. Därför bör Enisa stödja ett starkare unionsdeltagande och samarbete med tredjeländer och internationella organisationer genom att, när så är lämpligt, tillhandahålla nödvändig expertis och nödvändiga analyser till berörda unionsinstitutioner, organ och byråer.

(55) Enisa bör kunna besvara ad hoc-förfrågningar om råd och bistånd från medlemsstaterna och unionens institutioner, organ och byråer som omfattas av Enisas uppdrag.

(56) Det är klokt och tillrådligt att genomföra vissa principer för Enisas förvaltning i syfte att följa det gemensamma uttalande och den gemensamma ansats som den interinstitutionella arbetsgruppen för EU:s decentraliserade byråer enades om i juli 2012 och vars syfte är att effektivisera de decentraliserade byråernas verksamhet och förbättra deras resultat. Rekommendationerna i det gemensamma uttalandet och den gemensamma ansatsen bör också återspeglas, allt efter vad som är lämpligt, i Enisas arbetsprogram, utvärderingar av Enisa och Enisas rapportering och administration.

(57) Styrelsen, som består av företrädare för medlemsstaternas och kommissionens företrädare, bör fastställa den allmänna inriktningen för Enisas verksamhet och se till att den utför sina uppgifter i enlighet med denna förordning. Styrelsen bör ha de nödvändiga befogenheterna för att fastställa budgeten och kontrollera att den genomförs, anta lämpliga finansiella bestämmelser, utarbeta klara och tydliga förfaranden för Enisas beslutsfattande, anta Enisas samlade programdokument, anta sin egen arbetsordning, utse den verkställande direktören, besluta om förlängning och avslutande av hans eller hennes mandat.

(58) För att Enisa ska fungera väl och effektivt bör kommissionen och medlemsstaterna säkerställa att personer som utses till styrelseledamöter har lämplig yrkesmässig expertis och erfarenhet. Medlemsstaterna och kommissionen bör även eftersträva att begränsa omsättningen av deras respektive företrädare i styrelsen i syfte att skapa kontinuitet i dess arbete.

(59) För att Enisa ska fungera väl bör den verkställande direktören utses på grundval av meriter, dokumenterad skicklighet i förvaltning och ledarskap samt kompetens och erfarenheter som rör cybersäkerhet. Den verkställande direktörens uppgifter bör utföras med fullständigt oberoende. Den verkställande direktören bör utarbeta ett förslag till årligt arbetsprogram för Enisa, efter samråd med kommissionen, och bör vidta alla åtgärder som är nödvändiga för att säkerställa att arbetsprogrammet genomförs på rätt sätt. Den verkställande direktören bör utarbeta en årsrapport som ska föreläggas styrelsen, som omfattar genomförandet av Enisas årliga arbetsprogram, upprätta en preliminär beräkning av Enisas inkomster och utgifter samt genomföra budgeten. Den verkställande direktören bör också ha möjlighet att inrätta tillfälliga arbetsgrupper som i synnerhet ska behandla vetenskapliga, tekniska, rättsliga eller socioekonomiska frågor. Inrättandet av en tillfällig arbetsgrupp anses i synnerhet nödvändigt i samband med att ett särskilt förslag till europeisk ordning för cybersäkerhetscertifiering (nedan kallat *förslag till*

certifieringsordning) ska utarbetas. Den verkställande direktören bör se till att de tillfälliga arbetsgruppernas medlemmar väljs med utgångspunkt i högsta möjliga standard när det gäller expertkunskaper, med målsättningen att det bör finnas en balans mellan könen och, utifrån de specifika frågor som berörs, en lämplig balans mellan medlemsstaternas förvaltningar, unionens institutioner, organ och byråer och den privata sektorn, inklusive branschen, användare och akademiska experter på nätverks- och informationssäkerhet.

(60) Direktionen bör bidra till att styrelsen fungerar på ett effektivt sätt. Som ett led i det förberedande arbetet i samband med styrelsens beslut bör styrelsen i detalj granska relevant information och utforska tillgängliga alternativ och ge råd och lösningar för att utarbeta beslut av styrelsen.

(61) Enisa bör ha Enisas rådgivande grupp som rådgivande organ, för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter. Enisas rådgivande grupp, som inrättats av styrelsen på förslag av den verkställande direktören, bör koncentrera sig på frågor som är relevanta för intressenter och uppmärksamma Enisa på dem. Enisas rådgivande grupp bör särskilt rådfrågas om utkastet till Enisas årliga arbetsprogram. Sammansättning av Enisas rådgivande grupp och de uppgifter som anförtrotts den, bör säkerställa en tillräcklig representation av intressenter i Enisas arbete.

(62) Intressentgruppen för cybersäkerhetscertifiering bör inrättas för att hjälpa Enisa och kommissionen genom att underlätta samråd med berörda intressenter. Intressentgruppen för cybersäkerhetscertifiering bör vara sammansatt av medlemmar som i jämn proportion representerar branschen, såväl på efterfrågesidan som på utbudssidan när det gäller IKT-produkter och IKT-tjänster och särskilt innefattande små och medelstora företag, leverantörer av digitala tjänster, europeiska och internationella standardiseringsorgan, nationella ackrediteringsorgan, tillsynsmyndigheter med ansvar för dataskydd och organ för bedömning av överensstämmelse i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ([16]), den akademiska världen och konsumentorganisationer.

(63) Enisa bör ha regler för förebyggande och hantering av intressekonflikter. Enisa bör också tillämpa relevanta unionsbestämmelser om allmänhetens tillgång till handlingar enligt Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([17]). Enisas behandling av personuppgifter bör ske i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725 ([18]). Enisa bör efterleva de bestämmelser som gäller för unionens institutioner, organ och byråer och den nationella lagstiftning som rör hantering av information, i synnerhet känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter.

(64) För att garantera Enisas autonomi och oberoende och ge den möjlighet att utföra kompletterande uppgifter, också oförutsedda uppgifter i en krissituation, bör Enisa ges en tillräcklig egen budget där intäkterna främst bör bestå av ett bidrag från unionen och bidrag från tredjeländer som deltar i Enisas arbete. En adekvat budget är av största vikt för att säkerställa att Enisa har tillräcklig kapacitet att fullgöra alla sina växande uppgifter och uppnå sina mål. Huvuddelen av Enisas personal bör vara direkt delaktig i det operativa genomförandet av Enisas mandat. Värdmedlemsstaten, eller varje annan medlemsstat, bör ha rätt att lämna frivilliga bidrag till Enisas budget. Unionens budgetförfarande bör även i fortsättningen tillämpas på de bidrag som belastar unionens allmänna budget. Dessutom bör revisionsrätten granska Enisas räkenskaper för att säkerställa insyn och ansvarighet.

(65) Cybersäkerhetscertifiering har stor betydelse för att öka förtroendet för och säkerheten hos IKT-produkter, IKT-tjänster och IKT-processer. Den digitala inre marknaden, och särskilt den datadrivna ekonomin och sakernas internet, kan utvecklas framgångsrikt endast om allmänheten litar på att sådana produkter, tjänster och processer har en viss nivå i fråga om cybersäkerhet. Uppkopplade och automatiserade bilar, elektroniska medicintekniska produkter, styrsystem för industriell automation och smarta elnät är bara några exempel på sektorer inom vilka certifiering redan används eller kan komma att användas i en nära framtid. De sektorer som regleras av direktiv (EU) 2016/1148 är också sektorer där cybersäkerhetscertifiering är av yttersta vikt.

([16]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

([17]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

([18]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

(66) I sitt meddelande från 2016 *Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch* tog kommissionen upp behovet av billiga och interoperabla cybersäkerhetsprodukter och cybersäkerhetslösningar av hög kvalitet. Utbudet av IKT-produkter, IKT-tjänster och IKT-processer på den inre marknaden är fortfarande i hög grad geografiskt fragmenterat. Cybersäkerhetsbranschen i Europa har till stor del utvecklats med stöd av nationell statlig efterfrågan. Bristen på interoperabla lösningar (tekniska standarder), förfaranden och EU-mekanismer för certifiering är några av de andra faktorer som påverkar den inre marknaden för cybersäkerhet. Detta gör det svårt för europeiska företag att konkurrera på nationell nivå, unionsnivå och global nivå. Det minskar också utbudet av livskraftig och användbar cybersäkerhetsteknik som enskilda och företag har tillgång till. Även i meddelandet från 2017 om halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden – En ansluten digital inre marknad för alla underströk kommissionen behovet av säkra uppkopplade produkter och system, och framhöll att skapandet av en europeisk IKT-säkerhetsram med regler om hur IKT-säkerhetscertifiering ska organiseras i unionen kan bevara förtroendet för internet och samtidigt motverka den nuvarande fragmenteringen av den inre marknaden.

(67) För närvarande används cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster och IKT-processer endast i begränsad omfattning. I de fall det förekommer är det oftast på medlemsstatsnivå eller inom ramen för industridrivna system. Ett certifikat utfärdat av en nationell myndighet för cybersäkerhetscertifiering i ett sådant sammanhang erkänns i princip inte av andra medlemsstater. Företag kan därför behöva certifiera sina IKT-produkter, IKT-tjänster och IKT-processer i flera medlemsstater där de bedriver verksamhet, exempelvis för att kunna delta i nationella upphandlingsförfaranden, varvid de ökar sina omkostnader. Även om nya system utvecklas, tycks det inte finnas någon samlad helhetssyn på övergripande cybersäkerhetsfrågor, exempelvis inom området sakernas internet. Befintliga system uppvisar allvarliga brister och skillnader i fråga om produkttäckning, assuransnivå, grundläggande kriterier och faktisk användning, vilket utgör ett hinder för mekanismer för ömsesidigt erkännande inom unionen.

(68) Vissa ansträngningar har gjorts för att få till stånd ett ömsesidigt erkännande av certifikat inom unionen. De har dock endast delvis varit framgångsrika. Det främsta exemplet är det avtal om ömsesidigt erkännande (MRA) som ingåtts inom gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS). Även om det är den viktigaste modellen för samarbete och ömsesidigt erkännande av säkerhetscertifiering omfattar SOG-IS endast vissa av medlemsstaterna. Detta har begränsat SOG-IS-avtalets effektivitet för den inre marknaden.

(69) Det är därför nödvändigt att anta en gemensam ansats och att inrätta ett europeiskt ramverk för cybersäkerhetscertifiering som fastställer de viktigaste övergripande kraven för europeiska ordningar för cybersäkerhetscertifiering som ska utvecklas, och som gör att europeiska cybersäkerhetscertifikat och en EU-försäkran om överensstämmelse för IKT-produkter och IKT-tjänster kan erkännas och användas i samtliga medlemsstater. I detta sammanhang är det viktigt att bygga vidare på befintliga nationella och internationella system och på system för ömsesidigt erkännande, i synnerhet SOG-IS, och att möjliggöra en smidig övergång från befintliga ordningar inom ramen för sådana system till system inom ramen för den nya europeiska ramen för cybersäkerhetscertifiering. Den europeiska ramen för cybersäkerhetscertifiering bör ha ett dubbelt syfte. Å ena sidan bör den bidra till att öka förtroendet för IKT-produkter, IKT-tjänster och IKT-processer som har certifierats enligt europeiska ordningar för cybersäkerhetscertifiering. Å andra sidan bör den undvika att det uppstår flera olika motstridiga eller överlappande nationella ordningar för cybersäkerhetscertifieringar och därmed minska kostnaderna för företag som är verksamma på den digitala inre marknaden. De europeiska ordningarna för cybersäkerhetscertifiering bör vara icke-diskriminerande och grundas på europeiska eller internationella standarder såvida inte dessa standarder är ineffektiva eller olämpliga för att förverkliga unionens legitima mål i detta avseende.

(70) Den europeiska ramen för cybersäkerhetscertifiering bör inrättas på ett enhetligt sätt i alla medlemsstater i syfte att förhindra *certifieringsshopping* utifrån skillnader i kravnivå i olika medlemsstater.

(71) De europeiska ordningarna för cybersäkerhetscertifiering bör bygga på vad som redan existerar på internationell och nationell nivå och, om så krävs, på tekniska specifikationer från forum och konsortier, varvid man bör lära av nuvarande styrkor och utvärdera och rätta till svagheter.

(72) Flexibla cybersäkerhetslösningar är nödvändiga för att branschen ska kunna föregripa cyberhot, och därför bör alla certifieringsordningar utformas så att de inte riskerar att snabbt bli föråldrade.

(73) Kommissionen bör ges befogenhet att anta europeiska ordningar för cybersäkerhetscertifiering för särskilda grupper av IKT-produkter, IKT-tjänster och IKT-processer. Dessa ordningar bör genomföras och övervakas av nationella myndigheter för cybersäkerhetscertifiering, och certifikat utfärdade enligt dessa ordningar bör vara giltiga och erkännas i hela unionen. Certifieringsordningar som drivs av industrin eller andra privata organisationer bör inte ingå i denna förordnings tillämpningsområde. De organ som handhar sådana ordningar kan dock föreslå kommissionen att överväga sådana ordningar som en grund för att godkänna dem som en europeisk ordning för cybersäkerhetscertifiering.

(74) Bestämmelserna i denna förordning bör inte påverka tillämpningen av unionsrätt som innehåller särskilda bestämmelser om certifiering av IKT-produkter, IKT-tjänster och IKT-processer. Särskilt förordning (EU) 2016/679 innehåller bestämmelser för införandet av certifieringsmekanismer samt sigill och märkningar för dataskydd för att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens uppgiftsbehandling är förenlig med den förordningen. Dessa certifieringsmekanismer samt sigill och märkningar för dataskydd bör göra det möjligt för de registrerade att snabbt bedöma dataskyddsnivån för relevanta IKT-produkter, IKT-tjänster och IKT-processer. Den här förordningen påverkar inte certifieringen av uppgiftsbehandling enligt förordning (EU) 2016/679, inte heller om denna verksamhet ingår i IKT-produkter, IKT-tjänster och IKT-processer.

(75) Syftet med europeiska ordningar för cybersäkerhetscertifiering bör vara att säkerställa att IKT-produkter, IKT-tjänster och IKT-processer som certifierats enligt en sådan ordning uppfyller de angivna kraven i syfte att skydda tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller de därmed sammanhängande funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, tjänster och processer under hela livscykeln i den mening som avses i denna förordning. Det är inte möjligt att i detalj fastställa cybersäkerhetskraven för alla IKT-produkter, IKT-tjänster och IKT-processer i denna förordning. IKT-produkter, IKT-tjänster och IKT-processer och cybersäkerhetsbehov relaterade till dessa produkter, tjänster och processer är så olikartade att det är mycket svårt att ta fram allmänna cybersäkerhetskrav som är giltiga under alla omständigheter. Det är därför nödvändigt att anta ett brett och allmänt cybersäkerhetsbegrepp när det gäller certifieringsändamål, som bör kompletteras med en uppsättning specifika cybersäkerhetmål som måste beaktas vid utformningen av europeiska ordningar för cybersäkerhetscertifiering. Formerna för att uppnå dessa mål i specifika IKT-produkter, IKT-tjänster och IKT-processer bör sedan fastställas i detalj för den enskilda certifieringsordningen som antas av kommissionen, till exempel genom hänvisningar till standarder eller tekniska specifikationer om inga lämpliga standarder finns tillgängliga.

(76) De tekniska specifikationer som ska användas i europeiska ordningar för cybersäkerhetscertifiering bör iaktta principerna i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([19]). Vissa avvikelser från dessa krav kan dock anses nödvändiga i vederbörligen motiverade fall där dessa tekniska specifikationer ska användas i en europeisk ordning för cybersäkerhetscertifiering med hänvisning till assuransnivån ”hög”. Skälen för dessa avvikelser bör offentliggöras.

(77) En bedömning av överensstämmelse avser det förfarande genom vilket man utvärderar om fastställda krav för en IKT-produkt, IKT-tjänst eller IKT-process har uppfyllts. Detta förfarande utförs av en oberoende tredje part som inte är tillverkaren eller leverantören av de IKT-produkter, IKT-tjänster eller IKT-processer som bedöms. Ett europeiskt cybersäkerhetscertifikat bör utfärdas efter framgångsrik utvärdering av en IKT-produkt, IKT-tjänst eller IKT-process. Ett europeiskt cybersäkerhetscertifikat bör betraktas som en bekräftelse på att en utvärdering har genomförts på ett korrekt sätt. Beroende på assuransnivå bör den europeiska ordningen för cybersäkerhetscertifiering ange om det europeiska cybersäkerhetscertifikatet ska utfärdas av ett privat eller offentligt organ. Bedömning av överensstämmelse och certifiering utgör inte i sig någon garanti för att certifierade IKT-produkter och IKT-tjänster är cybersäkra. De är snarare förfaranden och tekniska metoder för att intyga att IKT-produkter, IKT-tjänster och IKT-processer har testats och att de uppfyller vissa cybersäkerhetskrav som fastställs på annan plats, till exempel i tekniska standarder.

(78) Valet av lämplig certifiering och därtill knutna säkerhetskrav av användarna av europeiska cybersäkerhetscertifikat bör grundas på en riskanalys som avser risker med användningen av IKT-produkten, IKT-tjänsten eller IKT-processen. Assuransnivån bör därför stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, IKT-tjänst eller IKT-process.

([19]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

(79) Europeiska ordningar för cybersäkerhetscertifiering skulle kunna ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster och IKT-processer möjlighet att på eget ansvar göra en bedömning av överensstämmelse (nedan kallad *självbedömning av överensstämmelse*). I sådana fall bör det vara tillräckligt att tillverkaren eller leverantören av IKT-produkter, IKT-tjänster och IKT-processer själv genomför alla kontroller för att säkerställa att IKT-produkten, IKT-tjänsten eller IKT-processen överensstämmer med den europeiska ordningen för cybersäkerhetscertifiering. Denna typ av bedömning av överensstämmelse bör anses lämplig för IKT-produkter och IKT-tjänster med lägre komplexitet (exempelvis enkel utformning och tillverkningsmetod) som inte utgör en stor risk för det allmänna samhällsintresset. Dessutom bör självbedömning av överensstämmelse endast tillåtas för IKT-produkter, IKT-tjänster eller IKT-processer när de motsvarar assuransnivån ”grundläggande”.

(80) Europeiska ordningar för cybersäkerhetscertifiering kan möjliggöra både självbedömning av överensstämmelse och certifiering för IKT-produkter, IKT-tjänster eller IKT-processer. I detta fall bör ordningen föreskriva tydliga och begripliga möjligheter för konsumenter och andra användare att skilja mellan IKT-produkter, IKT-tjänster eller IKT-processer med avseende på vilken tillverkare eller leverantör av IKT-produkter, IKT-tjänster eller IKT-processer som har ansvar för bedömningen, och IKT-produkter, IKT-tjänster eller IKT-processer som har certifierats av en tredje part.

(81) Tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer som utför en självbedömning av överensstämmelse bör kunna upprätta och underteckna en EU-försäkran om överensstämmelse som ett led i förfarandet för bedömning av överensstämmelse. En EU-försäkran om överensstämmelse är ett dokument som anger att en särskild IKT-produkt, IKT-tjänst eller IKT-process uppfyller kraven i den europeiska ordningen för cybersäkerhetscertifiering. Genom att upprätta och underteckna EU-försäkran om överensstämmelse tar tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer på sig ansvaret för att IKT-produkten, IKT-tjänsten eller IKT-processen uppfyller de rättsliga kraven i den europeiska ordningen för cybersäkerhetscertifiering. En kopia av EU-försäkran om överensstämmelse bör lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

(82) Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer bör under en period som fastställs i den berörda europeiska ordningen för cybersäkerhetscertifiering ge den behöriga nationella myndigheten för cybersäkerhetscertifiering tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas, IKT-tjänsternas eller IKT-processernas överensstämmelse med den relevanta europeiska ordningen för cybersäkerhetscertifiering. Den tekniska dokumentationen bör specificera de krav som är tillämpliga enligt ordningen och bör, i den mån det krävs för självbedömningen av överensstämmelse, även innehålla en beskrivning av IKT-produktens, IKT-tjänstens eller IKT-processens konstruktion, tillverkning och funktion. Den tekniska dokumentationen bör utarbetas på ett sätt som möjliggör bedömning av en IKT-produkts eller en IKT-tjänsts överensstämmelse med de krav som är tillämpliga enligt ordningen.

(83) I styrningen av den europeiska ramen för cybersäkerhetscertifiering beaktas medlemsstaternas deltagande och lämpligt deltagande av intressenter, dessutom definieras kommissionens roll under hela processen för planering samt förslag till, begäran om, utarbetande, antagande och översyn av europeiska ordningar för cybersäkerhetscertifiering.

(84) Kommissionen bör med stöd av europeiska gruppen för cybersäkerhetscertifiering och intressegruppen för cybersäkerhetscertifiering och efter öppna och omfattande samråd utarbeta ett löpande arbetsprogram på unionsnivå för de europeiska ordningarna för cybersäkerhetscertifiering och bör offentliggöra detta i form av ett instrument som inte är bindande. Unionens löpande arbetsprogram bör vara ett strategidokument som gör det möjligt för framför allt branschen, nationella myndigheter och standardiseringsorgan att förbereda sig inför framtida europeiska ordningar för cybersäkerhetscertifiering. Unionens löpande arbetsprogram bör inbegripa en flerårig översikt över de förslag till certifieringsordning som kommissionen har för avsikt att uppmana Enisa att utarbeta på specificerade grunder. Kommissionen bör beakta unionens löpande arbetsprogram vid utarbetandet av sin löpande plan för IKT-standardisering och standardiseringsförfrågningar till Europeiska standardiseringsorganisationer. Med tanke på den snabba utvecklingen och spridningen av ny teknik, uppkomsten av nya, tidigare okända cybersäkerhetsrisker samt lagstiftnings- och marknadsutvecklingar bör kommissionen eller europeiska gruppen för cybersäkerhetscertifiering ha rätt att begära att Enisa ska utarbeta förslag till certifieringsordning som inte finns med i unionens löpande arbetsprogram. Kommissionen och europeiska gruppen för cybersäkerhetscertifiering bör i sådana fall också göra en behovsbedömning av en sådan begäran genom att beakta denna förordnings övergripande syften och mål och behovet av att säkerställa kontinuiteten i Enisas planering och resursanvändning.

Efter mottagandet av en sådan begäran bör Enisa utan onödigt dröjsmål utarbeta förslag till certifieringsordning för särskilda IKT-produkter, IKT-tjänster eller IKT-processer. Kommissionen bör utvärdera de positiva och negativa konsekvenserna av begäran på den specifika marknad som berörs, särskilt för små och medelstora företag, innovation, hinder för tillträde till den marknaden och kostnader för slutanvändare. Kommissionen bör, på grundval av Enisas förslag till certifieringsordning, ges befogenhet att anta den europeiska ordningen för cybersäkerhetscertifiering genom genomförandeakter. Med beaktande av det allmänna syfte och de säkerhetsmålsättningar som fastställs i denna förordning bör den i europeiska ordningar för cybersäkerhetscertifiering som antas av kommissionen specificeras en minimiuppsättning komponenter avseende den enskilda ordningens föremål, tillämpningsområde och funktionssätt. Dessa delar bör bland annat omfatta cybersäkerhetscertifieringens tillämpningsområde och föremål, inklusive de kategorier av IKT-produkter, IKT-tjänster och IKT-processer som omfattas, den detaljerade specifikationen av cybersäkerhetskraven, exempelvis genom hänvisning till standarder eller tekniska specifikationer, de särskilda utvärderingskriterierna och utvärderingsmetoderna samt den avsedda assuransnivån (”grundläggande”, ”betydande” eller ”hög”) och i förekommande fall utvärderingsnivåerna. Enisa bör kunna avvisa en begäran från europeiska gruppen för cybersäkerhetscertifiering. Sådana beslut bör fattas av styrelsen och bör vederbörligen motiveras.

(85) Enisa bör upprätthålla en webbplats med information om och offentliggörande av europeiska ordningar för cybersäkerhetscertifiering som bör omfatta bland annat begäran om utarbetande av ett förslag till certifieringsordning samt den återkoppling som mottagits i den samrådsprocess som genomförs av Enisa i förberedelsefasen. Denna webbplats bör också tillhandahålla information om de europeiska cybersäkerhetscertifikaten och EU-försäkringar om överensstämmelse som utfärdas enligt denna förordning samt information om återkallande och utgång av sådana europeiska cybersäkerhetscertifikat och EU-försäkringar. På webbplatsen bör det också anges vilka nationella ordningar för cybersäkerhetscertifiering som har ersatts av en europeisk ordning för cybersäkerhetscertifiering.

(86) Assuransnivån för en europeisk certifieringsordning utgör förtroendegrunden för att en IKT-produkt, IKT-tjänst eller IKT-process, uppfyller säkerhetskraven i en särskild europeisk ordning för cybersäkerhetscertifiering. I syfte att säkerställa konsekvens i den europeiska ramen för cybersäkerhetscertifiering bör en europeisk ordning för cybersäkerhetscertifiering kunna specificera assuransnivån för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse som utfärdats inom ramen för den ordningen. Varje europeiskt cybersäkerhetscertifikat kan avse någon av assuransnivåerna ”grundläggande”, ”betydande” eller ”hög”, medan EU-försäkran om överensstämmelse endast kan avse assuransnivån ”grundläggande”. Assuransnivåerna avspeglar motsvarande stringens och djup i fråga om utvärdering av IKT-produkten, IKT-tjänsten och IKT-processen och fastställs genom hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska mildra eller förhindra incidenter. Varje assuransnivå bör vara konsekvent inom de olika sektoriella områden där certifiering tillämpas.

(87) En europeisk ordning för cybersäkerhetscertifiering kan ha flera utvärderingsnivåer beroende på hur stringent och djupgående utvärderingsmetoden är. Utvärderingsnivåer bör motsvara en av assuransnivåerna och vara kopplad till en lämplig kombination av assuranskomponenter. För samtliga assuransnivåer bör IKT-produkten, IKT-tjänsten eller IKT-processen omfatta en rad säkra funktioner som fastställs i ordningen, exempelvis följande: säker nyskapande konfiguration, signerad kod, säker uppdatering och mekanismer för begränsad exploatering samt fullt stack- eller minnesskydd. Dessa funktioner bör utarbetas och underhållas med säkerhetsinriktade utvecklingsstrategier och tillhörande verktyg för att säkerställa att effektiva mekanismer för maskin- och programvara är inbyggda på ett tillförlitligt sätt.

(88) För assuransnivån ”grundläggande” bör utvärderingen omfatta minst följande assuranskomponenter: I utvärderingen bör det åtminstone ingå en översyn av IKT-produktens, IKT-tjänstens eller IKT-processens tekniska dokumentation som utförs av organet för bedömning av överensstämmelse. Om certifieringen omfattar IKT-processer bör den process som använts för att utforma, utveckla och underhålla en IKT-produkt eller IKT-tjänst även omfattas av den tekniska översynen. Om en europeisk ordning för cybersäkerhetscertifiering ger möjlighet till självbedömning av överensstämmelse bör det vara tillräckligt att tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer har gjort en självbedömning av IKT-produktens, IKT-tjänstens eller IKT-processens överensstämmelse med certifieringsordningen.

(89) För assuransnivån ”betydande” bör utvärderingen, utöver kraven för assuransnivån ”grundläggande”, åtminstone omfatta en kontroll av överensstämmelsen mellan IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner och den tekniska dokumentationen.

(90) För assuransnivån ”hög” bör utvärderingen, utöver kraven för assuransnivån ”betydande”, åtminstone omfatta ett effektivitetstest som bedömer resistensen hos IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner gentemot genomtänkta cyberangrepp som utförs av personer med betydande kompetens och resurser.

(91) Användningen av europeisk cybersäkerhetscertifiering och EU-försäkran om överensstämmelse bör vara frivillig, om inte annat föreskrivs i unionsrätten eller medlemsstaternas nationella rätt som antagits i enlighet med unionsrätten. I avsaknad av harmoniserad unionsrätt får medlemsstaterna införa nationella tekniska föreskrifter som föreskriver obligatorisk certifiering inom ramen för en europeisk ordning för cybersäkerhetscertifiering i enlighet med Europaparlamentets och rådets direktiv (EU) 2015/1535 ([20]). Medlemsstaterna kan även använda europeisk cybersäkerhetscertifiering i samband med offentlig upphandling och Europaparlamentets och rådets direktiv 2014/24/EU ([21]).

(92) På vissa områden kan det bli nödvändigt att i framtiden införa särskilda krav på cybersäkerhet och göra cybersäkerhetscertifiering obligatorisk för vissa IKT-produkter, IKT-tjänster och IKT-processer för att förbättra cybersäkerheten i unionen. Kommissionen bör med jämna mellanrum följa upp vilka effekter antagna europeiska ordningar för cybersäkerhetscertifiering har på tillgången till säkra IKT-produkter, IKT-tjänster och IKT-processer på den inre marknaden och bör regelbundet bedöma i hur hög utsträckning tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer i unionen använder certifieringsordningarna. Effektiviteten hos de europeiska ordningarna för cybersäkerhetscertifiering, och huruvida bestämda ordningar borde göras obligatoriska, bör bedömas mot bakgrund av unionens lagstiftning med koppling till cybersäkerhet, särskilt direktiv (EU) 2016/1148, med beaktande av säkerheten i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster.

(93) Europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse bör hjälpa slutanvändarna att göra välinformerade val. IKT-produkter, IKT-tjänster och IKT-processer som certifierats eller varit föremål för en EU-försäkring om överensstämmelse bör därför åtföljas av information som anpassats till den avsedda slutanvändarens förväntade tekniska nivå. All sådan information bör finnas tillgänglig online och, om lämpligt, i fysisk form. Slutanvändaren bör ha tillgång till information om referensnumret för certifieringsordningen, assuransnivån, beskrivningen av de risker som är förenade med IKT-produkten, IKT-tjänsten och IKT-processen, och den utfärdande myndigheten eller det utfärdande organet, eller bör kunna få en kopia av det europeiska cybersäkerhetscertifikatet. Dessutom bör slutanvändaren informeras om supportpolicy för cybersäkerhet, dvs. hur länge slutanvändaren kan förvänta sig att motta cybersäkerhetsuppdateringar eller programkorrigeringar från tillverkarens eller leverantörens IKT-produkter, IKT-tjänster och IKT-processer. I tillämpliga fall bör slutanvändaren få vägledning om åtgärder och inställningar som denne kan genomföra för att underhålla eller öka cybersäkerheten för IKT-produkten eller IKT-tjänsten och kontaktinformation avseende den enda kontaktpunkten för rapportering av och support vid cyberattacker (utöver den automatiska rapporteringen). Informationen bör uppdateras regelbundet och göras tillgänglig på en med information om europeiska ordningar för cybersäkerhetscertifiering.

(94) I syfte att uppnå målen för denna förordning och undvika en fragmentering av den inre marknaden, bör nationella ordningar eller förfaranden för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster eller IKT-processer som omfattas av en europeisk ordning för cybersäkerhetscertifiering upphöra att ha verkan från och med en dag som fastställs av kommissionen genom genomförandeakter. Vidare bör medlemsstaterna inte införa nya nationella ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster eller IKT-processer som redan omfattas av en befintligt europeiskt ordning för cybersäkerhetscertifiering. Medlemsstaterna bör dock inte vara förhindrade att anta eller behålla nationella ordningar för cybersäkerhetscertifiering för att skydda den nationella säkerheten. Medlemsstaterna bör informera kommissionen och europeiska gruppen för cybersäkerhetscertifiering om alla eventuella avsikter att upprätta nya nationella ordningar för cybersäkerhetscertifiering. Kommissionen och europeiska gruppen för cybersäkerhetscertifiering bör utvärdera vilka effekter nya nationella ordningar för cybersäkerhetscertifiering har på den inre marknadens funktion och mot bakgrund av det strategiska intresset av att i stället begära en europeisk ordning för cybersäkerhetscertifiering.

(95) Europeiska ordningar för cybersäkerhetscertifiering kommer att bidra till att harmonisera cybersäkerhetsrutinerna inom unionen. De måste bidra till att öka cybersäkerhet inom unionen. Utformningen av europeiska ordningar för cybersäkerhetscertifiering bör även beakta och möjliggöra utveckling av innovationer på området cybersäkerhet.

([20]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

([21]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

(96) Europeiska ordningar för cybersäkerhetscertifiering bör även beakta olika befintliga metoder för program- och maskinvaruutveckling och framför allt vilken inverkan frekventa uppdateringar av programvara och fast programvara har på enskilda europeiska cybersäkerhetscertifikat. I de europeiska ordningarna för cybersäkerhetscertifiering bör det fastställas under vilka förhållanden en uppdatering kan kräva att en IKT-produkt, IKT-tjänst eller IKT-processer ska återcertifieras eller att ett specifikt europeiskt cybersäkerhetscertifikats tillämpningsområde ska begränsas med beaktande av eventuella negativa effekter av uppdateringen på överensstämmelsen med säkerhetskraven för det certifikatet.

(97) När en europeisk ordning för cybersäkerhetscertifiering har antagits bör tillverkarna eller leverantörerna av IKT-produkter, IKT-tjänster eller IKT-processer kunna lämna in en ansökan om certifiering av sina IKT-produkter eller IKT-tjänster till valfritt organ för bedömning av överensstämmelse var som helst i unionen. Organen för bedömning av överensstämmelse bör ackrediteras av ett nationellt ackrediteringsorgan, om de uppfyller vissa krav som fastställs i denna förordning. Ackrediteringen bör utfärdas för en period på högst fem år och bör kunna förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse fortfarande uppfyller kraven. Nationella ackrediteringsorgan bör begränsa, tillfälligt upphäva eller återkalla ackrediteringen av ett organ för bedömning av överensstämmelse om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot denna förordning.

(98) Hänvisningar i nationell lagstiftning till nationella standarder som har upphört att ha verkan i och med att en europeisk ordning för cybersäkerhetscertifiering har trätt i kraft kan orsaka förvirring. Medlemsstaterna bör därför se till att antagandet av en europeisk ordning för cybersäkerhetscertifiering avspeglas i deras nationella lagstiftning.

(99) För att uppnå likvärdiga standarder över hela unionen, underlätta ömsesidigt erkännande och främja godtagandet av europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse måste en ordning inrättas för inbördes granskning mellan nationella myndigheter för cybersäkerhetscertifiering. Inbördes granskning bör innefatta förfaranden för att övervaka IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med europeiska cybersäkerhetscertifikat, övervaka skyldigheterna för tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som utför självbedömningar av överensstämmelse, och för att övervaka organ för bedömning av överensstämmelse samt att personalen vid organ som utfärdar certifikat för assuransnivån ”hög” har lämplig sakkunskap. Kommissionen bör genom genomförandeakter kunna upprätta minst en femårsplan för den inbördes granskningen samt fastställa kriterier och metoder för hur denna ordning ska fungera.

(100) Utan att det påverkar den ordning för inbördes granskning som ska inrättas vid alla nationella myndigheter för cybersäkerhetscertifiering som omfattas av den europeiska ramen för cybersäkerhetscertifiering kan vissa europeiska ordningar för cybersäkerhetscertifiering innefatta en mekanism för inbördes bedömning för de organ som utfärdar europeiska cybersäkerhetscertifikat för IKT-produkter, IKT-tjänster och IKT-processer med assuransnivån ”hög” inom ramen för sådana ordningar. Den europeiska gruppen för cybersäkerhetscertifiering bör stödja tillämpningen av sådana mekanismer för inbördes bedömning. Den inbördes bedömningen bör framför allt bedöma huruvida organen i fråga utför sina uppgifter på ett harmoniserat sätt och de kan innefatta mekanismer för att överklaga. Resultaten av de inbördes granskningarna bör göras allmänt tillgängliga. De berörda organen får vidta lämpliga åtgärder för att anpassa sin praxis och expertis därefter.

(101) Medlemsstaterna bör utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som ska övervaka fullgörandet av skyldigheterna enligt denna förordning. En nationell myndighet för cybersäkerhetscertifiering kan vara en redan befintlig myndighet eller en ny myndighet. En medlemsstat bör också kunna fatta beslut, efter överenskommelse med en annan medlemsstat, om att utse en eller flera myndigheter för nationell cybersäkerhetscertifiering på den andra medlemsstatens territorium.

(102) Nationella myndigheter för cybersäkerhetscertifiering bör särskilt övervaka och verkställa de skyldigheter som åligger en tillverkare eller en leverantör av IKT-produkter, IKT-tjänster eller IKT-processer som är etablerad på deras respektive territorier med avseende på EU-försäkran om överensstämmelse, bör bistå de nationella ackrediteringsorganen med övervakning och kontroll av den verksamhet som bedrivs av organen för bedömning av överensstämmelse genom att förse dem med sakkunskap och relevant information, bör tillåta organ för bedömning av överensstämmelse att utföra sina uppgifter om dessa organ uppfyller de ytterligare krav som finns fastställda i en europeisk ordning för cybersäkerhetscertifiering och bör övervaka relevant utveckling på området för cybersäkerhetscertifiering. De nationella myndigheterna för cybersäkerhetscertifiering bör också behandla klagomål som lämnas in av fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av de myndigheterna eller avseende europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse, om sådana certifikat anger assuransnivå ”hög”, bör i lämplig utsträckning undersöka det ärende som

klagomålet gäller och bör underrätta den klagande om utvecklingen och resultatet av utredningen inom rimlig tid. De nationella myndigheterna för cybersäkerhetscertifiering bör dessutom samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller någon annan offentlig myndighet, bland annat genom att utbyta information om IKT-produkter, IKT-tjänster och IKT-processer som eventuellt avviker från kraven i denna förordning eller särskilda europeiska ordningar för cybersäkerhetscertifiering. Kommissionen bör underlätta sådant utbyte av information genom att erbjuda tillgång till ett allmänt stödsystem för elektronisk information, till exempel informations- och kommunikationssystemet för marknadskontroll (ICSMS) och systemet för snabb varning för farliga konsumentprodukter (Rapex) som redan används av marknadsövervakningsmyndigheterna i enlighet med förordning (EG) nr 765/2008.

(103) För att säkerställa en konsekvent tillämpning av den europeiska ramen för cybersäkerhetscertifiering bör det inrättas en europeisk grupp för cybersäkerhetscertifiering, bestående av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller andra berörda nationella myndigheter. Den europeiska gruppen för cybersäkerhetscertifierings främsta uppgifter bör vara att ge kommissionen råd och bistånd i dess arbete för att säkerställa konsekvent genomförande och tillämpning av den europeiska ramen för cybersäkerhetscertifiering, att bistå och ha ett nära samarbete med Enisa i utarbetandet av förslag till ordningar för cybersäkerhetscertifiering, att, i vederbörligen motiverade fall begära att Enisa utarbetar ett förslag till certifieringsordning, att anta yttranden till Enisa om förslag till certifieringsordning och att anta yttranden riktade till kommissionen om underhåll och översyn av befintliga europeiska ordningar för cybersäkerhetscertifiering. Den europeiska gruppen för cybersäkerhetscertifiering bör underlätta utbytet av god praxis och expertis mellan de olika nationella myndigheterna för cybersäkerhetscertifiering som är ansvariga för bemyndigande av organ för bedömning av överensstämmelse och utfärdande av europeiska cybersäkerhetscertifikat.

(104) För att öka medvetenheten och underlätta acceptansen för framtida europeiska ordningar för cybersäkerhetscertifiering kan kommissionen utfärda allmänna eller sektorsspecifika cybersäkerhetsriktlinjer, t.ex. vad gäller god praxis för cybersäkerhet eller ansvarsfullt cybersäkerhetsbeteende som belyser de positiva konsekvenserna av att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer.

(105) För att ytterligare underlätta handeln och erkänna att IKT-leveranskedjorna är globala får avtal om ömsesidigt erkännande av europeiska cybersäkerhetscertifikat ingås av unionen i enlighet med artikel 218 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Kommissionen får med beaktande av rådgivningen från Enisa och den europeiska gruppen för cybersäkerhetscertifiering rekommendera att relevanta förhandlingar inleds. Varje europeisk ordning för cybersäkerhetscertifiering bör föreskriva särskilda villkor för sådana avtal om ömsesidigt erkännande med tredjeländer.

(106) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([22]).

(107) Granskningsförfarandet bör användas för antagande av genomförandeakter om europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer, om formerna för Enisas utförande av utredningar, om en plan för inbördes granskning av nationella myndigheter för cybersäkerhetscertifiering samt för antagande av genomförandeakter om förhållanden, format och förfaranden för anmälningar av ackrediterade organ för bedömning av överensstämmelse från de nationella myndigheterna för cybersäkerhetscertifiering till kommissionen.

(108) Enisas verksamhet bör utvärderas regelbundet och på ett oberoende sätt. Utvärderingen bör beakta Enisas måluppfyllelse, dess arbetsmetoder och relevansen i dess uppgifter, särskilt dess uppgifter rörande operativt samarbete på unionsnivå. Utvärderingen bör även bedöma konsekvenserna, ändamålsenligheten och effektiviteten i fråga om den europeiska ramen för cybersäkerhetscertifiering. Vid en granskning ska kommissionen utvärdera hur Enisas roll som referenspunkt för råd och expertis kan stärkas och bör även utvärdera hur Enisa möjligen skulle kunna stödja bedömningen av IKT-produkter, IKT-tjänster och IKT-processer från tredjeländer som kommer in på unionsmarknaden och som inte är förenliga med unionsreglerna, om sådana IKT-produkter, IKT-tjänster och IKT-processer förs in i unionen

([22]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

(109) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, på grund av deras omfattning och verkningar, utan snarare kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(110) Förordning (EU) nr 526/2013 bör upphävas.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVDELNING I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. I syfte att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen, fastställer denna förordning

a) mål, uppgifter och organisatoriska frågor som rör Enisa (Europeiska unionens cybersäkerhetsbyrå), och

b) ett ramverk för inrättandet av europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för IKT-produkter, IKT-tjänster och IKT-processer i unionen samt i syfte att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen.

Den ram som avses i första stycket b ska användas utan att det påverkar tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsrättsakter.

2. Denna förordning påverkar inte medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

2. *nätverks- och informationssystem*: ett nätverks- och informationssystem enligt definitionen i artikel 4.1 i direktiv (EU) 2016/1148.

3. *nationell strategi för säkerheten i nätverks- och informationssystem*: en nationell strategi för säkerheten i nätverks- och informationssystem enligt definitionen i artikel 4.3 i direktiv (EU) 2016/1148.

4. *leverantör av samhällsviktiga tjänster*: en leverantör av samhällsviktiga tjänster enligt definitionen i artikel 4.4 i direktiv (EU) 2016/1148.

5. *leverantör av digitala tjänster*: en leverantör av digitala tjänster enligt definitionen i artikel 4.6 i direktiv (EU) 2016/1148.

6. *incident*: en incident enligt definitionen i artikel 4.7 i direktiv (EU) 2016/1148.

7. *incidenthantering*: incidenthantering enligt definitionen i artikel 4.8 i direktiv (EU) 2016/1148.

8. *cyberhot*: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer.

9. *europeisk ordning för cybersäkerhetscertifiering*: en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering eller bedömning av överensstämmelse av särskilda IKT-produkter, IKT-tjänster och IKT-processer.

10. *nationell ordning för cybersäkerhetscertifiering*: en komplett uppsättning regler, tekniska krav, standarder och förfaranden som utvecklas och antas av en nationell offentlig myndighet och som tillämpas vid certifiering eller vid bedömning av överensstämmelse av IKT-produkter, IKT-tjänster och IKT-processer som omfattas av tillämpningsområdet för den ordningen.

11. *europeiskt cybersäkerhetscertifikat*: ett dokument, utfärdat av behörigt organ, som intygar att en viss IKT-produkt, IKT-tjänst eller IKT-process, har utvärderats för kontroll av överensstämmelse med specifika säkerhetskrav som fastställs i en europeisk ordning för cybersäkerhetscertifiering.

12. *IKT-produkt*: en del, eller en grupp av delar, i nätverks- och informationssystem.

13. *IKT-tjänst*: en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem.

14. *IKT-process*: verksamhet som utförs för att utforma, utveckla, tillhandahålla eller underhålla en IKT-produkt eller IKT-tjänst.

15. *ackreditering*: ackreditering enligt definitionen i artikel 2.10 i förordning (EG) nr 765/2008.

16. *nationellt ackrediteringsorgan*: ett nationellt ackrediteringsorgan enligt definitionen i artikel 2.11 i förordning (EG) nr 765/2008.

17. *bedömning av överensstämmelse*: bedömning av överensstämmelse enligt definitionen i artikel 2.12 i förordning (EG) nr 765/2008.

18. *organ för bedömning av överensstämmelse*: organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008.

19. *standard*: en standard enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012.

20. *teknisk specifikation*: ett dokument som anger de tekniska krav som ska uppfyllas av, eller vilka förfaranden för bedömning av överensstämmelse som gäller för en IKT-produkt, IKT-tjänst eller IKT-process.

21. *assuransnivå*: förtroendegrund för att en IKT-produkt, IKT-tjänst eller IKT-process uppfyller säkerhetskraven i en särskild europeisk ordning för cybersäkerhetscertifiering och anger på vilken nivå en IKT-produkt, IKT-tjänst eller IKT-process har utvärderats, men som i sig inte mäter säkerheten i den berörda IKT-produkten, IKT-tjänsten eller IKT-processen.

22. *egenkontroll av överensstämmelse*: en åtgärd som genomförs av en tillverkare eller en leverantör av IKT-produkter, IKT-tjänster eller IKT-processer, som utvärderar om dessa IKT-produkter, IKT-tjänster eller IKT-processer uppfyller kraven i n särskild europeisk ordning för cybersäkerhetscertifiering.

AVDELNING II

ENISA (EUROPEISKA UNIONENS CYBERSÄKERHETSBYRÅ)

KAPITEL I

Mandat och mål

Artikel 3

Mandat

1. Enisa ska utföra de uppgifter som den tilldelas genom denna förordning i syfte att uppnå en hög gemensam nivå i fråga om cybersäkerhet i hela unionen, bland annat genom att aktivt stödja medlemsstaterna, unionens institutioner, organ och byråer i arbetet med att förbättra cybersäkerheten. Enisa ska fungera som en referenspunkt för rådgivning och expertis i fråga om cybersäkerhet för unionens institutioner, organ och byråer samt för andra berörda unionsaktörer.

Genom att utföra de uppgifter den anförtrotts enligt denna förordning ska Enisa bidra till att minska fragmenteringen på den inre marknaden.

2. Enisa ska utföra de uppgifter som den tilldelas genom unionsrättsakter som fastställer åtgärder för tillnärmning av medlemsstatens lagar och andra författningar som rör cybersäkerhet.

3. Vid utförandet av sina uppgifter ska Enisa agera självständigt och samtidigt undvika dubbelarbete i förhållande till medlemsstatens verksamhet och ta hänsyn till medlemsstatens befintliga expertis.

4. Enisa ska ta fram sina egna nödvändiga resurser, däribland teknisk och mänsklig kapacitet och kompetens, för att utföra de uppgifter som den tilldelas enligt denna förordning.

Artikel 4

Mål

1. Enisa ska vara ett expertcentrum inom området cybersäkerhet genom sitt oberoende, den vetenskapliga och tekniska kvaliteten på de råd, den assistans och den information den tillhandahåller, öppenheten i dess operativa förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter.

2. Enisa ska bistå unionens institutioner, organ och byråer, samt medlemsstaterna, med utarbetande och genomförande av unionens politiska åtgärder som rör cybersäkerhet, inbegripet sektorspolitik på cybersäkerhetsområdet.

3. Enisa ska stödja kapacitetsuppbyggnad och beredskap i hela unionen genom att bistå unionens institutioner, organ och byråer, liksom medlemsstaterna och offentliga och privata intressenter i syfte att öka skyddet av deras nätverks- och informationssystem, utveckla och förbättra cyberresiliens och insatskapacitet samt utveckla färdigheter och kompetens inom området cybersäkerhet.

4. Enisa ska främja samarbete, däribland informationsutbyte, och samordning på unionsnivå mellan medlemsstater, unionens institutioner, organ och byråer samt berörda privata och offentliga intressenter i frågor som rör cybersäkerhet.

5. Enisa ska bidra till att öka cybersäkerhetskapaciteten på unionsnivå i syfte att stödja medlemsstaternas åtgärder för att förebygga och vidta åtgärder mot cyberhot, särskilt vid gränsöverskridande incidenter.

6. Enisa ska främja användningen av europeisk cybersäkerhetscertifiering, i syfte att undvika en fragmentering av den inre marknaden. Enisa ska bidra till inrättandet och underhållandet av ett europeiskt ramverk för cybersäkerhetscertifiering i enlighet med avdelning III i denna förordning, i syfte att öka transparensen i fråga om cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer och därigenom stärka förtroendet för den digitala inre marknaden och dess konkurrenskraft.

7. Enisa ska främja en hög nivå av medvetenhet om cybersäkerhet, inklusive it-hygien och it-kompetens hos privatpersoner, organisationer och företag.

KAPITEL II

Uppgifter

Artikel 5

Utarbetande och genomförande av unionens politik och lagstiftning

Enisa ska bidra till utarbetandet och genomförandet av unionens politik och lagstiftning genom att

1. bistå och ge råd i fråga om utarbetande och översyn av unionens politik och lagstiftning inom området cybersäkerhet och i fråga om sektorsspecifika strategier och lagförslag där frågor som rör cybersäkerhet ingår, särskilt genom att tillhandahålla oberoende yttranden och analyser samt förberedande arbete,

2. hjälpa medlemsstaterna att på ett konsekvent sätt genomföra unionens politik och lagstiftning som rör cybersäkerhet, i synnerhet vad gäller direktiv (EU) 2016/1148, bland annat genom yttranden, riktlinjer, råd och bästa praxis i frågor såsom riskhantering, incidentrapportering och informationsutbyte, samt genom att underlätta utbytet av bästa praxis mellan behöriga myndigheter i detta avseende,

3. hjälpa medlemsstater och unionens institutioner, organ och byråer med att utveckla och främja politik på cybersäkerhetsområdet som rör underhållandet av den allmänna tillgängligheten till eller integriteten för den offentliga kärnan av ett öppet internet,

4. bidra till arbetet i samarbetsgruppen enligt artikel 11 i direktiv (EU) 2016/1148 genom att tillhandahålla expertis och bistånd,

5. stödja

   a) utarbetandet och genomförandet av unionens politik inom området elektronisk identitet och betrodda tjänster, i synnerhet genom att tillhandahålla råd och utfärda tekniska riktlinjer, samt genom att underlätta utbytet av bästa praxis mellan behöriga myndigheter,

   b) främjandet av en högre säkerhetsnivå för elektronisk kommunikation, bland annat genom att tillhandahålla råd och expertis, samt genom att underlätta utbytet av bästa praxis mellan behöriga myndigheter,

   c) medlemsstater vid genomförandet av specifika cybersäkerhetsaspekter av unionspolitik och lagstiftning som rör integritets- och personuppgiftsskydd, inbegripet genom att, på begäran, tillhandahålla rådgivning till Europeiska dataskyddsstyrelsen,

6. stödja den regelbundna översynen av unionens politiska verksamhet genom att utarbeta en årlig rapport om hur genomförandet av respektive rättsliga ramar framskrider avseende

   a) information om medlemsstaternas incidentrapporter som överlämnas av de gemensamma kontaktpunkterna till samarbetsgruppen enligt artikel 10.3 i direktiv (EU) 2016/1148,

   b) sammanfattningar av anmälningar om säkerhetsöverträdelser eller integritetsförlust som erhållits från leverantörerna av betrodda tjänster, som överlämnas av tillsynsorganen till Enisa, enligt artikel 19.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([23]),

   c) anmälningar om säkerhetsincidenter som överlämnats av tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, som överlämnas av de behöriga myndigheterna till Enisa, enligt artikel 40 i direktiv (EU) 2018/1972.

([23]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

Artikel 6

Kapacitetsuppbyggnad

1. Enisa ska bistå

a) medlemsstaterna i deras ansträngningar för att förbättra förebyggandet, upptäckten och analysen av, samt kapaciteten att reagera på, cyberhot och cyberincidenter genom att förse dem med kunskaper och nödvändig expertis,

b) medlemsstaterna och unionens institutioner, organ och byråer med att fastställa och genomföra frivilliga riktlinjer för offentliggörande av sårbarheter,

c) unionens institutioner, organ och byråer, i deras ansträngningar för att förbättra förebyggandet, upptäckten och analysen av cyberhot och cyberincidenter, samt förbättra kapaciteten att reagera på sådana cyberhot och cyberincidenter, särskilt genom lämpligt stöd för CERT-EU,

d) medlemsstaterna, på deras begäran, med inrättandet av nationella CSIRT-enheter enligt artikel 9.5 i direktiv (EU) 2016/1148,

e) medlemsstaterna, på deras begäran, med utarbetandet av nationella strategier för säkerhet i nätverks- och informationssystem, enligt artikel 7.2 i direktiv (EU) 2016/1148, och främja spridning av dessa strategier och notera framstegen med genomförandet av dessa i hela unionen i syfte att främja bästa praxis,

f) unionens institutioner med utarbetandet och översynen av unionens strategier avseende cybersäkerhet och därvid främja deras spridning och övervaka framstegen i genomförandet av dem,

g) nationella CSIRT-enheter och CSIRT-enheter på unionsnivå i deras arbete för att öka sin kapacitet, bland annat genom att främja dialog och informationsutbyte, för att säkerställa att alla CSIRT-enheter när det gäller den tekniska nivån har gemensamma minimikrav för kapaciteten och att deras verksamhet följer bästa praxis,

h) medlemsstaterna genom att organisera regelbundna cybersäkerhetsövningar på unionsnivå enligt artikel 7.5 i vart fall vartannat år och genom att avge policyrekommendationer som grundar sig på utvärderingar av övningarna och på lärdomar som dragits av dem,

i) behöriga offentliga organ genom att erbjuda utbildning om cybersäkerhet, om lämpligt i samarbete med intressenter,

j) samarbetsgruppen, med att utbyta bästa praxis, i synnerhet för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, enligt artikel 11.3 l i direktiv (EU) 2016/1148, inklusive vid gränsöverskridande beroenden, vad gäller risker och incidenter.

2. Enisa ska stödja informationsutbyte inom och mellan sektorer, i synnerhet i de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148, genom att tillhandahålla bästa praxis och vägledning i fråga om tillgängliga verktyg, om förfaranden samt om hur regleringsfrågor som rör informationsutbyte ska hanteras.

Artikel 7

Operativt samarbete på unionsnivå

1. Enisa ska stödja operativt samarbete mellan medlemsstaterna, unionens institutioner, organ och byråer och mellan intressenter.

2. Enisa ska samarbeta på operativ nivå och skapa synergier med unionens institutioner, organ och byråer, inbegripet CERT-EU, med de enheter som arbetar med it-brottslighet och med tillsynsmyndigheter som arbetar med integritets- och personuppgiftsskydd, i syfte att ta itu med frågor av gemensamt intresse, inbegripet genom

a) utbyte av sakkunskap och bästa praxis,

b) tillhandahållande av råd och utfärdande av riktlinjer om relevanta frågor som rör cybersäkerhet,

c) inrättande av praktiska arrangemang för utförande av särskilda uppgifter, efter samråd med kommissionen.

3. Enisa ska tillhandahålla sekretariatet för CSIRT-nätverket enligt artikel 12.2 i direktiv (EU) 2016/1148 och ska i denna egenskap aktivt stödja informationsutbytet och samarbetet mellan nätverkets medlemmar.

4. Enisa ska stödja medlemsstaterna i det operativa samarbetet inom CSIRT-nätverket genom att

a) ge råd om hur de kan förbättra sin kapacitet att förebygga, upptäcka och reagera på incidenter, och på begäran från en eller flera medlemsstater, tillhandahålla rådgivning avseende ett specifikt cyberhot,

b) på begäran från en eller flera medlemsstater bistå vid bedömningen av incidenter som har en betydande eller avsevärd inverkan genom att tillhandahålla expertis och underlätta den tekniska hanteringen av sådana incidenter, bland annat särskilt genom att stödja frivilligt utbyte av relevant information och tekniska lösningar mellan medlemsstaterna,

c) analysera sårbarheter och incidenter på grundval av allmänt tillgänglig information eller information som medlemsstaterna på frivillig basis tillhandahållit för det ändamålet, och

d) på begäran från en eller flera medlemsstater, ge stöd till tekniska efterhandsundersökningar av incidenter som har en betydande eller avsevärd inverkan i den mening som avses i direktiv (EU) 2016/1148.

Vid fullgörandet av dessa uppgifter ska Enisa och CERT-EU samarbeta på ett strukturerat sätt för att dra nytta av synergier och undvika dubbelarbete.

5. Enisa ska organisera regelbundna cybersäkerhetsövningar på unionsnivå och bistå medlemsstater och unionens institutioner, organ och byråer med att organisera cybersäkerhetsövningar på deras begäran. Sådana cybersäkerhetsövningar på unionsnivå får innehålla tekniska, operativa och strategiska element. En gång vartannat år ska Enisa organisera en storskalig heltäckande övning.

När det är lämpligt ska Enisa också bidra till och hjälpa till att organisera sektorsvisa cybersäkerhetsövningar tillsammans med berörda organisationer som även deltar i cybersäkerhetsövningar på unionsnivå.

6. Enisa ska, i nära samarbete med medlemsstaterna, regelbundet utarbeta en djupgående teknisk lägesrapport om cybersäkerheten i EU om incidenter och cyberhot på grundval av offentligt tillgänglig information, egna analyser och rapporter som den får från bland andra medlemsstaternas CSIRT-enheter eller de gemensamma kontaktpunkterna som inrättats genom direktiv (EU) 2016/1148, båda på frivillig grund, EC3 och CERT-EU.

7. Enisa ska bidra till att utveckla en samarbetsinriktad respons, på unions- och medlemsstatsnivå, för att hantera storskaliga gränsöverskridande incidenter eller kriser som rör cybersäkerhet, främst genom att

a) sammanställa och analysera rapporter från nationella källor som är allmänt tillgängliga eller har delats på frivillig grund i syfte att bidra till att skapa en gemensam situationsmedvetenhet,

b) säkerställa ett effektivt informationsflöde och tillhandahålla mekanismer för eskalering mellan CSIRT-nätverket och de tekniska och politiska beslutsfattarna på unionsnivå,

c) på begäran underlätta den tekniska hanteringen av sådana incidenter eller kriser, däribland särskilt genom att stödja frivilligt utbyte av tekniska lösningar mellan medlemsstaterna,

d) stödja unionens institutioner, organ och byråer och, på deras begäran, medlemsstater i den offentliga kommunikationen om sådana incidenter eller kriser,

e) testa samarbetsplanerna för hantering av sådana incidenter eller kriser på unionsnivå och på deras begäran stödja medlemsstaterna med att testa sådana planer på nationell nivå.

Artikel 8

Marknad, cybersäkerhetscertifiering och standardisering

1. Enisa ska stödja och främja utvecklingen och genomförandet av unionens politik för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer, enligt avdelning III i denna förordning, genom att

a) fortlöpande övervaka utvecklingen i fråga om standardisering inom anknutna områden och rekommendera lämpliga tekniska specifikationer för användning vid utveckling av de europeiska ordningarna för cybersäkerhetscertifiering enligt artikel 54.1 c där standarder inte finns tillgängliga,

b) utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (nedan kallade *förslag till certifieringsordning*) för IKT-produkter och IKT-tjänster och IKT-processer, i samarbete med branschen och i enlighet med artikel 49,

c) utvärdera antagna europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 49.8,

d) delta i sakkunnigbedömningar enligt artikel 59.4,

e) bistå kommissionen med att tillhandahålla sekretariatet för europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 62.5.

2. Enisa ska tillhandahålla sekretariatet för europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 22.4.

3. Enisa ska sammanställa och offentliggöra riktlinjer och utveckla god praxis, däribland om principer om it-hygien när det gäller cybersäkerhetskraven för IKT-produkter, IKT-tjänster och IKT-processer, i samarbete med nationella myndigheter för cybersäkerhetscertifiering och branschen på ett formellt, standardiserat och transparent sätt.

4. Enisa ska bidra till kapacitetsuppbyggnad i samband med utvärderings- och certifieringsprocesser genom att sammanställa och utfärda riktlinjer samt ge stöd till medlemsstaterna på deras begäran.

5. Enisa ska underlätta upprättandet och tillämpningen av europeiska och internationella standarder för riskhantering och för säkerheten hos IKT-produkter, IKT-tjänster och IKT-processer.

6. Enisa ska, i samarbete med medlemsstaterna och branschen, utarbeta råd och riktlinjer avseende de tekniska områden som har en koppling till säkerhetskraven för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, samt avseende redan befintliga standarder, inbegripet medlemsstaternas nationella standarder, i enlighet med artikel 19.2 i direktiv (EU) 2016/1148.

7. Enisa ska genomföra och sprida regelbundna analyser av de viktigaste trenderna på marknaden för cybersäkerhet på både efterfråge- och utbudssidan, i syfte att främja marknaden för cybersäkerhet i unionen.

Artikel 9

Kunskap och information

Enisa ska

a) genomföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om tekniska innovationers förväntade samhälleliga, rättsliga, ekonomiska och regleringsrelaterade konsekvenser för cybersäkerhet,

b) genomföra långsiktiga strategiska analyser av cyberhot och cybersäkerhetsincidenter i syfte att identifiera framväxande trender och bidra till att förebygga incidenter,

c) i samarbete med experter från medlemsstaternas myndigheter och berörda intressenter tillhandahålla råd, vägledning och bästa praxis avseende säkerheten i nätverks- och informationssystem, i synnerhet avseende säkerheten hos de infrastrukturer som understödjer de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148 och de som används av de leverantörer av digitala tjänster som förtecknas i bilaga III i det direktivet,

d) via en särskild portal samla, organisera och för allmänheten tillgängliggöra information om cybersäkerhet som tillhandahålls av unionens institutioner, byråer och organ och information om cybersäkerhet som tillhandahålls på frivillig grund av medlemsstaterna samt privata och offentliga intressenter,

e) samla in och analysera allmänt tillgänglig information om betydande incidenter och sammanställa rapporter i syfte att ge vägledning till privatpersoner, organisationer och företag i hela unionen.

Artikel 10

Medvetandehöjande åtgärder och utbildning

Enisa ska

a) öka allmänhetens medvetenhet om cybersäkerhetsrisker och ge vägledning om god praxis för enskilda användare, som är inriktad på privatpersoner, organisationer och företag, inklusive it-hygien och it-kompetens,

b) i samarbete med medlemsstaterna, unionens institutioner, organ, byråer och branschen organisera regelbundna informationskampanjer för att öka cybersäkerheten och dess synlighet i unionen och främja en bred offentlig debatt,

c) bistå medlemsstaterna i deras insatser för att öka medvetenheten om cybersäkerhet och främja utbildning i cybersäkerhet,

d) främja närmare samordning och utbyte av bästa praxis mellan medlemsstaterna vad gäller cybersäkerhetsutbildning och cybersäkerhetsmedvetenhet.

Artikel 11

Forskning och innovation

När det gäller forskning och innovation ska Enisa

a) ge råd till unionens institutioner, organ och byråer och medlemsstaterna om forskningsbehov och forskningsprioriteringar inom området cybersäkerhet, för att möjliggöra ett effektivt svar på befintliga och nya risker och cyberhot, bland annat när det gäller ny och framväxande informations- och kommunikationsteknik, och för att säkerställa en effektiv användning av riskförebyggande teknik,

b) delta, om kommissionen har delegerat relevanta befogenheter till den, i genomförandefasen av finansieringsprogram för forskning och innovation, eller som stödmottagare.

c) bidra till en strategisk forsknings- och innovationsagenda på unionsnivå inom området cybersäkerhet.

Artikel 12

Internationellt samarbete

Enisa ska bidra till unionens insatser för att samarbeta med tredjeländer och internationella organisationer samt inom ramarna för relevant internationellt samarbete för att främja internationellt samarbete i frågor som rör cybersäkerhet, genom att

a) om lämpligt delta som observatör i anordnandet av internationella övningar samt analysera och rapportera till styrelsen om resultaten av sådana övningar,

b) på begäran från kommissionen underlätta utbyte av bästa praxis,

c) på begäran från kommissionen tillhandahålla den expertis,

d) tillhandahålla rådgivning och stöd till kommissionen i frågor som rör avtal om ömsesidigt erkännande av cybersäkerhetscertifikat med tredjeländer i samarbete med den europeiska gruppen för cybersäkerhetscertifiering som inrättats enligt artikel 62.

KAPITEL III

Enisas organisation

Artikel 13

Enisas struktur

Enisas förvaltnings- och ledningsstruktur ska bestå av

a) en styrelse,

b) en direktion,

c) en verkställande direktör,

d) Enisas rådgivande grupp,

e) ett nätverk för nationella kontaktpersoner.

Avsnitt 1

Styrelse

Artikel 14

Styrelsens sammansättning

1. Styrelsen ska bestå av en ledamot som utses av varje medlemsstat och två ledamöter som utses av kommissionen. Samtliga ledamöter ska ha rösträtt.

2. Varje ledamot av styrelsen ska ha en suppleant. Den suppleanten ska företräda ledamoten i ledamotens frånvaro.

3. Styrelseledamöterna och deras suppleanter ska utses mot bakgrund av deras kunskaper inom området cybersäkerhet, med hänsyn till relevanta färdigheter i fråga om ledarskap, administration och budget. Kommissionen och medlemsstaterna ska bemöda sig om att begränsa omsättningen av sina företrädare i styrelsen för att säkerställa kontinuitet i styrelsens arbete. Kommissionen och medlemsstaterna ska sträva efter att uppnå en jämn könsfördelning i styrelsen.

4. Mandatperioden för styrelsens ledamöter och deras suppleanter ska vara fyra år. Mandatperioden får förnyas.

Artikel 15

Styrelsens uppgifter

1. Styrelsen ska göra följande:

a) Fastställa de allmänna riktlinjerna för Enisas arbete och även se till att Enisa agerar i enlighet med de regler och principer som fastställs i denna förordning; den ska även se till att Enisas arbete överensstämmer med det arbete som utförs av medlemsstaterna och på unionsnivå.

b) Anta Enisas utkast till samlat programdokument som avses i artikel 24 innan det överlämnas till kommissionen för yttrande.

c) Anta Enisas samlade programdokument, med beaktande av kommissionens yttrande

d) Övervaka genomförandet av den fleråriga och årliga programplaneringen som ingår i det samlade programdokumentet.

e) Anta Enisas årsbudget och utföra andra uppgifter rörande Enisas budget i enlighet med kapitel IV.

f) Bedöma och anta den konsoliderade årliga rapporten om Enisas verksamhet, inklusive räkenskaperna och en beskrivning av hur Enisa har uppnått sina resultatindikatorer, senast den 1 juli följande år sända både den årliga rapporten och bedömningen av denna till Europaparlamentet, rådet, kommissionen och revisionsrätten samt offentliggöra den årliga rapporten.

g) Anta de finansiella regler som ska tillämpas på Enisa i enlighet med artikel 32.

h) Anta en bedrägeribekämpningsstrategi som står i proportion till bedrägeririskerna med beaktande av en kostnads–nyttoanalys av de åtgärder som ska genomföras.

i) Anta regler för att förebygga och hantera intressekonflikter bland ledamöterna.

j) Säkerställa lämplig uppföljning av slutsatserna och rekommendationerna från utredningar som genomförs av Europeiska byrån för bedrägeribekämpning (Olaf) och från olika interna eller externa revisionsrapporter och utvärderingar.

k) Anta sin arbetsordning, inbegripet regler för interimistiska beslut om delegeringen av särskilda uppgifter enligt artikel 19.7.

l) Med avseende på Enisas personal, utöva de befogenheter som i tjänsteföreskrifterna för tjänstemän (nedan kallade *tjänsteföreskrifterna*) och i anställningsvillkoren för övriga anställda i Europeiska unionen (nedan kallade *anställningsvillkoren*), som fastställs i rådets förordning (EEC, Euratom, EKSG) nr 259/68 ([24]), tilldelas tillsättningsmyndigheten och den myndighet som har befogenhet att sluta anställningsavtal (nedan kallade *befogenheter som tillsättningsmyndighet*) i enlighet med punkt 2 i denna artikel.

m) Anta genomförandebestämmelser till tjänsteföreskrifterna och anställningsvillkoren i enlighet med förfarandet i artikel 110 i tjänsteföreskrifterna.

n) Utse den verkställande direktören och i förekommande fall förlänga dennes mandatperiod eller avsätta honom eller henne i enlighet med artikel 36.

o) Utse en räkenskapsförare, som kan vara kommissionens räkenskapsförare, som ska vara helt oberoende i sin tjänsteutövning.

p) Fatta alla beslut som rör inrättandet av Enisas interna strukturer och, vid behov, ändringar av dessa interna strukturer, med beaktande av Enisas verksamhetsbehov och en sund budgetförvaltning.

q) Godkänna fastställandet av samarbetsavtal med avseende på artikel 7.

r) Godkänna fastställandet eller ingåendet av samarbetsavtal i enlighet med artikel 42.

2. Styrelsen ska, i enlighet med artikel 110 i tjänsteföreskrifterna, anta ett beslut grundat på artikel 2.1 i tjänsteföreskrifterna och artikel 6 i anställningsvillkoren för övriga anställda om att delegera relevanta befogenheter som tillsättningsmyndighet till den verkställande direktören och fastställa på vilka villkor denna delegering av befogenheter kan dras in. Den verkställande direktören får vidaredelegera dessa befogenheter.

([24]) Rådets förordning (EEG, Euratom, EKSG) nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper samt om införande av särskilda tillfälliga åtgärder beträffande kommissionens tjänstemän (EGT L 56, 4.3.1968, s. 1).

3. Vid exceptionella omständigheter får styrelsen anta ett beslut om att tillfälligt dra in delegeringen till den verkställande direktören av befogenheterna som tillsättningsmyndighet samt de befogenheter som tillsättningsmyndighet som den verkställande direktören vidaredelegerat, och i stället utöva dem själv eller delegera dem till en av sina ledamöter eller till någon annan anställd än den verkställande direktören.

Artikel 16

Styrelsens ordförande

Styrelsen ska välja en ordförande och en vice ordförande bland sina ledamöter, med två tredjedelars majoritet av ledamöterna. Deras mandatperiod ska vara fyra år, som får förnyas en gång. Om deras uppdrag som styrelseledamot upphör någon gång under deras mandatperiod upphör deras mandatperiod automatiskt vid denna tidpunkt. Vice ordföranden ska inträda i ordförandens ställe om ordföranden inte kan fullgöra sina plikter.

Artikel 17

Styrelsens sammanträden

1. Styrelsens sammanträden ska sammankallas av dess ordförande.

2. Styrelsen ska hålla minst två ordinarie sammanträden per år. Den ska också hålla extra sammanträden på ordförandens begäran, på kommissionens begäran eller på begäran av minst en tredjedel av ledamöterna.

3. Den verkställande direktören ska delta i styrelsesammanträdena, men ska inte ha rösträtt.

4. Ledamöterna i Enisas rådgivande grupp får på inbjudan av ordföranden delta i styrelsens sammanträden, men ska inte ha rösträtt.

5. Styrelseledamöterna och deras suppleanter får, med förbehåll för styrelsens arbetsordning, låta sig biträdas av rådgivare eller experter vid styrelsens sammanträden.

6. Enisa ska tillhandahålla sekretariatet för styrelsen.

Artikel 18

Omröstningsbestämmelser för styrelsen

1. Styrelsen ska fatta beslut med en majoritet av sina ledamöter.

2. En majoritet med två tredjedelar av styrelsens ledamöter ska krävas för att anta det samlade programdokumentet och den årliga budgeten samt för utnämning av, förlängning av mandatet för eller avsättning av den verkställande direktören.

3. Varje ledamot ska ha en röst. I en ledamots frånvaro ska suppleanten ha rätt att utöva ledamotens rösträtt.

4. Styrelsens ordförande ska delta i omröstningen.

5. Den verkställande direktören ska inte delta i omröstningen.

6. Närmare bestämmelser om röstningsförfarandena, i synnerhet på vilka villkor en ledamot får agera på en annan ledamots vägnar, ska fastställas i styrelsens arbetsordning.

Avsnitt 2

Direktion

Artikel 19

Direktion

1. Styrelsen ska bistås av en direktion.

2. Direktionen ska

a) förbereda beslut som ska antas av styrelsen,

b) tillsammans med styrelsen säkerställa lämplig uppföljning av slutsatserna och rekommendationerna från utredningar som utförts av Europeiska byrån för bedrägeribekämpning (Olaf) och från olika interna eller externa revisionsrapporter och utvärderingar,

c) utan att det påverkar den verkställande direktörens ansvar enligt artikel 20 bistå och ge råd till den verkställande direktören vid genomförandet av styrelsens beslut i frågor som rör administration och budget enligt artikel 20.

3. Direktionen ska bestå av fem ledamöter. Ledamöterna i direktionen ska utses bland styrelseledamöterna. En av ledamöterna ska vara styrelsens ordförande, som även kan vara direktionens ordförande, och en annan ska vara en av kommissionens företrädare. Utnämningarna av ledamöter i direktionen ska syfta till att uppnå en jämn könsfördelning i direktionen. Den verkställande direktören ska delta i direktionens sammanträden, men ska inte ha rösträtt.

4. Mandatperioden för ledamöterna i direktionen ska vara fyra år. Mandatperioden får förnyas.

5. Direktionen ska sammanträda minst var tredje månad. Direktionens ordförande ska sammankalla extra sammanträden på begäran av direktionens ledamöter.

6. Direktionens arbetsordning ska fastställas av styrelsen.

7. Vid behov får direktionen, i brådskande fall, fatta vissa interimistiska beslut på styrelsens vägnar, särskilt i frågor som rör den administrativa ledningen, inklusive om indragning av delegeringen av befogenheterna som tillsättningsmyndighet och budgetfrågor. Sådana interimistiska beslut ska utan onödigt dröjsmål meddelas styrelsen. Styrelsen ska besluta huruvida det interimistiska beslutet ska godkännas eller avslås senast tre månader efter att beslutet fattades. Direktionen ska inte fatta beslut för styrelsens räkning som kräver godkännande av en majoritet med två tredjedelar av styrelsens ledamöter.

Avsnitt 3

Verkställande direktör

Artikel 20

Den verkställande direktörens ansvarsområden

1. Enisa ska ledas av den verkställande direktören, som ska vara oberoende i sin tjänsteutövning. Den verkställande direktören ska vara ansvarig inför styrelsen.

2. Den verkställande direktören ska på begäran rapportera till Europaparlamentet om resultatet av sitt arbete. Rådet får uppmana den verkställande direktören att rapportera om resultatet av sitt arbete.

3. Den verkställande direktören ska ha ansvar för följande:

a) Sköta Enisas dagliga förvaltning.

b) Genomföra de beslut som antas av styrelsen.

c) Utarbeta utkastet till det samlade programdokumentet och lämna det till styrelsen för godkännande innan det lämnas till kommissionen.

d) Genomföra det samlade programdokumentet och rapportera till styrelsen om detta.

e) Utarbeta den konsoliderade årliga rapporten om Enisas verksamhet, inbegripet genomförandet av det årliga arbetsprogrammet, och framlägga den för styrelsen för bedömning och antagande.

f) Utarbeta en handlingsplan för uppföljning av slutsatserna från efterhandsutvärderingarna samt rapportera vartannat år till kommissionen om de framsteg som gjorts.

g) Utarbeta en handlingsplan för uppföljning av slutsatserna från interna eller externa revisionsrapporter, liksom utredningar utförda av Olaf, samt rapportera om läget vartannat år till kommissionen och regelbundet till styrelsen.

h) Utarbeta ett utkast till finansiella regler som ska tillämpas på Enisa som avses i artikel 32.

i) Upprätta Enisas preliminära beräkning av inkomster och utgifter och genomföra dess budget.

j) Skydda unionens finansiella intressen genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda belopp samt vid behov genom effektiva, proportionella och avskräckande administrativa och ekonomiska sanktioner.

k) Utarbeta en strategi för bedrägeribekämpning för Enisa och lägga fram den för styrelsen för godkännande.

l) Utveckla och underhålla kontakter med näringslivet och konsumentorganisationer för att säkerställa en regelbunden dialog med berörda intressenter.

m) Regelbundet utbyta synpunkter och information med unionens institutioner, organ och byråer om deras cybersäkerhetsverksamhet för att säkerställa att unionens policy utvecklas och genomförs på ett enhetligt sätt.

n) Utföra andra uppgifter som den verkställande direktören tilldelas genom denna förordning.

4. När så är nödvändigt och inom ramen för Enisas mål och uppgifter, får den verkställande direktören inrätta arbetsgrupper bestående av experter, inbegripet experter från medlemsstaternas behöriga myndigheter. Den verkställande direktören ska underrätta styrelsen om detta i förväg. Förfarandena avseende i synnerhet sammansättningen av arbetsgrupperna, den verkställande direktörens tillsättning av arbetsgruppernas experter och arbetsgruppernas arbete ska anges i Enisas interna verksamhetsregler.

5. Där så är nödvändigt för att Enisa ska kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt och grundat på en ändamålsenlig kostnads–nyttoanalys, får den verkställande direktören besluta att inrätta ett eller flera lokala kontor i en eller flera medlemsstater. Innan den verkställande direktören beslutar att inrätta ett lokalt kontor ska han eller hon inhämta ett yttrande från den eller de berörda medlemsstaterna, däribland den medlemsstat där Enisa har sitt säte, och ett förhandsgodkännande från kommissionen och styrelsen. Om oenighet råder under samrådsprocessen mellan den verkställande direktören och de berörda medlemsstaterna ska frågan överlämnas till rådet för diskussion. Det sammanlagda antalet anställda vid alla lokala kontor ska begränsas till ett minimum och inte uppgå till över 40 % av antalet anställda vid Enisa i den medlemsstat där Enisa har sitt säte. Antalet anställda vid varje lokalt kontor ska inte uppgå till över 10 % av antalet anställda vid Enisa i den medlemsstat där Enisa har sitt säte.

I beslutet om att inrätta ett lokalt kontor ska man ange omfattningen av den verksamhet som ska bedrivas vid det lokala kontoret på ett sätt som undviker onödiga kostnader och överlappning av Enisas administrativa uppgifter.

Avsnitt 4

Enisas rådgivande grupp, intressentgruppen för cybersäkerhetscertifiering och nätverk för nationella kontaktpersoner

Artikel 21

Enisas rådgivande grupp

1. Styrelsen ska på förslag av den verkställande direktören på ett transparent sätt inrätta Enisas rådgivande grupp, som ska bestå av erkända experter som företräder berörda intressenter, exempelvis IKT-branschen, leverantörer av allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster, små och medelstora företag, leverantörer av samhällsviktiga tjänster, konsumentgrupper, experter på cybersäkerhetsområdet från den akademiska världen och företrädare för behöriga myndigheter som anmälts i enlighet med direktiv (EU) 2018/1972, europeiska standardiseringsorganisationer samt rättsvårdande myndigheter och tillsynsmyndigheter med ansvar för dataskydd. Styrelsen ska sträva efter att säkerställa lämplig könsfördelning, geografisk fördelning samt fördelning mellan olika intressentgrupper.

2. Förfaranden för Enisas rådgivande grupp, i synnerhet avseende gruppens sammansättning, förslaget från den verkställande direktören som avses i punkt 1, medlemsantal och samt utnämning av gruppens medlemmar, och den rådgivande gruppens arbete, ska anges i Enisas interna verksamhetsregler och ska offentliggöras.

3. Den verkställande direktören eller en person som han eller hon utser från fall till fall ska vara ordförande för Enisas rådgivande grupp.

4. Mandatperioden för medlemmar i Enisas rådgivande grupp ska vara två och ett halvt år. Styrelseledamöter får inte vara medlemmar i Enisas rådgivande grupp. Experter från kommissionen och medlemsstaterna får närvara vid mötena i Enisas rådgivande grupp och delta i dess arbete. Företrädare för andra organ som av den verkställande direktören anses som relevanta, men som inte är medlemmar av Enisas rådgivande grupp, får bjudas in att närvara vid den rådgivande gruppens möten och delta i dess arbete.

5. Enisas rådgivande grupp ska ge Enisa råd med avseende på genomförandet av Enisas verksamhet, med undantag av tillämpningen av avdelning III i denna förordning. Den ska i synnerhet ge den verkställande direktören råd om utarbetandet av förslaget till Enisas årliga arbetsprogram och om kommunikationen med berörda intressenter om frågor kopplade till det årliga arbetsprogrammet.

6. Enisas rådgivande grupp ska regelbundet informera styrelsen om sin verksamhet.

Artikel 22

Intressentgruppen för cybersäkerhetscertifiering

1. Intressentgruppen för cybersäkerhetscertifiering ska inrättas.

2. Intressentgruppen för cybersäkerhetscertifiering ska bestå av medlemmar som ska väljas bland erkända experter som företräder berörda intressenter. Kommissionen ska, genom en öppen och transparent inbjudan på förslag från Enisa, välja ut medlemmarna i intressentgruppen för cybersäkerhetscertifiering, och säkerställa lämplig fördelning mellan de olika intressentgrupperna samt en lämplig könsfördelning och geografisk fördelning.

3. Intressentgruppen för cybersäkerhetscertifiering ska

a) ge kommissionen råd i strategiska frågor om den europeiska ramen för cybersäkerhetscertifiering,

b) på begäran ge Enisa råd om allmänna och strategiska frågor om Enisas uppgifter när det gäller marknaden, cybersäkerhetscertifiering och standardisering,

c) bistå kommissionen vid utarbetandet av unionens löpande arbetsprogram som avses i artikel 47,

d) yttra sig över unionens löpande arbetsprogram i enlighet med artikel 47.4, och

e) i brådskande ärenden ge kommissionen och europeiska gruppen för cybersäkerhetscertifiering råd om behovet av ytterligare certifieringsordningar som inte ingår i unionens löpande arbetsprogram i enlighet med vad som beskrivs i artiklarna 47 och 48.

4. Ordförandeskapet i intressentgruppen för cybersäkerhetscertifiering ska innehas gemensamt av företrädare för kommissionen och Enisa, och Enisa ska tillhandahålla sekretariatet.

Artikel 23

Nätverk för nationella kontaktpersoner

1. Styrelsen ska, på förslag av den verkställande direktören, inrätta ett nätverk för nationella kontaktpersoner som består av företrädare för alla medlemsstater. Varje medlemsstat ska utse en företrädare till nätverket för nationella kontaktpersoner. Nätverket för nationella kontaktpersoners möten kan hållas i olika expertkonstellationer.

2. Nätverket för nationella kontaktpersoner ska särskilt underlätta informationsutbytet mellan Enisa och medlemsstaterna och stödja Enisa i dess arbete med att informera relevanta intressenter runtom i unionen om Enisas verksamhet, slutsatser och rekommendationer.

3. De nationella kontaktpersonerna ska fungera som en kontaktpunkt på nationell nivå för att underlätta samarbetet mellan Enisa och nationella experter inom ramen för genomförandet av Enisas årliga arbetsprogram.

4. De nationella kontaktpersonerna ska ha ett nära samarbete med styrelseledamöterna från deras respektive medlemsstater, men själva nätverket för nationella kontaktpersoner ska inte utföra samma arbete som styrelsen eller andra unionsforum.

5. Uppgifter och förfaranden avseende nätverket för nationella kontaktpersoner ska fastställas i Enisas interna verksamhetsregler och ska offentliggöras.

Avsnitt 5

Verksamhet

Artikel 24

Samlat programdokument

1. Enisa ska genomföra sin verksamhet i enlighet med ett samlat programdokument som innehåller Enisas årliga och fleråriga programplanering, vilket ska inbegripa all planerad verksamhet för Enisa.

2. Den verkställande direktören ska varje år utarbeta ett utkast till samlat programdokument som ska innehålla årlig och flerårig programplanering med motsvarande planering av ekonomiska resurser och personalresurser i överensstämmelse med artikel 32 i kommissionens delegerade förordning (EU) nr 1271/2013 ([25]), med hänsyn till kommissionens riktlinjer.

3. Senast den 30 november varje år ska styrelsen anta det samlade programdokument som avses i punkt 1 och ska senast den 31 januari följande år översända det, liksom eventuella senare uppdaterade versioner, till Europaparlamentet, rådet och kommissionen.

4. Det samlade programdokumentet ska anses vara slutgiltigt efter det att unionens allmänna budget slutligen har antagits och ska vid behov anpassas i enlighet därmed.

([25]) Kommissionens delegerade förordning (EU) nr 1271/2013 av den 30 september 2013 med rambudgetförordning för de organ som avses i artikel 208 i Europaparlamentets och rådets förordning (EU, Euratom) nr 966/2012 (EUT L 328, 7.12.2013, s. 42).

5. Det årliga arbetsprogrammet ska innehålla detaljerade mål och förväntade resultat, inklusive resultatindikatorer. Det ska också innehålla en beskrivning av de åtgärder som ska finansieras och uppgifter om vilka ekonomiska resurser och personalresurser som anslås till varje åtgärd, i enlighet med principerna om verksamhetsbaserad budgetering och förvaltning. Det årliga arbetsprogrammet ska överensstämma med det fleråriga arbetsprogram som avses i punkt 7. I programmet ska det klart anges vilka uppgifter som lagts till, ändrats eller strukits jämfört med föregående räkenskapsår.

6. Styrelsen ska ändra det antagna årliga arbetsprogrammet om Enisa tilldelas en ny uppgift. Varje betydande ändring av det årliga arbetsprogrammet ska antas enligt samma förfarande som det ursprungliga årliga arbetsprogrammet. Styrelsen får delegera befogenheten att göra icke-väsentliga ändringar i det årliga arbetsprogrammet till den verkställande direktören.

7. I det fleråriga arbetsprogrammet ska den övergripande strategiska programplaneringen, inbegripet mål, förväntade resultat och resultatindikatorer, fastställas. Även resursplanering, inklusive flerårig budget och personal, ska fastställas.

8. Resursplaneringen ska uppdateras årligen. Den strategiska programplaneringen ska uppdateras när det är lämpligt, och i synnerhet när det är nödvändigt för att beakta resultatet av den utvärdering som avses i artikel 67.

Artikel 25

Intresseförklaring

1. Styrelsens ledamöter, den verkställande direktören och tjänstemän som är tillfälligt utstationerade av medlemsstaterna ska var och en avge en åtagandeförklaring och en förklaring som anger om det föreligger eller inte föreligger några direkta eller indirekta intressen som skulle kunna anses inverka negativt på deras oberoende. Förklaringarna ska vara tillförlitliga och fullständiga, och de ska avges skriftligen varje år och uppdateras vid behov.

2. Styrelsens ledamöter, den verkställande direktören och externa experter som deltar i tillfälliga arbetsgrupper ska var och en senast i inledningen av varje möte exakt och fullständigt redovisa eventuella intressen som kan påverka deras oberoende i förhållande till frågorna på dagordningen samt avhålla sig från att delta i diskussioner och omröstningar om sådana frågor.

3. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om intresseförklaringar som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 26

Öppenhet

1. Enisa ska utföra sitt arbete med en hög grad av öppenhet och i enlighet med artikel 28.

2. Enisa ska säkerställa att allmänheten och eventuella berörda parter får lämplig, objektiv, tillförlitlig och lättillgänglig information, framför allt om resultaten av dess arbete. Den ska också offentliggöra de intresseförklaringar som avges i enlighet med artikel 25.

3. Styrelsen får, på förslag av den verkställande direktören, ge berörda parter tillstånd att observera delar av Enisas verksamhet.

4. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om öppenhet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 27

Konfidentialitet

1. Enisa ska inte för tredje part röja uppgifter som den behandlar eller mottar, om det i en motiverad ansökan har begärts att uppgifterna helt eller delvis ska behandlas konfidentiellt, dock utan att detta påverkar tillämpningen av artikel 28.

2. Ledamöterna i styrelsen, den verkställande direktören, medlemmarna i Enisas rådgivande grupp, de externa experter som deltar i olika tillfälliga arbetsgrupper och Enisas personal, inbegripet tjänstemän som är tillfälligt utstationerade av medlemsstaterna, ska omfattas av tystnadsplikt enligt artikel 339 i EUF-fördraget, även efter det att deras uppdrag har upphört.

3. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om konfidentialitet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

4. Styrelsen ska besluta om att tillåta Enisa att hantera säkerhetsskyddsklassificerade uppgifter, om så krävs för att Enisa ska kunna utföra sina uppgifter. I sådana fall ska Enisa efter överenskommelse med kommissionens avdelningar anta säkerhetsbestämmelser som tillämpar säkerhetsprinciperna i kommissionens beslut (EU, Euratom) 2015/443 ([26]) och 2015/444 ([27]). Dessa säkerhetsbestämmelser ska omfatta bestämmelser om utbyte, behandling och lagring av säkerhetsskyddsklassificerade uppgifter.

Artikel 28

Tillgång till handlingar

1. Förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos Enisa.

2. Styrelsen ska vidta åtgärder för att genomföra förordning (EG) nr 1049/2001 senast den 28 december 2019.

3. Beslut som fattas av Enisa i enlighet med artikel 8 i förordning (EG) nr 1049/2001 får bli föremål för ett klagomål till europeiska ombudsmannen enligt artikel 228 i EUF-fördraget eller väckande av talan vid Europeiska unionens domstol i enlighet med artikel 263 i EUF-fördraget.

KAPITEL IV

Upprättande av Enisas budget och budgetens struktur

Artikel 29

Upprättande av Enisas budget

1. Varje år ska den verkställande direktören upprätta en preliminär beräkning av Enisas inkomster och utgifter för det därpå följande räkenskapsåret, och ska översända den till styrelsen tillsammans med ett utkast till tjänsteförteckning. Inkomster och utgifter ska vara i balans.

2. Varje år ska styrelsen, på grundval av den preliminära beräkningen, lägga fram en beräkning av Enisas inkomster och utgifter för det därpå följande räkenskapsåret.

3. Styrelsen ska senast den 31 januari varje år överlämna beräkningen, som ska vara en del av utkastet till det samlade programdokumentet, till kommissionen och de tredjeländer med vilka unionen har slutit avtal i enlighet med artikel 42.2.

4. På grundval av den beräkningen ska kommissionen ta upp de medel som den anser vara nödvändiga för tjänsteförteckningen och storleken på det anslag som ska belasta den unionens allmänna budget i förslaget till unionens allmänna budget, som den ska förelägga Europaparlamentet och rådet i enlighet med artikel 314 i EUF-fördraget.

5. Europaparlamentet och rådet ska bevilja anslagen för bidraget från unionen till Enisa.

6. Europaparlamentet och rådet ska anta Enisas tjänsteförteckning.

([26]) Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41).
([27]) Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

7. Styrelsen ska anta Enisas budget tillsammans med det samlade programdokumentet. Enisas budget ska bli slutlig när unionens allmänna budget slutgiltigt har antagits. Styrelsen ska vid behov anpassa Enisas budget och det samlade programdokumentet till unionens allmänna budget.

Artikel 30

Enisas budgets struktur

1. Utan att det påverkar andra medel ska Enisas inkomster bestå av

a) ett bidrag från unionens allmänna budget,

b) inkomster avsatta för särskilda ändamål i enlighet med Enisas finansiella regler som avses i artikel 32,

c) unionsfinansiering via delegeringsavtal eller bidrag som beviljas från fall till fall, i enlighet med de finansiella regler som avses i artikel 32 och gällande bestämmelser för de instrument som inrättats till stöd för unionens politik,

d) bidrag från tredjeländer som deltar i Enisas arbete i enlighet med artikel 42,

e) eventuella frivilliga bidrag från medlemsstater i pengar eller in natura.

Medlemsstater som ger frivilliga bidrag enligt första stycket led e får inte göra anspråk på några särskilda rättigheter eller tjänster som en följd av bidragen.

2. Enisas utgifter ska täcka kostnaderna för personal, administrativt och tekniskt stöd, infrastruktur och drift samt utgifter till följd av avtal med tredje part.

Artikel 31

Genomförande av Enisas budget

1. Den verkställande direktören ska ansvara för att Enisas budget genomförs.

2. Kommissionens internrevisor ska ha samma befogenheter gentemot Enisa som gentemot kommissionens avdelningar.

3. Enisas räkenskapsförare översända de preliminära räkenskaperna för räkenskapsåret (år n) till kommissionens räkenskapsförare och till revisionsrätten senast den 1 mars följande räkenskapsår (år n + 1).

4. Efter mottagandet av revisionsrättens iakttagelser om Enisas preliminära räkenskaper enligt artikel 246 i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 ([28]), ska Enisas räkenskapsförare upprätta Enisas slutliga räkenskaper på eget ansvar och överlämna dem till styrelsen för ett yttrande.

5. Styrelsen ska avge ett yttrande om Enisas slutliga räkenskaper.

6. Senast den 31 mars år n + 1 ska den verkställande direktören översända rapporten om budgetförvaltningen och den ekonomiska förvaltningen till Europaparlamentet, rådet, kommissionen och revisionsrätten.

7. Senast den 1 juli år n + 1 ska Enisas räkenskapsförare överlämna Enisas slutliga räkenskaper, tillsammans med styrelsens yttrande, till Europaparlamentet, rådet, kommissionens räkenskapsförare och revisionsrätten.

([28]) Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012 (EUT L 193, 30.7.2018, s. 1).

8. Enisas räkenskapsföraren ska, samma dag som hans eller hennes slutliga räkenskaper överlämnas, också till revisionsrätten översända en bekräftelse som omfattar dessa slutliga räkenskaper, med en kopia till kommissionens räkenskapsförare.

9. Senast den 15 november år n + 1 ska den verkställande direktören offentliggöra Enisas slutliga räkenskaper i *Europeiska unionens officiella tidning*.

10. Senast den 30 september år n + 1 ska den verkställande direktören till revisionsrätten översända ett svar på dess synpunkter och även sända en kopia av detta svar till styrelsen och till kommissionen.

11. Den verkställande direktören ska på Europaparlamentets begäran, i enlighet med artikel 261.3 i förordning (EU, Euratom) 2018/1046, för Europaparlamentet lägga fram alla uppgifter som är nödvändiga för att förfarandet för beviljande av ansvarsfrihet för det berörda räkenskapsåret ska kunna tillämpas på ett smidigt sätt.

12. På rekommendation av rådet ska Europaparlamentet före den 15 maj år n + 2 bevilja den verkställande direktören ansvarsfrihet beträffande budgetens genomförande år n.

Artikel 32

Finansiella regler

De finansiella regler som ska tillämpas på Enisa ska antas av styrelsen efter samråd med kommissionen. De får inte avvika från delegerad förordning (EU) nr 1271/2013 såvida inte en sådan avvikelse är specifikt nödvändig för Enisas verksamhet och kommissionen har lämnat sitt samtycke i förväg.

Artikel 33

Bedrägeribekämpning

1. För att underlätta bekämpning av bedrägeri, korruption och andra olagliga handlingar enligt Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 ([29]) ska Enisa senast den 28 december 2019, ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 mellan Europaparlamentet, Europeiska unionens råd och Europeiska gemenskapernas kommission om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) ([30]). Enisa ska anta lämpliga bestämmelser som ska vara tillämpliga på alla anställda vid Enisa genom att använda den mall som anges i bilagan till det avtalet.

2. Revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och inspektioner på plats, hos alla stödmottagare, uppdragstagare och underleverantörer som erhållit unionsfinansiering från Enisa.

3. Olaf får göra utredningar, inbegripet kontroller och inspektioner på plats, i enlighet med bestämmelserna och förfarandena i förordning (EU, Euratom) nr 883/2013 och rådets förordning (Euratom, EG) nr 2185/96 ([31]), i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med bidrag eller kontrakt som finansierats av Enisa.

4. Utan att det påverkar tillämpningen av punkterna 1, 2 och 3 ska samarbetsavtal med tredjeländer eller internationella organisationer, kontrakt, bidragsavtal och bidragsbeslut från Enisa innehålla bestämmelser som uttryckligen tillerkänner revisionsrätten och Olaf rätten att utföra sådan revision och genomföra sådana utredningar inom ramen för sina respektive befogenheter.

([29]) Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999 (EUT L 248, 18.9.2013, s. 1).
([30]) EGT L 136, 31.5.1999, s. 15.
([31]) Rådets förordning (Euratom, EG) nr 2185/96 av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda Europeiska gemenskapernas finansiella intressen mot bedrägerier och andra oegentligheter (EGT L 292, 15.11.1996, s. 2).

KAPITEL V

Personal

Artikel 34

Allmänna bestämmelser

Tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda samt de bestämmelser som har antagits gemensamt av unionens institutioner för tillämpningen av tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda ska gälla för Enisas personal.

Artikel 35

Immunitet och privilegier

Enisa och dess personal ska omfattas av protokoll nr 7 om Europeiska unionens immunitet och privilegier, EU-fördraget och EUF-fördraget.

Artikel 36

Verkställande direktör

1. Den verkställande direktören ska vara tillfälligt anställd vid Enisa i enlighet med artikel 2 a i anställningsvillkoren för övriga anställda.

2. Den verkställande direktören ska utses av styrelsen från en förteckning över kandidater som föreslagits av kommissionen efter ett öppet och transparent urvalsförfarande.

3. I det anställningsavtal som sluts med den verkställande direktören ska Enisa företrädas av styrelsens ordförande.

4. Den kandidat som styrelsen väljer ska före utnämningen ombes att göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

5. Den verkställande direktörens mandatperiod ska vara fem år. I slutet av denna period ska kommissionen genomföra en utvärdering av den verkställande direktörens arbetsinsats och Enisas framtida uppgifter och utmaningar.

6. Styrelsen ska fatta beslut om att utse, förlänga mandatperioden för eller avsätta den verkställande direktören i enlighet med artikel 18.2.

7. Styrelsen får på förslag av kommissionen, med beaktande av den utvärdering som avses i punkt 5, förlänga den verkställande direktörens mandatperiod en gång med fem år.

8. Styrelsen ska underrätta Europaparlamentet om sin avsikt att förlänga den verkställande direktörens mandatperiod. Inom tre månader före en sådan förlängning ska den verkställande direktören på anmodan göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

9. En verkställande direktör vars mandat förlängts får inte delta i något ytterligare urvalsförfarande för samma befattning.

10. Den verkställande direktören får avsättas endast efter ett beslut av styrelsen på förslag av kommissionen.

Artikel 37

Utstationerade nationella experter och annan personal

1. Enisa får använda sig av utstationerade nationella experter och annan personal som inte är anställd av Enisa. Tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda ska inte gälla för sådan personal.

2. Styrelsen ska anta ett beslut om regler för utstationering av nationella experter till Enisa.

KAPITEL VI

Allmänna bestämmelser för Enisa

Artikel 38

Enisas rättsliga ställning

1. Enisa ska vara ett unionsorgan och ska vara en juridisk person.

2. Enisa ska i varje medlemsstat ha den mest vittgående rättskapacitet som tillerkänns juridiska personer enligt nationell rätt. Den får särskilt förvärva eller avyttra lös och fast egendom och föra talan inför domstolar och andra myndigheter.

3. Enisa ska företrädas av den verkställande direktören.

Artikel 39

Enisas ansvar

1. Enisas avtalsrättsliga ansvar ska regleras av den lagstiftning som är tillämplig på avtalet i fråga.

2. Europeiska unionens domstol ska vara behörig att träffa avgöranden med stöd av en skiljedomsklausul i ett avtal som Enisa ingått.

3. Vad beträffar utomobligatoriskt ansvar ska Enisa enligt de allmänna principer som är gemensamma för medlemsstaternas rättsordningar ersätta skada som vållats av Enisa själv eller dess personal under tjänsteutövning.

4. Europeiska unionens domstol ska vara behörig att avgöra tvister som rör ersättning för skador som avses i punkt 3.

5. Enisas anställdas personliga ansvar gentemot Enisa ska regleras av de relevanta bestämmelser som är tillämpliga på Enisas personal.

Artikel 40

Språkordning

1. Rådets förordning nr 1 ([32]) ska gälla för Enisa. Medlemsstaterna och övriga organ som utsetts av medlemsstaterna kan vända sig till Enisa och har rätt att få svar på det officiella språk vid unionens institutioner som de själva väljer.

2. De översättningar som krävs för Enisas verksamhet ska tillhandahållas av Översättningscentrum för Europeiska unionens organ.

Artikel 41

Skydd av personuppgifter

1. Enisa ska behandla personuppgifter i enlighet med förordning (EU) 2018/1725.

2. Styrelsen ska anta de genomföranderegler som avses i artikel 45.3 i förordning (EU) 2018/1725. Styrelsen får anta ytterligare åtgärder som behövs för Enisas tillämpning av förordning (EU) 2018/1725.

([32]) Rådets förordning nr 1 om vilka språk som skall användas i Europeiska ekonomiska gemenskapen (EGT 17, 6.10.1958, s. 385/58).

Artikel 42

Samarbete med tredjeländer och internationella organisationer

1. I den mån det är nödvändigt för att uppnå målen i denna förordning får Enisa samarbeta med de behöriga myndigheterna i tredjeländer eller med internationella organisationer, eller båda. För detta ändamål får Enisa, efter förhandsgodkännande från kommissionen, upprätta samarbetsavtal med myndigheterna i tredjeländer och med internationella organisationer. Dessa samarbetsavtal får inte medföra några juridiska förpliktelser för unionen och dess medlemsstater.

2. Enisa ska vara öppen för deltagande av tredjeländer som har ingått avtal med unionen i detta syfte. I enlighet med de relevanta bestämmelserna i dessa avtal ska det fastställas samarbetsavtal som särskilt anger karaktären hos, omfattningen av och utformningen av dessa tredjeländers deltagande i Enisas arbete, inklusive bestämmelser om deltagande i Enisas initiativ, finansiella bidrag och personal. När det gäller personalfrågor ska dessa samarbetsavtal under alla förhållanden vara förenliga med tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda.

3. Styrelsen ska anta en strategi för förbindelserna med tredjeländer och internationella organisationer i de frågor som Enisa har behörighet för. Kommissionen ska säkerställa att Enisa arbetar inom ramen för sitt mandat och den befintliga institutionella ramen genom att ingå lämpliga samarbetsavtal med Enisas verkställande direktör.

Artikel 43

Säkerhetsbestämmelser om skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade uppgifter

Efter samråd med kommissionen ska Enisa anta sina säkerhetsbestämmelser som tillämpar säkerhetsprinciperna i kommissionens säkerhetsbestämmelser för skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter och, i enlighet med beslut (EU, Euratom) 2015/443 och 2015/444. Enisas säkerhetsbestämmelser ska bland annat omfatta bestämmelser om utbyte, behandling och lagring av sådana uppgifter.

Artikel 44

Överenskommelse om säte och villkor för verksamheten

1. De nödvändiga bestämmelserna om de lokaler som ska tillhandahållas för Enisa i värdmedlemsstaten och de anläggningar som ska ställas till Enisas förfogande av den medlemsstaten, tillsammans med de särskilda regler i värdmedlemsstaten som ska tillämpas på den verkställande direktören, styrelseledamöterna, Enisas personal och deras familjemedlemmar, ska fastställas i en överenskommelse om säte mellan Enisa och värdmedlemsstaten, vilken ingås efter att ha godkänts av styrelsen.

2. Enisas värdmedlemsstat ska tillhandahålla bästa möjliga förutsättningar för att säkerställa en väl fungerande byrå, med beaktande av platsens tillgänglighet, adekvata utbildningsmöjligheter för personalens barn, lämplig tillgång till arbetsmarknad, social trygghet och sjukvård för personalens barn och makar.

Artikel 45

Administrativ kontroll

Enisas verksamhet ska övervakas av europeiska ombudsmannen i enlighet med artikel 228 i EUF-fördraget.

AVDELNING III

RAMVERK FÖR CYBERSÄKERHETSCERTIFIERING

Artikel 46

Ett europeiskt ramverk för cybersäkerhetscertifiering

1. Ett europeiskt ramverk för cybersäkerhetscertifiering ska inrättas för att förbättra förutsättningarna för den inre marknadens funktion genom att höja cybersäkerhetsnivån i unionen och möjliggöra en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering i syfte att skapa en digital inre marknad för IKT-produkter, IKT-tjänster och IKT-processer.

2. Genom det europeiska ramverket för cybersäkerhetscertifiering ska en mekanism fastställas för inrättandet av europeiska ordningar för cybersäkerhetscertifiering och för att intyga att de IKT-produkter, IKT-tjänster och IKT-processer som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, tjänster och processer under hela dess livscykel.

Artikel 47

Unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering

1. Kommissionen ska offentliggöra unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering (nedan kallat *unionens löpande arbetsprogram*) i vilket strategiska prioriteringar ska fastställas för framtida europeiska ordningar för cybersäkerhetscertifiering.

2. I unionens löpande arbetsprogram ska det särskilt ingå en förteckning över IKT-produkter, IKT-tjänster och IKT-processer eller kategorier av sådana som kan gagnas av att omfattas av en europeisk ordning för cybersäkerhetscertifiering.

3. Inkludering av specifika IKT-produkter, IKT-tjänster och IKT-processer eller kategorier av sådana i unionens löpande arbetsprogram ska motiveras av ett eller flera av följande skäl:

a) Tillgänglighet och utveckling av nationella ordningar för cybersäkerhetscertifiering omfattande en specifik kategori av IKT-produkter, IKT-tjänster eller IKT-processer, i synnerhet med hänsyn till risken för fragmentering.

b) Relevant unionsrätt eller unionspolitik, eller relevant nationell rätt eller nationell politik.

c) Efterfrågan på marknaden.

d) Utvecklingen av hotbilden inom cyberområdet.

e) Begäran om utarbetande av ett specifikt förslag till certifieringsordning av europeiska gruppen för cybersäkerhetscertifiering.

4. Kommissionen ska vederbörligen beakta de yttranden om utkastet till unionens löpande arbetsprogram som utfärdas av europeiska gruppen för cybersäkerhetscertifiering och intressentgruppen för certifiering.

5. Det första av unionens löpande arbetsprogram ska offentliggöras senast den 28 juni 2020. Unionens löpande arbetsprogram ska uppdateras minst en gång vart tredje år och oftare om det är nödvändigt.

Artikel 48

Begäran om en europeisk ordning för cybersäkerhetscertifiering

1. Kommissionen kan begära att Enisa utarbetar ett förslag till certifieringsordning eller ser över en befintlig europeisk ordning för cybersäkerhetscertifiering på grundval av unionens löpande arbetsprogram.

2. I vederbörligen motiverade fall kan kommissionen eller europeiska gruppen för cybersäkerhetscertifiering begära att Enisa utarbetar ett förslag till certifieringsordning eller ser över en befintlig europeisk ordning för cybersäkerhetscertifiering som inte ingår i unionens löpande arbetsprogram. Unionens löpande arbetsprogram ska uppdateras i enlighet därmed.

Artikel 49

Utarbetande, antagande och översyn av en europeisk ordning för cybersäkerhetscertifiering

1. Efter en begäran från kommissionen i enlighet med artikel 48 ska Enisa utarbeta ett förslag till certifieringsordning som uppfyller de krav som anges i artiklarna 51, 52 och 54.

2. Efter en begäran från europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 48.2 får Enisa utarbeta ett förslag till certifieringsordning som uppfyller de krav som anges i artiklarna 51, 52 och 54. Om Enisa avvisar en sådan begäran ska den lämna en motivering för detta. Beslut om att avvisa en sådan begäran ska fattas av styrelsen.

3. Vid utarbetandet av ett förslag till certifieringsordning ska Enisa samråda med alla berörda intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess.

4. För varje förslag till certifieringsordning ska Enisa inrätta en för ändamålet särskilt tillsatt arbetsgrupp i enlighet med artikel 20.4 i syfte att tillhandahålla Enisa särskild rådgivning och sakkunskap.

5. Enisa ska ha ett nära samarbete med europeiska gruppen för cybersäkerhetscertifiering. Europeiska gruppen för cybersäkerhetscertifiering ska ge Enisa bistånd och expertråd vid utarbetandet av förslaget till certifieringsordning och ska anta ett yttrande om förslaget till certifieringsordning.

6. Enisa ska ta största möjliga hänsyn till europeiska gruppen för cybersäkerhetscertifierings yttrande innan Enisa översänder till kommissionen det förslag till ordning som utarbetats i enlighet med punkterna 3, 4 och 5. Yttrandet från europeiska gruppen för cybersäkerhetscertifiering är inte bindande för Enisa, och frånvaron av ett sådant yttrande hindrar inte Enisa från att översända förslaget till certifieringsordning till kommissionen.

7. Med utgångspunkt i förslaget till certifieringsordning som Enisa lagt fram, får kommissionen anta genomförandeakter för europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer som uppfyller kraven i artiklarna 51, 52 och 54. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.

8. Enisa ska åtminstone vart femte år utvärdera varje antagen europeisk ordning för cybersäkerhetscertifiering och därvid beakta synpunkter från berörda intressenter. Kommissionen eller europeiska gruppen för cybersäkerhetscertifiering får, om det anses nödvändigt, begära att Enisa inleder processen med att utarbeta ett reviderat förslag till certifieringsordning i enlighet med artikel 48 och den här artikeln.

Artikel 50

Webbplats om europeiska ordningar för cybersäkerhetscertifiering

1. Enisa ska underhålla en särskild webbplats med information om och offentliggörande av europeiska ordningar för cybersäkerhetscertifiering, europeiska cybersäkerhetscertifikat och EU-intyg om överensstämmelse, även information med avseende på europeiska ordningar för cybersäkerhetscertifiering som inte längre är giltiga, på indragna och utgångna europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, och på förteckningen över länkar till cybersäkerhetsinformation som tillhandahålls i enlighet med artikel 55.

2. I tillämpliga fall ska det på webbplatsen som avses i punkt 1 också anges vilka nationella ordningar för cybercertifiering som har ersatts av en europeisk ordning för cybersäkerhetscertifiering.

Artikel 51

Säkerhetsmålsättningarna för europeiska ordningar för cybersäkerhetscertifiering

En europeisk ordning för cybersäkerhetscertifiering ska vara utformat för att, i tillämpliga fall, uppnå åtminstone följande säkerhetsmålsättningar:

a) Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten lagring, behandling eller åtkomst eller oavsiktligt eller otillåtet offentliggörande under hela IKT-produktens, IKT-tjänstens eller IKT-processens livscykel.

b) Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten förstöring eller förlust, oavsiktliga eller otillåtna ändringar eller bristande tillgänglighet under hela IKT-produktens, IKT-tjänstens eller IKT-processens livscykel.

c) Att behöriga personer, program eller maskiner kan få åtkomst endast till de data, tjänster eller funktioner som omfattas av deras åtkomsträttigheter.

d) Att identifiera och dokumentera kända beroenden och sårbarheter.

e) Att registrera vilka data, tjänster och funktioner som någon haft åtkomst till, som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem.

f) Att det är möjligt att kontrollera vilka data, tjänster eller funktioner som någon haft åtkomst till, eller som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem.

g) Kontrollera att IKT-produkter, IKT-tjänster och IKT-processer inte innehåller några kända sårbarheter.

h) Att återställa tillgängligheten och tillgången avseende data, tjänster och funktioner i rätt tid vid en fysisk eller teknisk incident.

i) Att IKT-produkter, IKT-tjänster och IKT-processer är säkra i sitt grundutförande och är säkra genom sin konstruktion.

j) Att IKT-produkter, IKT-tjänster och IKT-processer tillhandahålls med uppdaterad programvara och maskinvara som inte innehåller publikt kända sårbarheter, och med funktioner för säkra uppdateringar.

Artikel 52

Assuransnivåer för europeiska ordningar för cybersäkerhetscertifiering

1. En europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster och IKT-processer: ”grundläggande”, ”betydande” eller ”hög”. Assuransnivån ska stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, IKT-tjänst eller IKT-process, i form av sannolikhet för och inverkan av en eventuell incident.

2. Ett europeiskt cybersäkerhetscertifikat och en EU-försäkran om överensstämmelse ska hänvisa till alla assuransnivåer som anges i den europeiska ordningen för cybersäkerhetscertifiering enligt vilket det europeiska cybersäkerhetscertifikatet och EU-försäkran om överensstämmelse utfärdades.

3. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering, inbegripet motsvarande säkerhetsfunktioner och motsvarande stringens och djup i fråga om den utvärdering som IKT-produkten, IKT-tjänsten eller IKT-processen ska genomgå

4. Certifikatet eller EU-försäkran om överensstämmelse ska hänvisa till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som syftar till att minska risken för eller förhindra cybersäkerhetsincidenter.

5. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ”grundläggande” ska försäkra att IKT-produkter, IKT-tjänster och IKT-processer för vilka det certifikatet eller den EU-försäkran om överensstämmelse har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera kända grundläggande risker för incidenter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen. Om en sådan granskning inte är lämplig ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

6. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ”betydande” ska försäkra att IKT-produkter, IKT-tjänster och IKT-processer för vilka det certifikatet har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera kända cyberrisker, och risken för incidenter och cyberattacker som genomförs av aktörer med begränsade kunskaper och resurser. Den utvärdering som ska göras ska innefatta åtminstone följande en granskning för att visa att allmänt kända sårbarheter inte föreligger och testning för att visa att IKT-produkter, IKT-tjänster och IKT-processer på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner. Om sådana utvärderingar inte är lämpliga ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

7. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ”hög” ska försäkra att IKT-produkter, IKT-tjänster och IKT-processer för vilka det certifikatet har utfärdats uppfyller motsvarande säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats på en nivå som avser att minimera risken för avancerade cyberattacker som genomförs av aktörer med omfattande kunskaper och resurser. Den utvärdering som ska göras ska innefatta åtminstone följande: en granskning för att visa att allmänt kända sårbarheter inte föreligger, testning för att visa att IKT-produkter, IKT-IKT-tjänster eller IKT-processer på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner, med den senaste tekniken, och en bedömning av motståndskraften mot kunniga angripare genom penetrationsprovning. Om sådana utvärderingar inte är lämpliga får alternativa insatser utföras.

8. En europeisk ordning för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer beroende på hur stringent och djupgående den aktuella utvärderingsmetoden är. Var och en av utvärderingsnivåerna ska motsvara en av assuransnivåerna och definieras genom en lämplig kombination av assuranskomponenter.

Artikel 53

Självbedömning av överensstämmelse

1. En europeisk ordning för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer möjlighet att göra en självbedömning av överensstämmelse. En självbedömning av överensstämmelse ska endast tillåtas i förhållande till IKT-produkter, IKT-tjänster och IKT-processer med låg risk som motsvarar assuransnivån ”grundläggande”.

2. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer får utfärda en EU-försäkran om överensstämmelse med angivande av att det har visats att kraven i ordningen är uppfyllda. Genom att upprätta en sådan försäkran tar tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer ansvar för att IKT-produkten, IKT-tjänsten eller IKT-processen överensstämmer med de krav som anges i den ordningen.

3. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer ska, under en period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering, ge den nationella myndighet för cybersäkerhetscertifiering som avses i artikel 58 tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas eller IKT-tjänsternas överensstämmelse med ordningen. En kopia av EU-försäkran om överensstämmelse ska lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

4. Det är frivilligt att utfärda EU-försäkran om överensstämmelse om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

5. En EU-försäkran om överensstämmelse ska erkännas i alla medlemsstater.

Artikel 54

Komponenter i europeiska ordningar för cybersäkerhetscertifiering

1. En europeisk ordning för cybersäkerhetscertifiering ska innehålla åtminstone följande komponenter:

a) Föremålet och tillämpningsområdet för certifieringsordningen, inbegripet typen eller kategorierna av de IKT-produkter, IKT-tjänster och IKT-processer som omfattas av certifieringsordningen.

b) En tydlig beskrivning av syftet med ordningen och hur de valda standarderna, utvärderingsmetoderna och assuransnivåerna överensstämmer med behoven hos ordningens avsedda användare.

c) En hänvisning till de internationella, europeiska eller nationella standarder som följts vid utvärderingen eller, om sådana standarder inte finns tillgängliga eller de inte är lämpliga, till tekniska specifikationer som uppfyller kraven i bilaga II till förordning (EU) nr 1025/2012 eller, om sådana specifikationer inte finns tillgängliga, till tekniska specifikationer eller andra cybersäkerhetskrav som fastställs i den europeiska ordningen för cybersäkerhetscertifiering.

d) I tillämpliga fall, en eller flera assuransnivåer.

e) Angivelse av huruvida självbedömning av överensstämmelse är tillåtet inom ramen för ordningen.

f) I tillämpliga fall, särskilda eller ytterligare krav som gäller för organ för bedömning av överensstämmelse för att garantera deras tekniska kompetens att utvärdera cybersäkerhetskraven.

g) Särskilda bedömningskriterier och -metoder som använts, inklusive utvärderingstyper, i syfte att visa att de säkerhets mål som anges i artikel 51 uppnås.

h) I tillämpliga fall, uppgifter som är nödvändiga för certifieringen och som en sökande ska lämna till eller på annat sätt göra tillgängliga för organ för bedömning av överensstämmelse.

i) Om ordningen fastställer användning av märken eller etiketter, villkoren för deras användning.

j) Reglerna för övervakning av efterlevnaden av IKT-produkter, IKT-tjänster och IKT-processer vad gäller kraven i europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven.

k) I tillämpliga fall, villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat samt villkor för utvidgning eller inskränkning av tillämpningsområdet för certifiering.

l) Bestämmelser om följderna för IKT-produkter, IKT-tjänster och IKT-processer som har certifierats eller för vilka en EU-försäkran om överensstämmelse har utfärdats, men som inte överensstämmer med kraven i ordningen.

m) Bestämmelser om hur tidigare oupptäckta sårbarheter i fråga om cybersäkerhet hos KT-produkter, IKT-tjänster och IKT-processer ska rapporteras och hanteras.

n) I tillämpliga fall, bestämmelser om hur organ för bedömning av överensstämmelse ska bevara sina uppgifter.

o) Identifiering av nationella eller internationella ordningar för cybersäkerhetscertifiering som omfattar samma typ eller kategorier av IKT-produkter, IKT-tjänster och IKT-processer, säkerhetskrav, utvärderingskriterier och utvärderingsmetoder samt assuransnivåer.

p) Innehållet i och formatet på det utfärdade europeiska cybersäkerhetscertifikatet och EU-försäkran om överensstämmelse.

q) Den period under vilken tillverkaren eller leverantören av IKT-produkter, IKT-tjänster och IKT-processer ska hålla tillgänglig EU-försäkran om överensstämmelse, den tekniska dokumentationen och all annan relevant information som ska göras tillgänglig.

r) Längsta giltighetstid för europeiska cybersäkerhetscertifikat som utfärdats enligt ordningen.

s) Offentlighetspolicy för europeiska cybersäkerhetscertifikat som utfärdats, ändrats eller återkallats enligt ordningen.

t) Villkor för ömsesidigt erkännande av certifieringsordningar med tredjeländer.

u) I tillämpliga fall, bestämmelser om eventuell mekanism för inbördes bedömning som i ordningen inrättats för de myndigheter eller organ som utfärdar europeiska cybersäkerhetscertifikat med assuransnivån ”hög” enligt artikel 56.6. Sådana mekanismer ska inte påverka den inbördes granskning som föreskrivs i artikel 59.

v) Format och förfaranden som ska följas av tillverkare eller leverantörer av IKT-produkter, IKT-tjänster och IKT-processer när de lämnar och uppdaterar den kompletterande cybersäkerhetsinformationen i enlighet med artikel 55.

2. De angivna kraven för den europeiska ordningen för cybersäkerhetscertifiering ska vara förenliga med tillämpligt lagstadgat krav, i synnerhet inte krav som härrör från harmoniserad unionsrätt.

3. Om det föreskrivs i en viss unionsrättsakt får ett certifikat eller en EU-försäkran om överensstämmelse som utfärdats enligt en europeisk ordning för cybersäkerhetscertifiering användas för att påvisa presumtion om överensstämmelse med kraven i den rättsakten.

4. I avsaknad av harmoniserad unionsrätt får en medlemsstats nationella rätt också föreskriva att en europeisk ordning för cybersäkerhetscertifiering får användas för fastställande av presumtionen om överensstämmelse med de rättsliga kraven.

Artikel 55

Kompletterande cybersäkerhetsinformation för certifierade IKT-produkter, IKT-tjänster och IKT-processer

1. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer som är certifierade eller för vilka en EU-försäkran om överensstämmelse har utfärdats ska lämna följande kompletterande cybersäkerhetsinformation:

a) Vägledning och rekommendationer för att hjälpa slutanvändare med säker konfiguration, installation, ibruktagande, användning och underhåll av IKT-produkterna eller IKT-tjänsterna.

b) Uppgift om tidsperiod under vilken säkerhetsstöd kommer att erbjudas slutanvändare, särskilt vad gäller tillgång till cybersäkerhetsrelaterade uppdateringar.

c) Kontaktuppgifter för tillverkaren eller leverantören och uppgift om metoder som accepteras för mottagande av sårbarhetsinformation från slutanvändare och säkerhetsforskare.

d) Hänvisning till förteckningar online över offentliggjorda sårbarheter kopplade till IKT-produkten, IKT-tjänsten eller IKT-processen samt relevant cybersäkerhetsrådgivning.

2. Den information som avses i punkt 1 ska tillgängliggöras i elektroniskt format och finnas tillgänglig och vid behov uppdateras åtminstone fram till dess att motsvarande europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse löper ut.

Artikel 56

Cybersäkerhetscertifiering

1. IKT-produkter, IKT-tjänster och IKT-processer som har certifierats enligt en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 ska förutsättas överensstämma med kraven i en sådan ordning.

2. Cybersäkerhetscertifieringen ska vara frivillig, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

3. Kommissionen ska regelbundet bedöma effektiviteten hos och användningen av de antagna europeiska ordningarna för cybersäkerhetscertifiering och huruvida en specifik europeisk ordning för cybersäkerhetscertifiering ska göras obligatoriskt genom unionsrätten i syfte att säkerställa en adekvat cybersäkerhetsnivå för IKT-produkter, IKT-tjänster och IKT-processer i unionen och förbättra den inre marknadens funktion. Den första bedömningen ska göras senast den 31 december 2023, och efterföljande bedömningar ska göras minst en gång vartannat år därefter. Kommissionen ska, på grundval av resultatet av bedömningen, fastställa vilka IKT-produkter, IKT-tjänster och IKT-processer som ska omfattas av en existerande certifieringsordning som bör täckas av en obligatorisk certifieringsordning.

Kommissionen ska fokusera på de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148, vilka ska bedömas senast två år efter antagandet av den första europeiska ordningen för cybersäkerhetscertifiering.

Vid utarbetandet av bedömningen ska kommissionen

a) beakta åtgärdernas konsekvenser i kostnadsavseende för tillverkarna och leverantörerna av de berörda IKT-produkterna, IKT-tjänsterna eller IKT-processerna och för användarna samt de samhälleliga och/eller ekonomiska vinsterna med den förväntade höjningen av säkerhetsnivån för de berörda IKT-produkterna, IKT-tjänsterna eller IKT-processerna,

b) ta i beaktande existensen och införlivandet av relevant nationell rätt i medlemsstaterna och i tredjeländer,

c) genomföra en öppen, transparent och inkluderande samrådsprocess med alla berörda intressenter och medlemsstater,

d) beakta eventuella genomförandefrister och övergångsåtgärder och övergångsperioder, i synnerhet åtgärdens tänkbara inverkan på tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer, däribland små och medelstora företag,

e) föreslå hur man snabbast och mest effektivt ska genomföra övergången från ett frivilligt till en obligatorisk certifieringsordning.

4. De organ för bedömning av överensstämmelse som avses i artikel 60 ska utfärda europeiska cybersäkerhetscertifikat i enlighet med den här artikeln som avser assuransnivå ”grundläggande” eller ”betydande” på grundval av de kriterier som ingår i den europeiska ordningen för cybersäkerhetscertifiering, som antagits av kommissionen i enlighet med artikel 49.

5. Genom undantag från punkt 4, och i vederbörligen motiverade fall, får en europeisk ordning för cybersäkerhetscertifiering föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen kan utfärdas endast av ett offentligt organ. Ett sådant organ ska vara ett av följande:

a) En nationell myndighet för cybersäkerhetscertifiering som avses i artikel 58.1.

b) Ett offentligt organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 60.1.

6. Om en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 kräver assuransnivå ”hög” ska det europeiska cybersäkerhetscertifikatet enligt den ordningen endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller, i följande fall, av ett organ för bedömning av överensstämmelse:

a) Efter förhandsgodkännande av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse.

b) Efter allmän delegering på förhand av uppgiften att utfärda ett sådant europeiskt cybersäkerhetscertifikat till ett organ för bedömning av överensstämmelse från den nationella myndigheten för cybersäkerhetscertifiering.

7. Den fysiska eller juridiska person som lämnar in sina IKT-produkter, IKT-tjänster eller IKT-processer för certifiering ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndighet för cybersäkerhetscertifiering som avses i artikel 58, om denna myndighet är det organ som utfärdar det europeiska cybersäkerhetscertifikatet, eller för det organ för bedömning av överensstämmelse som avses i artikel 60.

8. Innehavaren av ett europeiskt cybersäkerhetscertifikat ska informera den myndighet eller det organ som avses i punkt 7 om alla sårbarheter eller oriktigheter som upptäcks senare och som rör säkerheten för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen som kan påverka överensstämmelsen med de krav som sammanhänger med certifieringen. Den myndigheten eller det organet ska utan onödigt dröjsmål vidarebefordra denna information till den berörda nationella myndigheten för cybersäkerhetscertifiering.

9. Ett europeiskt cybersäkerhetscertifikat ska utfärdas för den period som fastställs i den europeiska ordningen för cybersäkerhetscertifiering och får förnyas under förutsättning att de relevanta kraven alltjämt uppfylls.

10. Ett europeiskt cybersäkerhetscertifikat som utfärdats i enlighet med denna artikel ska erkännas i alla medlemsstater.

Artikel 57

Nationella ordningar och certifikat för cybersäkerhetscertifiering

1. Utan att det påverkar tillämpningen av punkt 3 i denna artikel ska de nationella ordningarna för cybersäkerhetscertifiering och därtill hörande förfaranden, för IKT-produkter, IKT-tjänster och IKT-processer som omfattas av en europeisk ordning för cybersäkerhetscertifiering, upphöra att ha verkan från och med den dag som anges i den genomförandeakt som antagits i enlighet med artikel 49.7. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster och IKT-processer som inte omfattas av en europeisk ordning för cybersäkerhetscertifiering ska kvarstå.

2. Medlemsstaterna ska inte införa nya nationella ordningar för cybersäkerhetscertifiering av de IKT-produkter, IKT-tjänster och IKT-processer som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.

3. Befintliga certifikat som utfärdats enligt nationella ordningar för cybersäkerhetscertifiering och som omfattas av en europeisk ordning för cybersäkerhetscertifiering ska förbli giltiga tills de löper ut.

4. I syfte att undvika en fragmentering av den inre marknaden ska medlemsstaterna underrätta kommissionen och europeiska gruppen för cybersäkerhetscertifiering om alla avsikter att utarbeta nya nationella ordningar för cybersäkerhetscertifiering.

Artikel 58

Nationella myndigheter för cybersäkerhetscertifiering

1. Varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium eller, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i denna andra medlemsstat som ansvariga för tillsynsuppgifterna i den utseende medlemsstaten.

2. Varje medlemsstat ska underrätta kommissionen om vilka nationella myndigheter för cybersäkerhetscertifiering som utsetts. Om en medlemsstat utser mer än en myndighet ska den också informera kommissionen om vilka uppgifter som var och en av dessa myndigheter tilldelats.

3. Utan att det påverkar tillämpningen av artikel 56.5 a och 56.6 ska varje nationell myndighet för cybersäkerhetscertifiering vara oberoende av de enheter som den utövar tillsyn över vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande.

4. Medlemsstaterna ska säkerställa att den verksamhet som bedrivs av den nationella myndigheten för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat som avses i artikel 56.5 a och 56.6 är strikt avskilda från deras uppgifter och ansvarsområden i förhållande till tillsynsverksamheten enligt den här artikeln och att dessa verksamheter utförs oberoende av varandra.

5. Medlemsstaterna ska säkerställa att de nationella myndigheterna för cybersäkerhetscertifiering har tillräckliga resurser för att kunna utöva sina befogenheter och kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt.

6. För en effektiv tillämpning av denna förordning är det lämpligt att nationella myndigheterna för cybersäkerhetscertifiering deltar i den europeiska gruppen för cybersäkerhetscertifiering på ett aktivt, effektivt, ändamålsenligt och säkert sätt.

7. Nationella myndigheter för cybersäkerhetscertifiering ska

a) övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering enligt artikel 54.1 j för övervakning av IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med kraven i de europeiska cybersäkerhetscertifikat som utfärdats inom deras respektive territorier, i samarbete med andra berörda marknadsövervakningsmyndigheter,

b) kontrollera att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer som är etablerade inom deras respektive territorier fullgör och verkställer sina skyldigheter och att de genomför självbedömning av överensstämmelse, särskilt fullgörandet och verkställandet av dessa tillverkares och leverantörers skyldigheter enligt artikel 53.2 och 53.3 och i motsvarande europeisk ordning för cybersäkerhetscertifiering.

c) utan att det påverkar tillämpningen av artikel 60.3 aktivt bistå och stödja de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning,

d) övervaka och kontrollera den verksamhet som bedrivs av de offentliga organ som avses i artikel 56.5,

e) i tillämpliga fall utfärda bemyndiganden för organ för bedömning av överensstämmelse i enlighet med artikel 60.3 och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organen för bedömning av överensstämmelse inte uppfyller kraven i denna förordning,

f) behandla klagomål från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av nationella myndigheter för cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 56.6, eller avseende en EU-försäkran av överensstämmelse som utfärdats enligt artikel 53, och ska i lämplig utsträckning undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen,

g) lämna en årlig sammanfattande rapport om den verksamhet som bedrivits enligt leden b, c och d i denna punkt eller enligt punkt 8 till Enisa och europeiska gruppen för cybersäkerhetscertifiering,

h) samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, bland annat genom att utbyta information om IKT-produkter, IKT-tjänster och IKT-processer som eventuellt avviker från kraven i denna förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och

i) övervaka relevant utveckling på området cybersäkerhetscertifiering.

8. Varje nationell myndighet för cybersäkerhetscertifiering ska åtminstone ha befogenheter att

a) begära att organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare en EU-försäkran om överensstämmelse ska lägga fram alla uppgifter som myndigheten behöver för att kunna fullgöra sin uppgift,

b) genomföra undersökningar, i form av kontroller, av organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse, för att kunna verifiera överensstämmelse med denna avdelning,

c) vidta lämpliga åtgärder, i enlighet med nationell rätt, för att säkerställa att organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse uppfyller kraven i denna förordning eller en europeisk ordning för cybersäkerhetscertifiering,

d) få tillgång till alla lokaler hos organ för bedömning av överensstämmelse eller innehavare av ett europeiskt cybersäkerhetscertifikat i syfte att genomföra utredningar i enlighet med unionsrätten eller medlemsstaternas processrätt,

e) i enlighet med nationell rätt, återkalla europeiska cybersäkerhetscertifikat som utfärdats av den nationella myndigheten för cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 56.6, om sådana certifikat inte uppfyller kraven i denna förordning eller en europeisk ordning för cybersäkerhetscertifiering,

f) utdöma sanktioner i enlighet med nationell rätt, enligt artikel 65, och kräva att överträdelser av skyldigheterna i denna förordning omedelbart upphör.

9. Nationella myndigheter för cybersäkerhetscertifiering ska samarbeta med varandra och med kommissionen, i synnerhet, genom att utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter IKT-tjänster och IKT-processer.

Artikel 59

Inbördes granskning

1. I syfte att uppnå likvärdiga standarder i hela unionen för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse ska de nationella myndigheterna för cybersäkerhetscertifiering omfattas av inbördes granskning.

2. Den inbördes granskningen ska företas utifrån gedigna och transparenta kriterier och förfaranden för utvärdering, särskilt när det gäller strukturella krav samt krav gällande personal och förfaranden och med hänsyn till konfidentialitet och klagomål.

3. Den inbördes granskningen ska omfatta en bedömning

a) i tillämpliga fall av om den verksamhet som bedrivs av nationella myndigheter för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat som avses i artikel 56.5 a och 56.6 är strikt åtskilda från deras tillsynsverksamhet enligt artikel 58 och om dessa verksamheter utförs oberoende av varandra,

b) av förfarandena för övervakning och kontroll av efterlevnaden av bestämmelserna om IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med europeiska cybersäkerhetscertifikat enligt artikel 58.7 a,

c) av förfarandena för övervakning och verkställande av de skyldigheter som tillverkare eller tillhandahållare av IKT-produkter, IKT tjänster eller IKT-processer har i enlighet med artikel 58.7 b,

d) av förfarandena för övervakning, bemyndigande och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse,

e) i tillämpliga fall av om personalen vid de myndigheter eller organ som utfärdar certifikat med assuransnivån ”hög” i enlighet med artikel 56.6 har lämplig sakkunskap.

4. Den inbördes granskningen ska utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och kommissionen och ska utföras minst vart femte år. Enisa får delta i den inbördes granskningen.

5. Kommissionen får anta genomförandeakter, som inrättar en plan för den inbördes granskningen som ska omfatta en period på minst fem år, med kriterier för sammansättningen av gruppen som ska utföra den inbördes granskningen, den metod som ska användas, tidsplanen, frekvensen och andra uppgifter som rör den inbördes granskningen. När kommissionen antar dessa genomförandeakter ska den ta vederbörlig hänsyn till synpunkterna från den europeiska gruppen för cybersäkerhetscertifiering. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.

6. Europeiska gruppen för cybersäkerhetscertifiering ska behandla resultaten av den inbördes granskningen och göra en sammanfattning som får offentliggöras samt vid behov utfärda riktlinjer eller rekommendationer om åtgärder som ska vidtas av de berörda enheterna.

Artikel 60

Organ för bedömning av överensstämmelse

1. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008. Sådan ackreditering ska endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till denna förordning.

2. Om ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a och 56.6 ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som ett organ för bedömning av överensstämmelse enligt punkt 1 i den här artikeln.

3. Om de europeiska ordningarna för cybersäkerhetscertifiering innehåller särskilda eller ytterligare krav enligt artikel 54.1 f ska endast organ för bedömning av överensstämmelse som uppfyller dessa krav bemyndigas av den nationella myndigheten för cybersäkerhetscertifiering att utföra uppgifter inom ramen för sådana ordningar.

4. Ackrediteringen som avses i punkt 1 ska utfärdas till organen för bedömning av överensstämmelse för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse fortfarande uppfyller kraven i denna artikel. Nationella ackrediteringsorgan ska vidta alla lämpliga åtgärder inom en rimlig tidsram för att begränsa, tillfälligt upphäva eller återkalla ackrediteringen av ett organ för bedömning av överensstämmelse som utfärdats i enlighet med punkt 1 om villkoren för ackrediteringen inte har uppfyllts, eller inte längre uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot denna förordning.

Artikel 61

Anmälan

1. För varje europeisk ordning för cybersäkerhetscertifiering ska de nationella myndigheterna för cybersäkerhetscertifiering till kommissionen anmäla de organ för bedömning av överensstämmelse som har ackrediterats och, i tillämpliga fall, bemyndigade i enlighet med artikel 60.3 att utfärda europeiska cybersäkerhetscertifikat på angivna assuransnivåer enligt artikel 52. De nationella myndigheterna för cybersäkerhetscertifiering ska, utan onödigt dröjsmål, till kommissionen anmäla eventuella senare ändringar av dessa.

2. Ett år efter ikraftträdandet av en europeisk ordning för cybersäkerhetscertifiering ska kommissionen offentliggöra en förteckning över de organ för bedömning av överensstämmelse som har anmälts enligt den ordningen i *Europeiska unionens officiella tidning*.

3. Om kommissionen mottar en anmälan efter utgången av den period som avses i punkt 2 ska den offentliggöra ändringarna av förteckningen över anmälda organ för bedömning av överensstämmelse i *Europeiska unionens officiella tidning* inom två månader från dagen för mottagandet av den anmälan.

4. En nationell myndighet för cybersäkerhetscertifiering får lämna in en begäran till kommissionen om att stryka ett organ för bedömning av överensstämmelse, som anmälts av den myndigheten, från den förteckning som avses i punkt 2. Kommissionen ska offentliggöra motsvarande ändringar av förteckningen i *Europeiska unionens officiella tidning* inom en månad från och med dagen för mottagandet av begäran från den nationella myndigheten för cybersäkerhetscertifiering.

5. Kommissionen får anta genomförandeakter för att fastställa förutsättningar, format och förfaranden för de anmälningar som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.

Artikel 62

Europeiska gruppen för cybersäkerhetscertifiering

1. Europeiska gruppen för cybersäkerhetscertifiering (nedan kallad *gruppen*) ska inrättas.

2. Gruppen ska bestå av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller företrädare för andra berörda nationella myndigheter. En gruppmedlem får inte företräda mer än två medlemsstater.

3. Intressenter och berörda tredje parter får bjudas in att delta i gruppens möten och delta i dess arbete.

4. Gruppen ska ha i uppgift att

a) ge råd till och bistå kommissionen i dess arbete för att säkerställa ett konsekvent genomförande och en konsekvent tillämpning av denna avdelning, särskilt när det gäller frågor som rör unionens löpande arbetsprogram, cybersäkerhetscertifiering, strategisamordning och utarbetandet av de europeiska ordningarna för cybersäkerhetscertifiering,

b) ge råd till, bistå och samarbeta med Enisa när det gäller utarbetande av förslag till certifieringsordning enligt artikel 49,

c) anta ett yttrande om förslagtill certifieringsordning som utarbetats av Enisa enligt artikel 49,

d) uppmana Enisa att utarbeta förslag till certifieringsordning enligt artikel 48.2,

e) anta yttranden riktade till kommissionen rörande underhåll och översyn av befintliga europeiska ordningar för cybersäkerhetscertifiering,

f) undersöka den relevanta utvecklingen på området cybersäkerhetscertifiering och utbyta information och god praxis om ordningar för cybersäkerhetscertifiering,

g) underlätta samarbetet mellan nationella myndigheter för cybersäkerhetscertifiering enligt denna avdelning genom kapacitetsuppbyggnad och utbyte av information, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om frågor som rör cybersäkerhetscertifiering,

h) tillhandahålla stöd för genomförandet av mekanismerna för inbördes bedömning i enlighet med de regler som fastställts i en europeisk ordning för cybersäkerhetscertifiering enligt artikel 54.1 u.

i) underlätta anpassningen av europeiska ordningar för cybersäkerhetscertifiering med internationellt erkända standarder, också genom att se över befintliga europeiska ordningar för cybersäkerhetscertifiering och, där så är lämpligt, lämna rekommendationer till Enisa om att samarbeta med relevanta internationella standardiseringsorganisationer för att åtgärda brister eller luckor i de befintliga internationellt erkända standarderna.

5. Med stöd från Enisa ska kommissionen vara ordförande i gruppen och kommissionen ska tillhandahålla gruppen ett sekretariat, i enlighet med artikel 8.1 e.

Artikel 63

Rätt att lämna in klagomål

1. Fysiska och juridiska personer ska ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller, när klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse som handlar i enlighet med artikel 56.6, till den berörda nationella myndigheten för cybersäkerhetscertifiering.

2. Myndigheten eller organet till vilket klagomålet har lämnats in ska underrätta den klagande om hur förfarandet fortskrider och vilket beslut som fattats, och ska informera den klagande om rätten till effektiva rättsmedel enligt artikel 64.

Artikel 64

Rätt till ett effektivt rättsmedel

1. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol ska fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende

a) beslut fattade av den myndighet eller det organ som avses i artikel 63.1, i tillämpliga fall, även om felaktigt utfärdande, icke-utfärdande eller erkännande av ett europeiskt cybersäkerhetscertifikat som innehas av dessa fysiska och juridiska personer,

b) underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till den myndighet eller det organ som avses i artikel 63.1.

2. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där myndigheten eller organet som det rättsmedlen avser är beläget.

Artikel 65

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av denna avdelning och överträdelser av europeiska ordningar för cybersäkerhetscertifiering, och ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt eventuella ändringar som berör dem.

AVDELNING IV

SLUTBESTÄMMELSER

Artikel 66

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5.4 b i förordning (EU) nr 182/2011 tillämpas.

Artikel 67

Utvärdering och granskning

1. Senast den 28 juni 2024, och därefter vart femte år, ska kommissionen utvärdera effekterna av och ändamålsenligheten och effektiviteten hos Enisas arbete samt dess arbetsmetoder, det eventuella behovet av att ändra Enisas mandat samt de finansiella följderna av sådana ändringar. Utvärderingen ska beakta alla synpunkter som Enisa mottagit beträffande sin verksamhet. Om kommissionen anser att Enisas fortsatta drift inte längre är motiverad mot bakgrund av de mål, mandat och uppgifter som den tilldelats, kan kommissionen föreslå att de bestämmelser i denna förordning som rör Enisa ändras.

2. Utvärderingen ska även bedöma effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i denna förordning i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer i unionen och förbättra den inre marknadens funktion.

3. I utvärderingen ska det bedömas om tillträde till den inre marknaden ska förutsätta att väsentliga cybersäkerhetskrav uppfyllts, för att förhindra att IKT-produkter, IKT-tjänster och IKT-processer som inte uppfyller de grundläggande cybersäkerhetskraven kommer in på unionsmarknaden.

4. Senast den 28 juni 2024 och vart femte år därefter ska kommissionen översända rapporten om utvärderingen tillsammans med dess slutsatser till Europaparlamentet, rådet och styrelsen. Rapportens resultat ska offentliggöras.

Artikel 68

Upphävande och succession

1. Förordning (EU) nr 526/2013 upphör att gälla med verkan från och med den 27 juni 2019.

2. Hänvisningar till förordning (EU) nr 526/2013 och till Enisa som inrättats genom den förordningen, ska anses som hänvisningar till den här förordningen och till Enisa som inrättats genom den här förordningen.

3. Enisa som inrättats genom den här förordningen efterträder Enisa som inrättades genom förordning (EU) nr 526/2013 när det gäller all äganderätt samt alla avtal, rättsliga skyldigheter, anställningskontrakt, finansiella åtaganden och ansvarsskyldigheter. Alla beslut som styrelsen och direktionen har fattat i enlighet med förordning (EU) nr 526/2013 ska fortsätta att gälla, förutsatt att de överensstämmer med den här förordningen.

4. Enisa ska inrättas på obestämd tid från den 27 juni 2019.

5. Den verkställande direktör som har utsetts i enlighet med artikel 24.4 i förordning (EU) nr 526/2013 ska kvarstå i tjänst och utöva de uppgifter för Enisas verkställande direktör som avses i artikel 20 i den här förordningen under den återstående delen av den verkställande direktörens mandatperiod. Övriga villkor i den verkställande direktörens avtal ska förbli oförändrade.

6. Styrelseledamöterna och deras suppleanter som utsetts i enlighet med artikel 6 i förordning (EU) nr 526/2013 ska kvarstå i tjänst och utöva de styrelsefunktioner som avses i artikel 15 i den här förordningen under den återstående delen av sina mandatperioder.

Artikel 69

Ikraftträdande

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Artiklarna 58, 60, 61, 63, 64 och 65 ska tillämpas från och med den 28 juni 2021.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den 17 april 2019.

På Europaparlamentets vägnar	*På rådets vägnar*
A. TAJANI	G. CIAMBA
Ordförande	*Ordförande*

BILAGA

KRAV SOM ORGANEN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE SKA UPPFYLLA

De organ för bedömning av överensstämmelse som önskar bli ackrediterade ska uppfylla följande krav:

1. Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell rätt och vara en juridisk person.

2. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller de IKT-produkter, IKT-tjänster eller IKT-processer som det bedömer.

3. Ett organ som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i konstruktion, tillverkning, leverans, installation, användning eller underhåll av de IKT-produkter, IKT-tjänster eller IKT-processer som det bedömer, får anses vara ett organ för bedömning av överensstämmelse, förutsatt att det kan styrkas att det är oberoende och att inga intressekonflikter föreligger.

4. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för att utföra bedömningen av överensstämmelse, får inte utgöras av den som konstruerar, tillverkar, levererar, installerar, köper, äger, använder eller underhåller den IKT-produkt, IKT-tjänst eller IKT-process som bedöms, eller de som företräder någon av dessa parter. Det förbudet ska inte hindra att bedömda IKT-produkter som är nödvändiga för verksamheten inom organet för bedömning av överensstämmelse används eller att IKT-produkterna används för personligt bruk.

5. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får varken delta direkt i konstruktionen, tillverkningen, marknadsföringen, installationen, användningen eller underhållet av dessa IKT-produkter, IKT-tjänster eller IKT-processer som bedöms, eller företräda de parter som bedriver denna verksamhet. Organen för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömningen av överensstämmelse. Det förbudet ska framför allt gälla konsulttjänster.

6. Om ett organ för bedömning av överensstämmelse ägs eller drivs av en offentlig myndighet eller institution ska det säkerställas och dokumenteras att organet har en oberoende ställning och att inga intressekonflikter föreligger mellan den nationella myndigheten för cybersäkerhetscertifiering och, organet för bedömning av överensstämmelse.

7. Organ för bedömning av överensstämmelse ska säkerställa att deras dotterbolags eller underentreprenörers verksamhet inte påverkar sekretessen, objektiviteten eller opartiskheten i organens bedömningar av överensstämmelse.

8. Organ för bedömning av överensstämmelse och deras personal ska utföra bedömningen av överensstämmelse med största möjliga yrkesintegritet, ha erforderlig teknisk kompetens på det specifika området och vara fria från alla påtryckningar och incitament, som kan påverka deras omdöme eller resultaten av deras bedömning av överensstämmelse, inklusive påtryckningar och incitament av ekonomisk natur, särskilt när det gäller personer eller grupper av personer som berörs av denna verksamhet.

9. Ett organ för bedömning av överensstämmelse ska vara i stånd att utföra alla de uppgifter för bedömning av överensstämmelse som det utsetts att utföra enligt denna förordning, oavsett om uppgifterna utförs av organet för bedömning av överensstämmelse självt eller av annan part för dess räkning och på dess ansvar. Om underleverantörer eller utomstående konsulter anlitas ska detta vara väl dokumenterat, inte inbegripa mellanhänder och det ska finnas ett skriftligt avtal som bland annat ska innehålla bestämmelser om sekretess och intressekonflikter. Det aktuella organet för bedömning av överensstämmelse ska åta sig fullt ansvar för de uppgifter som utförs.

10. Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ, kategori eller underkategori av IKT-produkter, IKT-tjänster eller IKT-processer, ska ett organ för bedömning av överensstämmelse ha till sitt förfogande

    a) personal med teknisk kunskap och tillräcklig och lämplig erfarenhet för att utföra de uppgifter som ingår i bedömningen av överensstämmelse,

    b) erforderliga beskrivningar av förfarandena i enlighet med vilka bedömningar av överensstämmelse utförs, som säkerställer insyn i dessa förfaranden och möjligheten att reproducera dem; organet ska förfoga över lämpliga riktlinjer och förfaranden för att skilja mellan de uppgifter som det utför i sin egenskap av anmält organ enligt artikel 61 och all annan verksamhet,

c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda IKT-produktteknikens, IKT-tjänsteteknikens eller IKT-processteknikens komplexitet och om det rör sig om massproduktion eller serietillverkning.

11. Ett organ för bedömning av överensstämmelse ska ha de nödvändiga medlen för att korrekt kunna utföra de tekniska och administrativa uppgifterna i samband med bedömningen av överensstämmelse och ska ha tillgång till den utrustning och de hjälpmedel som är nödvändiga.

12. Den personal som ansvarar för att utföra bedömningen av överensstämmelse ska ha

a) en grundlig teknisk utbildning och yrkesutbildning som omfattar all verksamhet i samband med bedömning av överensstämmelse,

b) tillfredsställande kunskap om kraven för de bedömningar av överensstämmelse som de utför och fullgod befogenhet att utföra dessa bedömningar,

c) lämpliga kunskaper och förståelse om de tillämpliga kraven och provningsstandarderna,

d) förmåga att upprätta intyg, protokoll och rapporter som visar att bedömningarna av överensstämmelse har utförts.

13. Det ska garanteras att organ för bedömning av överensstämmelse, deras högsta ledning, personal som är ansvarig för att utföra bedömningar av överensstämmelse och alla underleverantörer är opartiska.

14. Ersättningen till den högsta ledningen för och av personalen som ansvarar för bedömningen av överensstämmelse får inte vara beroende av antalet bedömningar av överensstämmelse som görs eller resultaten av bedömningarna.

15. Organ för bedömning av överensstämmelse ska vara ansvarsförsäkrade, såvida inte ansvaret åligger medlemsstaten enligt dess nationella rätt eller medlemsstaten själv tar direkt ansvar för bedömningen av överensstämmelse.

16. Organet för bedömning av överensstämmelse och dess personal, kommittéer, dotterbolag, underleverantörer och eventuella anslutna organ eller personal vid externa organ som ett organ för bedömning av överensstämmelse anlitar ska underhålla konfidentialitet och iaktta tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter avseende bedömning av överensstämmelse i enlighet med denna förordning eller de nationella bestämmelser som genomför den, utom i de fall då uppgifter måste lämnas enligt unionsrätten eller medlemsstaternas nationella rätt som är tillämplig på personen i fråga och utom gentemot de behöriga myndigheterna i de medlemsstater där verksamheten utförs. Immateriella rättigheter ska skyddas. Organet för bedömning av överensstämmelse ska ha infört dokumenterade förfaranden rörande kraven i denna punkt.

17. Förutom kraven i punkt 16 hindrar inget i denna bilaga utbyte av teknisk information och vägledning om gällande regler mellan organet för bedömning av överensstämmelse och en person som ansöker om certifiering, eller som överväger att ansöka, om certifiering.

18. Organen för bedömning av överensstämmelse ska fungera enligt konsekventa, rättvisa och rimliga villkor och bestämmelser och när det gäller avgifter beakta intressena hos små och medelstora företag.

19. Organen för bedömning av överensstämmelse ska uppfylla de krav som anges i relevant standard som harmoniserats enligt förordning (EG) nr 765/2008 för ackreditering av organ för bedömning av överensstämmelse som utför certifiering av IKT-produkter, IKT-tjänster eller IKT-processer.

20. Organen för bedömning av överensstämmelse ska säkerställa att de provningslaboratorier som används för att prova överensstämmelsen uppfyller de krav som anges i relevant standard som harmoniserats enligt förordning (EG) nr 765/2008 för ackreditering av laboratorier som utför provningar.

Sammanfattning av delbetänkandet SOU 2020:58

Uppdraget

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019. Förordningen började tillämpas direkt med undantag för vissa artiklar som kräver kompletterande bestämmelser på nationell nivå och som därför ska börja tillämpas först den 28 juni 2021. Det huvudsakliga syftet med förordningen är att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad.

Utredningens uppdrag i denna första del har varit att föreslå de anpassningar och kompletterande nationella författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till och som behöver finnas på plats när förordningen i sin helhet börjar tillämpas den 28 juni 2021.

I uppdraget har ingått att överväga och föreslå vilken befintlig nationell myndighet som ska utses att fullgöra de uppgifter och tilldelas de ansvarsområden som följer av EU:s cybersäkerhetsakt, bl.a. uppdraget att utöva tillsyn över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering. Det har även ingått att undersöka vilka kompletterande nationella bestämmelser, bl.a. processuella bestämmelser och bestämmelser om sanktioner, som förordningen kräver eller som det annars finns anledning att införa.

Utredningen kommer i slutbetänkandet att analysera och överväga om det bör införas krav på certifiering och godkännande av vissa produkter, tjänster och processer som ska användas i verksamheter som är av betydelse för Sveriges säkerhet. Denna del av uppdraget ska redovisas senast den 1 mars 2021.

Behovet av ökad cybersäkerhet

Digitaliseringen beskrivs som vår tids starkaste förändringsfaktor och innebär att en allt större andel av aktiviteterna i samhället är beroende av nätverk och informationssystem som används av myndigheter, organisationer, företag och privatpersoner. Den digitala utvecklingen ger stora möjligheter att förbättra och effektivisera människors vardag och olika verksamheter. Digitaliseringen har skapat nya former av kommunikation, datahantering och datalagring. I dag bygger många system för att hantera information huvudsakligen på digital informations- och kommunikationsteknik (IKT). Med den tilltagande digitaliseringen och globaliseringen, som ökar beroenden över nations-, sektors- och ansvarsgränser, har även följt en ökad betoning på cyberfrågor i samhället. Informations- och cybersäkerhetsarbete, av såväl offentliga som privata aktörer, ses som nödvändigt vid digitaliseringsprocesser för att samhället

ska kunna fungera och utvecklas i linje med de mål som finns inom olika politikområden. Samtidigt som allt fler länder utvecklar strategier, doktriner och förmågor inom cyberområdet ökar förekomsten av cyberattacker mot olika intressen och verksamheter. Hoten kan utgöras av politiskt, ekonomiskt och brottsligt motiverade angrepp, men även oavsiktliga incidenter som påverkar cybersäkerheten ökar. Cyberincidenterna kan störa tillhandahållandet av nödvändiga tjänster, exempelvis vatten, hälso- och sjukvård, elektricitet och mobila tjänster. Möjligheterna till påverkan i informationssystem i demokratiska valprocesser och desinformationskampanjer är också en utmaning. Beroende av digital infrastruktur och tjänster genom anslutna enheter och utbredd uppkoppling till internet skapar ökade sårbarheter vilket medför högre krav på informations- och cybersäkerhet. Genom att kontrollera och certifiera IKT-produkter, IKT-tjänster och IKT-processer kan man göra dem säkrare och även öka förtroendet för dessa.

EU:s cybersäkerhetsakt

EU:s cybersäkerhetsakt är uppdelad i två delar. Den första delen behandlar mål, uppgifter och organisatoriska frågor som rör Europeiska unionens cybersäkerhetsbyrå (Enisa). Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering. Kommissionen ska utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. Enisa ska med hjälp av expertråd och i nära samarbete med den Europeiska gruppen för cybersäkerhetscertifiering (ECCG) lämna förslag på europeiska certifieringsordningar. Syftet är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering kommer att medföra att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater. Förutom att beskriva de säkerhetsmålsättningar som ska beaktas i utformningen av de europeiska ordningarna för cybersäkerhetscertifieringar, anger EU:s cybersäkerhetsakt vad minimiinnehållet i sådana ordningar bör vara.

Ny lag som kompletterar EU:s cybersäkerhetsakt

Utredningen föreslår att de kompletterande nationella bestämmelser till EU:s cybersäkerhetsakt som krävs ska samlas i en ny lag och en ny förordning. I lagen anges att regeringen ska utse en nationell myndighet för cybersäkerhetscertifiering och ges kompletterande bestämmelser om myndighetens befogenheter och möjlighet att besluta om sanktioner för överträdelser av regelverket samt vissa processuella bestämmelser.

En nationell myndighet för cybersäkerhetscertifiering

EU:s cybersäkerhetsakt ställer krav på att en eller flera nationella myndigheter för cybersäkerhetscertifiering utses av medlemsstaterna. Med utgångspunkt i att en sådan myndighet ska utses bland befintliga myndigheter, krav på kunskap och erfarenhet av informations- och kommunikationsteknologi (IKT) och att det nationella certifieringsorganet för it-säkerhet vid Försvarets materielverk (FMV/CSEC) ska ha en roll när det gäller cybersäkerhetscertifiering på högsta assuransnivån föreslås Försvarets materielverk som nationell myndighet för cybersäkerhetscertifiering. Myndigheten ska därmed fullgöra de uppgifter som följer av det europeiska ramverket för cybersäkerhetscertifiering. I uppgifterna ingår omvärldsbevakning av området för cybersäkerhet, samverkan med nationella och internationella aktörer, ansvar för cybersäkerhetscertifiering på den högsta assuransnivån samt ansvar för tillsyn över regelsystemets efterlevnad.

Det nationella certifieringsorganet vid myndigheten, CSEC, föreslås som ackrediterat organ för bedömning av överensstämmelse enligt artiklarna 56.5 och 56.6 i EU:s cybersäkerhetsakt. Det innebär att CSEC eller det ackrediterade organ för bedömning av överensstämmelse som bemyndigas ska ansvara för cybersäkerhetscertifiering på högsta assuransnivån. I syfte att säkerställa certifieringsorganets oberoende som ackrediterat organ för bedömning av överensstämmelse föreslås att det i författning anges att vid Försvarets materielverk ska finnas ett ackrediterat organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt. När chefen för det ackrediterade organet för bedömning av överensstämmelse utövar verksamhet enligt cybersäkerhetsakten är denne inte underställd myndighetschefen. Certifieringsorganets ekonomiska resurser bör beslutas i särskild ordning av regeringen.

Tillsyn

EU:s cybersäkerhetsakt anger att den nationella myndigheten för cybersäkerhetscertifiering ska övervaka och kontrollera efterlevnaden av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering.

Utredningen föreslår att Försvarets materielverk som nationell myndighet för cybersäkerhetscertifiering ska fullgöra de tillsynsuppgifter som följer av EU:s cybersäkerhetsakt och får således de befogenheter som redan framgår av aktens bestämmelser.

Myndigheten ska behandla klagomål som rör en utfärdad EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat. Myndigheten ska också kontrollera att tillverkare eller leverantörer som genomför självbedömning av överensstämmelse av IKT-produkter, IKT-tjänster och IKT-processer, dvs. när en EU-försäkran om överensstämmelse utfärdas, fullgör sina skyldigheter och att ett europeiskt cybersäkerhetscertifikat som utfärdas överensstämmer med kraven i den aktuella europeiska ordningen för cybersäkerhetscertifiering.

Myndigheten ska även bistå det nationella ackrediteringsorganet med övervakning och kontroll av verksamhet som bedrivs av organen för

bedömning av överensstämmelse i enlighet med cybersäkerhetsaktens bestämmelser.

Befogenheter

I EU:s cybersäkerhetsakt ges den nationella myndigheten för cybersäkerhetscertifiering vissa minimibefogenheter för att kunna fullgöra sina tillsynsuppgifter.

Utredningen föreslår vissa kompletterande bestämmelser om tillsynsbefogenheter. Myndigheten ska besluta de förelägganden som behövs för att EU:s cybersäkerhetsakt, de genomförandeakter som har meddelats med stöd av den förordningen, den nya lagen och föreskrifter som har meddelats i anslutning till lagen ska följas. Myndigheten kan förelägga en berörd aktör att lämna information eller vidta någon annan åtgärd. Myndigheten får även besluta om cybersäkerhetscertifikat och kan återkalla ett utfärdat certifikat. Myndigheten kan besluta att ett föreläggande ska gälla omedelbart. Ett beslut om föreläggande får förenas med vite. Myndigheten får även i syfte att genomföra en kontroll göra en undersökning i den berörda aktörens lokaler. Rätten till tillträde till lokal ska dock inte gälla bostäder. Myndigheten föreslås få rätt att få biträde av Kronofogdemyndigheten vid tillsyn. Regeringen eller den myndighet som regeringen bestämmer föreslås få meddela närmare föreskrifter om formerna för lämnandet av information, kontrollförfarandet vid undersökningar och utredningsförfarandet vid tillträde till lokaler.

Sanktioner

EU:s cybersäkerhetsakt anger att medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Utredningen föreslår att den nationella myndigheten för cybersäkerhetscertifiering får besluta att sanktionsavgift ska påföras den som utfärdar en EU-försäkran om överensstämmelse utan att fastställda krav på cybersäkerhet är uppfyllda, lämnar oriktiga eller ofullständiga uppgifter vid ansökan om cybersäkerhetscertifieringen, innehar ett europeiskt cybersäkerhetscertifikat och underlåter att informera om alla sårbarheter eller oriktigheter som upptäcks, utfärdar en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som underlåter att lämna kompletterande säkerhetsinformation. Sanktionsavgift ska även kunna påföras den som bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat samt villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering, överträder ett beslut om förbud eller använder ett europeiskt cybersäkerhetscertifikat som blivit återkallat. Avgiften kan således påföras utfärdare av EU-försäkran om överensstämmelse och certifikatinnehavare (IKT-tillverkare och leverantörer) samt organ för bedömning av överensstämmelse.

Avgiften ska tas ut även om överträdelsen inte skett uppsåtligen eller av oaktsamhet, dvs. ett strikt ansvar ska gälla. Om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt

att ta ut sanktionsavgiften får avgiften sättas ned. Avgiften ska bestämmas till lägst 10 000 kronor och högst 15 miljoner kronor.

Nationell strategi

Regeringen bör överväga att ta fram en nationell strategi för att tillvarata nationella intressen när det europeiska ramverket för cybersäkerhetscertifiering utvecklas. I arbetet bör berörda myndigheter, andra offentliga aktörer och näringslivet ges möjlighet att delta.

Samverkan

För att säkerställa att nationella intressen kan representeras och tillvaratas i arbetet med det europeiska ramverket för cybersäkerhetscertifiering ska det finns en adekvat nationell representation i Europeiska gruppen för cybersäkerhetscertifiering. Det ställer krav på en utbyggd och väl fungerande samverkan mellan berörda myndigheter, berörda näringslivsorganisationer och företag.

Konsekvenser

Utredningens förslag syftar till att uppfylla kraven i EU:s cybersäkerhetsakt och att bidra till ett ändamålsenligt och effektivt genomslag och tillämpning av det europeiska ramverket för cybersäkerhetscertifiering. Analysen av behovet av kompletterande nationella bestämmelser har dock försvårats av osäkerheten om det närmare innehållet i de framtida europeiska ordningarna för cybersäkerhetscertifiering (genomförandeakter).

Utredningen anser att det för närvarande inte är möjligt att överblicka vilka direkta konsekvenser som införandet av det europeiska ramverket för cybersäkerhetscertifiering kommer att medföra för den utpekade nationella myndigheten för cybersäkerhetscertifiering eller för andra aktörer som berörs av det angivna ramverket eftersom några genomförandeakter ännu inte antagits. Det går inte heller att bedöma i vilken omfattning som berörda aktörer kommer att använda sig av möjligheten till EU-försäkran om överensstämmelse eller utfärda europeiska cybersäkerhetscertifikat, vilket också påverkar behovet och omfattningen av tillsyn. Det går därför inte heller att sätta författningsförslagen i relation till ekonomiska beräkningar, annat än när det gäller behovet av vissa tillkommande resurser för den nationella myndigheten för cybersäkerhetscertifiering.

Utredningen har vid utformningen av förslagen, bl.a. när det gäller uppgifter för och organisering av den nationella myndigheten för cybersäkerhetscertifiering, tagit hänsyn till de alternativ som kan förväntas vara mest ändamålsenliga och kostnadseffektiva. Myndighetens åligganden enligt EU:s cybersäkerhetsakt medför kostnader för administrativt arbete och för tillsyn, bl.a. medför nya befogenheter och sanktionsmöjligheter behov av att utbilda personal och ändra vissa arbetsformer. Inledningsvis bedöms dock kostnaderna för detta vara

begränsade. Det nationella certifieringsorganet CSEC:s verksamhet föreslås fortsatt vara anslagsfinansierat för vissa grundläggande funktioner och fortsatt avgiftsfinansierat för uppdragen med cybersäkerhets-certifiering.

Utredningens förslag om kompletterande bestämmelser avseende myndighetens befogenheter och möjligheten att besluta om sanktions-avgift bedöms inte medföra några ekonomiska konsekvenser i sig.

De förslag till framför allt samverkan och samordning mellan berörda myndigheter som utredningen föreslår bedöms i kostnadsavseende vara marginella.

Det europeiska ramverket för cybersäkerhetscertifiering innebär i nuläget frivillig cybersäkerhetscertifiering. I framtiden kan emellertid användningen av europeisk cybersäkerhetscertifiering bli obligatorisk. En ekonomisk aktör beslutar om att tillhandahålla IKT-produkter eller -tjänster på unionsmarknaden under förutsättning att bestämmelserna om cybersäkerhetscertifiering följs. Det är inte möjligt att uppskatta hur många företag som berörs av utredningens förslag. Det är inte heller möjligt att göra någon närmare bedömning av förslagens effekter på företag eller företagandet i Sverige, annat än att de företag som väljer att utfärda en EU-försäkran om överensstämmelse eller ansöka om ett europeiskt cybersäkerhetscertifikat kommer att få kostnader i samband med förfarandet. En effektiv tillsyn ökar även förutsättningarna för att företagare ska kunna konkurrera på lika villkor. De föreslagna bestämmelserna förväntas på sikt leda till ökad cybersäkerhet och en bättre fungerande marknad, vilket i förlängningen är till fördel för både ekonomiska aktörer och unionsmarknadens funktion.

Den nya lagen och övriga författningsändringar föreslås träda i kraft den 28 juni 2021.

Lagförslaget i delbetänkandet SOU 2020:58

Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt (cybersäkerhetsakten)

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten), här benämnd EU:s cybersäkerhetsakt.

Termer och uttryck i denna lag har samma betydelse som i EU:s cybersäkerhetsakt.

Nationell myndighet för cybersäkerhetscertifiering

2 § Den myndighet som regeringen bestämmer är

1. nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt, och
2. utövar tillsyn över efterlevnaden av denna lag och föreskrifter som har meddelats i anslutning till lagen.

Ackreditering av organ för bedömning

3 § I Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse enligt artikel 60.1 i EU:s cybersäkerhetsakt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

Tillsynsbefogenheter och sanktioner

4 § Den nationella myndigheten för cybersäkerhetscertifiering har de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt även vid tillsynen över efterlevnaden av denna lag och föreskrifter som har meddelats i anslutning till lagen.

5 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för att EU:s cybersäkerhetsakt, de genomförandeakter som har meddelats med stöd av den förordningen, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

Den nationella myndigheten för cybersäkerhetscertifiering har rätt att få biträde av Kronofogdemyndigheten för tillsyn i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

6 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla europeiska cybersäkerhetscertifikat som utfärdats av den myndigheten eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om sådana certifikat inte uppfyller kraven i akten eller en europeisk ordning för cybersäkerhetscertifiering.

7 § Den nationella myndigheten för cybersäkerhetscertifiering ska ta ut en sanktionsavgift av den som

1. utfärdar en EU-försäkran om överenstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt utan att fastställda krav på cybersäkerhet i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering är uppfyllda,
2. lämnar oriktiga eller ofullständiga uppgifter vid ansökan om cybersäkerhetscertifieringen enligt artikel 56.7 i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och underlåter att i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt informera den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. utfärdat en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som underlåter att lämna kompletterande säkerhetsinformation enligt artikel 55 i EU:s cybersäkerhetsakt,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat samt villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering enligt EU:s cybersäkerhetsakt eller motsvarande europeisk ordning för cybersäkerhetscertifiering
6. överträder ett beslut om förbud enligt 5 §, eller
7. använder ett europeiskt cybersäkerhetscertifikat som blivit återkallat enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

8 § En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

9 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den som begått överträdelsen tidigare begått en överträdelse och de kostnader som denne undvikit till följd av överträdelsen.

10 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa eller om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

11 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

12 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

13 § En sanktionsavgift ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

14 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Tystnadsplikt

15 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

Den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).

Avgifter

16 § Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela förskrifter om avgiftssystemets utformning enligt första stycket.

Omprövning hos privata organ för bedömning av överensstämmelse

17 § Finner ett privat organ för bedömning av överensstämmelse att ett beslut som det meddelat är uppenbart oriktigt på grund av nya omständigheter eller av någon annan anledning ska organet ändra beslutet, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Överklagande

18 § Beslut enligt EU:s cybersäkerhetsakt och denna lag får överklagas till allmän förvaltningsdomstol. Även beslut av ett privat organ för

bedömning av överensstämmelse enligt dessa författningar får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 28 juni 2021.

Förteckning över remissinstanserna (delbetänkandet SOU 2020:58)

Remissvar har lämnats av Bolagsverket, Domstolsverket, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Försäkringskassan, Förvaltningsrätten i Stockholm, Inspektionen för strategiska produkter, Integritetsskyddsmyndigheten, Internetstiftelsen, Justitiekanslern, Kammarkollegiet, Kammarrätten i Stockholm, Kommerskollegium, Konkurrensverket, Konsumentverket, Kronofogdemyndigheten, Kungl. Tekniska högskolan, Kustbevakningen, Luftfartsverket, Lunds universitet (Juridiska fakulteten), Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Västra Götalands län, Myndigheten för digital förvaltning, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Riksarkivet, Riksrevisionen, RISE Research Institutes of Sweden AB, Skatteverket, Småföretagarnas Riksförbund, Statens servicecenter, Statistiska centralbyrån, Statskontoret, Stockholms universitet (Juridiska fakulteten), Styrelsen för ackreditering och teknisk kontroll, Svenska Journalistförbundet, Sveriges advokatsamfund, Sveriges Kommuner och Regioner, Säkerhets- och försvarsföretagen, Säkerhetspolisen, Totalförsvarets forskningsinstitut, Trafikverket, Transportstyrelsen, Tullverket, Upphandlingsmyndigheten, Verket för innovationssystem, Vetenskapsrådet/SUNET och Åklagarmyndigheten.

Innovationsföretagen, It- och telekomföretagen, Näringslivets regelnämnd, Riksdagens ombudsmän SKL Kommentus, Svensk Handel, Svenskt Näringsliv, Sveriges Standardiseringsförbund och Teknikföretagen har avstått från att lämna synpunkter på förslagen i delbetänkandet eller har inte svarat på remissen.

Synpunkter har även lämnats av Energiföretagen, Huawei, Svenska statsnätsföreningen och Vattenfall AB.

Lagrådsremissens lagförslag

Regeringen har följande förslag till lagtext.

Förslag till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten), här benämnd EU:s cybersäkerhetsakt.

Ord och uttryck i denna lag har samma betydelse som i EU:s cybersäkerhetsakt.

Nationell myndighet för cybersäkerhetscertifiering

2 § Den myndighet som regeringen bestämmer

1. är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt, och
2. utövar tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

Ackreditering av organ för bedömning av överenstämmelse

3 § I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.

I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.

Tillsynsbefogenheter

4 § Vid tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs har den nationella myndigheten för cybersäkerhetscertifiering de befogenheter som anges i artikel 58.8 i EU:s cybersäkerhetsakt.

5 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta de förelägganden som behövs för tillsynen och för att EU:s cybersäkerhetsakt, genomförandeakter som har meddelats med stöd av EU:s cybersäkerhetsakt, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett beslut om föreläggande får förenas med vite.

6 § Den nationella myndigheten för cybersäkerhetscertifiering får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, för att genomföra utredningar i enlighet med artikel 58.8 d i EU:s cybersäkerhetsakt.

Vid handräckning tillämpas bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Om den nationella myndigheten för cybersäkerhetscertifiering begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.

7 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i EU:s cybersäkerhetsakt, om certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering.

Administrativa sanktionsavgifter

8 § Den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift av den som

1. utfärdar en EU-försäkran om överenstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt utan att kraven enligt EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering är uppfyllda,
2. lämnar oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering enligt artikel 56.7 i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering,
3. innehar ett europeiskt cybersäkerhetscertifikat och inte informerar, i enlighet med artikel 56.8 i EU:s cybersäkerhetsakt, den myndighet eller det organ som avses i artikel 56.7 om alla sårbarheter eller oriktigheter som upptäcks och som kan påverka överensstämmelsen med de säkerhetskrav som gäller för den certifierade IKT-produkten, IKT-tjänsten eller IKT-processen,
4. har utfärdat en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som inte lämnar kompletterande säkerhetsinformation i enlighet med artikel 55 i EU:s cybersäkerhetsakt, om detta medför en ökad risk för sårbarhet eller skada,
5. bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering enligt EU:s cybersäkerhetsakt eller motsvarande europeisk ordning för cybersäkerhetscertifiering,

6. överträder ett beslut om föreläggande enligt 5 § som innebär ett förbud, eller

7. använder ett europeiskt cybersäkerhetscertifikat som har återkallats enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

9 § En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 000 000 kronor.

10 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppkommit till följd av överträdelsen,

2. om den som har begått överträdelsen tidigare begått en överträdelse, och

3. den vinst som den avgiftsskyldige har gjort till följd av överträdelsen.

11 § Den nationella myndigheten för cybersäkerhetscertifiering får besluta att sätta ned eller avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

12 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

13 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

14 § Sanktionsavgiften tillfaller staten.

15 § En sanktionsavgift ska betalas till den nationella myndigheten för cybersäkerhetscertifiering inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

16 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Tystnadsplikt

17 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cybersäkerhetsakt får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400).

Avgifter

18 § Den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för sin verksamhet enligt EU:s cybersäkerhetsakt och denna lag.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana avgifter.

Ändring av beslut av privata organ för bedömning av överensstämmelse

19 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och
2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Överklagande

20 § Beslut av den nationella myndigheten för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt och denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 28 juni 2021.

Förslag till lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Härigenom föreskrivs att 3 § lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska ha följande lydelse.

Lydelse enligt förslaget i 2.1	*Föreslagen lydelse*
3 §	
I artikel 60.1 i EU:s cybersäkerhetsakt och i bilagan till EU:s cybersäkerhetsakt finns bestämmelser om ackreditering av organ för bedömning av överensstämmelse i fråga om cybersäkerhetscertifiering.	
I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering *och marknadskontroll i samband med saluföring av produkter* och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.	I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för ackreditering av organ för bedömning av överensstämmelse enligt artikel 60 i EU:s cybersäkerhetsakt.	

Denna lag träder i kraft den 16 juli 2021.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2021-04-01

Närvarande: F.d. justitierådet Eskil Nord samt justitieråden Inga-Lill Askersjö och Petter Asp

Kompletterande bestämmelser till EU:s cybersäkerhetsakt

Enligt en lagrådsremiss den 24 mars 2021 har regeringen (Försvarsdepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt,
2. lag om ändring i lagen (2021:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Förslagen har inför Lagrådet föredragits av rättssakkunniga Karin Byström.

Förslagen föranleder följande yttrande.

Förslaget till lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt

3 §

Bestämmelsen i andra stycket i paragrafen ger upplysning om att det i en EU-förordning, som gäller krav för ackreditering och marknadskontroll i samband med saluföring av produkter, finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse. Lydelsen kommer att gälla endast under tiden 28 juni 2021−16 juli 2021. Vid sistnämnda tidpunkt kommer nämligen förordningen att byta namn genom att orden ”och marknadskontroll i samband med saluföring av produkter” utgår.

I lagrådsremissen föreslås att ändringen av ordalydelsen i bestämmelsen ska ske genom en ändringslag (förslag 2.2 i lagrådsremissen). Ändringslagen reglerar således endast ett namnbyte på en EU-förordning i en upplysningsbestämmelse. Förfarandet är i och för sig formellt korrekt, men enligt Lagrådets mening leder en sådan ordning enbart till att lagstiftningen blir svårare att överskåda. Den som ska kontrollera ändringar i lagen kommer alltid att vara tvungen att passera denna ändring, utan att den kommer att ha någon betydelse.

När det gäller en ändring av förevarande slag skulle en mer ändamålsenlig ordning kunna vara att ändringen genomförs i form av en övergångsbestämmelse till den nya lagen. I 3 § andra stycket i den nya lagen kan den bestämmelse som föreslås i ändringslagen tas in. I övergångsbestämmelserna kan därefter föreskrivas ”Bestämmelsen i 3 § andra stycket har fram till 16 juli 2021 följande lydelse” och följas av den lydelse som föreslås i 3 § andra stycket i den nya lagen i lagrådsremissen. Ändringslagen blir härigenom överflödig.

5 §

Enligt förslagen i lagrådsremissen ska den nationella myndigheten för cybersäkerhetscertifiering ha möjlighet att med stöd av denna paragraf besluta om förelägganden mot tillverkare, leverantörer och organ för

bedömning av överensstämmelse. Ett sådant föreläggande kan avse också förbud. I 8 § 6 finns en anslutande bestämmelse som anger att en sanktionsavgift ska kunna tas ut av den som överträder ett beslut om föreläggande som innebär ett förbud.

Ett föreläggande kan alltså riktas mot och en avgift tas ut av en tillverkare eller en leverantör som innehar ett certifikat och av något skäl har meddelats ett förbudsföreläggande. Det framgår emellertid inte om avsikten också är att ett föreläggande ska kunna riktas mot någon som saluför en produkt som certifierad, trots att något certifikat inte finns. Syftet med EU:s cybersäkerhetsakt är enligt artikel 1 bl.a. att säkerställa en väl fungerande inre marknad (inom den aktuella sektorn). Det är sannolikt att det syftet inte uppnås om regleringen omfattar endast leverantörer som innehar certifikat och som av någon anledning förelagts ett förbud, men inte omfattar dem som inte har något certifikat men ändå saluför en produkt som certifierad.

Enligt Lagrådets mening bör denna fråga klargöras i det fortsatta lagstiftningsarbetet.

7 §

Av bestämmelsen framgår att den nationella myndigheten för cybersäkerhetscertifiering får återkalla ett certifikat som har utfärdats av myndigheten eller, i vissa fall, av ett organ för bedömning av överensstämmelse. För att ett certifikat ska kunna återkallas fordras att ”certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering”. Vad som avses med detta, dvs. att certifikatet inte uppfyller nyss nämnda krav, framstår som mycket oklart. Någon ledning ges inte i författningskommentaren till bestämmelsen.

En möjlig tolkning är att bestämmelsen tar sikte på den situationen att det har tillkommit nya normer på EU-nivå som innebär nya krav vilka certifikatet inte uppfyller (jfr lagrådsremissen s. 30 och SOU 2020:58 s. 207 där det talas om att ett certifikat inte ”längre” uppfyller kraven). Det är emellertid också möjligt att förstå bestämmelsen så att den därutöver − eller i stället − tar sikte på certifikat som på något sätt varit felaktiga från början.

I tillägg är det näraliggande att fråga sig om inte ett certifikat borde kunna återkallas om det visar sig att en viss produkt, tjänst eller process som har certifierats inte uppfyller de krav som ställs för att erhålla certifikatet. Det framstår emellertid – eftersom lagtexten tar sikte på själva certifikatets överensstämmelse med vissa angivna normer – som mycket tveksamt om lagtexten kan anses omfatta ett sådant fall.

Oklarheterna går visserligen tillbaka på den bestämmelse i EU:s cybersäkerhetsakt (artikel 58.8 e) som mer eller mindre ordagrant har förts över till paragrafen. Det bör dock i den fortsatta beredningen utvecklas i författningskommentaren hur regleringen ska förstås. Något hinder på EU-rättslig grund mot att åtminstone i huvudsak ange regeringens bedömning av vad paragrafen är avsedd att omfatta kan inte anses finnas. Tvärtom synes detta vara nödvändigt för att åstadkomma en rimlig stabilitet i rättstillämpningen.

8 §

I paragrafen regleras när den nationella myndigheten för cybersäkerhetscertifiering ska besluta att ta ut en sanktionsavgift.

Punkt 1 gäller det fall då någon har utfärdat en EU-försäkran om överensstämmelse enligt artikel 53.2 i EU:s cybersäkerhetsakt, trots att vissa krav inte är uppfyllda. En sådan försäkran avser enligt artikeln att tillverkaren eller leverantören tar ansvar för att IKT-produkten, IKT-tjänsten eller IKT-processen överensstämmer med de krav som anges i den europeiska ordning för cybersäkerhetscertifiering som gäller för dessa. I punkt 1 anges emellertid att sanktionsavgift även ska utgå om kraven enligt EU:s cybersäkerhetsakt inte är uppfyllda. Eftersom den försäkran som avses i artikel 53.2 inte innefattar detta måste – om sanktionsavgift ska kunna utgå vid överträdelse av kraven i EU:s cybersäkerhetsakt och det inte kan anses täckas av övriga punkter i 8 § − det regleras på annat sätt. Bestämmelsens ordalydelse bör också justeras, bl.a. för att klargöra vad som avses med ”motsvarande europeiska ordning”. Lagrådet föreslår att bestämmelsen ges följande lydelse.

> 1. har utfärdat en EU-försäkran om överensstämmelse enligt 53.2 i EU:s cybersäkerhetsakt trots att kraven enligt den europeiska ordning som gäller för IKT-produkten, IKT-tjänsten eller IKT-processen inte är uppfyllda,

Enligt *punkt 2* ska sanktionsavgift tas ut av den som lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering enligt artikel 56.7 i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering. I artikel 56.7 finns emellertid inte någon reglering av ansökan och det är inte heller klart om sådana bestämmelser kommer att tas in i de europeiska ordningarna. Även i denna punkt är det oklart vad som avses med ”motsvarande europeisk ordning”. Enligt Lagrådets mening saknas emellertid skäl att i aktuell bestämmelse föreskriva var ansökan om cybersäkerhetscertifiering regleras och föreslår därför att bestämmelsen ges följande lydelse.

> 2. har lämnat oriktiga eller ofullständiga uppgifter av betydelse vid ansökan om cybersäkerhetscertifiering,

I *punkt 5* föreslås att sanktionsavgift ska få tas ut av den som bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat eller mot villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering enligt EU:s cybersäkerhetsakt eller motsvarande europeisk ordning för cybersäkerhetscertifiering. Även i denna bestämmelse, liksom i övriga punkter i paragrafen där uttrycket förekommer, är det oklart vad ”motsvarande europeisk ordning” syftar på. Men inte heller här finns skäl att ha koppling till cybersäkerhetsakten eller de europeiska ordningarna. Bestämmelsen kan därför avslutas med orden ”tillämpningsområdet för certifieringen”. Därutöver bör bestämmelsen ändras på så sätt att uppräkningen av villkor i första ledet bör sammanbindas med ”eller” i stället för ”och”.

Beträffande *punkten 6* se Lagrådets synpunkter under 5 §.

Punkten 7 ger den nationella myndigheten möjlighet att ta ut en avgift av den som använder ett återkallat certifikat. Det framstår som klart att detta gäller gentemot den som i Sverige använder ett certifikat som återkallats av den nationella myndighet som regeringen kommer att bestämma enligt 2 §. Men det framgår inte vad som gäller i den situationen att en tillverkare eller leverantör på den svenska marknaden använder ett certifikat som återkallats av en behörig myndighet i någon annan medlemsstat.

Certifieringen inom unionen bygger på att ett certifikat som utfärdats av en behörig myndighet inom unionen gäller inom den inre marknaden. Därmed följer också att en återkallelse som en sådan myndighet beslutar innebär att certifikatet inte längre gäller inom denna marknad.

Eftersom kravet i punkt 7 för att avgift ska kunna tas ut endast är att ett certifikat har återkallats med stöd av angiven artikel i cybersäkerhetsakten, förefaller det sannolikt att även certifikat som återkallats av ett annat lands myndighet kan omfattas av punkten, men frågan bör belysas i det fortsatta lagstiftningsarbetet.

10 och 11 §

I 10 § anges vad som särskilt ska beaktas vid bestämmande av en sanktionsavgifts storlek. Av 11 § framgår vidare att myndigheten får ”besluta att sätta ned eller avstå från att ta ut en sanktionsavgift” under vissa förutsättningar.

Det som i den sistnämnda paragrafen anges som ett ”beslut att sätta ned” avgiften är i praktiken inget annat än ett integrerat moment i den bedömning som ligger till grund för ett beslut om sanktionsavgiftens storlek enligt 10 §. Vid tillämpning av 10 § är det fråga om en bedömning där man kan beakta omständigheter som går i såväl skärpande som mildrande riktning. Vid den bedömningen måste i mildrande riktning sådana omständigheter som tas upp i 11 § − att överträdelsen är ringa och att det finns ”särskilda skäl” − kunna beaktas (jfr s. 69 i lagrådsremissen där det framgår att uppräkningen i 10 § inte är avsedd att vara uttömmande och att myndigheten vid bestämmande av sanktionsavgiftens storlek bör beakta samtliga relevanta omständigheter). Det förhållandet att fråga inte är om ett särskilt beslut om nedsättning bör på ett bättre sätt återspeglas i lagtexten.

Motsvarande problem uppstår inte i de fall det blir aktuellt att besluta om att helt avstå från att ta ut en sanktionsavgift, eftersom det när ett sådant beslut fattas inte behövs någon bedömning av sanktionens storlek.

En möjlighet att komma till rätta med det nu beskrivna problemet är att utforma 11 § på följande sätt.

Den nationella myndigheten för cybersäkerhetscertifiering får besluta att avstå från att ta ut en sanktionsavgift om överträdelsen är ringa, om det finns särskilda skäl eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Om det inte bedöms finnas skäl att avstå från att ta ut sanktionsavgift ska nu nämnda omständigheter i stället beaktas vid bestämmande av avgiftens storlek.

Om detta förslag inte kan godtas kan den variant som används i bl.a. 32 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster utgöra ett alternativ. Där används lokutionen att

sanktionsavgiften ”får efterges helt eller delvis” i stället för att myndigheten ”får besluta att sätta ned eller avstå”. Men också detta alternativ är problematiskt eftersom det innebär att den omständigheten att överträdelsen är ringa (vilket otvetydigt är en omständighet som måste kunna beaktas enligt 10 §) framställs som ett skäl för att delvis efterge sanktionsavgiften, när det i själva verket är en integrerad del av bedömningen av hur stor sanktionsavgiften ska vara.

Lagrådets förslag bygger på förutsättningen att ”beslut att sätta ned” avgiften inte uteslutande tar sikte på att göra det möjligt att gå under den miniminivå, 10 000 kr, som anges i 9 §. Det framstår emellertid som osannolikt att så skulle vara fallet, men det framgår inte klart av remissen. Huruvida 11 § överhuvudtaget avses ge en möjlighet att bestämma sanktionsavgiften till ett belopp som understiger 10 000 kr framgår inte heller av remissen. Det bör klargöras i det fortsatta lagstiftningsarbetet.

12 §

Av paragrafen följer att det är möjligt att påföra en sanktionsavgift för en viss gärning även om gärningen omfattas av ett vitesföreläggande, under förutsättning att en ansökan om utdömande av vitet inte har gjorts. Bestämmelsen anger emellertid inte att påförandet av en sådan avgift hindrar en efterföljande ansökan om utdömande av vite. Som Lagrådet har noterat i sitt yttrande över lagrådsremissen Anpassningar till EU:s förordningar om medicinteknik – del 2, förekommer bestämmelser som är utformade på detta sätt i lagstiftningsfloran. Lagrådet vill dock även i detta ärende uppmärksamma den mer principiella frågan om regleringen inte borde täcka också den sist nämnda situationen.

20 §

Bestämmelsen i första stycket i paragrafen bör justeras så att det blir klart att ”enligt EU:s cybersäkerhetsakt och enligt denna lag” även syftar på beslut av den nationella myndigheten. Lagrådet föreslår att bestämmelsen ges följande lydelse.

Beslut enligt EU:s cybersäkerhetsakt och enligt denna lag av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Förslaget till lag om ändring i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Om Lagrådets förslag om en övergångsbestämmelse till 3 § lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt godtas, ska förevarande förslag till ändringslag utgå.

Försvarsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 29 april 2021

Närvarande: statsminister Löfven, ordförande, och statsråden Bolund, Johansson, Baylan, Hultqvist, Andersson, Damberg, Shekarabi, Ygeman, Linde, Ekström, Eneroth, Dahlgren, Nilsson, Ernkrans, Lindhagen, Lind, Hallberg, Nordmark, Micko, Stenevi, Olsson Fridh

Föredragande: statsrådet Hultqvist

Regeringen beslutar proposition Kompletterande bestämmelser till EU:s cybersäkerhetsakt