EU:s cybersäkerhetsakt

– kompletterande nationella bestämmelser om cybersäkerhetscertifiering

Delbetänkande av Cybersäkerhetsutredningen

Stockholm 2020

STATENS OFFENTLIGA UTREDNINGAR

SOU 2020:58

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2020

ISBN 978-91-38-25098-3
ISSN 0375-250X

Till statsrådet Peter Hultqvist

Regeringen beslutade den 31 oktober 2019 att tillkalla en särskild utredare (dir. 2019:73) med uppdrag att lämna förslag till anpassningar och kompletterande författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till och att överväga behovet av vissa ytterligare krav till skydd för Sveriges säkerhet.

Den 3 februari 2020 förordnades lagmannen Nils Cederstierna som särskild utredare. Som sakkunniga förordnades den 2 mars 2020 rättssakkunniga Karin Byström, Försvarsdepartementet, ämnesrådet Catharina Hallström, Försvarsdepartementet, ämnesrådet Richard Henriksson, Utrikesdepartementet, departementssekreteraren Linnéa Jannes, Utrikesdepartementet, departementssekreteraren Staffan Lindmark, Infrastrukturdepartementet, rättssakkunniga Emelie Smiding, Justitiedepartementet, och militärsakkunniga Anna Weibull, Försvarsdepartementet. Samma dag förordnades bedömningsledaren Curt-Peter Askolin, Styrelsen för ackreditering och teknisk kontroll (Swedac), verksjuristen Charlotte Hakelius, Säkerhetspolisen, tf. enhetschefen Ronny Harpe, Myndigheten för samhällsskydd och beredskap (MSB), kommendören Per-Ola Johansson, Försvarsmakten, juristen Britt-Marie Jönson, Post- och telestyrelsen, director Mats Nilsson, Teknikföretagen, ordföranden för Cyberförsvarsgruppen Richard Oehme, Säkerhets- och försvarsföretagen (SOFF), handläggaren Tommy Schönberg, Vinnova, och chefen för FMV/CSEC Dag Ströman, Försvarets materielverk, som experter i utredningen. Den 13 mars 2020 förordnades även kanslirådet Anneli Hagdahl, Försvarsdepartementet, som sakkunnig i utredningen och biträdande säkerhetsskyddschefen Ylva Söderlund, Trafikverket, som expert.

Som sekreterare i utredningen anställdes den 3 februari 2020 hovrättsassessorn Patrik Roos. Seniora rådgivaren Thomas Wallander anställdes som huvudsekreterare den 10 februari 2020.

Utredningen har tagit namnet Cybersäkerhetsutredningen (Fö 2019:1).

Genom tilläggsdirektiv den 14 maj 2020 förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av EU:s cybersäkerhetsakt (dir. 2020:57).

Härmed överlämnar utredningen delbetänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58). Uppdragets första del är härigenom slutfört.

Stockholm i september 2020

Nils Cederstierna

/Thomas Wallander
Patrik Roos

Innehåll

Bilagor

Förkortningar

CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CSEC	Sveriges certifieringsorgan för IT-säkerhet
CERT	Computer Emergency Response Team
cPP	collaborative Protection Profile
CSCG	Focus Group on Cybersecurity
CSIRT	Computer Security Incident Response Team
EAL	Evaluation Assurance Level
ECCG	Europeiska gruppen för cybersäkerhets-certifiering
ECSO	Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	Europeiska unionen
FIDI	Forum för informationsdelning om informations-säkerhet
FMV	Försvarets materielverk
FRA	Försvarets radioanstalt
IKT	Informations- och kommunikationsteknik
MISWG	Multinational Industrial Security Working Group
MSB	Myndigheten för samhällsskydd och beredskap
MUST	Militära underrättelse- och säkerhetstjänsten
NCIRC	NATOComputer Incident Response Capability
NCSA	National Communications Security Authority
NDA	National Distribution Authority

PP	Protection Profile
PTS	Post- och telestyrelsen
SAMFI	Samverkansgruppen för informationssäkerhet
SIS	Svenska Institutet för Standarder
SOG-IS MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
SOU	Statens offentliga utredningar
Swedac	Styrelsen för ackreditering och teknisk kontroll
ST	Security target

Sammanfattning

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 verksam-

heter 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 befint-

liga 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 cybersäkerhets-

certifikat. 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 cybersäkerhetscertifiering.

Utredningens förslag om kompletterande bestämmelser avseende myndighetens befogenheter och möjligheten att besluta om sanktionsavgift 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.

Summary

Remit

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) entered into force on 27 June 2019, with the exception of certain articles which require supplementary provisions at national level and which therefore will not be applied until 28 June 2021. The main purpose of the Regulation is to achieve a high level of cybersecurity, cyber resilience and trust within the Union, and to ensure the proper functioning of the internal market.

The Inquiry's remit for this first part consisted of proposing the adaptations and supplementary national statutory provisions necessitated by the EU Cybersecurity Act and which must be in place when the entire Regulation begins to apply on 28 June 2021.

The remit included considering and proposing which existing national authority should be designated to perform the tasks and assigned the areas of responsibility ensuing from the EU Cybersecurity Act, including the task of supervising compliance with the European cybersecurity certification framework. It also included examining which supplementary national provisions – including procedural provisions and provisions on penalties – are required by the Regulation or which should be introduced for other reasons.

In its final report, the Inquiry will analyse and consider whether requirements should be introduced on certification and approval of certain products, services and processes that will be used in activities of importance to Sweden's security. A report on this part of the remit is to be presented by 1 March 2021.

Need for increased cybersecurity

Digitalisation is described as the strongest factor for change of our time and means that a growing proportion of social activities depend on networks and information systems used by public authorities, organisations, companies and private individuals. The digital transformation provides major opportunities to improve and streamline people's normal lives and different activities. Digitalisation has created new forms of communication, data management and data storage. Today, many information management systems are based primarily on digital information and communications technology (ICT). Following in the wake of the increasing digitalisation and globalisation, which increase dependencies over national and sectoral borders and across areas of responsibility, is also increased focus on cyber issues in society. Information and cybersecurity efforts – by both public and private actors – are seen as necessary in digitalisation processes so that society is able to function and develop in line with the objectives that have been set in the different policy areas. At the same time as a growing number of countries are developing their cyber strategies, doctrines and capabilities, cyberattacks against different interests and activities are increasing. These threats may consist of attacks that have political, financial or criminal motives, but unintentional incidents that affect cybersecurity are also increasing. Cyber incidents can disrupt the provision of essential services, such as water, health and medical care, electricity and mobile services. The possibilities of influencing information systems in democratic election processes and disinformation campaigns are also a challenge. Dependency on digital infrastructure and services through connected devices and widespread internet connectivity creates increased vulnerability, which places higher demands on information security and cybersecurity. The importance of information and cybersecurity increases to a corresponding degree. Monitoring and certifying ICT products, ICT services and ICT processes can make them more secure and also increase trust in them.

EU Cybersecurity Act

The EU Cybersecurity Act is divided into two parts. The first part deals with objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA). The second part regulates the establishment of a European cybersecurity certification framework. The Commission will prepare a rolling work programme for European cybersecurity certification which sets out strategic priorities for future European cybersecurity certification schemes. With the help of expert advice and in close cooperation with the European Cybersecurity Certification Group (ECCG), ENISA will submit proposals for European certification schemes. The aim is to ensure an adequate level of cybersecurity for information and communication technology (ICT) in the Union, and to avoid fragmentation of the internal market with regard to cybersecurity certification schemes in the Union. The creation of the European cybersecurity certification schemes will mean that certificates issued under these certification schemes will be valid and recognised in all Member States. In addition to describing the security objectives that must be considered when designing the European cybersecurity certification schemes, the EU Cybersecurity Act specifies what the minimum contents of such schemes should be.

New legislation that supplements the EU Cybersecurity Act

The Inquiry proposes that the necessary supplementary national provisions to the EU Cybersecurity Act be collected in a new law and a new ordinance. The law will specify that the Government is to designate a national cybersecurity certification authority and provide supplementary provisions on this authority's powers and ability to impose penalties for infringements of the regulatory framework, and also certain procedural provisions.

A national cybersecurity certification authority

The EU Cybersecurity Act requires that Member States designate one or more national authorities for cybersecurity certification. Considering that an existing authority is to be selected for this role,

requirements on knowledge and experience of information and communication technology (ICT), and bearing in mind that the Swedish Certification Body for IT Security (CSEC) at the Swedish Defence Materiel Administration must be involved when it comes to cybersecurity certification at the highest assurance level, it is proposed that the Swedish Defence Materiel Administration be designated as the national authority for cybersecurity certification. Accordingly, the Swedish Defence Materiel Administration will therefore carry out the tasks that follow from the European cybersecurity certification framework. These tasks include international monitoring of the cybersecurity certification field, cooperating with national and international actors, taking responsibility for cybersecurity certification at the highest assurance level and supervising compliance with the regulatory system.

The Swedish Certification Body for IT Security (CSEC) at the Swedish Defence Materiel Administration is proposed as the accredited conformity assessment body under Articles 56.5 and 56.6 of the EU Cybersecurity Act. This means that the CSEC, or any other accredited conformity assessment body that is appointed, will be responsible for cybersecurity certification at the highest assurance level.

In order to ensure the certification body's independence as the accredited conformity assessment body, it is proposed that it be specified in law that there is to be an accredited conformity assessment body at the Swedish Defence Materiel Administration pursuant to the EU Cybersecurity Act.

When the head of the accredited conformity assessment body conducts activities pursuant to the EU Cybersecurity Act, they are not subordinate to the head of the Swedish Defence Materiel Administration. The certification body's financial resources should be determined by the Government in a special procedure.

Supervision

The EU Cybersecurity Act states that the national authority for cybersecurity certification is to supervise and enforce the provisions of the European cybersecurity certification framework.

The Inquiry proposes that as the national authority for cybersecurity certification, the Swedish Defence Materiel Administration

is to carry out the supervisory tasks that follow from the EU Cybersecurity Act and thus be granted the powers as regulated in the the Act.

The Swedish Defence Materiel Administration will deal with complaints concerning an EU statement of conformity that has been issued or a European cybersecurity certificate. It will also check that manufacturers or providers that conduct conformity self-assessments of ICT products, ICT services and ICT processes (i.e. when an EU statement of conformity is issued) carry out their obligations and that a European cybersecurity certificate that is issued complies with the requirements of the relevant European cybersecurity certification scheme. The Defence Materiel Administration will also assist the national accreditation body in the monitoring and supervision of the activities of conformity assessment bodies in accordance with the provisions of the Cybersecurity Act.

Powers

The EU Cybersecurity Act grants the national authority for cybersecurity certification certain minimum powers so that it can fulfil its supervisory tasks.

The Inquiry proposes certain supplementary provisions concerning supervisory powers. The authority will determine the orders necessary to ensure compliance with the EU Cybersecurity Act, the implementing acts issued pursuant to the Regulation, the new act and regulations issued in connection with the act. It can order a relevant actor to provide information or take some other appropriate action. The authority can also approve cybersecurity certificates and revoke a certificate that has been issued. The authority may decide that an order is to apply with immediate effect. A decision to issue an order may be accompanied by a conditional financial penalty. The authority may also conduct an examination of the relevant actor's premises for supervisory purposes. However, the right to access premises will not apply to living accommodations. It is proposed that the authority have the right to be assisted by the Swedish Enforcement Authority when conducting supervision. It is also proposed that the Government or the authority designated by the Government be permitted to issue more detailed regulations on the

forms for submitting information, the supervisory procedure for investigations and examination procedures when accessing premises.

Penalties

The EU Cybersecurity Act states that Member States are to establish rules on penalties for infringements of the provisions in the European cybersecurity certification framework. The penalties are to be effective, proportionate and dissuasive.

The Inquiry proposes that the national authority for cybersecurity certification be allowed to impose fines on those who: fail to report an EU statement of conformity or possession of a European cybersecurity certificate; issue an EU statement of conformity without meeting established requirements on cybersecurity; submit incorrect or incomplete information when applying for cybersecurity certification; hold a European cybersecurity certificate and fail to provide information on vulnerabilities or irregularities that are detected; or issue an EU statement of conformity or who hold a cybersecurity certification and who fail to submit supplementary security information. It will also be possible to impose fines on those who violate the conditions for issuing, maintaining, continuing and renewing European cybersecurity certificates, as well as the conditions for reducing or extending the scope of certification, infringe on a prohibition decision or use a European cybersecurity certificate that has been revoked. Accordingly, the fee may be imposed on issuers of European cybersecurity certificates and certificate holders (ICT manufacturers and providers), and conformity assessment bodies.

The fee is to be imposed even if the infringement was not committed intentionally or through negligence, e.g. strict liability applies. If there are special grounds or if, in view of the circumstances, it would otherwise not be reasonable to impose a fine, it may be reduced. The fine is to be set at no less than SEK 10 000 and no more than SEK 15 000 000.

National strategy

The Government should consider preparing a national strategy to safeguard national interests when the European cybersecurity certification framework is developed. Relevant public authorities, other public sector actors and business should have the chance to participate in this work.

Cooperation

To ensure that national interests can be represented and safeguarded in work on the European cybersecurity certification framework, there must be adequate national representation in the European Cybersecurity Certification Group. This requires expanded and efficient cooperation among relevant public authorities, business organisations and companies.

Impact

The aim of the Inquiry's proposals is to meet the requirements of the EU Cybersecurity Act and to contribute to effective and efficient acceptance and application of the European cybersecurity certification framework. However, the analysis of the need for supplementary national provisions has been hampered by the uncertainty about the detailed contents of future European cybersecurity certification schemes (implementing acts).

The Inquiry considers that it is not currently possible to assess the direct impact that introduction of the European cybersecurity certification framework will have for the designated national authority for cybersecurity certification or for other actors affected by the specified framework, since no implementing act has yet been adopted. Nor is it possible to assess the extent to which relevant actors will make use of the option to obtain EU statements of conformity or issue European cybersecurity certificates, which also affects the need and scope of supervision. Consequently, it is also not possible to estimate the funding needed for implementation of the legislative proposals, except regarding the national authority for cybersecurity certification's need for certain additional resources.

When drafting the proposals concerning matters such as tasks for and the organisation of the national authority for cybersecurity certification, the Inquiry took account of the alternative that can be expected to be the most appropriate and cost-effective. Under the EU Cybersecurity Act, the authority's duties entail costs for administrative work and for supervision. Among other things, new powers and the possibility to impose penalties entail a need to train staff and change certain working methods. However, the initial costs for this are expected to be limited. It is proposed that the CSEC's activities continue to be funded by appropriations for certain basic functions, and continue to be funded by fees for cybersecurity certification tasks.

The Inquiry's proposals on supplementary provisions regarding the authority's powers and the possibility to impose fines are not expected to entail any financial consequences in themselves.

The proposals presented by the Inquiry that primarily deal with cooperation and coordination between the relevant authorities are expected to have a marginal impact in terms of costs.

The European cybersecurity certification framework involves voluntary or mandatory cybersecurity certification. A financial actor decides to provide ICT products or services in the Union market on condition that the provisions on cybersecurity certification are followed. It is not possible to estimate the number of companies affected by the Inquiry's proposals. Nor is it possible to make a more detailed assessment of the impact of the proposals on companies or enterprises in Sweden, other than that the companies that choose to issue an EU statement of conformity or apply for a European cybersecurity certificate will incur costs in connection with the procedure. Effective supervision also increases the possibilities for entrepreneurs to compete on equal terms. In the long term, the proposed provisions are expected to lead to increased cybersecurity and a more efficient market, which will ultimately benefit both financial actors and the functioning of the Union market.

It is proposed that the new act and other legislative amendments enter into force on 28 June 2021.

1 Författningsförslag

1.1 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.

1.2 Förslag till förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt (cybersäkerhetsakten)

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Denna förordning innehåller bestämmelser i anslutning till lagen (0000:000) med kompletterande bestämmelser till EU:s förordning om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

Förordningen innehåller också bestämmelser som 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).

Försvarets materielverks funktion

2 § Försvarets materielverk är nationell myndighet för cybersäkerhetscertifiering enligt lagen (0000:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

3 § Försvarets materielverk ska beakta nationella säkerhetsintressen vid tillämpningen av EU:s cybersäkerhetsakt.

4 § Försvarets materielverk är nationell representant enligt artikel 62.2 i EU:s cybersäkerhetsakt.

5 § Försvarets materielverk får meddela de föreskrifter som behövs för verkställigheten av EU:s cybersäkerhetsakt, lagen (0000:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt och denna förordning.

Ackrediterat organ för bedömning av överensstämmelse

6 § Vid Försvarets materielverk ska finnas ett ackrediterat organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt.

7 § När chefen för det ackrediterade organet för bedömning av överensstämmelse utövar verksamhet enligt EU:s cybersäkerhetsakt är denne inte underställd myndighetschefen.

Överklagande

8 § I 40 § förvaltningslagen (2017:900) finns bestämmelser om överklagande hos allmän förvaltningsdomstol.

Denna förordning träder i kraft den 28 juni 2021.

1.3 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att bilagan till offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Bilaga[1]

Verksamheten består i	Särskilda begränsningar i sekretessen
162. utredning och tillsyn enligt Europaparlamentets och rådets förordning (EU) nr 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) och lagen (0000:000) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.	

Denna förordning träder i kraft den 28 juni 2021.

[1] Senaste lydelse 2020:717. Tillägget innebär inte att någon punkt i bilagan upphävs.

2 Uppdraget

2.1 Bakgrund

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 kommunikationsteknologi (IKT).

Med den tilltagande digitaliseringen och globaliseringen, som ökar beroenden över nations-, sektors- och ansvarsgränser, har 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. Den kraftiga tillväxten av sakernas internet (IoT), molnet (cloud) och stordata (Big Data) medför större utsatthet för säkerhetsbrister.

Cyberincidenterna kan t.ex. 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. Genom att samhället och människorna blir alltmer beroende

av digital infrastruktur och tjänster genom anslutna enheter och utbredd uppkoppling till internet ökar sårbarheten mot cyberattacker till alltmer oroande nivåer. Därutöver syns en ökad hotbild avseende antagonistiska aktörer med hög förmåga till cyberattacker. Vikten av fullgod informations- och cybersäkerhet ökar i motsvarande grad.

Genom att kontrollera och certifiera produkter, tjänster och processer kan man göra dem säkrare och därigenom även öka förtroendet för dessa. Det finns certifieringsordningar inom ett stort antal områden, bl.a. inom informationssäkerhetsområdet men även på områden som lednings-, miljö- och trafikledningssystem samt inom hälso- och sjukvård. Motsvarande gäller för provning och kontroll inom dessa områden, som utförs av olika ackrediterade organ för bedömning av överensstämmelse av fastställda krav och standarder. Bedömning av överensstämmelse är det gemensamma begreppet för certifiering, provning och kontroll som görs av tredje part för att visa att en produkt, tjänst eller process uppfyller ställda krav. Företag som certifierar, provar och kontrollerar granskas med hänsyn till opartiskhet och kompetens av ett ackrediteringsorgan. Certifieringar, prov och kontroller som utförs av ackrediterade organ för bedömning grundas i stor utsträckning på internationella standarder.

Avtal om ömsesidigt erkännande av certifikat inom EU har ingåtts mellan några av medlemsstaterna (se avsnitt 3.5.1). Eftersom avtalen inte omfattar alla medlemsstater begränsas dess tillämplighet och genomslag samt effektiviteten på den inre marknaden. Ett certifikat utfärdat av en nationell myndighet för cybersäkerhetscertifiering erkänns dessutom i begränsad omfattning av andra medlemsstater. Det medför att inom EU är cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer begränsad och fragmenterad. I de fall de förekommer är det oftast på medlemsstatsnivå eller inom ramen för industridrivna system. Företag kan därför behöva certifiera sina IKT-produkter, IKT-tjänster och IKT-processer i flera medlemsstater där de bedriver verksamhet.

I syfte att uppnå en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom EU och sträva efter att säkerställa en väl fungerande inre marknad antogs den 17 april 2019 Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). Cybersäkerhetsakten är en EU-

förordning vars bestämmelser har direkt effekt och tillämpning i medlemsstaten samt ger utrymme för medlemsstaten att besluta om kompletterande nationell lagstiftning och annan författningsreglering. EU:s cybersäkerhetsakt är uppdelad i två delar, där den första delen reglerar Enisa:s mandat och uppgifter i byråns arbete med att stärka informations- och cybersäkerheten i unionen och dess medlemsstater. Genom den andra delen av akten införs ett europeiskt ramverk för cybersäkerhetscertifiering som bl.a. ålägger medlemsstaterna att utse nationella myndigheter med ansvar för certifierings- och tillsynsverksamheten samt i de nationella rättsordningarna införa sanktionssystem och effektiva rättsmedel i syfte att säkerställa en ändamålsenlig och effektiv tillämpning av cybersäkerhetsakten i medlemsstaterna. Dessa bestämmelser i akten träder i kraft den 28 juni 2021.

2.2 Uppdraget

Utredningens uppdrag i denna del av utredningsarbetet är att föreslå de anpassningar och kompletterande författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till på nationell nivå. Syftet är att säkerställa att den kompletterande nationella reglering som behövs finns på plats när cybersäkerhetsakten börjar tillämpas i sin helhet den 28 juni 2021.

Utredningen ska bl.a.

- analysera om kompletterande bestämmelser behöver införas i den svenska regleringen när det gäller utfärdande av EU-försäkran om överensstämmelse respektive europeiska cybersäkerhetscertifikat,
- analysera om kompletterande bestämmelser behöver införas i den svenska regleringen för organ för bedömning av överensstämmelse,
- föreslå vilken befintlig nationell myndighet som ska få i uppdrag att ansvara för certifierings- respektive tillsynsverksamhet, och
- analysera och föreslå vilka övriga kompletterande nationella bestämmelser, bl.a. vad avser handläggning av ärenden, effektiva rättsmedel och sanktioner, som cybersäkerhetsakten kräver eller Sverige bör införa.

Utredningen ska i nästa fas av utredningsarbetet överväga om det finns anledning att införa krav på certifiering och godkännande av produkter, tjänster och processer inom nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet. Arbetet i den delen ska redovisas i ett slutbetänkande under 2021.

Direktiven finns i sin helhet i bilagorna 1 och 2.

2.3 Utgångspunkter

Utredningen kan konstatera att införandet av det europeiska ramverket för cybersäkerhetscertifiering berör frågor och verksamheter som behandlas i 2015 års försvarsbeslut, Försvarsberedningens rapporter och flera av de policy- och strategidokument och handlingsplaner som antagits på nationell nivå för att stärka informations- och cybersäkerheten i samhället. Den nationella strategin för informations- och cybersäkerhet i samhället blir styrande för hur organisering och utformning av uppgifter och ansvarsområden på den nationella nivån kan ske och som behöver komplettera det europeiska ramverket för cybersäkerhetscertifiering.

Detta gäller särskilt frågorna om vilken myndighet som bör utses att vara nationell myndighet för cybersäkerhetscertifiering och hur systemet för tillsyn av efterlevnaden av cybersäkerhetsakten och europeiska ordningar för cybersäkerhetscertifiering bör organiseras och utformas. Det finns därför skäl att i detta sammanhang inledningsvis återge några av de principiella ställningstaganden som kommer till uttryck i de olika dokumenten på området och vad som anges i den av de berörda myndigheterna antagna handlingsplanen.

2015 års försvarsbeslut

I 2015 års försvarsbeslut (prop. 2014/15:109, bet. 2014/15:FöU11, rskr. 2014/15:251) fastslogs att den samlade svenska förmågan att förebygga, motverka och aktivt hantera konsekvenserna av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas. Grunden i en robust cyberförsvarsförmåga är att säkerställa funktionalitet i samhällsviktiga funktioner och att skydda den mest skyddsvärda verksamheten, inklusive sådana system som är vitala för totalförsvaret, mot antagonistiska angrepp från kva-

lificerade aktörer. Ett svenskt cyberförsvar kräver samordning och koordinering av kompetenser, samt utpekade och övade beslutsvägar, mellan olika myndigheter och samhällsfunktioner. Det pågår ständigt intrångsförsök mot internetanslutna system. Sårbarheter måste hanteras på både hård- och mjukvarusidan. Den som ansvarar för ett it-system måste utgå från att intrång och attacker kan lyckas, trots att en stor mängd faktiskt avvärjs.

Försvarsberedningens rapporter

Försvarsberedningen framhåller i sin delrapport *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025* (Ds 2017:66) att cybersäkerhet och internetrelaterade frågor diskuteras i allt fler multilaterala sammanhang och utgör en alltmer integrerad del i utrikespolitiken. Frågorna spänner över ett brett fält och innefattar bl.a. folkrätt, försvars- och säkerhetspolitik, mänskliga rättigheter och global utveckling. Samtidigt tilltar motsättningarna kring normer för internet och dess utveckling. Försvarsberedningen konstaterar att cybersäkerhetsfrågor får allt större betydelse i utrikes- och säkerhetspolitiken liksom för den nationella säkerheten. De globala cyberdiskussionerna befinner sig i ett formativt skede. De internationella skeendena har tydliga och långtgående konsekvenser för nationella förhållanden. Cyberattacker är ett allvarligt hot mot befolkningens liv och hälsa, samhällets funktionalitet och vår förmåga att upprätthålla våra grundläggande värden. Medvetenheten om detta har ökat de senaste åren. De mest skyddsvärda verksamheterna bedrivs inte solitärt utan är beroende av funktionalitet och säkerhet inom andra verksamheter. Arbetet med skydd för de mest skyddsvärda verksamheterna kan därför inte bedrivas isolerat, utan måste ske koordinerat med det samlade arbetet med samhällets informations- och cybersäkerhet.

Försvarsberedningen framhåller att en utvecklad förmåga på informations- och cybersäkerhetsområdet, inklusive en god underrättelseförmåga i den digitala miljön, ökar möjligheten att upprätthålla vår nationella suveränitet och aktivt bidrar med skydd för kritisk infrastruktur. Vidare konstaterar man att ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet spelar en avgörande roll

för att samhällets aktörer ska kunna upprätthålla en väl avvägd cyberförmåga i totalförsvaret.

Försvarsberedningen framhåller också att skyddsarbetet är ett gemensamt ansvar för hela samhället och måste bedrivas på central, regional och lokal nivå, hos myndigheter, företag och organisationer i Sverige. Den tekniska säkerheten behöver fortsatt stärkas samtidigt som hänsyn tas till att det i många fall är den mänskliga faktorn som ligger bakom incidenter eller utnyttjas vid angrepp. De åtgärder som vidtas för att exempelvis höja lägstanivån i informations- och cybersäkerhetsarbetet anses hänga samman med arbetet att skydda samhället mot avsiktliga cyberattacker.

I Försvarsberedningens rapport *Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025* (Ds 2019:8) noteras att de mest kvalificerade hoten inom cyberområdet utgörs i första hand av cyberangrepp utförda av statliga eller statsunderstödda aktörer. Det konstateras vidare att med tillräcklig tid, kompetens och resurser kan alla enheter som är uppkopplade till internet hackas. Många stater har genom utveckling av avancerade metoder och offensiva verktyg skapat förmåga att genom cyberattacker slå brett mot många mål och upprätthålla uthållighet över tiden. De cyberangrepp som Sverige kontinuerligt utsätts för kan t.ex. syfta till att hitta information om landets försvarsförmåga och planering eller ståndpunkter inför en förhandling. Det kan röra sig om att stjäla patent, forskningsresultat eller industrihemligheter för att t.ex. främja ekonomisk utveckling i sitt eget land. Det kan också röra sig om att störa eller förstöra funktionaliteten i för Sverige kritisk infrastruktur. Cyberattacker bedöms kunna få lika stora konsekvenser för samhällsviktiga funktioner och kritisk infrastruktur som ett konventionellt väpnat angrepp.[1]

Försvarsberedningen anser att Sveriges cyberförsvar med både defensiva och offensiva åtgärder ska kunna agera proaktivt för att upptäcka, få information om och hantera cyberintrång, olika former av cyberangrepp, en hotande cyberoperation, eller för att fastställa en cyberoperations ursprung. Cyberattacker och olika former av intrång i it-system kan utgöra ett separat antagonistiskt hot såväl som ett delmoment tillsammans med andra politiska, diplomatiska, ekonomiska och militära maktmedel. Spionage och angrepp från statliga

[1] Försvarsberedningen noterar att såväl EU som Nato slagit fast att ett cyberangrepp kan utlösa förpliktelser enligt artikel 42.7 i EU-fördraget respektive artikel 5 i Washingtonfördraget.

och statsunderstödda aktörer mot skyddsvärd verksamhet i Sverige eller mot svenska intressen i utlandet kan syfta till att tillskansa sig information om svenska ekonomiska intressen, företag, forskning, försvarsförmåga och planering, våra säkerhetspolitiska avsikter, samhällsviktig verksamhet och kritisk infrastruktur. Det kan också handla om att en motståndare vill vilseleda, binda begränsade resurser eller försvåra effektivt beslutsfattande inför ett väpnat angrepp och på det sättet försämra våra förutsättningar att sätta oss till motvärn. Redan i fredstid är beroendet av elförsörjning och elektroniska kommunikationer mycket stort i Sverige. Den långtgående digitaliseringen i samhället har möjliggjort avancerade välfärdstjänster som inte kommer att kunna upprätthållas under de störda förhållanden som kan komma att råda under en allvarlig säkerhetspolitisk kris eller i krig.

Nationell säkerhetsstrategi

2017 fattade regeringen beslut om en ny nationell säkerhetsstrategi för Sverige.[2] I strategin, som var en utgångspunkt för att stärka Sveriges nationella säkerhet, framhålls att Sverige aktivt ska värna nationella intressen och försvara dem närhelst de riskerar att undermineras, bl.a. vad avser hot och risker som finns på det informationsteknologiska området. För att bemästra utmaningarna inom informations- och cybersäkerhetsområdet är det viktigt att fortlöpande arbeta för att minska sårbarheter. Detta är en uppgift för alla aktörer i samhället. Förmågan att förebygga, identifiera och hantera it-incidenter och antagonistiska attacker behöver förbättras inom alla samhällsviktiga funktioner. De mest skyddsvärda verksamheterna ska dessutom svara upp mot de krav som ställs i säkerhetsskyddslagstiftningen. Arbetet med att minska sårbarheter tar sin grund i verksamhetens risk- och sårbarhetsanalys och/eller säkerhetsanalys. En förutsättning för arbetet är en utvecklad samordning och samverkan mellan myndigheter och andra aktörer, för att identifiera vad som ska skyddas och vilka ytterligare säkerhetsåtgärder som behöver sättas in. En robust cyberförsvarsförmåga framhålls som en viktig del av vår samlade ansats att stå emot riktade angrepp och försök till påverkan.

[2] Nationell säkerhetsstrategi, Statsrådsberedningen, januari 2017.

Digitaliseringsstrategin

I digitaliseringsstrategin[3] framhålls att förutsättningarna i Sverige ska vara de bästa för alla att på ett säkert sätt ta del av, ta ansvar för och ha tillit till det digitala samhället.

Nationell informations- och cybersäkerhetsstrateg

I den nationella strategin för samhällets informations- och cybersäkerhet[4] framhålls att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. I strategin framhålls att ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet bidrar till att säkerställa den fortsatta digitaliseringen av samhället och samtidigt hävda Sveriges säkerhet och nationella intressen. Ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet är också en viktig förutsättning för svensk tillväxt och konkurrenskraft, samt en nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster. För att informationshantering och it-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet, som ska vara en självklar och integrerad del i allt arbete på alla nivåer i samhället.

I strategin framhålls att ett systematiskt informations- och cybersäkerhetsarbete är nödvändigt för att samhällets aktörer ska kunna upprätthålla en väl avvägd nivå av informations- och cybersäkerhet, även om alla system för informations- och cybersäkerhet i samhället inte kan skyddas mot alla typer av hot och risker. Den tekniska säkerheten behöver därför fortsatt stärkas samtidigt som hänsyn måste tas till att det i många fall är den mänskliga faktorn som ligger bakom incidenter eller utnyttjas vid angrepp. Av den anledningen är det viktigt att även öka medvetenheten såväl som hanteringsförmågan hos alla användare av it-system och att skapa förutsättningar för utvecklingen av en säkerhetskultur i hela samhället. Vidare anges att arbetet med samhällets informations- och cybersäkerhet framför allt behöver prioritera att säkerställa en systematisk och samlad ansats i arbetet och öka säkerheten i nätverk, produkter och system. Myndigheter, kommuner, regioner, företag och andra organisationer ska

[3] För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi, Regeringskansliet (dnr N2017/03643/D).
[4] Nationell strategi för samhällets informations- och cybersäkerhet, regeringens skr. 2016/17:213.

ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete. Vidare behöver förmågan att förebygga, upptäcka och hantera cyberattacker- och andra it-incidenter stärkas. Även möjligheterna att förebygga och bekämpa it-relaterad brottslighet behöver stärkas. Också kunskapen och kompetensutvecklingen på området behöver stärkas och det internationella samarbetet öka.

I strategin anges även att i syfte att få genomslag för strategins målsättningar ska det finnas en nationell modell till stöd för det systematiska informationssäkerhetsarbetet. I dagsläget bedriver de olika aktörerna i samhället sitt informationssäkerhetsarbete på delvis olika sätt, utifrån olika förutsättningar och behov, baserat på flera olika regelverk och delvis olika uppfattningar om hot och risker. Samma information kan få olika skydd i olika organisationer och kunskapen om vilket skydd som är lämpligt och tillgängligt för en viss typ av information är hos många aktörer ofullständig. När många aktörer är beroende av varandra i sin informationshantering är det dock nödvändigt med samordnade åtgärder för att reducera risker och behålla säkerhetsnivån. Aktörer som har en sämre informationssäkerhet kan äventyra säkerheten för övriga. Detta har betydelse för möjligheterna till en digitalt samverkande förvaltning, men även för den återupptagna planeringen för civilt försvar som är beroende av goda förutsättningar att dela känslig information inom statsförvaltningen.

I strategin anges att en nationell modell bedöms även kunna bidra till att aktörer gör mer enhetliga bedömningar av hot, risker och säkerhetsåtgärder och att likartade uppgifter och informationssystem hos olika verksamhetsutövare uppnår en adekvat och likartad skyddsnivå. Genom att de myndigheter som har ett särskilt ansvar på informationssäkerhetsområdet, och de övriga myndigheter som t.ex. har föreskriftsrätt eller tillsyn på området, aktivt bidrar i arbetet med den nationella modellen kan den motverka fragmentering av styrningen och öka samverkan inom området. Genom att den nationella modellen ska bygga på erkända standarder, vara flexibel och skalbar kan verksamheter med olika förutsättningar dra nytta av modellen. Modellen bör i första steget inriktas mot statliga myndigheter, men utformas med målet att den ska kunna vara till nytta för hela den offentliga sektorn, andra organisationer och företag.

I strategin framhålls även vikten av samverkan och informationsdelning inom och mellan berörda aktörer och att samverkan och in-

formationsdelning på informations- och cybersäkerhetsområdet ska stärkas, bl.a. då informationssäkerhetens komplexitet, karaktär och snabba utvecklingstakt samt gränsöverskridande kräver en effektiv samverkan.

I strategin framhålls att samverkansgruppen för informationssäkerhet (SAMFI), som består av ett antal statliga myndigheter med särskilda uppgifter på informationssäkerhetsområdet, spelar en viktig roll genom att verka för säkra informationstillgångar i samhället.[5] Vidare framhålls att på informations- och cybersäkerhetsområdet finns flera exempel på plattformar för offentlig-privat samverkan, bl.a. ett antal forum för informationsdelning (FIDI) inom olika sektorer och områden. Det finns ett behov av att fortsatt utveckla informationsdelningen gällande hot, risker och säkerhetsåtgärder i syfte att skyddet snabbt ska kunna anpassas hos fler aktörer.

I strategin anges att det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för en ökad informations- och cybersäkerhet i samhället. En förutsättning för att reglerna på informationssäkerhetsområdet ska få det genomslag som är avsett är att det finns en tillsyn som kan utföras på ett ändamålsenligt och effektivt sätt. Vidare framhålls att ett flertal åtgärder behöver vidtas när det gäller tillsyn. I första hand behöver tillsynen av sådan verksamhet som omfattas av samhällsviktig verksamhet inom de sektorer som pekas ut i NIS-direktivet och säkerhetsskyddslagstiftningen utvecklas.

SAMFI-myndigheternas handlingsplan

I SAMFI samarbetar myndigheter med av regeringen särskilt utpekat ansvar för informationssäkerhetsfrågor i samhället. Genom informationsutbyte och samverkan stödjer deltagande myndigheter varandras arbete med samhällets informationssäkerhet.

Den samlade informations- och cybersäkerhetshandlingsplanen[6] innehåller åtgärder som myndigheterna enskilt, tillsammans eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. Av 2020 års redovisning framgår

[5] I samverkansgruppen ingår Myndigheten för samhällsskydd och beredskap (MSB), Försvarets materielverk, Försvarets radioanstalt (FRA), Försvarsmakten, Polismyndigheten, Post- och Telestyrelsen (PTS) samt Säkerhetspolisen. MSB har det administrativa ansvaret för gruppen.
[6] MSB, FRA, FMV, Försvarsmakten, PTS, Polisen, Säkerhetspolisen (1 mars 2019): Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.

vilken myndighet som är ansvarig för respektive åtgärd, vilka som deltar i arbetet samt vad åtgärden omfattar. Åtgärderna i handlingsplanen ligger inom ramen för de ansvarsområden och uppdrag som myndigheterna har. Handlingsplanen utgör dock inte någon samlad redovisning av alla de åtgärder som de olika myndigheterna avser att genomföra inom sina respektive verksamheter på informations- och cybersäkerhetsområdet. Samtliga åtgärder i handlingsplanen ansluter till någon eller några av de sex strategiska prioriteringar som regeringen beslutat i den nationella strategin för samhällets informations- och cybersäkerhet[7]. Huvuddelen av åtgärderna syftar till att

– säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet,
– öka säkerheten i nätverk, produkter och system samt
– stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.

Nationellt cybersäkerhetscenter

FRA, Försvarsmakten, MSB och Säkerhetspolisen formaliserade under 2019 en fördjupad samverkan på informations- och cybersäkerhetsområdet (inom SAMFI). Denna fördjupade samverkan etablerades innan regeringen aviserade att ett cybersäkerhetscenter skulle inrättas 2020 och kan ses som ett ingångsvärde för regeringens uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter.[8]

I september 2019 fick de fyra myndigheterna ett uppdrag av regeringen att förbereda ett inrättande av ett cybersäkerhetscenter samt ge förslag på hur ett sådant center skulle kunna utformas. Myndigheterna lämnade en gemensam uppdragsredovisning till regeringen i december 2019 som underlag för inrättandet av ett cybersäkerhetscenter. Arbetet har skett i nära samverkan med Polismyndigheten, FMV och PTS. Dessa tre myndigheter ingår sedan början av 2020 i överenskommelsen om en fördjupad myndighetssamverkan inom cybersäkerhet.

[7] Skr. 2016/17:213.
[8] Regeringsbeslut 2019-09-26 (Fö2019/01000/SUND), Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter. Redan i regeringsförklaringen i januari 2019 aviserades ett nationellt center för ökad informations- och cybersäkerhet.

Ett nationellt cybersäkerhetscenter och en nationell modell för systematiskt informationssäkerhetsarbete är en ny åtgärd i den nationella handlingsplanen som bedöms kunna utveckla samhällets informations- och cybersäkerhet. Som samverkansplattformar kan de även samla och samordna arbetet med många av åtgärderna.

Centret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska sårbarheter. En tilltänkt fördel är att de i centret ingående myndigheterna kan och bör dela information och kunskap så att respektive myndighet kan lösa sitt uppdrag på ett effektivare sätt.

Ett av centrets syften är att stödja aktörer inom offentlig och privat sektor. Därför har samverkansfrågor utgjort en central del i arbetet med uppdraget.

Myndigheterna har arbetat fram ett förslag på hur centret kan bemannas och föreslår att centret ska byggas upp stegvis under 2020–2025.

2.4 Definitioner och avgränsning

Definitioner

Begreppen cybersäkerhet och informationssäkerhet förekommer i många olika sammanhang, såväl nationellt som internationellt. Utredningen kan samtidigt konstatera att begreppen förekommer i såväl olika författningar som i nationella styrdokument, handlingsplaner och allmänna råd. Det finns enligt utredningens mening skäl för att begreppen i största möjliga utsträckning bör ges samma betydelse såväl nationellt som internationellt.

Det ska samtidigt noteras att EU:s cybersäkerhetsakt, som är en unionsrättslig författning som är direkt tillämplig i medlemsstaterna, innehåller definitioner av de olika begrepp som förekommer i akten, bl.a. cybersäkerhet och informationssäkerhet. Eftersom cybersäkerhetsakten är direkt tillämplig på nationell nivå bör förekommande begrepp ges samma innebörd och mening när de förekommer i den kompletterande nationella lagstiftningen. Den närmare innebörden av vissa begrepp och bestämmelser som förekommer i cybersäkerhetsakten och som berör effektiva rättsmedel, sanktioner och den nationella processordningen kan dock behöva anpassas till nationella förhållanden.

Avgränsning av uppdraget

I EU:s cybersäkerhetsakt anges att regleringen inte påverkar medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Utredningen bedömer samtidigt att många av de IKT-produkter, IKT-tjänster och IKT-processer som kan komma att omfattas av regleringens tillämpningsområde kommer att användas i verksamheter som berör samhällsviktiga tjänster och i verksamhet som berör säkerhetskänslig verksamhet och det svenska totalförsvaret, såväl det civila som det militära försvaret.

En av utgångspunkterna för utredningens arbete har därför varit att i de analyser och de överväganden som gjorts i olika frågor även beakta hur utredningens ställningstaganden och förslag kan komma att beröra informations- och cybersäkerhet i bl.a. säkerhetskänslig verksamhet.

2.5 Utredningsarbetet

Utredningen började sitt arbete i februari 2020. Utredningen har inledningsvis inhämtat underlag i form av offentliga utredningar, propositioner, faktapromemorior, nationella strategier, olika studier m.m. Givet rådande omständigheter har arbetet i stor utsträckning kunnat bedrivas på sedvanligt sätt med sammanträden med sakkunniga och experter, där bl.a. myndigheternas företrädare informerade och lämnade faktauppgifter i olika utredningsfrågor.

Utredningen har därutöver haft möten med berörda myndighetsledningar för att informera sig om förutsättningar för dessa myndigheter att kunna ansvara för en eller flera av de uppgifter och verksamheter som utredningen har i uppdrag att analysera och lämna förslag om. Sekretariatet har haft enskilda möten med experter i utredningen i syfte att inhämta fördjupad kunskap inom vissa av de sakområden som behandlas i uppdraget samt haft möten med privata aktörer med en nära koppling till området.

Utredningen har bedömt att det inte är nödvändigt att i delbetänkandet närmare redogöra för den information som inhämtats från berörda myndigheter i andra länder då informationen inte kunnat kvalitetssäkras på sedvanligt sätt, bl.a. då besök hos berörda myndigheter i dessa länder inte kunnat genomföras på grund av rådande

pandemi. Informationen i de skriftliga underlagen präglas dessutom av viss osäkerhet då ingen av länderna fullt ut fastställt eller genomfört åtgärder till stöd för införandet av EU:s cybersäkerhetsakt.

Utredningen har i enlighet med direktiven hållit sig informerad om arbetet med betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82).

Utredningen har löpande hållit företrädare för Försvarsdepartementet informerade om utredningsarbetet.

2.6 Delbetänkandets disposition

I detta kapitel presenteras uppdraget, utgångspunkter, definitioner, avgränsningar, utredningsarbetets genomförande samt betänkandets utformning.

I kapitel 3 redogörs för begreppet EU:s arbete med cybersäkerhet samt cybersäkerhet och standarder. I kapitel 4 lämnas en redogörelse för strukturen och bestämmelserna i EU:s cybersäkerhetsakt. I kapitel 5 beskrivs översiktligt den nationella ordningen för certifiering av it-säkerhet i system och produkter samt berörda aktörer. Del två av betänkandet innehåller utredningens överväganden och förslag. I kapitel 6 analyseras behovet av och lämnas förslag på formen för kompletterande nationella författningar. I kapitel 7 analyseras behovet av kompletterande nationell reglering avseende utfärdande av EU-försäkran om överenstämmelse och europeiska cybersäkerhetscertifikat. I kapitel 8 analyseras och lämnas förslag på nationell myndighet för cybersäkerhetscertifiering. I kapitel 9 analyseras och lämnas förslag på kompletterande nationella författningar avseende tillsynsbefogenheter och sanktioner. I kapitel 10 analyseras behovet av kompletterande nationella författningar avseende ackreditering av organ för bedömning av överenstämmelse. I kapitel 11 behandlas handläggningsregler och rättsmedel. Sekretessfrågor behandlas i kapitel 12. I kapitel 13 behandlas övriga frågor, bl.a. behovet av samverkan. I kapitel 14 lämnas en konsekvensbeskrivning. Slutligen lämnas författningskommentarer i kapitel 15. Bilagorna 1 och 2 innehåller kommittédirektiven. EU:s cybersäkerhetsakt finns i bilaga 3.

3 Cybersäkerhet

3.1 Inledning

EU:s cyberekosystem är komplext och mångfacetterat. Det omfattar ett stort antal inrikespolitiska områden såsom rättsliga och inrikes frågor, den digitala inre marknaden och forskningspolitik. Inom utrikespolitiken är cybersäkerhet viktigt för diplomatin och ämnet spelar en allt viktigare roll i EU:s framväxande försvarspolitik.

I detta kapitel lämnas en översiktlig beskrivning över EU:s strategier och policy på cybersäkerhetsområdet. Vidare behandlas begreppen cybersäkerhet och standardisering.

3.2 EU:s strategier och policy på cybersäkerhetsområdet

Den digitala agendan för Europa (DAE)

*Den digitala agendan för Europ*a (DAE) lades fram 2010 som en del av *Europa 2020-strategin*.[1] Den digitala agendan föreslår ett bättre utnyttjande av potentialen i informations- och kommunikationsteknologin (IKT) för att främja innovation, ekonomisk tillväxt och framåtskridande. Några av åtgärderna är att verkställa en digital inre marknad, stärka interoperabilitet och standarder, forskning och innovation och dra fördel av en smart teknikanvändning i samhället, exempelvis e-hälsa, telemedicinsystem och smarta transportsystem.[2]

[1] Europa 2020 är EU:s gemensamma strategi för tillväxt och sysselsättning. Strategin har tre övergripande prioriteringar: smart tillväxt, hållbar tillväxt och tillväxt för alla. Kvantitativa mål på EU-nivå fastställdes av Europeiska rådet 2010 och ska vara uppfyllda senast 2020 inom fem områden: sysselsättning, social delaktighet, utbildning, forskning och utveckling samt klimat och energi.

[2] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén: En digital agenda för Europa, KOM(2010)245 slutlig, 2010-05-19.

EU:s cybersäkerhetsstrategi

Kommissionen antog 2013, tillsammans med den höga representanten för utrikesfrågor och säkerhetspolitik, *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd*. Strategin har en helhetssyn och omfattar såväl de civila aspekterna av cybersäkerhet som cyberförsvar till stöd för den gemensamma försvars- och säkerhetspolitiken. Strategin anger huvuddragen av EU:s vision inom området, förtydligar olika aktörers roller och ansvarsområden, samt presenterar de åtgärder som bör vidtas. Strategin syftar till att göra EU:s digitala miljö säkrast i världen, samtidigt som grundläggande värden och friheter försvaras.[3] Det är huvudsakligen en uppgift för EU:s medlemsstater att arbeta med utmaningar inom cyberrymden, men särskilda åtgärder föreslogs som kunde förbättra unionens samlade insatser. Vidare presenterades strategiska prioriteringar och olika EU-institutioner tilldelades uppgifter.

Utifrån cyberfrågornas komplexitet, de många inblandade aktörerna och riskernas gränslösa natur föreslogs att cybersäkerhetsfrågorna fördelas över tre skilda pelare: nätverks- och informationssäkerhet, upprätthållande av lag och ordning samt försvar. Vidare framhölls att medlemsländerna och kommissionen borde underrätta varandra om större cyberincidenter och -angrepp.

Strategin för cybersäkerhet har kommit att bli en hörnsten i EU:s politik, även om strategin formulerats brett och snarare ger uttryck för en vision än ett mätbart mål.[4] Strategin är sammanlänkad med tre strategier som antagits senare, dvs. den europeiska säkerhetsagendan, strategin för den digitala inre marknaden samt den globala strategin för EU:s utrikes- och säkerhetspolitik.

EU:s policyramverk för cyberförsvar

Rådet antog 2014 ett ramverk för policy för cyberförsvar, vilket efterfrågats i cybersäkerhetsstrategin. I ramverket ges prioriteringar och olika EU-institutioner tilldelas uppgifter att utföra.[5] I fokus är en

[3] Gemensamt meddelande från Europeiska kommissionen och Europeiska avdelningen för yttre åtgärder, EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd, JOIN(2013) 1 slutlig, 2023-02-07.
[4] Europeiska kommissionen, Commision staff working document: Assessment of the EU 2013 cybersecurity strategy, SWD(2017) 295 final, 2017-09-13.
[5] Europeiska unionens råd, 2014, EU Cyber Defence Policy Framework.

förmågeutveckling för den gemensamma säkerhets- och försvarspolitiken (GSFP). I takt med att cyberrymden under senare år blivit alltmer militariserad har den kommit att ses som det femte krigföringsområdet. Cyberförsvar skyddar cyberrymdens system, nätverk och kritiska infrastruktur mot angrepp med militära metoder eller andra slags metoder.

Strategi för en digital inre marknad (DSM)

Kommissionen antog 2015 en strategi för en digital inre marknad, vilket var en av åtgärderna i den digitala agendan (se ovan). Syftet med strategin för en digital inre marknad är att förbättra tillgången till digitala varor och tjänster genom att skapa rätt villkor för att maximera den digitala ekonomins tillväxtpotential.[6] Kommissionen framhöll att den globala ekonomin snabbt blev alltmer digitaliserad och att IKT utgjorde ett fundament för moderna ekonomiska system. För att främja den europeiska digitala ekonomins tillväxt och förbättra förutsättningarna för utvecklingen av digitala nät och tjänster bedömdes det finnas behov av samordnade åtgärder.

En säkerhetsagenda för Europa

Kommissionen antog 2015 en ny säkerhetsagenda för Europa (2015–2020) som ersatte den tidigare interna säkerhetsstrategin. Den europeiska säkerhetsagendans mål är att förbättra brottsbekämpning och rättsliga åtgärder mot it-brottslighet, främst genom att förnya och uppdatera befintlig politik och lagstiftning.[7] Den syftar också till att identifiera hinder för rättsliga utredningar av it-brottslighet och förbättra cyberkapacitetsuppbyggnaden.[8] De nya och komplexa hot som har vuxit fram de senaste åren, präglade av att vara alltmer internationella och gränsöverskridande, ansågs kräva ett effektivt och samordnat svar från europeisk nivå. Alla berörda aktörer måste därför grunda sitt arbete bl.a. på ett mer sektoröverskridande tillvägagångs-

[6] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En strategi för en inre digital marknad i Europa (COM(2015) 192 final), 2015-05-06.
[7] Europeiska kommissionen, Europeiska säkerhetsagendan, COM(2015) 185 final, 2015-04-28.
[8] Meddelande från kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En säkerhetsagenda för Europa (COM(2015) 185 final), 2015-04-28.

sätt, dvs. att policy och praktisk handling ska samordnas mellan alla relevanta EU-institutioner. Vidare ska säkerhetens interna och externa aspekter förenas, dvs. ska säkerhetsåtgärderna såväl inom som utanför EU samordnas, eftersom de är ömsesidigt beroende.

Rådets slutsatser om cyberdiplomati

Europeiska unionens råd presenterade under 2015 sina slutsatser om cyberdiplomati och konstaterade att frågor rörande cyberrymden stod för betydande möjligheter men också föränderliga utmaningar för EU:s utrikespolitik. Det handlade särskilt om cybersäkerhet, främjande och skydd av mänskliga rättigheter på internet, tillämpningen av befintlig internationell rätt, rättsstatsprincipen och uppförandenormer på internet, förvaltning av internet, den digitala ekonomin, cyberkapacitetsuppbyggnad samt strategiska relationer i cyberfrågor. Rådet ansåg att EU och dess medlemsstater borde hantera dessa övergripande och mångfasetterade frågor genom en enhetlig internationell politik för cyberrymden som främjade EU:s politiska, ekonomiska och strategiska intressen. En sådan politik borde enligt rådet bygga på befintliga policydokument. Man skulle också fortsätta dialogen med såväl viktiga internationella partners och organisationer som det civila samhället och den privata sektorn.[9]

På politisk nivå utvecklades därefter en ram för en gemensam diplomatisk respons (”Joint EU Diplomatic Response”) från EU mot offensiva cyberaktiviteter, den s.k. verktygslådan för cyberdiplomati.[10] EU ska även stödja framtagningen av frivilliga, ickebindande normer för ansvarsfullt agerande för stater i cyberrymden samt de regionala förtroendeskapande åtgärder (CBM) som OSSE arbetat fram. Dessa är avsedda att förstärka mellanstatligt samarbete, transparens, förutsägbarhet och stabilitet och minska risken att konflikter uppkommer p.g.a. användningen av IKT.

[9] Europeiska unionens råd, Rådets slutsatser som cyberdiplomati, 6122/15, 2015-02-10.
[10] Europeiska unionens råd, Slutsatser om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet, 9916/17, 2017-06-07. För övrigt har verktygslådan för cyberdiplomati bl.a. använts för att inleda en dialog med USA efter ”Wannacry-angreppet”. Detta ledde inte till en gemensam åtgärd, utan enskilda medlemsstater antog i stället USA:s ståndpunkt.

En global strategi för Europeiska unionens utrikes- och säkerhetspolitik

Den höga representanten för utrikesfrågor och säkerhetspolitik föreslog 2016 en global strategi för EU:s utrikes- och säkerhetspolitik (GUSP) *Delade visioner, gemensamma åtgärder: Ett starkare Europa*. Den globala strategin syftade till att främja EU:s roll i världen genom bl.a. ett förnyat åtagande avseende cybersäkerhetfrågor. Större strategisk autonomi var ett mål. EU ska navigera vad som beskrivs som en svår och omstridd, sammankopplad och komplex värld.[11] En av prioriteringarna är unionens säkerhet, vilket avseende cybersäkerhet bl.a. innebär att utveckla de teknologiska förmågorna för att öka resiliensen i kritisk infrastruktur, nätverk och tjänster, att utveckla innovativa IKT-system som garanterar datas tillgänglighet och integritet, att integrera cyberfrågorna inom alla politikområden och att utveckla plattformarna för samarbete.

EU:s cybersäkerhetsinitiativ

EU har stärkt sina strategier på cyberområdet under de senaste åren genom att inkludera cybersäkerhet i politiska prioriteringar. Förtroende och säkerhet var kärnan i strategin för en digital inre marknad, medan kampen mot cyberbrott var en av de tre pelarna i den europeiska säkerhetsagendan. Efter att ha genomfört nämnda strategier presenterade kommissionen 2016 ytterligare åtgärder för att utöka cybersäkerhetsindustrin och hantera cyberhot. Vid sammanställningar avseende cybersäkerhetsarbete, där EU och den privata marknaden behövt arbeta tillsammans, har bl.a. certifiering identifieras som ett område. Man har i detta sammanhang sett behov av att motverka fragmenteringen p.g.a. skiftande nationella system samt förbättra effektiviteten i de som används.[12]

[11] Europeiska unionens råd 2016. Shared vision, Common action: A stronger Europe: A global strategy for the European Union's Foreign and Security Policy.
[12] Europeiska kommissionen, Commission Staff Working Document, Contractual Public Partnership on Cybersecurity & Accompanying Measures, SWD(2016) 2016 final.

Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch

För att förverkliga cybersäkerhetsstrategin och strategin för en inre digital marknad antog kommissionen den 5 juli 2016 ett meddelande om stärkt motståndskraft i nätverk och informationssystem (cyberresiliens). Kommissionen ansåg att skyddet mot cyberincidenter, trots många initiativ, fortfarande var otillräckligt, vilket kunde undergräva den digitala inre marknaden, det ekonomiska livet och samhällslivet i stort. Mot denna bakgrund åtog sig kommissionen att undersöka hur den föränderliga cybersäkerhetssituationen kunde mötas och analyserade vilka ytterligare åtgärder som behövdes för att öka EU:s cyberresiliens, förmåga att hantera incidenter och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch i Europa. Åtgärderna delades in i tre huvudområden:

– ett intensifierat samarbete för att stärka beredskapen och hantera cyberincidenter,
– utmaningar på Europas inre marknad för cybersäkerhet, och
– främjande av industriell kapacitet på cybersäkerhetsområdet.

Åtgärder för främjandet av den framväxande inre marknaden för cybersäkerhetsprodukter och -tjänster i EU handlar om skapandet av en ram för säkerhetscertifiering av IKT-produkter och IKT-tjänster och att öka kunskaperna om befintliga finansieringsmekanismer bland cybersäkerhetsaktörer för att öka investeringarna i cybersäkerhet i små och medelstora företag. Området industriell kapacitet på cybersäkerhetsområdet avser att främja konkurrenskraft och innovation för den europeiska cybersäkerhetsbranschen.

Gemensamt ramverk för att motverka hybridhot

2016 antog kommissionen ett gemensamt ramverk för att motverka hybridhot,[13] baserat på bl.a. säkerhetsagendan, den globala strategin för utrikes- och säkerhetspolitik och cybersäkerhetsstrategin. Ramen inriktades på cyberhot mot både kritisk infrastruktur och privata användare och betonade att cyberangrepp kunde genomföras genom desinformationskampanjer på sociala medier.[14] Inom ramen noterades också behovet av att förbättra medvetenheten och samarbetet mellan EU och Nato, vilket specificerades i de gemensamma förklaringarna från EU och Nato 2016 och 2018.[15]

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

Kommissionen lämnade i september 2017 en beskrivning över tillståndet i unionen, ett s.k. state of the union, som specifikt behandlade cybersäkerhet.[16] I ett gemensamt meddelande till Europaparlamentet och rådet beskrev kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik att EU:s medborgare och privata sektor blivit alltmer beroende av digitala tjänster och teknologier, samtidigt som antalet cyberattacker ökat. För att möta denna situation föreslogs åtgärder på tre områden:[17]

– bygga upp EU:s resiliens mot cyberangrepp,
– skapa effektiva avskräckningsmedel mot cyberbrott, och
– stärka det internationella samarbetet om cybersäkerhet.

[13] Medlemsstaterna har huvudansvaret för att motverka hybridhot riktade mot den nationella nivån. Flera av EU:s medlemsstater står dock inför liknande hot, vilka dessutom kan vara riktade mot gränsöverskridande nätverk och infrastrukturer. Dessa hot bemöts mer effektivt genom ett samordnat svar från EU-nivån. Detta genom att skapa synergier mellan alla relevanta verktyg och instrument och genom att främja samarbete mellan samtliga relevanta aktörer.
[14] Europeiska kommissionen/Europeiska utrikestjänsten, Gemensam ram för att motverka hybridhot – Europeiska unionens insatser, JOIN(2016) 18 final, 2016-04-06.
[15] Gemensam förklaring från Europeiska rådets ordförande, Europeiska kommissionens ordförande och Nordatlantiska fördragsorganisationens generalsekreterare, 2016-07-08 och 2018-07-10.
[16] Europeiska kommissionen 2017, State of the Union 2017, Cybersecurity.
[17] Europeiska kommissionen och unionens höga representant for utrikes frågor och säkerhetspolitik, Gemensamt meddelande till Europaparlamentet och rådet, Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU (JOIN/2017/450 final), 2017-09-13.

Meddelandet inbegrep en uppdatering av strategin för cybersäkerhet från 2013. Under den första punkten föreslogs bl.a. en ny cybersäkerhetsmyndighet som skulle bygga på Enisa, men med ett starkare mandat, liksom en certifieringsram för cybersäkerhet på EU-nivå som ett steg mot en inre cybersäkerhetsmarknad. Det nya cybersäkerhetspaketet presenterade ett antal lagstiftningsförslag, bl.a. avseende cybersäkerhetsakten. En plan för genomförandet av NIS-direktivet och snabb incidenthantering upptogs som andra områden för åtgärder.

Cybersecurity in the European Digital Single Market

Utifrån den kommande revisionen av EU:s cybersäkerhetsstrategi lämnade kommissionens mekanism för vetenskaplig rådgivning – dvs. högnivågruppen av vetenskapliga rådgivare – ett antal rekommendationer i mars 2017. De tio rekommendationerna riktade sig mot policynivån i EU med utgångspunkt i cybersäkerhet för den digitala inre marknaden.[18] Gruppen gjorde också några observationer som inte direkt riktade sig till något politikområde. En avsåg förhållandet att cyberhoten var komplexa, multidisciplinära och snabbrörliga och att cybersäkerhet inte kunde ses som en väldefinierad vetenskaplig disciplin. En annan observation var att det fanns en obalans mellan ledtiderna för EU-lagstiftning och den höga omsättningshastigheten på digitala teknologier. Exempelvis riskerade delar av det emotsedda NIS-direktivet att vara utdaterat vid tidpunkten för dess implementering. De som utformade EU-politiken behövde innovativa processer för att hantera detta. I en tredje observation lyftes några spänningar i debatten, där det inte fanns vare sig bevis eller konsensus mellan experter. En sådan avsåg valet mellan centraliserad och decentraliserad it-styrning för online-transaktioner. Valet hade politiska implikationer och det fanns teknisk argumentation för båda sidor.

[18] Europeiska kommissionen 2017, Cybersecurity in the European Digital Single Market, Scientific Advice Mechanism (SAM), High Level Group of Scientific Advisors, Scientific Opinion No. 2/2017, mars 2017.

Cybersäkerhetsstudie av Enisa

Enisa redogjorde i maj 2017 för en studie på uppdrag av Europaparlamentet avseende cybersäkerhet i GSFP. Även här konstaterades att cybersäkerhet gick utöver GSFP och krävde samarbete för att hanteras. Vidare krävdes samordning mellan de många olika aktiviteterna, tillika med internationella partners. Avseende internationella insatser behövde man även kunna skydda tillgångar utanför EU:s gränser. Fem framtida alternativ identifierades, som inte uteslöt varandra: fortsatt sammanhållna strategier och policys på EU-nivå, främjande av en ansvarsfull cyberkultur, utvecklat kunnande på området, förstärkning av regelverk och utvecklade standarder, organisationer och förmågor. Dessa bröts ner i de tre lagren politiskt/strategiskt, operativt och taktiskt/tekniskt.[19]

EU:s policy för cyberförsvar

Ramen för EU:s policy för cyberförsvar uppdaterades i november 2018. Uppdateringen behövdes för att EU skulle kunna hantera de föränderliga säkerhetsutmaningarna. I uppdateringen identifieras sex prioriteringar, inbegripet utveckling av cyberförsvarskapacitet samt skydd av kommunikations- och informationsnätverken för GSFP. Målet med den uppdaterade ramen var att ytterligare utveckla EU:s politik på området och tydligare definiera den miniminivå av cybersäkerhet och förtroende som ska uppnås utifrån tidigare EU-omfattande erfarenheter.[20] It-försvar utgör också en del av det permanenta strukturerade samarbetet (Pesco) och EU-Natosamarbetet.

[19] Europaparlamentet, 2017, Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU.
[20] Europeiska unionens råd, 2018, Ram för EU:s politik för it-försvar.

3.3 EU:s aktörer inom cybersäkerhet

Inledning

Både civil infrastruktur och militär kapacitet är beroende av säkra digitala system. Det finns emellertid en global kompetensbrist inom cybersäkerhet.[21] Inte minst i Europa är expertisen fragmenterad. EU är i stor utsträckning beroende av icke-europeiska leverantörer av cybersäkerhetsprodukter och lösningar.[22] EU:s institutioner och organ har identifierat behovet av att utveckla sin cyberkapacitet och sina metoder för riskhantering på ett konsekvent sätt.[23] Den Europeiska revisionsrätten har gjort bedömningen att utmaningarna med cyberhotsbedömningar förvärras av en ovilja att utbyta information och en underrapportering av incidenter.[24]

Också organisationer i den privata sektorn, inbegripet industrin, internetförvaltningsorgan och den akademiska världen är partners inom och bidragsgivare till politisk utveckling och genomförande på cybersäkerhetsområdet. Bl.a. har ett avtalsbaserat offentlig-privat partnerskap om cybersäkerhet (cPPP) etablerats inom EU. Partnerskapet var ett första steg att sammanföra forskarsamhället, näringslivet och den offentliga sektorn för främjande av forskning och innovation inom cybersäkerhet. Samtidigit har det funnits behov av att göra större satsningar för att mer effektivt kunna lösa cybersäkerhetsutmaningarna inom EU. Kommissionen har föreslagit att det inrättas ett europeiskt kompetenscentrum för cybersäkerhet med ett nätverk av nationella samordningscentrum.[25]

Medlemsstaterna kan ha ett stort ansvar för att hantera cybersäkerhetsincidenter, men den gränsöverskridande karaktären med-

[21] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 52.
[22] Jfr Regeringskansliet Faktapromemoria 2018/19:FPM11, 2018-10-17, s. 2 och 6.
[23] Kommissionen, rådet och Europeiska utrikestjänsten ska 2020 presentera en rapport för den övergripande arbetsgruppen för cyberfrågor om styrning och de framsteg som gjorts när det gäller att klargöra och harmonisera styrningen av cybersäkerhet vid EU:s institutioner och byråer (Europeiska unionens råd, Handlingsplan för genomförandet av rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU, 15748/17, 2017-12-12, s. 9).
[24] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 35.
[25] Kommissionen föreslår att kompetenscentret, som ska utgöra en grund i europeisk säkerhetspolitik och bidra till ökad forskning och utveckling av cybersäkerhet i unionen, inrättas för perioden från den 1 januari 2021 till och med den 31 december 2029. Se kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum, COM(2018) 630 final, 2018-09-12.

för inte sällan att EU också behöver vara involverad i arbetet. Som tidigare berörts delar EU:s cybersäkerhetsstrategi upp i tre delområden: nätverks- och informationssäkerhet, brottsbekämpning och försvar, där olika aktörer tilldelas roller och ansvar. Då cybersäkerhet berör många områden ligger ansvar, roller och utgifter spridda över flertalet aktörer och kräver samarbeten inom EU, med medlemsstaterna och med privata aktörer.

Styrning av informations- och cybersäkerhet

Styrning av informationssäkerhet handlar om att upprätta strukturer och politik för att säkerställa konfidentialitet, integritet och tillgänglighet för data. Det är mer än en teknisk fråga. Styrning av cybersäkerhet omfattar alla slags cyberrelaterade hot, inbegripet målinriktade, sofistikerade angrepp, överträdelser eller incidenter som är svåra att upptäcka eller åtgärda.

Modellerna för styrning av cybersäkerhet skiljer sig åt mellan EU:s medlemsstater. I tillgängliga studier dras slutsatsen att styrningen av cybersäkerhet kan stärkas för att främja det globala samfundets förmåga att hantera cyberangrepp och incidenter. Samtidigt är det omöjligt att förhindra alla angrepp. Viktiga utmaningar som måste tas itu med är därför snabb detektering och hantering, skydd av kritisk infrastruktur och kritiska samhällsfunktioner samt bättre utbyte och samordning avseende information mellan offentlig och privat sektor.[26]

Beslutsprocesser

Man kan dela in EU-samarbetet i överstatliga och mellanstatliga frågor, där flera frågor av straffrättslig och polisiär natur inordnas i den överstatliga strukturen. För utrikes- och (den externa) säkerhetspolitiken gäller dock som regel att beslut fattas mellanstatligt.[27] Vilken befogenhet EU har att besluta inom ett visst politikområde framgår av fördraget om unionens funktionssätt, EUF-fördraget. Enligt uppräkningen i nämnda fördrag, benämnd kompetenskatalo-

[26] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 52.
[27] Cini, Michelle & Pérez-Solórzano Borragán, Nieves (red), 2016: European Union Politics.

gen, har EU tre skilda befogenheter. Inom somliga områden har EU ensamrätt att lagstifta. Inom andra har EU och medlemsländerna delad befogenhet, vilket innebär att medlemsländerna kan lagstifta i dessa frågor så länge EU inte redan gjort det. Det gäller exempelvis området frihet, säkerhet och rättvisa. Inom ytterligare andra områden, som civilskydd, har EU endast rätt att stödja, komplettera eller samordna medlemsländernas åtgärder. EU ska dock ha rätt att fastställa och genomföra en gemensam utrikes- och säkerhetspolitik (GUSP), inklusive en gradvis utformning av en gemensam säkerhets- och försvarspolitik (GSFP).[28]

EU-institutioner

Europeiska unionens råd, Europeiska rådet, Europaparlamentet och Europeiska kommissionen inriktar EU:s arbete och är därigenom betydelsefulla även för cybersäkerhetsarbetet.

Europeiska unionens råd (ministerrådet eller rådet) företräder medlemsländernas nationella intressen. Ministerrådet består av ministrar från medlemsländernas respektive regeringar, beroende på vilken sakfråga som behandlas. Tillsammans med EU-parlamentet beslutar man om de lagförslag som initieras av kommissionen.[29]

Medlemsstaterna ansvarar först och främst för den egna cybersäkerheten och agerar på EU-nivå genom rådet, som har ett antal samordnande och informationsdelande organ. I rådet hanteras cybersäkerhet av den övergripande arbetsgruppen för cyberfrågor som samordnar strategiska och horisontella cyberfrågor och bidrar till att förbereda övningar och utvärdera resultatet av dem. Den har ett nära samarbete med kommittén för utrikes- och säkerhetspolitik, som har en central beslutsfattande roll avseende alla cyberrelaterade diplomatiska åtgärder. Eftersom cybersäkerhet är ämnesövergripande är det inte enkelt att samordna alla relevanta intressen; åtminstone 24 arbetsgrupper och förberedande organ har nyligen hanterat cyberrelaterade frågor.[30]

Europeiska rådet är stats- och regeringschefernas särskilda forum. Rådet framlägger visioner om EU-samarbetets utveckling, exempelvis genom att förhandla om nya fördrag eller medlemmar inom unio-

[28] EU:s makt varierar således mellan olika politikområden.
[29] Kenealy, Daniel et al (red). 2015. The European Union: How does it work?
[30] Europeiska unionens råd, EU cybersecurity roadmap, 8901/17, 2017-05-11.

nen. Europeiska rådets huvuduppgift är enligt tidigare att bestämma EU:s generella politiska riktning och prioriteringar, dvs. att fastställa EU:s politiska dagordning. Europeiska rådet antar slutsatser, där särskilda frågor av betydelse för EU och huvuddragen i särskilda åtgärder som ska vidtas eller mål som ska uppnås anges.

EU-parlamentet företräder medlemsländernas medborgare och består av direktvalda parlamentariker. Europaparlamentet fattar beslut tillsammans med rådet och ska även kontrollera EU-kommissionen.

Europeiska kommissionen är den största institutionen och företräder det all-europeiska intresset. Kommissionen tar initiativ till lagstiftning och verkställer den politik som beslutas om inom EU. Sakfrågorna sköts i så kallade generaldirektorat som hanterar olika politikområden.[31] Kommissionen strävar efter att stärka resurser och samverkan kring cybersäkerheten, göra EU till en starkare spelare avseende cybersäkerhet och integrera detta i övrig EU-politik.

Kommissionens olika generaldirektorat ansvarar för olika delar avseende cybersäkerhet. Generaldirektoratet för kommunikationsnät, innehåll och teknik (DG CONNECT) har det huvudsakliga ansvaret för cybersäkerhet som sådant, medan Generaldirektoratet för migration och inrikesfrågor (DG HOME) ansvarar för cyberbrottslighet. När det gäller investeringar (nationella och regionala) för att bidra till att EU når målen om smart och hållbar tillväxt utgör EU:s struktur- och investeringsfonder ett viktigt inslag. Det kan handla om forskning och innovation, stöd till små företag samt digital teknik. Likaså har DG GROW ett ansvar för att främja cybersäkerhetsindustri och underlätta företagens tillgång till finansieringsmekanismer.[32]

[31] Blomgren, Magnus & Bergman, Torbjörn (2005), EU och Sverige: Ett sammanlänkat statsskick.
[32] Arbetsgruppen för säkerhetsunionen (Security Union Task Force) inrättades för att spela en central roll i samordningen av kommissionens olika generaldirektorat i syfte att stödja säkerhetsunionens agenda. DG CONNECT är ordförande i arbetsgruppens underarbetsgrupp om cybersäkerhet.

EU-organ

Enisa

Enisa är ett av de viktigaste organen för EU:s cybersäkerhetspolitik. Byrån inrättades ursprungligen 2004 och dess mandat har förlängts vid ett antal tillfällen fram till 2019 när den genom cybersäkerhetsakten fick ett permanent mandat.[33] Enisa har i uppdrag att utföra de uppgifter som den tilldelas genom EU:s cybersäkerhetsakt och andra unionsrättsakter på cybersäkerhetsområdet genom att bl.a. tillhandahålla rådgivning och expertis och fungera som unionens informations- och kunskapscentrum. Enisa bör skapa förtroende för den inre marknaden genom sin opartiskhet, högkvalitativa råd och ett kompetent utförande av sina uppgifter i fullt samarbete med unionens institutioner, organ och byråer samt medlemsstaterna. Genom en uppsättning uppgifter fastställer cybersäkerhetsakten hur Enisa ska uppnå sina mål samtidigt som flexibilitet i verksamheten eftersträvas.[34] Uppnående av målen förutsätter att Enisa samarbetar med berörda aktörer i EU.[35]

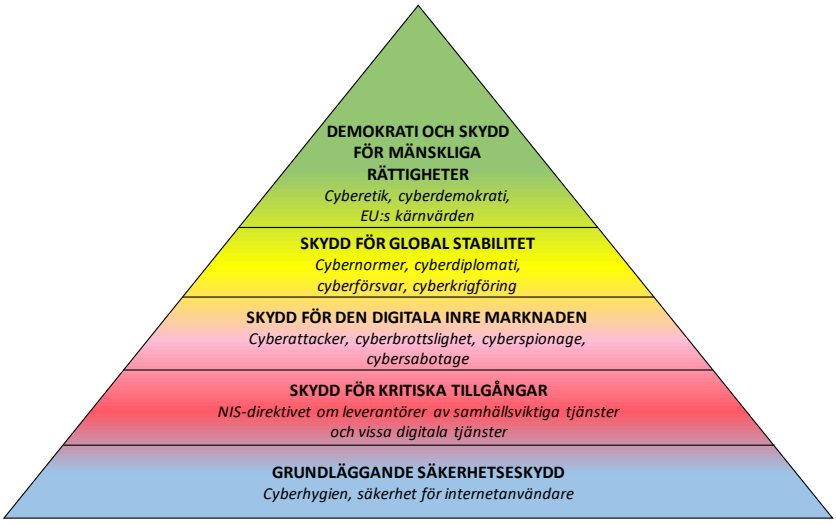
Enisa genomför bl.a. ett omfattande och kontinuerligt arbete för att kartlägga den generella hotbilden mot it-system. Arbetet har pågått under ett antal år och resulterat i flera rapporter. *Enisa threat landscape report 2018* tar upp 15 hotområden inom cybersäkerhet. En annan rapport tar upp ett antal risker och rekommendationer kopplat till upphandling och inköp av it-produkter och it-tjänster.[36]

För att höja den totala nivån av online-säkerhet i Europa organiserar byrån varje oktober en medvetenhetskampanj, ”The European Cybersecurity Month”, med stöd av NIS-kontaktpunkter i alla medlemsstater.[37]

När det gäller cyberrymden förespråkar EU:s cybersäkerhetsbyrå Enisa en strategi som sammanhängande hanterar olika behovsnivåer som rör cyberrymden (se nedan figur 3.1) Varje EU-strategi bör – enligt byrån – täcka alla aspekter av cyberrymden för att kunna möta morgondagens cyberutmaningar.

[33] Aktuell cybersäkerhetsbyrå efterträder den byrå som inrättades genom förordning (EU) nr 526/2013.
[34] Skäl 17 och 20.
[35] Skäl 44 ff.
[36] Några av de risker som lyfts fram, utöver misstag och insiderhot, är missförstånd kring faktisk kravbild runt säkerhetsfunktioner, oklar ansvarsfördelning vid incidenter, bristande styrning av leverantörens underleverantörer samt bristande kompetens hos leverantörens personal.
[37] För en närmare beskrivning av Enisas mandat enligt cybersäkerhetsakten, se kapitel 4.

Figur 3.1 Enisas perspektiv på skyddsbehov i cyberrymden



Källa: Enisa. Se ENISA overview of cybersecurity and related terminology, version 1, september 2017, s. 4. Figurens engelska text är översatt till svenska av utredningen.

Enisa framhåller att välgrundade och kontinuerliga hot- och riskbedömningar är viktiga verktyg för både offentliga och privata organisationer. Avsaknaden av standardiserade tillvägagångssätt för att klassificera och kartlägga cyberhot eller utföra riskbedömningar har inneburit en avsevärd variation av innehållet i bedömningarna, något som utgjort en utmaning för en konsekvent EU-omfattande strategi för cybersäkerhet.[38]

Förslag till Europeiskt kompetenscentrum för cybersäkerhet[39]

2018 föreslog kommissionen att det skulle inrättas ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning samt ett nätverk av nationella samordningscentrum, vilket

[38] Europeiska ekonomiska och sociala kommittén, Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks, mars 2018.
[39] En granskning som Europeiska revisionsrätten gjort visar att det på cybersäkerhetsområdet krävs en övergång till en resultatkultur med inbyggda utvärderingsmetoder för att säkerställa meningsfullt ansvarstagande och meningsfull utvärdering. Revisionsrätten konstaterade vidare att det fanns vissa luckor i lagstiftningen och att den befintliga lagstiftningen inte införlivats konsekvent av medlemsstaterna. Det kan göra det svårt att utnyttja lagstiftningen fullt ut. (Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet Briefingdokument, mars 2019, s. 52).

utgjorde en del av cybersäkerhetspaketet från 2017.[40] Lagstiftningsförslaget är särskilt utformat för att ta itu med fragmentering och dubbelarbete. En drivande faktor bakom nätverket av kompetenscentrum för cybersäkerhet och ett kompetenscentrum för forskning har varit att åtgärda de brister som NIS-direktivets kooperativa strukturer inte löser eftersom de inte utformades för att stödja utvecklingen av spetslösningar.

Europeiska utrikestjänsten

Europeiska utrikestjänsten (EEAS) har en ledande roll inom it-försvar, cyberdiplomati och strategisk kommunikation samt driver ett underrättelse- och analyscentrum. EEAS har till uppgift att göra EU:s utrikespolitik mer samstämmig och effektiv. EEAS stödjer genomdrivandet av EU:s utrikes- och säkerhetspolitik, sköter diplomatiska förbindelser och strategiska partnerskap med länder utanför EU och samarbetar med EU-ländernas utrikesministerier, Förenta nationerna (FN) och andra ledande aktörer. Man strävar efter att upprätthålla EU:s kärnvärden och främja en fredlig, öppen och transparent användning av cyberteknik. EEAS och kommissionen upprättar också i nära samarbete med medlemsstaterna strategiska länkar och dialoger om internationell cyberpolitik och säkerhet för informations- och kommunikationsteknik. EEAS ska även garantera säkerheten genom den gemensamma säkerhets- och försvarspolitiken (GSFP).

För att stärka sin agenda när det gäller styrning av cyberrymden har EU formaliserat sex cyberpartnerskap[41] i syfte att upprätta regelbundna politiska dialoger som strävar efter att bygga tillit och gemensamma samarbetsområden.

EU:s gemensamma enhet för hybridhot,[42] som är en del av Europeiska utrikestjänsten, inrättades för att förbättra situationsmedvetenheten och stödja EU:s strategiska beslutsfattande genom utbyte av analyser. Enheten har fokus på indikationer och varningar avse-

[40] Europeiska kommissionen, Förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum, COM(2018) 630 final, 2018-09-12.
[41] USA, Kina, Japan, Sydkorea, Indien och Brasilien.
[42] EU:s gemensamma enhet för hybridhot inrättades 2016 inom Europeiska utrikestjänstens underrättelse- och lägescentral. Den tar emot och analyserar sekretessbelagd information och information från öppna källor från olika aktörer angående hybridhot.

ende hybridhot mellan EEAS, kommissionen (inklusive EU:s myndigheter) och medlemsstaterna. I arbetet med analys av globala frågor beaktas cyberdomänen.[43] Enheten måste dock, enligt Europeiska revisionsrätten, bredda sin expertis inom cybersäkerhet.[44]

Europeiska försvarsbyrån

Europeiska försvarsbyrån (EDA) strävar efter att utveckla it-försvarskapaciteten. EDA arbetar i enlighet med cybersäkerhetsstrategin med att involvera cyberförsvarsdimensionen i EU:s cybersäkerhetsarbete. Det handlar bl.a. om förmågeutveckling och att främja civil-militär samverkan och synergier med andra policys avseende cyber inom EU.

EDA driver också en serie cyberövningar för att koordinera hanteringen av cybersäkerhetsincidenter på politisk nivå och möjliga konsekvenser av en offensiv cyberattack.

Computer Emergency Response Team (CERT-EU)[45]

EU:s Computer Emergency Response Team (CERT-EU) inrättades 2012 med målet att effektivt och ändamålsenligt besvara informationssäkerhetsincidenter och cyberhot för EU:s institutioner, organ och byråer. Kommissionen har några av sina it-säkerhetsexperter i CERT-EU:s kärnteam tillsammans med experter från generalsekretariatet från rådet, Europaparlamentet, Regionkommittén och Ekonomiska och sociala kommittén. Också Enisa bistår CERT-EU. Teamet arbetar under strategisk övervakning av en interinstitutionell styrelse.

CERT-EU förser EU:s institutioner, organ och byråer med rapporter om och genomgångar av cyberhot mot dem. CERT-EU samarbetar också med andra CERT-funktioner i medlemsstaterna samt med specialiserade it-säkerhetsföretag; de utbyter information om hur man hanterar hot.

[43] FOI Memo 6150, Initiativ avseende cybersäkerhet i EU, 2017-10-20.
[44] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 35.
[45] Se allmänt om CERT-nätverk i avsnitt 3.4.

Europols europeiska it-brottscentrum (EC3)

European Cybercrime Center (EC3) inrättades 2013 inom Europol som ett resultat av EU:s interna säkerhetsstrategi. EC3 arbetar, tillsammans med cyberbrottlighetsenheten på DG HOME, med att stärka rättsväsendets svar på gränsöverskridande cyberbrottslighetenen inom EU. EC3 ska särskilt fokusera på tre typer av cyberbrottslighet: den utförd av organiserade kriminella grupper, den som medför allvarlig skada för offren (såsom barnpornografi) och den som påverkar kritisk infrastruktur och kritiska informationssystem inom EU.

EC3 har inrättat ett antal rådgivande grupper med aktörer från den privata sektorn, EU:s institutioner och byråer samt andra internationella organisationer för att förbättra samarbetet genom nätverkande och strategiskt underrättelseutbyte. De arbetar enligt planer i linje med målen för EU:s policycykel.[46]

3.4 Samarbeten och nätverk

Inledning

Flera tvärgrupper inom EU och nätverk som inbegriper olika typer av aktörer har etablerats för att öka samsyn och stärka utvecklingen på cybersäkerhetsområdet.

I detta avsnitt beskrivs några av de samarbetsforum och nätverk som etablerats internt på EU-nivå eller internationellt i syfte att öka cybersäkerheten.

FoP on Cyber Issues/Horizontal Working Party on Cyber Issues

Implementeringen och uppföljning av relevanta strategier och frågor som berör EU:s internationella cyberpolitik har hanterats övergripande i den tillfälliga arbetsgruppen inom rådet, Friends of the Presidency Group on Cyber Issues (Ordförandeskapets vängrupp för cyberfrågor). FoP tillsattes av Coreper (de ständiga representanternas kommitté) 2012 i syfte att förbättra det horisontella arbetet, öka medlemsstaternas insyn och stärka samordningen såväl internt

[46] Se www.europol.europa.eu/empact (2020-09-14).

som externt avseende cyberfrågor i vid mening. Gruppen skulle utgöra ett strategiskt verktyg för unionens övergripande politiska mål på området. Under hösten 2013 fattades beslut om att utsträcka FoP-gruppens mandat med ytterligare tre år.

Under 2016 bildades ”Horizontal Working Party on Cyber Issues”. Genom denna vill rådet säkerställa en plattform för att stödja ett sammanhängande angreppssätt avseende cyberpolitiska frågor, genom att ge en översikt över de tvärgående frågorna, och därigenom undvika fragmenterad policyutveckling och beslutsfattande. Gruppen ska vidare hjälpa till att identifiera EU:s cyberprioriteringar och strategiska mål som en del av en omfattande politisk ram och stödja samarbete och samverkan, både inom rådet, mellan medlemsstater och mellan EU och medlemsstaterna. Gruppen arbetar bl.a. med ramverket för en EU-gemensam cyberdiplomati.

NIS Cooperation Group

Genom NIS-direktivet etableras ett samarbete på EU-nivå för att främja strategiskt samarbete och informationsutbyte. Denna ska bestå av representanter för medlemsstaterna, kommissionen och Enisa. Samarbetsgruppen ska arbeta i tvååriga arbetsprogram inom fyra olika områden: planering, styrning, informationsdelning och rapportering. Verksamheter inom de olika områdena är exempelvis vägledning för det nätverk av CSIRT som också etableras i och med direktivet, stöd till medlemsstater i kapacitetsuppbyggnad, diskussion kring standarder samt informationsutbyte om risker, incidenter och forskning.

Computer Security Incident Response Team (CSIRT)

Vid en genomgång 2011 av medlemsländernas insatser för att skydda kritisk informationsinfrastruktur från it-attacker och avbrott identifierades åtgärder för att upprätta ett nätverk av organisationer för incidenthantering (CERT). Detta då händelser visat att det behövs ett väl fungerande nätverk med statliga/nationella organisationer för incidenthantering och att man behöver se över frågor på statlig nivå rörande säkerheten hos ny teknik som t.ex. datormoln. Även om en majoritet av medlemsländerna hade upprättat nationella organisationer för incidenthantering behövdes det internationella samarbetet ut-

vecklas. Kommissionen behövde därför arbeta med medlemsländerna och den privata sektorn, på olika nivåer, för att upprätta CERT i resten av medlemsländerna och för EU:s institutioner och utveckla en europeisk beredskapsplan för it-incidenter. Likaså behövde övningsverksamheten stärkas upp, både på nationell och europeisk nivå.

I NIS-direktivet (artikel 12) fastställs att ett nätverk av CSIRT (Computer Security Incident Response Team) behövs för att bidra till förtroende mellan medlemsstaterna och för att främja effektivt operativt samarbete. Nätverket består av representanter från nationella CSIRT och företrädaren för EU, CERT-EU. Detta erbjuder ett forum för samarbete, utbyte av information och förtroendeskapande. Avsikten är att stärka förmågan hos nationella CSIRT att hantera gränsöverskridande incidenter och koordinera insatser för att bekämpa attacker. Enisa utgör sekretariatet och stödjer arbetet, bl.a. med expertis.

European Judicial Cybercrime Network (EJCN)

EU avser att underlätta för utredande myndigheter att få tillgång till krypterad information. Sommaren 2016 inrättade EU the European Judicial Cybercrime Network (EJCN) med målet att underlätta utbyte av sakkunskap och bästa praxis, förbättra samarbetet mellan behöriga rättsliga myndigheter vid hanteringen av cyberrelaterad brottslighet och utredning, samt att främja dialog för att säkerställa rättssäkerhet i cyberrymden. EJCN ska samarbeta med Eurojust och Europol för att stärka internationellt rättsligt stöd och etablera ett bättre samarbete med internetleverantörer.

EU:s internationella samarbeten

EU har dialoger med externa parter såsom G7 och FN samt med länder utanför västvärlden. Detta avsnitt beskriver vilken typ av frågor man samarbetar kring i de mer utvecklade internationella samarbetena.

EU-NATO Technical Arrangement

EU och Nato har samarbetat kring cybersäkerhetsfrågor sedan 2010, och sedan 2011 har NATO Computer Incident Response Capability (NCIRC) samarbetat med CERT-EU i och med den senares grundande. 2016 tecknade EU och Nato en teknisk uppgörelse mellan CERT-EU och nämnda NCIRC för att motverka, upptäcka och svara på cyberincidenter. Uppgörelsen var ett led i implementeringen av EU:s ramverk för cyberförsvar, och utgör i sig ett ramverk för delande av bl.a. teknisk information och utbyte av bästa praxis för incidenthantering och säkra konfigurationer för nätverk.

I juli 2016 kom Europeiska rådet, EU-kommissionen och Nato med ett gemensamt meddelande avseende det strategiska samarbetet. Cybersäkerhet och -försvar angavs som ett av sju områden där man behövde utöka koordineringen sinsemellan, inbegripet såväl insatser som utbildning och övning. EU och Nato ska utbyta koncept om integrering av it-försvarsaspekter i planering och utförande av respektive uppdrag och insatser för att främja interoperabilitet i krav och standarder för it-försvar. Man ska vidare stärka utbildningssamarbetet genom att harmonisera utbildningskraven, i förekommande fall, och öppna respektive utbildningskurser för ömsesidigt deltagande av tjänstemännen. Man ska också främja samarbete inom forskning och teknisk innovationsverksamhet avseende it-försvar genom att utveckla kopplingar mellan EU, Nato och NATO CCD COE (Cooperative Cyber Defence Centre of Excellence), för att utforska innovation på området för it-försvar. Med hänsyn till att it-området omfattar dubbla användningsområden kommer EU och Nato att öka interoperabiliteten i standarderna för it-försvar genom medverkan av industrin, när så är relevant. En åtgärd är att också stärka samarbetet i it-insatser genom ömsesidigt deltagande av tjänstemän i övningar, inklusive framför allt Cyber Coalition och Cyber Europe.

US-EU Cyber Related Work Streams – Cyber Dialogue

2010 grundande EU och USA en arbetsgrupp för cybersäkerhet och cyberbrottslighet. Gemensamma intressen föranledde att man 2014 fördjupade samarbetet genom en s.k. cyberdialog, som förs av höga representanter från EU och USA. Dialogen erbjuder ett forum för strategiska diskussioner och samarbete gällande exempelvis inter-

nationella utvecklingar inom cyberrymden, främjande och skydd av de mänskliga rättigheterna online samt kapacitetsutveckling inom cyber i tredjeländer.

Samarbeten med näringslivet

NIS-plattformen

EU:s cybersäkerhetsstrategi resulterade i bildandet av en offentlig-privat plattform för nätverks- och informationssäkerhet. Syftet var att sammanföra relevanta europeiska parter för att identifiera god cybersäkerhetspraxis över hela värdekedjan och skapa gynnsamma marknadsvillkor för utvecklandet och anammandet av säkra IKT-lösningar. NIS-plattformen kompletterar och bidrar till implementeringen av NIS-direktivets åtgärder och harmoniserar dess tillämpning i Europa. Plattformen är uppdelad i tre skilda arbetsgrupper:

– riskhantering, vilket bl.a. innefattar arbete med medvetandehöjning, informationssäkring och riskmätning,
– informationsutbyte och samordning av incidenter, vilket bl.a. innefattar incidentrapportering och riskmätningar med avseende på informationsutbyte, och
– forskning och innovation för säker IKT.

Contractual Public Private Partnership on cybersecurity

För att kunna leverera i enlighet med strategierna om cybersäkerhet och den digitala inre marknaden (se avsnitt 3.2) initierades ett offentligt-privat partnerskap om cybersäkerhet (cPPP) under 2016, genom en överenskommelse mellan kommissionen och the European Cyber Security Organisation (ECSO) som företräder marknadsaktörer inom cybersäkerhet. EU investerar i initiativet inom ramen för forsknings- och innovationsprogrammet Horisont 2020, men marknadsaktörerna förväntas investera betydligt mer. Samarbetet omfattar också parter från nationella, regionala och lokala myndigheter, forskningscentrum och universitet. Syftet är att på ett tidigt skede i forsknings- och innovationsprocessen främja samarbete och skapa cybersäkerhetslösningar för olika sektorer, t.ex. energi, hälsa, transport och finans.

Slutmålet med partnerskapet är att stimulera den europeiska konkurrenskraften och bidra till att överbrygga fragmenteringen av cybersäkerhetsmarknaden.

3.5 Cybersäkerhet och standardisering

I detta avsnitt redogörs närmare för begreppen cybersäkerhet och standardisering.

Begreppet cybersäkerhet

Det finns ingen standardiserad, allmänt accepterad definition av cybersäkerhet. I stort handlar det om alla typer av skydd och åtgärder som införs för att försvara informationssystem och deras användare mot obehörig åtkomst, angrepp och skada, för att säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet.[47] Det finns en något bredare definition av termen cybersäkerhet som omfattar även bevarande av spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation hos information i cyberrymden.[48]

Cybersäkerhet inbegriper förebyggande, detektering och hantering av samt återställning efter cyberincidenter. Incidenter kan vara planerade eller oplanerade och t.ex. omfatta oavsiktligt röjande av information, angrepp mot företag och kritisk infrastruktur, stöld av personuppgifter och till och med inblandning i demokratiska processer. Allt detta kan ha omfattande skadliga effekter på individer, organisationer och samhällen.

Som en term som används i EU-politiska kretsar är cybersäkerhet inte begränsat till nätverks- och informationssäkerhet. Termen omfattar all olaglig verksamhet som inbegriper användning av digital teknik i cyberrymden. Cybersäkerhet kan därför innefatta sådan itbrottslighet som att initiera datorvirusangrepp och genomföra kontantlösa betalningsbedrägerier, men också brottslighet i gränslandet mellan system och innehåll, t.ex. spridning av material med sexuella

[47] I EU:s cybersäkerhetsakt definieras cybersäkerhet som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot” (artikel 2.1). Se Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 7.
[48] SIS, Terminologi för informationssäkerhet, teknisk rapport SIS-TR 50:2015, 2015-10-27.

övergrepp mot barn online. Termen kan också omfatta desinformationskampanjer för att påverka onlinedebatten och misstänkt inblandning i val. Dessutom ser Europol ett samband mellan it-brottslighet och terrorism.[49]

Olika aktörer – inbegripet stater, kriminella grupper och ”hacktivister” – anstiftar cyberincidenter med olika motiv som bakgrund. Konsekvenserna av dessa incidenter är kännbara på nationell, europeisk och till och med global nivå. Men internets immateriella och i stor utsträckning gränslösa natur samt de verktyg och den taktik som används gör det ofta svårt att identifiera gärningsmannen bakom ett angrepp (det s.k. tillskrivningsproblemet).

De olika typerna av cybersäkerhetshot kan klassificeras enligt hur uppgifterna påverkas – antingen genom röjande, ändring, förstörelse eller nekad åtkomst – eller enligt de grundläggande informationssäkerhetsprinciper som överträds. I takt med att angreppen mot informationssystem blir allt mer sofistikerade blir försvarsmekanismerna mindre effektiva.[50]

Enligt Enisa behöver det inte finnas en definition av cybersäkerhet i den konventionella bemärkelsen att vi tenderar att tillämpa definitioner för enkla saker som autentisering av en identitet. Problemet är att cybersäkerhet är en omslutande term, och det är inte möjligt att skapa en definition som täcker omfattningen av de saker som begreppet täcker. Därför bör en kontextuell definition, baserad på en som är relevant, passande och som redan används av en viss standardiseringsorganisation eller annan berörd organisation övervägas. T.ex. definieras cybersäkerhet vid International Telecommunications Union (ITU) enligt följande.

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and

[49] Europol, Internet Organised Crime Threat Assessment 2017.
[50] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet Briefingdokument, mars 2019, s. 7 f. samt Europeiska cybersäkerhetsorganisationen (Ecso), European Cybersecurity Industry Proposal for a contractual Public-Private Partnership, juni 2016.

> user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
> • Availability
> • Integrity, which may include authenticity and non-repudiation
> • Confidentiality.[51]

På grund av områdets bredd förekommer olika definitioner hos standardiseringsorganisationer och andra organisationer.

I fråga om den närmare terminologin har Enisa rekommenderat följande.

> Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack).[52]

Enisa har även förklarat att cybersäkerhet innefattar alla aktiviteter som är nödvändiga för att skydda cyberrymden, dess användare och påverkade personer från cyberhot. Cybersäkerhet täcker alla aspekter av förebyggande, prognostisering, tolerans, detektering, begränsning, borttagning, analys och utredning av cyberincidenter[53]. Med tanke på de olika typerna av komponenter av cyberrymden anser Enisa att cybersäkerhet bör täcka följande attribut: tillgänglighet, tillförlitlighet, säkerhet, konfidentialitet, integritet, underhållbarhet (för fysiska system, information och nätverk), konfidentialitet, överlevnadsförmåga, resiliens (för att stödja dynamiken hos cyberrymden), tillräknelighet, autenticitet och oavvislighet (för att stödja informationssäkerhet).[54]

[51] Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity.
[52] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, v1.0, December 2015, s. 30.
[53] Med cyberincident förstås varje händelse som påverkar någon av komponenterna i cyberrymden eller dess funktion, oberoende av om det är naturligt eller mänskligt skapat, illvillig eller icke-illvillig avsikt, avsiktlig, oavsiktlig eller på grund av inkompetens eller operationella interaktioner. Också varje incident som genereras av någon av cyberrymdkomponenterna, även om skadan/störningen eller dysfunktionen orsakas utanför cyberrymden, kallas cyberincident (ENISA overview of cybersecurity and related terminology, version 1, september 2017, s. 6).
[54] ENISA overview of cybersecurity and related terminology, version 1, September 2017, s. 6.

Enisa uppmuntrar standardiseringsorganisationer att anamma begreppet cybersäkerhet som tillhandahållandet av säkerhetsfunktioner att tillämpas på cyberrymden. Skydd mot cyberhot avser mekanismer som syftar till att inrätta försvarsåtgärder som gör det möjligt att minska sannolikheten för manifestation av cyberhändelser eller attacker som kan härröra från återstående hot och som kan orsaka någon form av skador eller störningar i system eller deras komponenter. Cyberförsvar är fakulteten för systemen att motstå sådana negativa händelser om och när de inträffar trots förebyggande och skyddsåtgärder. Detta innebär att man känner igen, svarar på och återhämtar sig från cyberhoten. Cyberresiliens innebär i vissa sammanhang kombinationen av cybersäkerhet och cyberförsvar.

Cybersäkerhet kräver samarbete mellan offentlig och privat sektor, först och främst genom utbyte av information och bästa praxis. Tillit är avgörande på alla nivåer för att skapa rätt miljö för utbyte av känslig information över gränserna. Dålig samordning leder till fragmentering, dubbelarbete och utspridd expertis. Ändamålsenlig samordning kan leda till påtaglig framgång. Trots de framsteg som har gjorts under de senaste åren är tillitsnivåerna fortfarande otillräckliga på EU-nivå[55] och i vissa medlemsstater[56].

EU:s institutioner och byråer har saknat gemensamma definitioner på cybersäkerhetsområdet. NIS Cooperation Group har emellertid utformat en relevant incident-taxonomi[57] i syfte att underlätta effektivt gränsöverskridande samarbete.

Vidare har EU-kommissionens gemensamma forskningscentrum (JRC) tagit fram en omarbetad forskningstaxonomi med utgångspunkt i olika internationella standarder. Tanken är att den ska bli en referenspunkt som kan användas som ett index av forskningsorganisationer i hela Europa.[58]

[55] Europeiska kommissionen, Impact assessment, proposal for a regulations of the European parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final, 2018-09-12.
[56] Europeiska unionens råd, Slutrapport om den sjunde omgången av ömsesidiga utvärderingar om det praktiska genomförandet och verkan av europeisk politik för förebyggande och bekämpning av it-brottslighet, 12711/1/17 REV 1, 2017-10-09.
[57] NIS Cooperation Group, Cybersecurity Incident Taxonomy, CG Publication 04/2018, juli 2018.
[58] JRC:s tekniska rapporter, karta över europeiska cybersäkerhetsexpertcentrum: Definitioner och taxonomi. Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final, 2018-09-12.

Sammanfattning

Utredningen kan mot bakgrund av det ovan angivna konstatera att det förekommer olika defintioner av begreppet cybersäkerhet bland stratgi- och policydokument och berörda aktörer. Utredningen har uppdraget att analysera behovet av kompletterande nationella bestämmelser med anledning av EU:s cybersäkerhetsakt och utgår följaktligen från den definition av cybersäkerhet som anges i cybersäkerhetsakten, dvs. ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”. Utredningen kan notera att denna definition beaktar den antagonistiska faktorn.[59]

Standarder

Inledning

Standardisering syftar till att förenkla för verksamheter i samhället. Bl.a. kan en effektiv marknad skapas när lagstiftningen sätter de övergripande kraven av allmänt intresse och där standardisering skapar lösningar för en mer detaljerad nivå.[60] Dessutom syftar en sådan metod till att undvika nationella särkrav. Standarder erbjuder verksamheter möjligheter att arbeta utifrån beprövade erfarenheter, vilket också skapar förutsättningar för bättre säkerhet. Digitaliseringen och den snabba teknikutvecklingen leder till behov av nya standarder.[61] För närvarande finns det begränsade EU-omfattande standarder för certifiering.[62]

Standarder förutsätter ett samarbete och samförstånd mellan företrädare för olika samhällsintressen. Standardisering avser att tillgodose behov och önskemål från många olika parter och att så långt möjligt möta olika intressen. Standarder ökar också transparensen mellan organisationer, vilket underlättar kravställning och bedömning av säkerhetsnivåer i produkter, system och hela verksamheter.

[59] Begreppet cybersäkerhet kan därmed användas på sådant sätt att det innefattar såväl skydd av nätverk och infrastrukturer som innehåller information, som skyddet av den information dessa innehåller.
[60] Standarder är frivilliga verktyg som ger hjälp att följa lagstiftningen.
[61] Jfr Europeiska kommissionen, Prioriteringar för informations- och kommunikationsteknisk standardisering på den digitala inre marknaden, COM(2016) 176 final, 2016-04-19.
[62] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019.

Standarder är relevanta vid kontrollorgans arbete med cybersäkerhetscertifiering, särskilt då berörda organ för bedömning av överensstämmelse ska uppfylla kraven i vanliga standarder för behövlig ackreditering.

Standardiseringsarbete med avseende på informationssäkerhet kopplat till ISO (International Organization for Standardization) har utvecklats till att omfatta flera arbetsgrupper med olika inriktningar, däribland säkerhetsevaluering.

Standarder ska ge en lägsta skyddsnivå när det gäller väsentliga krav som fastställs i direktiv. Det ska också finnas möjlighet att bestrida en produkts överensstämmelse eller att kunna påtala fel eller brister hos de standarder som harmoniserats.

Nedan redogörs för ett urval av samarbeten inom europeisk cybersäkerhetsstandardisering.

Common Criteria Recognition Arrangement (CCRA)

Den huvudsakliga utvecklingen av standarden *Common Criteria* (se nedan) som används inom cybersäkerhetscertifiering sker inom den internationella organisationen *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, vanligen benämnd *Common Criteria Recognition Arrangement* (CCRA).

CCRA avser både en internationell överenskommelse och en samarbetsorganisation för ömsesidigt erkännande av certifikat. Samarbetsorganisationen har formats av de länder som signerat CCRA-överenskommelsen. Ett övergripande mål med samarbetet är att granskning av it-säkerhet i produkter och system ska ske med hög tillförlitlighet och konsistens genom att CC används för kravställning. Därigenom ökar den nationella säkerheten och förtroendet för produkterna. Överenskommelsen förutsätter också att deltagarna har som mål att förbättra tillgängligheten till utvärderade säkerhetsförbättrade it-produkter och skyddsprofiler, undvika duplicering av utvärderingar av dessa samt att kontinuerligt förbättra effektiviteten i evaluerings- och certifieringsprocessen.

CCRA verkar således för att öka antalet säkra it-produkter och försöker minska kostnaderna som uppstår i samband med certifiering genom att effektivisera metodiken. Överenskommelsen eftersträvar

en situation där it-produkter och skyddsprofiler som erhållit ett CC-certifikat kan anskaffas eller användas utan behov av ytterligare evaluering. De utfärdade CC-certifikaten erkänns av alla CCRA:s signatärer. CCRA accepterar enbart statliga certifieringsorgan.

För närvarande är 31 nationer medlemmar i CCRA. Av dessa är 17 länder (däribland Sverige) utfärdare av certifikat inom CC.

Sveriges Certifieringsorgan för IT-säkerhet (CSEC) vid FMV är signatär för Sverige i CCRA. Signatärskapet innebär bl.a. att CSEC avger Sveriges röst i samband med att nya länder söker medlemskap i CCRA.

Standarden Common Criteria (CC)

Common Criteria (CC) är en internationellt erkänd standard med standardbeteckningen ISO/IEC IS 15408 innehållande evalueringskriterier för it-säkerhet. Den beskriver hur man kan specificera krav på säkerhetsfunktioner och assurans.[63] CC är sammanläggning av tre olika standarder, varav den äldsta it-säkerhetsstandarden kallas *the Orange Book*.[64] Kanada tog fram en liknande men anpassad standard och sedermera tog även Europa fram en europeisk standard (ITSEC).[65]

CC har utvecklats i nära samarbete mellan flera länders säkerhetsmyndigheter och anses många gånger vara obligatoriskt för it-produkter i kritiska infrastrukturer.

CC fokuserar på det behov av it- och informationssäkerhet som uppstår på grund av avsiktliga eller oavsiktliga hot utgående från krav på sekretess, riktighet och tillgänglighet. Säkerheten hos it-produkter och it-system ska utvärderas av ett oberoende organ och certifieras sedan av ett certifieringsorgan som bekräftar giltigheten av utvärderingsresultaten. Standarden erkänns internationellt av flera av världens ledande länder inom it-säkerhet. Forskning har emellertid visat att certifieringsregler och tekniska skydd inte är tillräckliga

[63] Evalueringskrav finns fördefinierade enligt sju assuransnivåer (EAL 1 till 7).
[64] Till en början handlande skapandet av en standard för granskning av it-säkerhet nästan enbart om operativsystemet.
[65] ITSEC-standarden kompletterades dessutom med en överenskommelse kallad Senior Officials Group – Information Security – Mutual Recognition Agreement, SOGIS – MRA, där myndigheterna i länderna som skapade ITSEC kom överens om att lita på varandras granskningar genomförda enligt standarden. När européerna utvecklade ITSEC blev dock amerikanska leverantörer tvungna att först granska mot Orange book i USA och sedan mot ITSEC i något av de anslutna europeiska länderna och vice versa.

för att uppnå fullgod it-säkerhet, bl.a. då certifierade produkter förhållandevis enkelt kan användas på fel sätt.[66]

CC är således ett ramverk som används vid kravställning och utvärdering av produkters it-säkerhet. Kraven definieras på ett standardiserat format i en produktsäkerhetsdeklaration, även kallad evalueringsmål (Security Target, ST), eller i en skyddsprofil (Protection Profile, PP). Ett evalueringsmål beskriver säkerhetsbehoven för en specifik produkt, t.ex. en brandvägg från en specifik leverantör. Skyddsprofilen anger säkerhetsbehoven för en viss typ av produkt, t.ex. en viss typ av brandvägg.[67]

Kraven på säkerhet ställs utifrån två aspekter:[68]

- Säkerhetsegenskaper – vilka säkerhetsegenskaper behövs för att möta de potentiella hoten?
- Assuranskrav – hur noggrant bör säkerhetsegenskaperna evalueras?

CC för evaluering av it-säkerhet består av tre delar:

- en introduktion till metoden och allmän modell (del 1),
- funktionella säkerhetskomponenter (del 2), och
- assuranskrav (del 3).

Säkerheten verifieras i de ovan nämnda skyddsprofilerna, PP, och i ST beskrivs närmare vilka tillgångar som ska skyddas, vilka hot som man ska kunna stå emot och vilken förmåga en tänkbar angripare har att göra ett angrepp.[69]

Nästa del i CC är ett stöd i arbetet att välja bra säkerhetsfunktioner. Den delen är en katalog av väldefinierade funktioner. Det är små delkrav som leverantören lägger in i sin ST. När listningen är färdig är det dags för produkten att verifieras. Del 3 av CC är ett brett utbud av granskningsåtgärder som man kan genomföra för att verifiera säkerheten.

---

[66] Synpunkt från FOI 2020-06-17.
[67] Standarden reglerar inte vem som sätter kraven.
[68] CC ställer inte några egna krav på it-säkerhet utan är snarare ett slags formulär som hjälper beställaren att själv effektivt formulera kraven.
[69] Om det är en avancerad angripare som man vill skydda sig mot ställer CC mycket höga krav på designen. Produkten utsätts då också för fler och mer omfattande penetrationstester. Standarden anpassar sig alltså till det anspråk på säkerhetsnivå som leverantörer gör.

Ett evalueringsföretag (It Security Evaluation Facility, ITSEF) testar och verifierar produkten mot de krav som ställts. Evalueringsföretaget är licensierat av certifieringsorganet och oberoende av leverantören.[70] Evalueringsföretaget rapporterar till certifieringsorganet som därefter lämnar en certifieringsrapport.[71]

Europeisk samverkan – SOG-IS MRA

Senior Officials Group Information Systems Security (SOG-IS) är en grupp av nationella it-säkerhetsexperter som utsågs av EU:s ministerråd i början av 1990-talet. Samtidigt anmodade rådet att de medlemsstater som arbetade aktivt med evaluering och certifiering av it-säkerhet skulle skapa ett avtal om ömsesidigt erkännande av certifieringar av it-säkerhetsprodukter inom Europa. Med denna anmodan som grund ingick dessa medlemsstater *Mutual Recognition Agreement of Information Technology Security Evalution Certificates*. Överenskommelsen benämns SOG-IS MRA *(Senior Officials Group Information Systems Security – Mutual Recognition Agreement)* och liknar CCRA, men är endast öppet för EU och EEA-länder.[72]

Deltagare i SOG-IS MRA är statliga organisationer eller myndigheter från länder i EU som representerar deras land eller länder. Överenskommelsen föreskriver att länderna kan delta antingen som certifikatutgivare eller certifikatkonsumenter. Överenskommelsen har för närvarande 17 länder som medlemmar (däribland Sverige).[73]

Medlemmarna arbetar tillsammans för:

- att koordinera standardiseringen av CC-skyddsprofiler och certifieringspolicyer mellan europeiska certifieringsorgan för att ha en gemensam position i den snabbt växande internationella CCRA-gruppen, och
- att koordinera utvecklingen av skyddsprofiler när EU-kommissionen lanserar ett direktiv som ska genomföras i nationell rätt.

[70] I Sverige finns för närvarande två licensierade evalueringsföretag som utför sådana testningar: Combitech och Atsec.
[71] Certifieringsprocessen beskrivs även i kapitel 5.
[72] SOGIS-överenskommelsen framställdes som svar på EU-rådets beslut den 31 mars 1992 (92/242/EEG) inom informationssystemets säkerhet och efterföljande rådets rekommendation den 7 april (1995/144/ EG) om säkerhet för informationsteknologi utvärderingskriterier.
[73] Av dessa är sju (Frankrike, Tyskland, Italien, Nederländerna, Norge, Spanien och Sverige) certifikatutgivare.

SOG-IS MRA ger möjlighet att ömsesidigt erkänna it-produkters säkerhet upp till EAL 4. För evalueringsnivåer däröver, s.k. högassuransgranskning på nivå EAL 5–7, är grundregeln ett ömsesidigt godkännande inom specifika teknikområden (t.ex. smarta kort), vilket regleras genom tilläggsavtal. SOG-IS MRA tillämpar således såväl Common Criteria som ITSEC[74] och används som verktyg då CCRA inte bedöms lämpligt.

Standardiseringsorganisationer

CEN-CENELEC Focus Group on Cybersecurity (CSCG) analyserar den tekniska utvecklingen och dess betydelse för den digitala inre marknaden, utvärderar hur standarder kan stödja inriktning och regelverk avseende cybersäkerhet och dataskydd samt utformar rekommendationer för internationella standarder. Eftersom det är av stor vikt att undvika dubbelt och överlappande standardiseringsarbete står koordinering av standardiseringsarbete i fokus för CSCG.

I den av CSCG publicerade vitboken *Recommendations for a Strategy on European Cybersecurity Standardisation* ges rekommendationer om digital säkerhet som en väsentlig tillgång för digital suveränitet och ett digitalt samhälle. Rekommendationerna understryker vikten av standardisering av cybersäkerhet för att fullborda den europeiska inre marknaden och höja nivån av cybersäkerhet i Europa generellt. Gruppen har för övrigt bl.a. rekommenderat att kommissionen bör etablera en tydlig och gemensam förståelse för omfattningen och innebörden av begreppet cybersäkerhet i EU.

Därutöver finns ett flertal andra organisationer som är delaktiga i standardiseringsaktiviteter relaterade till cybersäkerhet. Den europeiska standardiseringsorganisationen CEN är en oberoende och icke-statlig organisation med 34 europeiska länders standardiseringsorgan som medlemmar. Svenska Institutet för Standarder (SIS) är medlem och representerar Sverige i organisationen.

[74] Information Technology Security Evaluation Criteria (ITSEC) från 1990 är en uppsättning kriterier för it-säkerhetsevaluering skapade av Storbritannien, Frankrike, Tyskland och Nederländerna under åren 1988–1991. ITSEC har till stor del ersatts av Common Criteria.

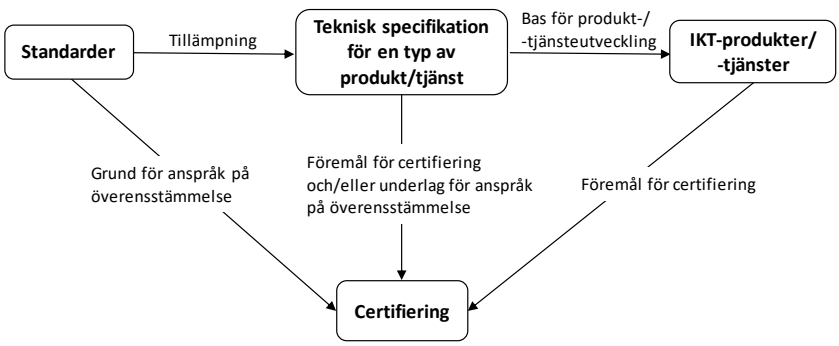
Standardisering till stöd för cybersäkerhetscertifiering

För att stödja skapandet av certifieringsordningar inom det europeiska ramverket för cybersäkerhetscertifiering är standardiseringsorganens roll viktig.[75] Standardiseringsorganisationerna kommer att tillhandahålla nödvändiga standarder till stöd för den ram som ska definieras av Enisa på begäran av kommissionen.

När det gäller standardiseringsaktiviteter har Enisa, utöver förbättringar av diverse samarbeten, bl.a. rekommenderat att standardiseringsorganisationer företrädesvis väljer att använda redan befintliga internationella standarder om sådana finns på det specifika området och att ISO/IEC JTC1/SC27 bör betraktas som den första referensen för cybersäkerhetsstandardisering.[76]

Standardernas typsika roll i evaluerings- och certifieringsprocessen avseende IKT illustreras i figuren nedan.

Figur 3.2 Standarders roll i cybersäkerhetscertifieringsprocessen



Källa: Enisa. Utredningen har översatt texten i originalfiguren till svenska.

Enisa har en viktig roll när det gäller skapandet av en harmoniserad ram för att utveckla standarder på lämplig nivå. Enisa rekommenderar bl.a. att EU:s löpande arbetsprogram för standardisering anpassas till unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering så att standardiseringsorganisationerna kan tillhandahålla lämpliga standarder för certifieringsordningarna. Enisa föreslår vidare att

[75] I t.ex. artikel 54.1 c i EU:s cybersäkerhetsakt anges att en europeisk ordning för cybersäkerhetscertifiering ska innehålla en hänvisning till standarder som följts vid utvärderingen, om lämpliga sådana finns.
[76] ENISA, Standardisation in support of the cybersecurity certification, December 2019, s. 23 f.

horisontella standarder (multisektoriella) för cybersäkerhet ska privilegieras i utvärderingen av cybersäkerhet. Man invänder även mot konkurrens mellan standardiseringsorganisationer och förespråkar i stället bättre samarbete mellan inblandade aktörer. När en internationell standard finns inom ett specifikt område och täcker en måldomän – åtminstone delvis – måste den enligt Enisa väljas i första hand. Enisa har även presenterat vissa konkreta förslag på vilka standarder som bör användas vid cybersäkerhetsstandardisering och -evaluering.[77]

[77] ENISA, Standardisation in support of the cybersecurity certification, December 2019.

4 EU:s cybersäkerhetsakt

4.1 Inledning

Det europeiska ramverket för cybersäkerhetscertifiering utgörs av EU:s cybersäkerhetsakt och de europeiska ordningar för cybersäkerhetscertifiering som ska antas (genomförandeakter).

I detta kapitel lämnas en närmare redogörelse för strukturen och bestämmelserna i EU:s cybersäkerhetsakt och vad som anges om innehållet i en europeisk ordning för cybersäkerhetscertifiering.

4.2 Bakgrund

Det internationella samfundets förmåga att hantera och begränsa cyberangrepp har påverkats av att det inte finns något internationellt ramverk för styrning av cybersäkerhet. Försöken att upprätta bindande internationella cyberrymdsstandarder har präglats av spänningar.[1] EU har etablerat ett antal strategiska partnerskap[2] på cybersäkerhetsområdet för att kunna föra regelbundna politiska diskussioner i syfte att bygga tillit och gemensamma samarbetsområden. Resultaten har varit blandade då EU inte setts som en stor aktör inom cybersäkerhet i det internationella samfundet.[3] EU:s förmåga att hantera cyberangrepp på politisk och operativ nivå vid en storskalig, gränsöverskridande incident har ansetts som begränsad, bl.a. på grund av att cybersäkerhet inte integrerats i befintliga samordningsmekanismer

[1] Vilket sågs bl.a. i bristen på samförstånd i FN-gruppen med myndighetsexperter 2017 (2016–2017 UN Group of Governmental Experts) om hur internationell lagstiftning bör tillämpas på staters hantering av incidenter. Se även Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 32.
[2] Med USA, Kina, Japan, Sydkorea, Indien och Brasilien.
[3] Europeiska säkerhets- och försvarsakademin (T. Renard och A. Barrinha), Handbook on cyber security, kap. 3.4 The EU as a partner in cyber diplomacy and defence, 2018-11-23.

för krishantering på EU-nivå.[4] NIS-direktivet var ett första steg för att främja en gemensam riskhanteringskultur genom införandet av säkerhetskrav bestående av rättsliga skyldigheter för de centrala ekonomiska aktörerna, särskilt leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster.

Under 2016 presenterade EU-kommissionen ett meddelande om ett stärkt system i Europa för cyberresiliens och främjande av en konkurrenskraftig och innovativ cybersäkerhetsbransch.[5] I meddelandet föreslog kommissionen att det skulle upprättas en ram för säkerhetscertifiering av IKT-produkter och IKT-tjänster (informations- och kommunikationsteknik) i syfte att öka förtroendet och säkerheten på den digitala inre marknaden. Enligt kommissionen framstod IKT-cybersäkerhetscertifiering som särskilt relevant mot bakgrund av den ökade användningen av teknik som krävde en hög nivå av cybersäkerhet, såsom uppkopplade och automatiserade bilar, elektronisk hälsovård och industriella automatiseringskontrollsystem (IACS).[6]

Europeiska unionens råd noterade att det krävdes ett fortsatt och närmare samarbete för att skydda EU mot cyberhoten, särskilt vad gällde att hantera gränsöverskridande storskaliga cybersäkerhetsincidenter. Vidare noterades att de cyberrelaterade hoten och sårbarheterna fortsatte att utvecklas och intensifieras. I slutsatserna bekräftades att Enisa-förordningen[7] utgjorde en av de centrala delarna av en EU-ram för cyberresiliens, och kommissionen uppmanades att vidta ytterligare åtgärder i frågan om certifiering på EU-nivå.[8] Inrättandet av ett certifieringssystem skulle kräva att det även inrättades ett lämpligt styrningssystem på EU-nivå, inklusive tillhandahållande av djupgående sakkunskap från ett oberoende EU-organ. Kommissionen angav i sitt meddelande 2017 om halvtidsöversynen av strategin

[4] Samarbetet kring tidiga varningar och ömsesidigt bistånd kräver också ytterligare utveckling, se Rådets slutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser, 10085/18, 2018-06-26.
[5] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén (KOM(2016) 410 slutlig): Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch.
[6] Det har funnits meningsskiljaktighet mellan stater om hur befintliga regler i internationell rätt ska gälla för staters användning av informations- och kommunikationsteknik (UNIDIR, The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century, 2017, s. 2).
[7] Europaparlamentets och rådets förordning (EU) nr 526/2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning.
[8] Rådets slutsatser om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch – den 15 november 2016.

för den digitala inre marknaden att den senast i september 2017 skulle se över Enisas mandat för att definiera dess roll i det förändrade cybersäkerhetslandskapet och ta fram förslag på standarder, certifiering och märkning på cybersäkerhetsområdet i syfte att öka cybersäkerheten hos IKT-baserade system.[9]

Den 4 oktober 2017 presenterade kommissionen ett förslag till en förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”).[10] Syftet med förslaget var att

– öka medlemsstaternas och företagens kapacitet och beredskap,
– förbättra samarbetet och samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ,
– öka EU:s förmåga att komplettera medlemsstaternas åtgärder, i synnerhet när det gäller gränsöverskridande cyberkriser,
– öka allmänhetens och företagens medvetenhet om cybersäkerhetsfrågor,
– öka den övergripande transparensen i fråga om assuransnivån för cybersäkerhet hos IKT-produkter och IKT-tjänster i syfte att stärka förtroendet för den digitala inre marknaden och för digital innovation, och
– undvika splittring av certifieringssystemen i EU och av de tillhörande säkerhetskraven och utvärderingskriterierna i de olika medlemsstaterna och sektorerna.

Den föreslagna reformen av Enisa, som förutsågs få en större operativ roll i hantering av storskaliga cybersäkerhetsincidenter, stöddes inte av medlemsstaterna, som hellre såg att byråns roll skulle stödja och komplettera deras egna operativa åtgärder.[11]

[9] Meddelande från Kommissionen om halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden, COM(2017) 228 final.
[10] Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå och) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).
[11] Europaparlamentets utredningstjänst, Briefing EU Legislation in Progress: ENISA and a new cybersecurity act, PE 614.643, september 2018. Det finns redan många CERT/CSIRT-enheter på medlemsstatsnivå, men deras kapaciteter varierar avsevärt.

4.3 EU:s cybersäkerhetsakt

4.3.1 Syfte och tillämpningsområde

Den 17 april 2019 antogs Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). EU:s cybersäkerhetsakt 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 cybersäkerhetsakten 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.

Det europeiska ramverket för cybersäkerhetscertifiering är avsett att bl.a. ge följande fördelar för företag och enskilda:[12]

- cybersäkerhetsakten ska stödja och underlätta utvecklingen av en europeisk cybersäkerhetspolitik genom att harmonisera villkoren och de materiella kraven för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster i EU,
- europeiska ordningar för cybersäkerhetscertifiering ska hänvisa till gemensamma standarder eller kriterier för utvärderings- och testmetoder, vilket bidrar till användningen av gemensamma säkerhetslösningar i EU och undanröjer hinder för den inre marknaden,
- cybersäkerhetsakten ska stödja och komplettera genomförandet av NIS-direktivet genom att förse de företag som omfattas av direktivet med ett verktyg för att visa att nät- och informationssäkerhetskraven uppfylls i hela unionen,
- de europeiska ordningarna för cybersäkerhetscertifiering ska ha företräde framför de nationella systemen och ersätter befintliga parallella nationella ordningar avseende samma IKT-produkter eller IKT-tjänster på en angiven tillförlitlighetsnivå,

[12] Se motiveringen i kommissionens förslag till cybersäkerhetsakten, COM (2017)477 final, s. 13.

– företag ska bara behöva certifiera produkten en gång, och certifikat som utfärdas enligt de europeiska ordningarna ska gälla i alla medlemsstater,
– företag ska få en kontaktpunkt för cybersäkerhetscertifiering inom EU, och
– en produkt eller tjänst ska – beroende på cybersäkerhetsbehov – certifieras enligt en högre eller lägre nivå av säkerhet.

EU:s cybersäkerhetsakt finns intagen som bilaga till delbetänkandet.

Enisas roll och uppgifter

Artiklarna 3–45 i EU:s cybersäkerhetsakt anger mål och uppgifter samt reglerar organisatoriska frågor som rör Enisa. Enisa ska främja spridningen av cybersäkerhetscertifiering i unionen, bl.a. genom att bidra till inrättandet och underhållandet av ett ramverk för cybersäkerhetscertifiering på unionsnivå (europeiskt ramverk för cybersäkerhetscertifiering). I en av kommissionen gjord utvärdering av Enisa noterades att EU:s strategi för cybersäkerhet inte samordnades i tillräcklig utsträckning och att detta ledde till bristande synergieffekter mellan Enisas verksamhet och andra aktörers.[13] EU:s cybersäkerhetsakt syftar till att stärka Enisas samordnande roll.[14] En mer översiktlig beskrivning av Enisas roll och uppdrag har lämnats i kapitel 3.

Ett övergripande europeiskt ramverk för cybersäkerhetscertifiering

I artiklarna 46–65 i EU:s cybersäkerhetsakt finns bestämmelser om ett övergripande europeiskt ramverk för cybersäkerhetscertifiering. Genom cybersäkerhetsakten skapas en ram för inrättandet av certifieringsordningar för IKT-produkter, IKT-tjänster och IKT-processer[15] (europeiska ordningar för cybersäkerhetscertifiering).

[13] Europeiska kommissionen, Study on the Evaluation of the European Union Agency for Network and Information Security, Final Report, 2017.
[14] Europeiska revisionsrätten, Utmaningar för en ändamålsenlig EU politik för cybersäkerhet, Briefingdokument, mars 2019, s. 41, och skäl 20 i EU:s cybersäkerhetsakt.
[15] Med sådana produkter, tjänster och processer avses delar, eller en grupp av delar, i nätverks- och informationssystem, tjänster som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem och verksam-

EU:s cybersäkerhetsakt inför 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 särskild IKT-produkt, IKT-tjänst eller IKT-process uppfyller kraven i en europeisk ordning för cybersäkerhetscertifiering.

En EU-försäkran om överenstämmelse eller ett europeiskt cybersäkerhetscertifikat ska intyga att produkterna, tjänsterna och processerna 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 dessa produkter, tjänster och processer.

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.[16]

I skäl 71 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. I ordningarna ska befintliga standarder användas i förhållande till de tekniska kraven och utvärderingsförfaranden som produkterna måste uppfylla. Inga egna tekniska standarder bör utvecklas.[17]

I EU:s cybersäkerhetsakt anges att certifieringsordningar som drivs av industrin eller andra privata organisationer inte bör ingå i cybersäkerhetsaktens tillämpningsområde.[18]

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, GDPR).[19]

---

heter som utförs för att utforma, utveckla, tillhandahålla eller underhålla en IKT-produkt eller IKT-tjänst (artikel 2.12–2.14).

[16] Skäl 93 och 95.

[17] När det gäller europeiska standarder ombesörjs detta av de europeiska standardiseringsorganisationerna, och det godkänns av Europeiska kommissionen genom offentliggörande i Europeiska unionens officiella tidning (se förordning (EU) nr 1025/2012).

[18] Skäl 73.

[19] Skäl 74 och artikel 1 andra stycket.

Cybersäkerhetsakten 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 sammanhanget produkterna och tjänsterna ska användas och den snabba tekniska utvecklingen. Därför bör det – enligt cybersäkerhetsakten – även fortsättningsvis 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.[20]

Kommissionen ska 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, -tjänster och -processer i unionen använder certifieringsordningarna, effektiviteten hos de europeiska ordningarna för cybersäkerhetscertifiering och huruvida bestämda ordningar borde 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.[21]

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 beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

[20] Skäl 92.
[21] Skäl 92.

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.[22]

I syfte att säkerställa en harmonisering och undvika fragmentering kommer nationella ordningar eller förfaranden för certifiering av IKT-produkter, -tjänster eller -processer som omfattas av en europeisk ordning för cybersäkerhetscertifiering upphöra att gälla från och med den dag som fastställs av kommissionen genom en sådan ordning (genomförandeakt).[23]

Medlemsstaterna får inte heller införa nya nationella ordningar för cybersäkerhetscertifiering av IKT-produkter, -tjänster eller -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.[24]

4.3.2 Artiklar i EU:s cybersäkerhetsakt

I detta avsnitt lämnas en översiktlig redogörelse för de artiklar i EU:s cybersäkerhetsakt som berör utredningens uppdrag.

Europeiskt ramverk för cybersäkerhetscertifiering

I *artikel 46* anges att 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.

[22] Se motiveringen i förslaget till cybersäkerhetsakten, COM (2017) 477, s. 12. Jfr även skäl 91, artikel 1 andra stycket och artikel 57 i cybersäkerhetsakten.
[23] Skäl 94.
[24] Skäl 94.

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.

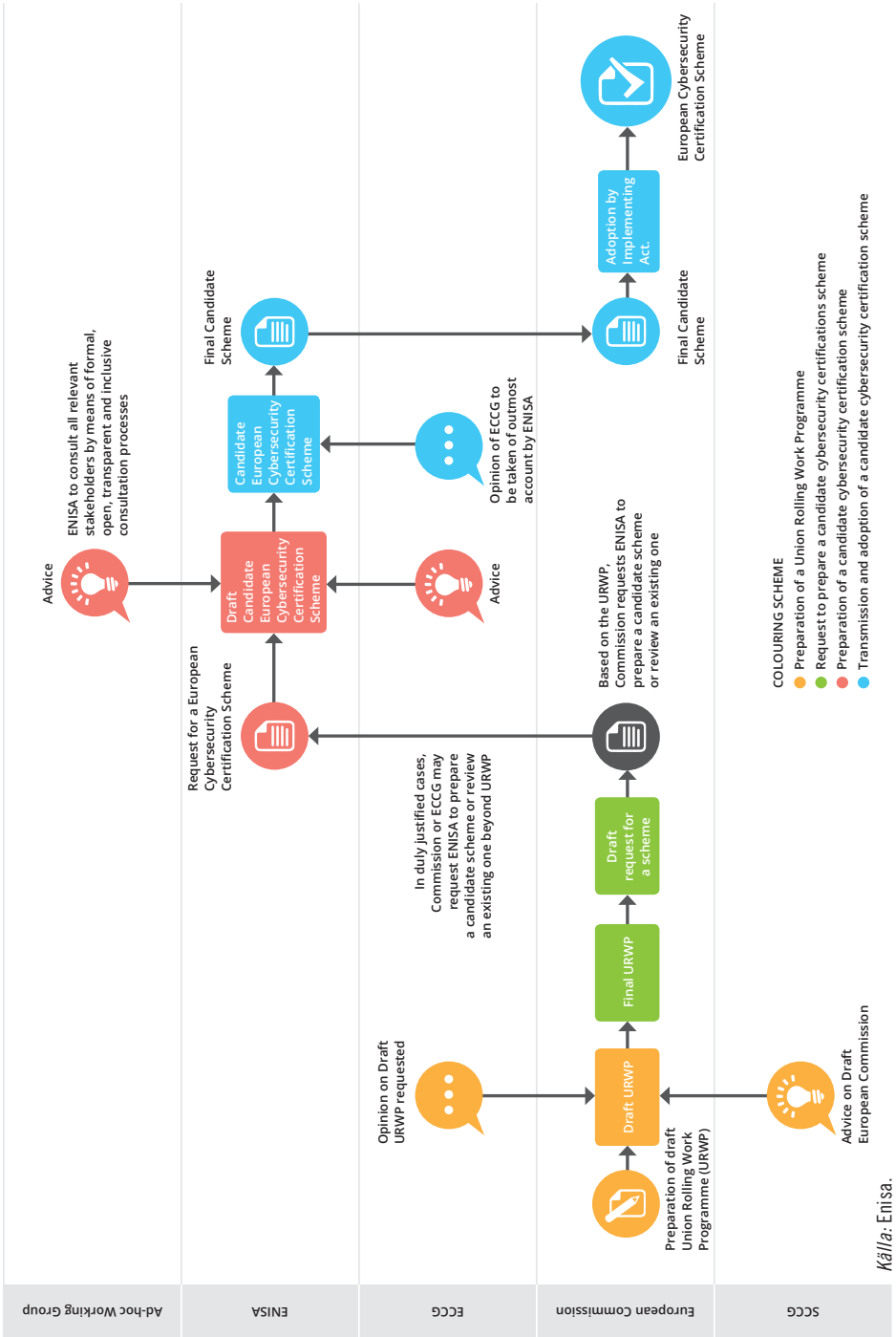
Begäran om en europeisk ordning för cybersäkerhetscertifiering

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 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 (se avsnitt 13.2.1).

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. Figuren nedan illustrerar förfarandet för framtagande av de europeiska ordningarna för cybersäkerhetscertifiering.

Figur 4.1 Europeiska certifieringsordningar



Källa: Enisa.

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

I *artikel 51* föreskrivs att en europeisk ordning för cybersäkerhetscertifiering ska vara utformad för att, i tillämpliga fall, uppnå minst de säkerhetsmålsättningar som anges i bestämmelsen.

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 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, -tjänsten eller -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, -tjänster och -processer med låg risk som motsvarar assuransnivån grundläggande. Denna typ av bedömning av överensstämmelse bedöms lämplig för IKT-produkter och -tjänster med lägre komplexitet som inte utgör en stor risk för det allmänna samhällsintresset.[25]

Komponenter i europeiska ordningar för cybersäkerhetscertifiering

Av *artikel 54* framgår att en europeisk ordning för cybersäkerhetscertifiering ska innehålla bl.a. 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 assurans-

[25] Skäl 79.

nivåerna överensstämmer med behoven hos ordningens avsedda användare.

En europeisk ordning för cybersäkerhetscertifiering kan möjliggöra både självbedömning av överensstämmelse och certifiering för IKT-produkter, -tjänster eller -processer. I dessa fall bör ordningen föreskriva tydliga möjligheter för konsumenter och andra användare att skilja mellan IKT-produkter, -tjänster eller -processer med avseende på vilken tillverkare eller leverantör av IKT-produkter, -tjänster eller -processer som har ansvar för bedömningen, och IKT som har certifierats av en tredje part.[26]

En bedömning av överensstämmelse avser det förfarande genom vilket man utvärderar om fastställda krav för en IKT-produkt, -tjänst eller -process har uppfyllts. Detta förfarande utförs av en oberoende tredje part som inte är tillverkaren eller leverantören av de IKT-produkter, -tjänster eller -processer som bedöms. Bedömning av överensstämmelse och certifiering utgör inte i sig någon garanti för att certifierade IKT-produkter och -tjänster är cybersäkra. De är snarare förfaranden och tekniska metoder för att intyga att IKT-produkter, -tjänster och -processer har testats och att de uppfyller vissa cybersäkerhetskrav som fastställs på annan plats, t.ex. i tekniska standarder.[27]

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, -tjänsten eller -processen. Assuransnivån bör därför stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, -tjänst eller -process.[28]

Kompletterande cybersäkerhetsinformation för certifierade IKT-produkter, IKT-tjänster och IKT-processer

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 bestämmelsen.

[26] Skäl 80.
[27] Skäl 77.
[28] Skäl 78.

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 *punkten 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 *punkten 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 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.

Av *punkten 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:

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.

I *punkten 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 *punkten 10* framgår att ett europeiskt cybersäkerhetscertifikat som utfärdats i enlighet med denna artikel ska erkännas i alla medlemsstater.

Nationella ordningar och certifikat för cybersäkerhetscertifiering

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, -tjänster och -processer som inte omfattas av en europeisk ordning för cybersäkerhetscertifiering får kvarstå.

Av *punkten 2* framgår att medlemsstaterna inte får införa nya nationella ordningar för cybersäkerhetscertifiering av de IKT-produkter, -tjänster och -processer som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.

Av *punkten 3* framgår att 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.

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.[29] Medlemsstaterna bör därför se till att antagandet av en europeisk ordning för cybersäkerhetscertifiering avspeglas i deras nationella lagstiftning.[30]

[29] Skäl 98.
[30] Skäl 104.

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 *punkten 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 *punkten 7 f*ramgår att nationella myndigheter för cybersäkerhetscertifiering bl.a. ska

- övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering,
- övervaka att 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,
- 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 artikel 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 *punkten 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 *punkten 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, -tjänster och -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 *punkten 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 *punkten 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 *punkten 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 *punkten 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 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

I *artikel 61.1* anges att de nationella myndigheterna för cybersäkerhetscertifiering ska anmäla till kommissionen 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 *punkten 2* följer att kommissionen ska, ett år efter ikraftträdandet av en europeisk ordning för cybersäkerhetscertifiering, offentliggöra en förteckning över de organ för bedömning av överensstämmelse som har anmälts.

Av *punkten 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

a) beslut avseende ett europeiskt cybersäkerhetscertifikat som innehas av fysiska och juridiska personer och som meddelats av den myndighet eller det organ som avses i artikel 63.1, och

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.

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 Cybersäkerhetscertifiering i Sverige

5.1 Inledning

I detta kapitel redogörs för den nationella ordningen för certifiering av it-säkerhet i system och produkter som tillämpas av certifieringsorganet CSEC vid Försvarets materielverk. Vidare lämnas en översiktlig redogörelse för några av de övriga myndigheter som hanterar frågor om cybersäkerhet. Avslutningsvis redogörs översiktligt för Samverkansgruppen för informationssäkerhet. Förslaget med att utveckla ett nationellt cybersäkerhetscenter har behandlats i avsnitt 2.3.4.

5.2 Bakgrund

Certifiering innebär godkänd revision. Certifiering är den process som utförs av ett certifieringsorgan som kan leda till utfärdandet av ett certifikat. Organ med uppgift att utfärda certifikat finns på många olika områden och dessa organ är normalt inte myndigheter. Certifikatet är ett offentligt dokument utfärdat av certifieringsorganet som bekräftar att en specifik produkt framgångsrikt genomgått utvärdering. Certifikatet kan t.ex. vara i form av en licens, ett diplom eller en legitimation. För att få ett certifikat ska organisationen ha genomgått en s.k. certifieringsrevision. Certifieringen består av en formell och oberoende utvärdering av produkter, tjänster och processer utifrån fastställda kriterier. Certifiering kan även avse personer. Oftast innebär certifieringsrevisionen att en extern revisor granskar organisationens processer och rutiner på det område som aktuell standard handlar om. Certifiering informerar och försäkrar köparna och användarna om säkerhetsegenskaperna hos produkterna och

tjänsterna. Genom att certifiera sig mot en standard visar man att sin organisation uppfyller kraven i den standarden.

Certifiering under ackreditering innebär att en organisation, produkt eller person av ett ackrediterat certifieringsorgan bedöms uppfylla krav som ställs i standarder eller andra styrdokument. Här görs det även regelbundna kontroller av att t.ex. certifierad personal håller sin kompetens uppdaterad eller att en certifierad produkt fortsätter att överensstämma med kraven.

Certifiering av t.ex. it-säkerhet består av ett formellt fastställande av resultatet från en evaluering,[1] och det finns alltså organ med uppgiften att fatta beslut om utfärdande av certifikat rörande it-säkerhet. CCRA och svensk standard EN ISO/IEC 17065:2012[2] innehåller krav på certifieringsorgans opartiskhet och oberoende. Behovet av certifieringsorgan för it-säkerhet grundar sig på att man med internationellt accepterade standarder kan bidra med tillit och förtroende (s.k. assurans) såväl inom som mellan organisationer, nationellt och internationellt. Inom cybersäkerhetsområdet finns i många länder myndigheter som utgör nationella certifieringsorgan för it-säkerhet; ofta med nära koppling till myndigheter med ansvar för nationell säkerhet eller landets regering.[3]

Utöver ett behov av generellt arbete för bättre cybersäkerhet har det funnits en efterfrågan från Försvarsmakten och it-industrin på ett svenskt system för att kunna evaluera och certifiera it-säkerhetsprodukter och system. Certifieringsfunktionen är sålunda att betrakta som ett stöd för såväl försvarssektorn som övriga delar av samhället, däribland näringslivet.[4]

I Sverige är det för närvarande endast det offentliga organet CSEC (vid FMV) som är erkänt inom CCRA och SOG-IS MRA och som certifierar enligt Common Criteria på it-säkerhetsområdet.

[1] I detta sammanhang ingår granskning att evalueringsarbetet genomförts med erforderlig noggrannhet och med utnyttjande av godkänd metodik samt att resultatet påvisat att evalueringsobjektet svarar mot någon viss kravnivå enligt givna evalueringskriterier. Certifiering utgör ofta ett väsentligt underlag vid ackreditering av system.
[2] Denna standard innehåller krav vid certifiering av produkter, processer och tjänster.
[3] SIS, Terminologi för informationssäkerhet, teknisk rapport SIS-TR 50:2015, 2015-10-27, s. 59.
[4] Viss översyn av verksamhet och organisation på informationssäkerhetsområdet, SOU 2010:25, s. 25.

5.3 Försvarets materielverk (FMV)

FMV:s organisation och uppgifter

Försvarets materielverk (FMV) ska i enlighet med Försvarsmaktens investeringsplan och uppdrag ansvara för upphandling av bl.a. varor och tjänster inom den del av materielförsörjningsområdet som inte omfattas av Försvarsmaktens upphandlingsansvar. FMV ska även biträda Försvarsmakten i bl.a. planeringen av materiel- och logistikförsörjningen samt med materielsystemkunskap. FMV ska också biträda Försvarsmakten med kompetens när det gäller upphandling och vidmakthållande.

FMV får inom sitt verksamhetsområde även tillhandahålla tjänster åt andra än Försvarsmakten.[5]

FMV är en s.k. industrisäkerhetsmyndighet enligt säkerhetsskyddslagen och har i betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) föreslagits bli tillsynsmyndighet enligt säkerhetsskyddslagen för försvarsföretag.

Genom stärkt internationell samverkan under 2019 har FMV bidragit till att ta fram ett ramverk för stöd till att hantera cyberhot, sårbarheter och motåtgärder – något som kan användas av säkerhetsexperter inom både stat och näringsliv. Arbetet är ett resultat av ett samarbete inom Multinational Industrial Security Working Group (MISWG) gällande strategier för nationell cybersäkerhet, policyer för nationell industrisäkerhet och bästa praxis i detta sammanhang. Mot bakgrund av att flera av deltagarländerna i MISWG redan har motsvarande nationella modeller kan dessutom harmonisering uppnås.[6]

FMV/CSEC har att, i samverkan med MSB, medverka i europeiska och internationella arbetsgrupper i syfte att utarbeta detaljerade krav på it-säkerhet och evalueringsmetodik för specifika typer av it-produkter av intresse för Sverige, t.ex. USB-minnen och databashanterare.

[5] FMV bedriver också försvarsunderrättelseverksamhet enligt 2 § förordningen (2000:131) om försvarsunderrättelseverksamhet.
[6] Samlad informations- och cybersäkerhetshandlingsplan 2019–2022, Redovisning mars 2020, s. 21.

FMV och det nationella certifieringsorganet CSEC

Enligt myndighetens instruktion (5 §) ska det vid FMV finnas ett nationellt certifieringsorgan för it-säkerhet i produkter och system. FMV/certifieringsorganet ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Inom FMV bedrivs arbetet av enheten CSEC (Sveriges Certifieringsorgan för it-säkerhet) som har en oberoende ställning inom myndigheten.[7]

CSEC verkar som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system enligt den internationella standarden Common Criteria (CC). CSEC ackrediterades som nationellt certifieringsorgan 2008. Swedac utövar regelbunden tillsyn över CSEC för att säkerställa att certifieringsorganet håller den standard som ligger till grund för ackrediteringen.[8]

CSEC:s huvuduppgifter är att utöva tillsyn över evalueringar, granska evalueringsrapporter, skriva certifieringsrapporter, utfärda certifikat och publicera en lista på certifierade produkter. Produkter som certiferats av CSEC används bl.a. av Försvarsmakten.

CSEC ska licensiera[9] evalueringsföretag och utöva tillsyn över deras verksamhet samt bidra med stöd och råd vid utnyttjandet av CC för kravspecifikation. CSEC deltar vidare i internationellt samarbete för tolkningar av CC och utveckling av standarder samt marknadsför CC.[10] CSEC har även haft till uppgift att utveckla en nationell certifieringsordning för it-säkerhet med regler och metoder för oberoende granskning[11] och se till att ordningen följs. CSEC:s verksamhet styrs bl.a. av standarden ISO/IEC 17065 och lagen om ackreditering och teknisk kontroll.

Chefen för CSEC ansvarar för att förvalta och vidareutveckla certifieringsordningen inom given budget och leder certifieringsorganets dagliga verksamhet inom ramen för certifieringsorganets uppgift.

[7] FMV:s överdirektör har ansvaret för certifieringsorganet i de frågor där oberoende krävs.
[8] Närmare bestämt är CSEC ackrediterat av Swedac som ett certifieringsorgan för säkerhet i it-produkter.
[9] Licensieringen sker efter de principer som tillämpas inom CCRA och SOG-IS MRA.
[10] CSEC ska medverka i svenska och internationella standardiseringsorgan och forum för att utveckla och förbättra standarder för kravställning och evaluering av it-säkerhet och kryptografi.
[11] I den tidigare lydelsen av FMV:s instruktion (SFS 2007:854) föreskrevs att certifieringsorganet skulle upprätta och driva en certifieringsordning för säkerhet i it-produkter och system.

Chefen rapporterar till myndighetens överdirektör i frågor som rör certifieringsorganets verksamhet.[12]

CSEC representerar Sverige inom CCRA (Common Criteria Recognition Arrangement) i rollerna som nationellt certifieringsorgan och signatär. CSEC:s arbete bedrivs inom ramen för CCRA där samverkan för närvarande sker mellan 31 länder och deras berörda myndigheter (varav 17 är ackrediterade att utfärda certifikat).[13] CSEC representerar även Sverige inom den europeiska organisationen SOG-IS MRA.[14] Medlemmarna i CCRA- och SOG-IS MRA-grupperna utövar tillsyn över CSEC och dess certifieringsordning i enlighet med respektive arrangemang. CSEC ingår för övrigt i Samverkansgruppen för informationssäkerhet (SAMFI, se avsnitt 5.10).

Mot bakgrund av Försvarsmaktens ansvar för kryptogodkännande verkar CSEC i nära samarbete med MUST (Militära underrättelse- och säkerhetstjänsten).[15]

Sveriges certifieringsordning för it-säkerhet

Under CSEC:s överinseende har en nationell certifieringsordning enligt CC inrättats för att säkerställa att utvärderingar av IKT-produkter och skyddsprofiler utförs enligt höga och konsekventa standarder.[16] Detta bidrar till förtroende för säkerheten i produkterna och profilerna. En certifieringsordning består av regler som gäller i certifieringsarbetet, dvs. inte bara tekniska krav utan samtliga regler om hur certifiering går till och vilka förutsättningarna är. CSEC är ägare av Sveriges certifieringsordning för it-säkerhet och har därmed haft ansvar för att utveckla och upprätthålla den. Vid implementeringen av ordningen verkar CSEC i enlighet med CCRA.[17] Certifieringsord-

[12] Överdirektörens befogenheter innefattar att godkänna CSEC-chefens beslut i ärenden rörande överklaganden.
[13] Evalueringsnivå (Evaluation Assurance Level, EAL) är en numerisk bedömning från 1–7 av hur ingående och rigorös en säkerhetsgranskning enligt Common Criteria är. EAL 1 är den mest grundläggande nivån och den billigaste att såväl implementera som utvärdera, medan EAL 7 därmed är den mest rigorösa och dyraste. I CCRA erkänns upp till EAL 2 generellt och upp till EAL 4 för godkända internationella skyddsprofiler.
[14] CCRA och SOG-IS MRA tillåter endast statliga certifieringsorgan.
[15] CSEC har i enlighet med mål i en handlingsplan för informationssäkerhet 2012 tagit fram en särskild kryptopolicy.
[16] För ett certifieringsorgan är ISO/IEC 17065, Conformity assessment – Requirements for bodies certifying products, processes and services, tillämplig i enlighet med regleringarna av CCRA, SOG-IS MRA och Swedac, för att säkerställa kvalitet på certifieringarna.
[17] Certifieringsordningen drivs också i enlighet med SOG-IS MRA.

ningar tillhandahåller ramar för internationellt erkännande av certifikat som utfärdats enligt respektive ordning. Den svenska certifieringsordningen ger grunder för utvärderingar och certifieringar genom att beskriva och genomföra nödvändiga rättsliga ramar och processer. Därmed upprätthålls principer om lämplighet, opartiskhet, korrekthet och effektivitet i alla utvärderingsaktiviteter.[18]

CSEC har tagit fram ett dokument som beskriver processen för klagomålshanteringen (SP-007 Quality Manual). CSEC dokumenterar och utreder alla formella klagomål som är riktade mot certifieringsaktiviteter där certifieringsorganet är ansvarigt. CSEC registrerar ändringsförfrågningar och hanterar identifierade avvikelser genom internrevisioner. Ställning tas till om klagomålet avser certifieringsverksamheten och klaganden informeras om att klagomålet tagits emot och att det kommer att behandlas som ett klagomål. Klagomålet ska sedan undersökas, vid behov med hjälp av oberoende tekniska experter. CSEC ska bestämma om åtgärder vidtagits på felaktiga grunder och upprätta en plan för genomförande av korrigerande åtgärder. Rapportering sker till Change Control Board och chefen för CSEC ansvarar för beslutet vid styrelsen om ett klagomål. När klagoärendet avslutats kommer ska kvalitetsansvarig (Quality Manager) se till att klaganden informeras om resultatet av klagomålet och informera denne om sin rätt att överklaga.

En klagande som inte är nöjd med ett beslut eller resultatet av ett klagomål som gäller certifieringsverksamheten kan lämna in ett överklagande.[19] För att bevara opartiskheten behandlas överklaganden av personal som inte är inblandad i det överklagade beslutet. Överklagandet hanteras av kvalitetsansvarig.[20] Beslutet om resultatet av överklagandet fattas av chefen för CSEC. Det beslutade utfallet av överklagandet ska godkännas av ledande befattningshavare.

Ömsesidigt erkännande av certifikat

Certifikat som utfärdas inom ramen för den svenska certifieringsordningen kan vara föremål för ömsesidigt erkännande enligt CCRA, EA MLA (The European cooperation for accreditation multilateral

[18] CSEC:s dokument SP-001, Certification and Evaluation Scheme – Scheme Overview, version 28.0, den 24 september 2019.
[19] Överklagandet ska göras inom 30 dagar efter det ursprungliga beslutet.
[20] Kvalitetsansvarig ska informera klaganden om förfarandets gång.

agreement) och SOG-IS MRA. Ett certifikat utfärdat av CSEC kan omfattas av alla dessa avtal. Det är möjligt att delta i en certifiering där endast ett av avtalen refereras till. Vilken överenskommelse om ömsesidigt erkännande som är tillämpligt på en specifik certifiering kommer att dokumenteras i certifieringsavtalet. En kund som ansöker om certifiering kan välja vilka avtal om ömsesidigt erkännande som certifieringen ska omfattas av.

Numera begränsas giltigheten av CC-certifikat som är ömsesidigt erkända inom CCRA och SOG-IS MRA över tid. Giltighetstiden är högst fem år från dagen för utfärdandet av certifikatet.

CCRA och SOG-IS MRA medför bl.a. inom krypto- och säkerhetsskyddsområdet endast ett begränsat ömsesidigt erkännande av certifikat. De nationella reglerna kring vilka kryptografiska funktioner som får användas, hur dessa ska kontrolleras och vem som får utföra kontrollerna kan vara mycket känsligt. De nationella reglerna har företräde framför såväl CCRA som SOG-IS MRA.

CSEC kan utfärda certifikat med krav på överensstämmelse mot CC på samtliga assuransnivåer, mot CCRA avseende CC-assuranskomponenter i antingen en gemensam skyddsprofil (collaborative Protection Profile, cPP) eller lägre assuransnivåer (EAL 1 och 2), samt mot SOG-IS MRA gällande assuransnivåerna 1–4[21]. CSEC kan också utfärda nationella certifikat som inte omfattas av något av de ovanstående avtalen om ömsesidigt erkännande och med krav på överensstämmelse mot CC på samtliga assuransnivåer.

Ömsesidigt erkännande enligt CCRA[22] av certifikat som utfärdats inom den nationella certifieringsordningen är föremål för vissa krav på själva ordningen, som att genomgå periodiska utvärderingar av andra deltagare i CCRA och uppfylla särskilda restriktioner för hantering av skyddad information som delas mellan deltagarna.

[21] Deltagarna i SOG-IS MRA accepterar CSEC som certifieringsorgan upp till assuransnivå 4.
[22] Detta gäller även SOG-IS MRA.

5.4 Myndigheten för samhällsskydd och beredskap (MSB)

Uppgifter

Myndigheten för samhällsskydd och beredskap (MSB) har ansvar för att stödja samhällets beredskap för olyckor, kriser och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en allvarlig olycka, kris, krig eller krigsfara.

MSB är också Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur enligt artikel 10.1 i rådets direktiv 2008/114/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna.

MSB är även nationell kontaktpunkt avseende NIS-arbetet, tillika nationell Computer Security Response Team (CSIRT) med tillhörande uppgifter enligt NIS-direktivet.

Vidare har MSB enligt sin instruktion till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet och har föreskriftsrätt inom samma område. MSB ska dessutom på informations- och cybersäkerhetsområdet analysera och bedöma omvärldsutvecklingen samt rapportera till regeringen om förhållanden som kan resultera i behov av åtgärder på olika nivåer och områden i samhället.[23]

MSB:s uppgifter inom området informations- och cybersäkerhet är bl.a. att ansvara för utveckling och förvaltning av säkra kommunikationer[24], vara råd- och stödgivande i informationssäkerhetsarbetet samt hantera respektive förebygga it-incidenter. MSB har också till uppgift att tillhandahålla kommunikationstjänster för ledning och samverkan inom och mellan samhällsviktiga verksamheter.

Vid myndigheten finns en avdelning för cybersäkerhet och säkra kommunikationer (CS). Avdelningen, som är indelad i enheter, bl.a. för strategi och samordning, operativ cybersäkerhet, incidenthantering, tekniska resurser och säkerhet i cyberfysiska system. Vidare finns en enhet för systematiskt informationssäkerhet som lämnar råd och stöd om det förebyggande arbetet inom informations- och cyber-

[23] 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.
[24] Inom området säkra kommunikationer ansvarar MSB för utveckling och förvaltning av Rakel, SGSI och WIS (myndighetens externa kommunikationstjänster).

säkerhetsområdet till andra statliga myndigheter, kommuner och regioner samt företag.

Myndigheten bedriver också verksamhet avseende Rakel och ledningssystem, bl.a. strategisk inriktning, utveckling och förvaltning av kommunikationstjänster som används för ledning och samverkan inom och mellan samhällsviktiga verksamheter.

MSB har nyligen lämnat förslag till föreskrifter och allmänna råd om informationssäkerhet för statliga myndigheter som skickats på remiss.[25] Föreskrifterna innehåller bestämmelser om säkerhetskrav och stipulerar bl.a. att myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av vissa standarder.

MSB har fått ett uppdrag av regeringen som avser att utforska hur ett utvecklat Rakel skulle kunna etableras för tillhandahållande av tjänster för mobil datakommunikatoin, varvid 5G-nät kan ingå som en komponent. MSB har påbörjat arbetet med att utveckla och etablera Rakel Generation 2 (Rakel G2).

Samverkan

MSB har en uttalad samordningsroll, och när det gäller övriga myndigheter med uppgifter inom området informationssäkerhet sker dessutom ett formaliserat samarbete. MSB har bl.a. till uppgift att inrikta och samordna civila myndigheters signalskyddsverksamhet och arbete med säkra kryptografiska funktioner[26]. Detta innebär att MSB beslutar om vilka civila myndigheter och andra samhällsviktiga verksamheter som kan tilldelas signalskyddssystem och säkra kryptografiska funktioner för möjlighet till säkrare samverkan.[27] MSB kan även ge ut kompletterande föreskrifter inom området, t.ex. om civila myndigheters kryptoberedskap.[28]

MSB deltar i internationella samarbeten som rör informations- och cybersäkerhet, t.ex. informationsdelning och samarbete mellan nordiska nationella CERT-funktioner och samarbete inom nätverket

[25] Förslag till revidering av föreskrifter (MSB 2016:1) om informationssäkerhet.
[26] Säkra kryptografiska funktioner används för att förhindra förlust av riktighet, tillgänglighet och konfidentialitet hos organisationens informationstillgångar.
[27] MSB använder inte föreskrifter för att ålägga aktörer krav på signalskydd utan bedömningen är individuell och behovsdriven. Man skriver sedan avtal med berörda om regleringen och fattar beslut om tilldelning av signalskydd (med stöd från FRA).
[28] Försvarsmakten leder signalskyddsverksamheten och arbetet med säkra kryptografiska funktioner. Försvarsmakten har också till uppgift att granska och att nationellt godkänna kryptosystem (se vidare avsnitt 5.7).

European Governmental CERTs (EGC), samt internationell samverkan kring säkerhet i it-produkter, säkerhet i industriella informations- och styrsystem och cybersäkerhet i finansiella tjänster. MSB deltar i EU-kommissionens expertgrupp European forum for member states (EFMS) och den privat-offentliga plattformen för nät- och informationssäkerhet (NIS-plattformen) samt representerar Sverige i Natos planeringsgrupp för industriella resurser och kommunikation (IRCSG). MSB deltar också aktivt i standardiseringsarbetet inom området informationssäkerhet.[29] I sitt arbete med Common Criteria ger MSB ut rekommendationer för användning av en skyddsprofil eller certifierad produkt.[30] MSB bedriver omvärldsbevakning kring CC-standarden både på nationell och internationell nivå för att i första hand kunna inventera och representera det civila samhällets behov av produktkategorier som är lämpliga att ta fram skyddsprofiler emot.

MSB har, i samråd med övriga myndigheter som ingår i SAMFI[31], tagit fram en nationell handlingsplan för samhällets informationssäkerhet. MSB har rollen som ordförande i arbetsgrupperna som SAMFI bildat och förvaltar en nationella handlingsplan för samhällets informationssäkerhet. Handlingsplanen publicerades 2012 och innehåller ett 30-tal åtgärder för att öka informationssäkerheten i samhället. Handlingsplanen har uppdaterats årligen för att kunna delredovisa och slutföra åtgärderna.[32]

MSB har även knutit till sig ett informationssäkerhetsråd med bred representation från både offentlig förvaltning och näringslivet: Cybersäkerhetsrådet. Cybersäkerhetsrådet ska i huvudsak bistå MSB med information om utvecklingstrender inom området informationssäkerhet.

I dagsläget administrerar MSB fem forum för informationsdelning om informationssäkerhet (FIDI, se nedan): FIDI-SCADA, FIDI-Vård och omsorg, FIDI-Drift, FIDI-Telekom och FIDI-Finans.

MSB:s medverkan i samarbetsgruppen och nätverket för nationella Computer Security Incident Response Teams (CSIRT) inom ramen

[29] Standardiseringen med avseende på informationssäkerhet bedrivs i huvudsak inom ramen för Svenska institutet för standarders (SIS) arbete kopplat till ISO:s (International Organization for Standardization) grupp ISO/IEC JTC 1/SC 27 IT Security Techniques.
[30] Förvaltningen av en referenslista över rekommenderade skyddsprofiler kommer att ingå i MSB:s löpande arbete för vidareutveckling av stöd inom it-säkerhet.
[31] Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Post- och telestyrelsen (PTS), Säkerhetspolisen och Polismyndigheten.
[32] MSB, Nationell handlingsplan för samhällets informationssäkerhet, Slutrapport, mars 2016.

för NIS-direktivet har skapat ett strategiskt samarbete och informationsutbyte mellan medlemsländerna på cybersäkerhetsområdet. Samarbetet skapar även mervärde inom områden såsom bevakning av framväxande teknologier.

CERT-SE

CERT-SE är Sveriges nationella Computer Emergency Response Team med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Verksamheten bedrivs vid MSB.

CERT-SE:s tjänster riktar sig till såväl offentlig sektor som näringslivet och till uppgifterna hör bl.a. att vid it-incidenter sprida information, att samarbeta med andra aktörer på informationssäkerhetsområdet och att vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla informationsutbytet med dessa.[33]

CERT-SE strävar efter att öka it-säkerhetsmedvetandet i Sverige genom att förmedla kunskap och fakta. CERT-SE utfärdar kontinuerligt varningar och råd om sårbarheter i it-system.

CERT-SE är medlem i flera internationella nätverk som TF-CSIRT (Task Force – Collaboration of Security Incident Response Teams), FiRST (Forum of Incident Response and Security Teams), IWWN (International Watch and Warning Network), EGC (European Government CERT), CNW (CSIRT's Network for EU-members) och NCC (Nordic CERT Cooperation).

Forum för informationsdelning om informationssäkerhet (FIDI)

FIDI (forum för informationsdelning om informationssäkerhet) är privat-offentliga samverkansfora som syftar till att genom informationsutbyte, omvärldsanalys och produktion av gemensamt informationsmaterial öka informationssäkerheten hos alla deltagande aktörer. Som tidigare anförts finns FIDI-nätverk inom olika sektorer.

Det övergripande målet med FIDI-nätverken är att skapa förutsättningar för att förbättra säkerheten i de sektorer där FIDI-nätverk finns och därigenom bidra till förbättrad nationell säkerhet.

[33] CERT-SE stöttar för övrigt polismyndigheten i vissa utredningar avseende it-relaterad brottslighet.

Den information som delas inom FIDI-nätverken ska avse hot, sårbarheter eller incidenter inom informations- och cybersäkerhetsområdet. Man eftersträvar lösningar för att hantera identifierade risker, och informationen ska kunna ligga till grund för säkerhetshöjande åtgärder som initieras av enskilda deltagande organisationer eller av flera organisationer tillsammans.

FIDI-nätverken är sektorsspecifika och består förutom en eller flera representanter, tillika administratörer, från MSB, av utvalda medlemmar verksamma inom sektorn. Medlemmarna ska vara stora aktörer inom den sektor som nätverket täcker. De representanter som företagen skickar ska ha mandat att diskutera informations- och cybersäkerhetsfrågor och kunna se till att erhållen information inkorporeras i det dagliga säkerhetsarbetet.

Det finns flera exempel där FIDI-nätverk kompletteras av andra nätverk inom samma eller närliggande områden, som PTS samverkansforum inom telekom, exempelvis Nationella telesamverkansgruppen (NTSG).

5.5 Post- och telestyrelsen (PTS)

Post- och telestyrelsen (PTS) är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation. Av 1 § förordningen (2007:951) med instruktion för Post- och telestyrelsen framgår att PTS är en förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten ska verka för att målen inom politiken för informationssamhället uppnås. Myndigheten ska även, inom ramen för sina uppgifter enligt lagen (2003:389) om elektronisk kommunikation, verka för att de mål som anges i denna lag uppnås.

Myndigheten ska beskriva och analysera utveckling och resultat inom sitt ansvarsområde och rapportera detta till regeringen. Myndigheten ska särskilt uppmärksamma och analysera eventuella problem inom området och, när det är påkallat, vidta eller lämna förslag till lämpliga åtgärder. Myndigheten ska vidare regelbundet göra strategiska analyser inom området för elektronisk kommunikation och redovisa den långsiktiga inriktningen av myndighetens tillämpning av regleringen på området.

Det anges också i 4 § i förordningen (2007:951) med instruktion för Post- och telestyrelsen att PTS inom området för elektronisk kommunikation bl.a. har till uppgift att

- främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att tillse att samhällsomfattande tjänster finns tillgängliga,
- följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation,
- pröva frågor om tillstånd och skyldigheter och utöva tillsyn enligt lagen (2003:389) om elektronisk kommunikation,
- meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation,
- utöva tillsyn enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,
- utöva tillsyn enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,
- verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, samt verka för ökad krishanteringsförmåga,
- verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,
- lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet, och
- vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I 7 § samma förordning anges att PTS beträffande EU-arbetet och annat internationellt samarbete bl.a. ska utreda behovet av och medverka vid tillkomsten av överenskommelser mellan Sverige och andra länder, handlägga frågor som rör Sveriges deltagande i verksamheten inom internationellt samarbete och delta i nationellt och internationellt standardiseringsarbete.

Tidigare var PTS det behöriga organ som fick begära råd och stöd enligt Europaparlamentets och rådets förordning (EU) nr 526/2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).[34]

PTS arbetar med informationssäkerhet i enlighet med sin instruktion och lagen om elektronisk kommunikation. PTS har tagit fram en vägledning för användare om hur man kan anskaffa robust kommunikation. Råd lämnas bl.a. om hur man ställer adekvata krav vid anskaffningen och hur man identifierar kritiska funktioner genom en risk- och sårbarhetsanalys.

PTS har alltså ansvar för tillsyn eller andra uppgifter inom områdena elektronisk kommunikation, post, kontanthantering, betrodda tjänster och digitala tjänster (bl.a. molntjänster och internetbaserade marknadsplatser). När det gäller betrodda tjänster innefattar PTS tillsyn verksamheter som granskats och certifierats av oberoende organ för bedömning av överensstämmelse.

PTS har under 2019 analyserat möjligheter till att öka spårbarheten i betrodda tjänster, exempelvis elektroniska underskrifter och stämplar. Analysen har diskuterats med europeiska tillsynsmyndigheter. Frågan kommer att lyftas av flera tillsynsmyndigheter i samband med den pågående översynen av eIDAS-förordningen. Det förväntade resultatet av åtgärden, på lång sikt, är ett ökat skydd i transaktioner baserade på kvalificerade certifikat.

I syfte att öka säkerheten i nätverk har PTS tillsammans med teleoperatörer tydliggjort vilka egenskaper som ur ett regionalt perspektiv bör eftersträvas för att öka motståndskraft och uthållighet i allmänt tillgängliga elektroniska kommunikationsnät.

PTS ingår även i SAMFI (se avsnitt 5.10).

[34] Se tidigare lydelse av 7 § i SFS 2019:191. Ändringen har påkallats av Enisa-förordningens upphävande genom Cybersäkerhetsakten.

5.6 Försvarets radioanstalt (FRA)

Försvarets radioanstalt (FRA) bedriver verksamhet främst inom områdena signalunderrättelsetjänst och informationssäkerhetstjänst. Det förstnämnda är att på uppdrag av regeringen och de myndigheter som regeringen bestämmer. Syftet är att kartlägga yttre militära hot och andra utländska förhållanden som kan påverka Sveriges säkerhet, t.ex. internationell terrorism och cyberhot mot samhällets infrastruktur. Det andra området avser informationssäkerhet där FRA har ett expertuppdrag sedan 2003. FRA ska enligt sin instruktion ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och statliga bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.[35]

FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. Bland myndighetens tjänster ingår också forensisk analys, teknisk rådgivning och utbildning i it-säkerhet. Vid informationssäkerhetsanalyser kontrolleras sårbarheter i uppdragsgivarens it-system och en bild ges av vilka brister som behöver åtgärdas.

FRA ska vidare samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. Myndigheten deltar både i bilaterala och multilaterala internationella samarbeten för informationsdelning inom informations- och cybersäkerhetsområdet. FRA har även till uppgift att förse civila myndigheter, kommuner och företag med säkra kryptografiska funktioner.

FRA har, i samverkan med Säkerhetspolisen, tillgängliggjort Tekniskt detekterings- och varningssystem (TDV) till flera av de mest skyddsvärda verksamheterna.

[35] Vid myndigheten finns en forsknings- och utvecklingsenhet med uppgift att metodiskt upptäcka och analysera sårbarheter i informationsmiljöer.

5.7 Försvarsmakten

Försvarsmaktens övergripande ansvar är att upprätthålla och utveckla ett militärt försvar. Myndigheten ska kunna försvara Sverige och främja svensk säkerhet genom insatser nationellt och internationellt.[36] Uppgifterna inbegriper cyberförsvar, vilket är ett område där Försvarsmakten intensifierat utvecklingen av sin förmåga under de senaste åren. Vidare ska myndigheten med befintlig förmåga och resurser kunna lämna stöd till civil verksamhet.

Försvarsmaktens ansvar på informationssäkerhetsområdet omfattar säkra kryptografiska funktioner, säkerhetsskydd och signalskydd. Säkerhetsskyddstjänsten förebygger bl.a. att uppgifter som omfattas av sekretess och som rör rikets säkerhet inte röjs, och att endast personer som är pålitliga utifrån säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet. Bland säkerhetsskyddsåtgärder ingår att lämna stöd till andra myndigheter inom området säkra kommunikationer. Signalskyddstjänsten förhindrar att obehöriga får insyn i, eller kan påverka totalförsvarets telekommunikationer. Signalskydd omfattar även användning av krypton i it-system.

Militära underrättelse- och säkerhetstjänsten (Must) vid Högkvarteret leder och ansvarar för Försvarsmaktens verksamhetsområde underrättelse- och säkerhetstjänst. Vid Must finns ett säkerhetskontor, en säkerhetsunderrättelseavdelningen, en säkerhetsskyddsavdelningen och en avdelning för Krypto och it-säkerhet. Sistnämnda avdelning producerar och distribuerar kryptonycklar, aktiva kort och certifikat till totalförsvaret samt utövar rollen som CA (Certification Authority).[37] Avdelningen deltar i projekten med kravställning, verifiering, bedömning och godkännande av signalskyddssystem och krypto för skyddsvärda uppgifter (KSU). Avdelningen stödjer Utrikesdepartementet i rollen som National Security Authority avseende NCSA (National Communications Security Authority) och tecknar med bemyndigande från Regeringskansliet COMSEC-avtal med andra länder och deltar i EU CSC(IA), avseende NDA (National Distri-

[36] Försvarsmakten har under 2019, med stöd av FRA, utvecklat sin förmåga att genomföra såväl defensiva som offensiva operationer mot en kvalificerad motståndare i cybermiljön (Samlad informations- och cybersäkerhetshandlingsplan 2019–2022, Redovisning mars 2020, s. 19).
[37] FMV upphandlar efter beställning från Försvarsmakten system (signalskydd och krypto) av industrin.

bution Authority) med ansvar för kryptonyckelproduktion, distribution och materieluppföljning samt TA (Tempest Authority) med bedömningar och deltagande i EU ITTF. Avdelningen har vidare funktionen som AQUA (Appropriately Qualified Authority), dvs. godkänd andrapartsevaluerare av krypto inom EU.[38]

När det gäller it-säkerhet kravställer, verifierar, bedömer och godkänner avdelningen it-säkerhetsprodukter/mekanismer för Försvarsmakten. Avdelningen har hand om inriktningen av Försvarsmaktens utveckling av it-system med avseende på it-säkerhet och signalskydd. Vidare stödjer avdelningen utvecklingen av it-system.[39] Avdelningen har tagit fram krav på säkra funktioner (KSF), i vilka specificeras de it-säkerhetsegenskaper som it-system i Försvarsmakten ska ha.

Försvarsmakten arbetar för internationell harmonisering av krav för informationssäkerhet. Detta görs genom samverkan för att dela och utveckla kunskap inom olika områden och för att samordna informationssäkerhetsåtgärder.[40]

5.8 Säkerhetspolisen

Säkerhetspolisen är en säkerhetstjänst med ett nationellt uppdrag som polismyndighet. En av myndighetens uppgifter är enligt 3 § polislagen (1984:387) att fullgöra uppgifter enligt säkerhetsskyddslagen.

Säkerhetspolisen har, tillsammans med Försvarsmakten, det övergripande tillsynsansvaret över säkerhetsskyddet hos de verksamhetsutövare, såväl myndihgeter som enskilda, som bedriver säkerhetskänslig verksamhet. Säkerhetspolisen får meddela föreskrifter inom sitt tillsynsområde.

Säkerhetspolisen ska på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter och till Justitiekanslern. Därutöver får myndigheten ge råd om säkerhetsskydd. Inom ramen för sin rådgivningsverksamhet har Säkerhetspolisen tagit fram vägledningar för att stödja de verksamhetsutövare som omfattas av säkerhetsskyddslagen.

[38] Det finns i dag fem svenska kryptosystem som godkänts av Europeiska unionens råd.
[39] Arbetet inbegriper bedömning och godkännande av säkerhetsfunktioner för Försvarsmaktens it-system.
[40] Samlad informations- och cybersäkerhetshandlingsplan 2019–2022, Redovisning mars 2020, s. 34. Arbetet bedrivs exempelvis inom ITTF (Implementation Tempest Task-Force), olika grupper inom kryptoområdet och inom till exempel FMN-samarbetet (Federated Mission Networking).

Beträffande informationssäkerhet har Säkerhetspolisen inom ramen för sin föreskriftsrätt föreskrivit om informationssäkerhet i informationssystem.[41]

Som samrådsmyndighet verkar Säkerhetspolisen i vissa upphandlingssituationer och vid förändring och idrifttagande av informationssystem. Vidare är det Säkerhetspolisen som tar emot anmälningar vid säkerhetshotande händelser och verksamhet, bl.a. it-incidenter eller om säkerhetsskyddsklassificerade uppgifter kan ha röjts.

Säkerhetspolisen ansvarar därutöver för att utföra registerkontroll vid säkerhetsprövning av personer vars anställning har placerats i säkerhetsklass eller som annars ska delta i säkerhetskänslig verksamhet.

5.9 Datainspektionen

Datainspektionen bedriver bl.a. tillsyn för att säkerställa att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter. Datainspektionen är tillsynsmyndighet enligt GDPR och lagen (2018:218) om kompletterande bestämmelser till EU:s dataskyddsförordning. Myndigheten får även i enskilda fall besluta att andra än myndigheter får behandla vissa personuppgifter. Myndigheten har varit remissinstans bl.a. avseende utveckling av standarder inom it- och informationssäkerhet.[42]

5.10 Samverkansgruppen för informationssäkerhet – SAMFI

Samverkansgruppen för informationssäkerhet, SAMFI, bildades 2003 i samband med en framtagen strategi för samhällets informationssäkerhet. I samband med att MSB bildades den 1 januari 2009 övertog myndigheten ansvaret för SAMFI. SAMFI är en samarbetsgrupp som består av svenska myndigheter med av regeringen särskilt utpekat ansvar för informationssäkerhetsfrågor i samhället.[43] MSB av-

[41] Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).
[42] SOU 2010:25, s. 29.
[43] Se regeringens skrivelse Samhällets krisberedskap – stärkt samverkan för ökad säkerhet (2009/10:124) som betonar betydelsen av gruppens arbete: ”SAMFI […] har en särskilt viktig roll då den syftar till att åstadkomma samverkan mellan de statliga myndigheter som har särskilda uppgifter på informationssäkerhetsområdet.”

sätter resurser för ett SAMFI-kansli. Övriga SAMFI-myndigheter bidrar med resurser vid behov och efter förmåga.

Regeringen har 2018 fastställt en nationell strategi för samhällets informations- och cybersäkerhet. För att realisera denna strategi har SAMFI tagit fram en nationell handlingsplan för samhällets informationssäkerhet. Nuvarande handlingsplan gäller åtgärder som ska vidtas under 2019–2022. Regeringen anser att en fördjupad samverkan mellan SAMFI-myndigheterna, vilka alltså har centrala uppdrag i arbetet med informations- och cybersäkerhet i samhället, är en förutsättning för att stärka Sveriges förmåga till skydd mot cyberattacker och andra allvarliga it-incidenter. SAMFI:s verksamhet fokuseras på genomförande av åtgärdsförslagen i den nationella handlingsplanen för samhällets informationssäkerhet.[44]

[44] MSB, Nationell handlingsplan för samhällets informationssäkerhet, Slutrapport, mars 2016, s. 26.

6 Behovet av kompletterande författningsreglering

Förslag: De nationella bestämmelser som behövs för att komplettera EU:s cybersäkerhetsakt och genomförandeakter ska samlas i en ny lag och i en ny förordning.

Regeringen eller berörda myndigheter ska bemyndigas att kunna utfärda föreskrifter.

Termer och uttryck i de nya författningarna ska ha samma betydelse som i EU:s cybersäkerhetsakt och genomförandeakter.

Bedömning: Det behövs inte några författningsåtgärder för att EU:s cybersäkerhetsakt ska bli direkt tillämplig i Sverige.

Flera artiklar i EU:s cybersäkerhetsakten förutsätter dock kompletterande nationell reglering och vissa artiklar i akten behöver kompletteras med nationella bestämmelser för att dessa ska kunna tillämpas på ett effektivt sätt.

6.1 Inledning

I utredningsdirektiven anges att utredningen ska föreslå de anpassningar och kompletterande författningsbestämmelser som EU:s cybersäkerhetsakt ger anledning till. Syftet är att säkerställa att den kompletterande nationella reglering som behövs finns på plats när hela förordningen börjar tillämpas den 28 juni 2021.

Bestämmelserna i EU:s cybersäkerhetsakt utgör ett nytt ramverk för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer i unionen och som innebär harmoniserad unionslagstiftning på aktens tillämpningsområde. Cybersäkerhetsakten är en-

dast tillämplig i den mån det inte finns några specifika bestämmelser med samma syfte, karaktär eller verkan i annan unionslagstiftning.

För att kunna bedöma vilka bestämmelser i EU:s cybersäkerhetsakt som behöver kompletteras av bestämmelser i svensk rätt har utredningen gjort en analys av den svenska lagstiftning som kompletterar eller genomför cybersäkerhetsakten.

I följande kapitel redovisar utredningen, utifrån regleringen i EU:s cybersäkerhetsakt och resultatet av analysen, sina överväganden i fråga om utrymmet för och behovet av kompletterande nationell lagstiftning.

6.2 Utgångspunkter

I artikel 46.1 i EU:s cybersäkerhetsakt, som är en EU-förordning, anges att ett europeiskt ramverk för cybersäkerhetscertifiering ska inrättas som ska höja cybersäkerhetsnivån i unionen och möjliggöra en harmoniserad strategi på unionsnivå för europeiska ordningar för cybersäkerhetscertifiering. Genom ramverket ska en mekanism fastställas för inrättandet av europeiska ordningar för cybersäkerhetscertifiering.

Med stöd av artikel 49.7 får kommissionen anta genomförandeakter för europeiska ordningar för cybersäkerhetscertifiering.

Av EU:s cybersäkerhetsakt framgår det förfarande som kommissionen ska följa vid utarbetande och antagande av en europeisk ordning för cybersäkerhetscertifiering (genomförandeakt). En sådan ordning ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2. Av artikeln 66.2 framgår att när det hänvisas till denna punkt ska artikel 5.4 b i förordning (EU) nr 182/2011 tillämpas.[1]

I förordning (EU) nr 182/2011 fastställs de allmänna principerna för genom vilka mekanismer EU-länderna styr kommissionens utövande av genomförandebefogenheter. I enlighet med förordningen använder kommittéerna två former av förfaranden, dvs. granskning eller rådgivning. Vilket förfarande som en kommitté använder beror på karaktären på de genomförandebefogenheter som fastställs i den grundläggande förordningen, direktivet eller beslutet.

[1] 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.

EU:s cybersäkerhetsakt trädde i kraft den 27 juni 2019, dock ska vissa av artiklarna tillämpas först från den 28 juni 2021. EU:s cybersäkerhetsakt och de europeiska ordningar för cybersäkerhetscertifiering (genomförandeakter) som utfärdas med stöd av akten är unionsrättsliga författningar som är bindande i sin helhet och direkt tillämpliga i varje medlemsstat. Någon europeisk ordning för cybersäkerhetscertifiering (genomförandeakt) har – som tidigare angetts – ännu inte fastställts, dock finns det tidigare angivna offentliggjorda utkastet till europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter (se kapitel 4).

EU:s cybersäkerhetsakt ger medlemsstaterna rätt, men förskriver även en skyldighet, att vidta vissa åtgärder, bl.a. för att säkerställa att regelverket i det europeiska ramverket för cybersäkerhetscertifiering införs och tillämpas på ändamålsenligt och effektivt sätt. En medlemsstat får dock inte vidta några särskilda åtgärder för att införliva de materiella bestämmelserna i det europeiska ramverket med nationell rätt. Det är endast då nationell rätt kan anses strida mot cybersäkerhetsakten, då akten ger möjlighet eller föreskriver en skyldighet att vidta lagstiftningsåtgärder på det nationella planet och då det behövs andra nationella åtgärder till stöd för regelverkets syfte, som ändringar i nationell rätt aktualiseras.

Som konstateras ovan förutsätter flera av artiklarna i EU:s cybersäkerhetsakt att nationella kompletterande bestämmelser införs, bl.a. artiklarna 58, 64 och 65.

Av artikel 58.1 följer att medlemsstaterna ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering och som ansvariga för tillsynsuppgifterna i medlemsstaten.

Av artikel 64 följer att fysiska och juridiska personer ska ha rätt till effektiva rättsmedel i de fall som anges i bestämmelsen.

Av artikel 65 framgår att medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av artiklarna 49–65 i EU:s cybersäkerhetsakt och ska vidta alla nödvändiga åtgärder för att se till att de tillämpas.

Detta innebär således att den svenska rättsordningen behöver kompletteras med nationell reglering på de områden som behandlas i följande kapitel. Formerna för och utformningen av det kompletterande nationella regelsystemet behandlas i nästa avsnitt.

6.3 En ny lag och en ny förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt införs

EU:s cybersäkerhetsakt och europeiska ordningar för cybersäkerhetscertifiering (genomförandeakter) behöver som ovan anges kompletteras med nationella bestämmelser som bl.a. reglerar nationell myndighet för cybersäkerhetscertifiering, tillsynsverksamhet, sanktioner och vissa processuella frågor.

Det finns olika sätt att utforma den nationella kompletterande regleringen som stöd för EU:s cybersäkerhetsakt i svensk rätt. Ett alternativ är genom ett samlat regelverk som specifikt avser det europeiska ramverket för cybersäkerhetscertifiering, dvs. genom en ny lag med en anslutande förordning.

Fördelarna med ett samlat regelverk för genomförandet är att det blir tydligt för myndigheter, enskilda och tillsynsmyndigheten vilken reglering som finns när det gäller ramverkets tillämpningsområde. Bestämmelser som behöver anpassas till en europeisk ordning för cybersäkerhetscertifiering kan då regleras i myndighetsföreskrifter. Regleringen blir heltäckande och ingen certifieringsordning riskerar att sakna den eventuella kompletterande reglering som kan behövas. Det blir också lättare att komplettera och ändra regelverket om ett sådant behov uppkommer. Vidare kan det underlätta tillämpningen, inte minst mot bakgrund av att myndigheter och enskilda kan komma att omfattas av det europeiska ramverkets tillämpning i flera medlemsstater. En nackdel som kan uppkomma är att myndigheter och enskilda i vissa fall kan komma att behöva tillämpa olika regelverk för samma nätverk och informationssystem men med olika syften. För myndigheter och enskilda som även omfattas av andra EU-rättsakter finns också en risk för att det kan bli otydligt vilken reglering som gäller eftersom EU-rättsliga och nationella regler är mer utvecklade inom vissa områden inom cybersäkerhet och informationssäkerhet. Vissa bestämmelser i nationell rätt tar inte heller direkt sikte på informationssäkerhet utan syftar till att upprätthålla kontinuiteten i tjänsten utifrån andra aspekter eller till att analysera eller hantera risker mer allmänt.

En kompletterande nationell reglering till det europeiska ramverket för cybersäkerhetscertifiering bör ske genom ett samlat regelverk. Ramverket innebär skyldigheter för både offentliga aktörer

och enskilda och den kompletterande regleringen kan därför i vissa fall behöva ske i form av lag. Det bör därför införas en ny lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt. I vilken utsträckning det finns behov av bestämmelser i lag, förordning eller myndighetsföreskrifter behandlas löpande i delbetänkandets olika avsnitt. För att betona att den lag som utredningen föreslår endast utgör ett komplement till EU:s cybersäkerhetsakt bör den benämnas lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Vissa av de bestämmelser som behövs för att komplettera EU:s cybersäkerhetsakt kan regeringen besluta om inom ramen för sin restkompetens. Det gäller exempelvis att utse en nationell myndighet för cybersäkerhetscertifiering och bemyndiga en myndighet att meddela verkställighetsföreskrifter. Sådana bestämmelser kan lämpligen införas på förordningsnivå. Det bör därför införas en ny förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Termer och uttryck i författningar ska ha samma betydelse som i EU:s cybersäkerhetsakt och genomförandeakter.

7 Reglering av cybersäkerhetscertifiering

7.1 Inledning

I utredningsdirektiven noteras att det europeiska ramverket för cybersäkerhetscertifiering kommer att reglera den cybersäkerhetscertifiering som följer av EU:s cybersäkerhetsakt och en europeisk ordning för cybersäkerhetscertifiering som fastställts av kommissionen.

I direktiven framhålls att i dag bestämmer en producent själv om en produkt, tjänst eller process ska certifieras och i så fall vilket certifieringsorgan som ska utföra certifieringen. Utgångspunkten – enligt direktiven – är att certifiering även i framtiden ska vara frivillig, oavsett om en europeisk ordning för cybersäkerhetscertifiering finns på plats eller inte. Detta är dock upp till varje medlemsstat att bestämma. Den största skillnaden är att när en europeisk ordning för cybersäkerhetscertifiering finns på plats, får inte längre nationella cybersäkerhetscertifieringar utföras inom det område som täcks av den europeiska ordningen för cybersäkerhetscertifiering. När en europeisk ordning för cybersäkerhetscertifiering ska användas reglerar cybersäkerhetsakten vilka krav som ställs på certifieringen, certifieringsorganen och de leverantörer och leverantörer som innehar ett sådant certifikat. I direktiven görs bedömningen att det finns ett behov av att ta fram en nationell reglering som kompletterar EU:s cybersäkerhetsakt. Utredningens uppdrag i denna del är att lämna eventuella förslag som behövs för att komplettera cybersäkerhetsakten. Utredningen ska bl.a. analysera om det mot bakgrund av de krav som ställs i certifieringsordningar finns behov av kompletterande nationella bestämmelser när det gäller självbedömning av överensstämmelse som utförs av tillverkare och leverantörer av IKT-produkter, -tjänster och -processer enligt artikel 53 i EU:s cybersäkerhetsakt.

Utredningen ska också analysera om det på motsvarande sätt finns behov av kompletterande bestämmelser för organ för bedömning av överensstämmelse som med stöd av bl.a. artikel 56 utfärdar europeiska cybersäkerhetscertifikat avseende IKT-produkter, -tjänster och -processer.

Enligt direktiven ska utredningen även analysera och föreslå hur certifiering på assuransnivån ”hög” ska genomföras i Sverige och utreda om detta kan och bör regleras genom författning, varvid utgångspunkten är att FMV/CSEC ska ha en roll då det gäller denna typ av certifiering.

7.2 Utgångspunkter

Syftet med kompletterande nationella bestämmelser är i första hand att bidra till ett ändamålsenligt och effektivt genomförande av det europeiska ramverket för cybersäkerhetscertifiering. Utgångspunkten för en analys är hur det regelverk som nationella bestämmelser är avsedda att komplettera är utformat. Mer grundläggande frågor om hur det europeiska ramverket för cybersäkerhetscertifiering kan bedömas och formerna för kompletterande nationell reglering har tidigare behandlats i kapitel 6.

Med utgångspunkt i de ställningstaganden som redovisas i det kapitlet avgränsas frågan om behovet kompletterande bestämmelser i detta avsnitt till de frågor som kan bedömas uppkomma i verksamhet som avser självbedömning av överensstämmelse, dvs. utfärdande av EU-försäkran om överensstämmelse enligt artikel 53, och utfärdande och innehav av europeiska cybersäkerhetscertifikat enligt bl.a. artikel 56.

Vad gäller frågan hur cybersäkerhetscertifiering på assuransnivån ”hög” enligt artikel 56.6 ska genomföras i Sverige och om detta kan och bör regleras genom författning kan noteras att frågan rymmer såväl behörighetsfrågor som frågor om handläggningen av ärenden som avser sådana certifikat. Utredningen behandlar frågan om vilken myndighet/organ för bedömning av överensstämmelse som bör ansvara för dessa prövningar i anslutning till frågan om nationell myndighet för cybersäkerhetscertifiering i kapitel 8. Behovet av kompletterande regler för handläggning och beslut av sådana organ behandlas i kapitel 11.

Då EU:s cybersäkerhetsakt och de framtida bestämmelserna i de europeiska ordningarna för cybersäkerhetscertifiering har direkt effekt och ska tillämpas i medlemsstaterna uppkommer frågan i vilken utsträckning det finns behov av och möjlighet att införa av kompletterande reglering på nationell nivå för utfärdande av EU-försäkran om överensstämmelse enligt artikel 53 respektive utfärdande och innehav av ett europeiskt cybersäkerhetscertifikat enligt artikel 56. Till grund för en sådan bedömning bör ligga en analys av dels hur det befintliga regelverket är utformat på området och dels de eventuella bemyndiganden som redan nu kan iakttas när det gäller möjligheterna till kompletterande regler på området.

7.3 Närmare om cybersäkerhetscertifiering

I detta avsnitt redogörs för hur det europeiska ramverket för cybersäkerhetscertifiering är utformat, dvs. regleringen i EU:s cybersäkerhetsakt och vad som i akten anges ska framgå av en europeisk ordning för cybersäkerhetscertifiering.

Allmänt

Av artikel 54 framgår att en europeisk ordning för cybersäkerhetscertifiering ska innehålla minst de komponenter och regleringar som anges i artikeln (se kapitel 4). Utredningen bedömer att de olika europeiska ordningarna i betydande omfattning kommer att reglera såväl de olika krav som ska gälla vid själva bedömning av överensstämmelse som vid handläggningen av olika ärenden som omfattas av cybersäkerhetsaktens tillämpningsområde.

Som tidigare framgått har ett utkast till en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter offentliggjorts för allmän konsultation. Utredningen anser att vad som anges i utkastet kan belysa vissa av de frågeställningar som behandlas i detta kapitel samtidigt som det måste anses föreligga en betydande osäkerhet om i vilken utsträckning som förslagen i utkastet kommer att utgöra formell reglering på området.

Syftet med europeiska ordningar för cybersäkerhetscertifiering är 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. Samtidigt är det inte möjligt att i detalj fastställa cybersäkerhetskraven för alla IKT-produkter, -tjänster och -processer i cybersäkerhetsakten. IKT-produkter, IKT-tjänster och IKT-processer och cybersäkerhetsbehov relaterade till dessa produkter, tjänster och processer är så olikartade att det bedöms som mycket svårt att ta fram allmänna cybersäkerhetskrav som är giltiga under alla omständigheter. Det bedöms 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, -tjänster och -processer bör sedan fastställas i detalj för den enskilda certifieringsordningen som antas av kommissionen, t.ex. genom hänvisningar till standarder eller tekniska specifikationer om inga lämpliga standarder finns tillgängliga.[1]

Europeiska ordningar för cybersäkerhetscertifiering kommer att bidra till att harmonisera cybersäkerhetsrutinerna inom unionen. De ska bidra till att öka cybersäkerheten inom unionen. Utformningen av europeiska ordningar för cybersäkerhetscertifiering bör även beakta och möjliggöra utveckling av innovationer på området cybersäkerhet.[2]

Europeiska ordningar för cybersäkerhetscertifiering bör även beakta olika befintliga metoder för program- och maskinvaruutveckling och vilken inverkan 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, -tjänst eller -process ska återcertifieras eller att ett specifikt europeiskt cybersäkerhetscertifikats tillämpningsområde ska begränsas.

[1] Skäl 75.
[2] Skäl 95.

Allmänna eller sektorsspecifika cybersäkerhetsriktlinjer

För att öka medvetenheten och underlätta acceptansen för framtida europeiska ordningar för cybersäkerhetscertifiering får 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.

Europeiska ordningar för cybersäkerhetscertifiering kan möjliggöra både självbedömning av överensstämmelse och certifiering för IKT-produkter, -tjänster eller -processer. I dessa fall ska ordningen föreskriva tydliga möjligheter för konsumenter och andra användare att skilja mellan IKT-produkter, -tjänster eller -processer, detta med avseende på vilken tillverkare eller leverantör av IKT-produkter, -tjänster eller -processer som har ansvar för bedömningen och IKT som har certifierats av en tredje part.[3]

Assuransnivåer

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 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, -tjänsten och -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.

[3] Skäl 80.

Utvärderingskriterier

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, 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.

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, -tjänster eller -processer har gjort en självbedömning av IKT-produktens, -tjänstens eller -processens överensstämmelse med certifieringsordningen.[4]

För assuransnivån ”betydande” bör utvärderingen, utöver kraven för assuransnivån ”grundläggande”, omfatta en kontroll av överensstämmelsen mellan IKT-produktens, -tjänstens eller -processens säkerhetsfunktioner och den tekniska dokumentationen.[5]

För assuransnivån ”hög” bör utvärderingen, utöver kraven för assuransnivån ”betydande”, omfatta ett effektivitetstest som bedömer resistensen hos IKT-produktens, -tjänstens eller -processens säkerhetsfunktioner gentemot genomtänkta cyberangrepp som utförs av personer med betydande kompetens och resurser.[6]

[4] Skäl 88.
[5] Skäl 89.
[6] Skäl 90.

Självbedömning av överensstämmelse

Europeiska ordningar för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster och IKT-processer möjlighet att på eget ansvar göra en bedömning av överensstämmelse (självbedömning av överensstämmelse). I sådana fall bör det vara tillräckligt att tillverkaren eller leverantören själv genomför alla kontroller för att säkerställa att IKT-produkten, -tjänsten eller -processen överensstämmer med den europeiska ordningen för cybersäkerhetscertifiering. Denna typ av bedömning av överensstämmelse bedöms 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, -tjänster eller -processer när de motsvarar assuransnivån ”grundläggande”.[7]

En EU-försäkran om överensstämmelse är ett dokument som anger att en särskild IKT-produkt, -tjänst eller -process uppfyller kraven i den europeiska ordningen för cybersäkerhetscertifiering. En tillverkare eller leverantör av IKT-produkter, -tjänster eller -processer som utför en självbedömning av överensstämmelse ska upprätta och underteckna en EU-försäkran om överensstämmelse som ett led i förfarandet för bedömning av överensstämmelse. Genom att upprätta och underteckna en EU-försäkran om överensstämmelse tar tillverkaren eller leverantören ansvaret för att IKT-produkten, -tjänsten eller -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.

Tillverkaren eller leverantören av IKT-produkter, -tjänster eller -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, -tjänsternas eller -processernas överensstämmelse med den relevanta europeiska ordningen för cybersäkerhetscertifiering. Den tekniska dokumentationen ska specificera de krav som är tillämpliga enligt ordningen

[7] Skäl 79.

och ska, i den mån det krävs för självbedömningen av överensstämmelse, även innehålla en beskrivning av IKT-produktens, -tjänstens eller -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.

Cybersäkerhetscertifikat efter bedömning av överensstämmelse

Ett europeiskt cybersäkerhetscertifikat utfärdas efter utvärdering av en IKT-produkt, IKT-tjänst eller IKT-process. Ett certifikat är en bekräftelse på att en utvärdering har genomförts på ett korrekt sätt. En bedömning av överensstämmelse avser det förfarande genom vilket man utvärderar om fastställda krav för en IKT-produkt, -tjänst eller -process har uppfyllts. Detta förfarande utförs av en oberoende tredje part som inte är tillverkaren eller leverantören av de IKT-produkter, -tjänster eller -processer som bedöms.

Bedömning av överensstämmelse och certifiering utgör inte i sig någon garanti för att certifierade IKT-produkter och -tjänster är cybersäkra. De är snarare förfaranden och tekniska metoder för att intyga att IKT-produkter, -tjänster och -processer har testats och att de uppfyller vissa cybersäkerhetskrav som fastställs på annan plats, t.ex. i tekniska standarder.[8]

Valet av lämplig certifiering och därtill knutna säkerhetskrav av användarna av europeiska cybersäkerhetscertifikat grundas på en riskanalys som avser risker med användningen av IKT-produkten, -tjänsten eller -processen. Assuransnivån står i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, -tjänst eller -process.[9] Beroende på assuransnivå ska den europeiska ordningen för cybersäkerhetscertifiering även ange om det europeiska cybersäkerhetscertifikatet ska utfärdas av ett privat eller offentligt organ.

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

[8] Skäl 77.
[9] Skäl 78.

med jämna mellanrum följa upp vilka effekter antagna europeiska ordningar för cybersäkerhetscertifiering har på tillgången till säkra IKT-produkter, -tjänster och -processer på den inre marknaden och bör regelbundet bedöma i hur hög utsträckning tillverkare och leverantörer av IKT-produkter, -tjänster och -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.[10]

Ansökan om certifiering av IKT-produkter eller IKT-tjänster till valfritt organ för bedömning av överensstämmelse

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 -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 cybersäkerhetsakten. 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.[11]

Slutanvändarens tillgång till information

EU-försäkringar om överensstämmelse och europeiska cybersäkerhetscertifikat ska hjälpa slutanvändarna att göra välinformerade val. IKT-produkter, IKT-tjänster och IKT-processer som certifierats

[10] Skäl 92.
[11] Skäl 97.

eller varit föremål för en EU-försäkran om överensstämmelse bör därför åtföljas av information som anpassats till den avsedda slutanvändarens förväntade tekniska nivå.[12] 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, -tjänsten och -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, -tjänster och -processer.

I tillämpliga fall kan slutanvändaren få vägledning om åtgärder och inställningar som denne kan genomföra för att underhålla eller öka cybersäkerheten för IKT-produkten eller -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.

Information om EU-försäkran om överensstämmelse och europeiskt cybersäkerhetscertifikat

Enisa ska 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.

[12] Skäl 93.

För att säkerställa enhetliga villkor för tillämpningen av EU:s cybersäkerhetsakt har kommissionen fått genomförandebefogenheter,[13] som ska utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011.

7.4 Behov av kompletterande reglering

Utredningen kan notera att kommissionen i unionens löpande arbetsprogram kommer att fastställa strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. Även om något arbetsprogram ännu inte offentliggjorts har Enisa den 2 juli 2020 offentliggjort ett första utkast till en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter som uppfyller kraven för på assuransnivåerna ”betydande” respektive ”hög”. Enligt vad som anges i utkastet ger den föreslagna ordningen möjlighet för tillverkare och leverantörer att frivilligt ansöka om cybersäkerhetscertifiering av sådana IKT-produkter som omfattas av den föreslagna certifieringsordningen och som tillhandahålls av en tillverkare eller leverantör på EU:s inre marknad.

Utredningen noterar att den föreslagna ordningen utöver att närmare ange vilka krav som ska uppfyllas för att ett cybersäkerhetscertifikat ska kunna utfärdas och villkor för innehav av ett certifikat även innehåller en detaljerad och omfattande reglering av bl.a. olika frågor som kan uppkomma i samband med handläggningen av en ansökan, utfärdande och underhåll av ett certifikat samt vad som gäller ett eventuellt återkallande av certifikatet. Samtidigt kan konstateras att eftersom några europeiska ordningar för cybersäkerhetscertifiering ännu inte formellt antagits eller fastställts och att endast det angivna utkastet till en sådan ordning offentliggjorts föreligger en betydande osäkerhet om behovet av nationell reglering på området.

Utredningen gör ändå bedömningen att EU:s cybersäkerhetsakt förutsätter och ger utrymme för att för att med en tillräcklig grad av säkerhet lämna förslag om kompletterande reglering när behov av sådan bedöms föreligga. Utredningen gör samtidigt bedömningen att utrymmet för berörda myndigheter att meddela kompletterande föreskrifter på området i dagsläget blir begränsat då eventuella myndig-

[13] Skäl 106.

hetsföreskrifter måste beakta den framtida unionsrättens reglering på området.

Utredningen behandlar i avsnittet nedan frågan om behovet av kompletterande nationella bestämmelser för EU-försäkran om överensstämmelse respektive utfärdande och innehav av cybersäkerhetscertifikat enligt EU:s cybersäkerhetsakt. Frågan om behov av kompletterande bestämmelser för handläggning av dessa ärenden behandlas i kapitel 11.

7.4.1 EU-försäkran om överensstämmelse

Bedömning: Den som utfärdar en EU-försäkran om överensstämmelse enligt artikel 53.3 i EU:s cybersäkerhetsakt bör vara skyldig att anmäla en sådan försäkran till myndigheten för cybersäkerhetscertifiering.

Regeringen eller den myndighet som regeringen bestämmer bör ha möjlighet att meddela föreskrifter om hur anmälningsskyldigheten, skyldigheten att ge tillgång till dokumentationen enligt artikel 53.3 och skyldigheten att lämna kompletterande cybersäkerhetsinformation enligt artikel 55.1 ska fullgöras.

Av artikel 53.1 i EU:s cybersäkerhetsakt framgår att en europeisk ordning för cybersäkerhetscertifiering kan ge utrymme för en tillverkare eller leverantör av IKT-produkter, IKT-tjänster eller IKT-processer till självbedömning av överensstämmelse med de krav som anges i eller följer av en sådan ordning. En självbedömning av överensstämmelse får dock endast avse IKT-produkter, -tjänster och -processer med låg risk som motsvarar assuransnivån ”grundläggande”.

I artikel 53.2 anges att tillverkaren eller leverantören av IKT-produkter, -tjänster eller -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 ansvar för att produkten, tjänsten eller processen överensstämmer med de krav som anges i den ordningen.

Vidare anges i artikel 53.3 att tillverkaren eller leverantören av IKT-produkter, -tjänster eller -processer under den period som fastställts i den europeiska ordningen för cybersäkerhetscertifiering ska ge den nationella myndigheten för cybersäkerhetscertifiering som

avses i artikel 58 tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas eller -tjänsternas överensstämmelse med ordningen. En kopia av EU-försäkran om överensstämmelse ska också lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

Av artikel 55.1 följer att tillverkaren eller leverantören av IKT-produkter, -tjänster eller -processer som för vilka en EU-försäkran om överensstämmelse utfärdats även ska lämna kompletterande cybersäkerhetsinformation enligt vad som anges i den bestämmelsen. Av andra punkten i bestämmelsen följer att informationen ska tillgängliggöras i elektroniskt format och finnas tillgänglig och vid behov uppdateras åtminstone fram till dess att EU-försäkran om överensstämmelse löper ut.

Utredningen kan notera att den som utfärdar en EU-försäkran om överensstämmelse är skyldig att lämna en kopia av denna till Enisa.

Utredningen anser att det på motsvarande sätt finns behov av att även den nationella myndigheten för cybersäkerhetscertifiering (se kapitel 8), som ansvarar för tillsyn enligt artikel 58, får kännedom om att en EU försäkran enligt en europeisk certifieringsordning har utfärdats. EU:s cybersäkerhetsakt innehåller inga bestämmelser om skyldighet för en tillverkare eller leverantör som utfärdar en EU-försäkran att *anmäla* detta till den nationella myndigheten för cybersäkerhetscertifiering. Om myndigheten inte får kännedom om att en sådan försäkran utfärdats finns risk för att myndigheten inte kan fullgöra tillsynsuppgiften enligt artikel 58.7 b. Av den bestämmelsen följer att den nationella myndigheten för cybersäkerhetscertifiering ska kontrollera att tillverkare eller leverantörer av IKT-produkter, -tjänster eller -processer fullgör sina skyldigheter i samband med att de genomför självbedömning av överensstämmelse i syfte att utfärda en EU-försäkran om överensstämmelse. I bestämmelsen framhålls att det gäller särskilt fullgörandet och verkställandet av en tillverkares och leverantörers skyldigheter enligt artiklarna 53.2 och 53.3 och i motsvarande europeisk ordning för cybersäkerhetscertifiering.

Utredningen bedömer att vikten av att den nationella myndigheten för cybersäkerhetscertifiering ges rimliga förutsättningar att kunna fullgöra sin tillsynsuppgift väger tyngre än den börda som anmälningsskyldigheten innebär för de tillverkare och leverantörer som utfärdar en EU-försäkran om överensstämmelse. Det finns där-

för skäl att ålägga tillverkare och leverantörer som utfärdar en EU-försäkran att anmäla detta till den angivna myndigheten. Det finns även ett behov av att närmare reglera formerna för hur detta ska gå till. Regeringen eller de myndigheter som regeringen bestämmer bör därför kunna meddela föreskrifter om hur denna anmälningsskyldighet ska fullgöras. Det ska samtidigt betonas att en självklar utgångspunkt i detta sammanhang är att myndigheten inte begär in fler uppgifter än vad som krävs för att den ska få kännedom om att en EU-försäkran har utfärdats. Myndighetens möjligheter att infordra ytterligare uppgifter regleras i artikel 53.3. Som ovan framgår följer av denna bestämmelse att den som utfärdar en EU-försäkran om överensstämmelse ska ge den nationella myndigheten för cybersäkerhetscertifiering som avses i artikel 58 tillgång till teknisk dokumentation och all annan relevant information avseende produkternas eller tjänsternas överensstämmelse med ordningen under den period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering. Eftersom det inte är frågan om en obligatorisk skyldighet att lämna dokumentationen till myndigheterna utan denna inträder först på begäran begränsas också den administrativa bördan på tillverkare och leverantörer. Utgångspunkten bör även i detta sammanhang vara att myndigheterna endast bör efterfråga relevant och nödvändig dokumentation som behövs i det enskilda fallet. Det finns även i detta fall behov av att myndigheten ska kunna meddela föreskrifter som närmare anger formerna och omfattningen för hur denna skyldighet ska fullgöras. Regeringen och den myndighet som regeringen bestämmer bör meddela föreskrifter om formerna för hur skyldigheten att lämna dokumentation ska fullgöras.

Myndigheterna bör även kunna meddela föreskrifter om hur skyldigheten att lämna kompletterande cybersäkerhetsinformation enligt artikel 55.1 ska fullgöras.

Utredningen kan i detta sammanhang samtidigt konstatera att avsaknaden av en fastställd europeisk ordning för cybersäkerhetscertifiering som ger utrymme för och, i sådant fall, närmare anger omfattningen för när en självbedömning av överensstämmelse som medför att en EU-försäkran kan utfärdas samt närmare reglerar vad som ska gälla vid ett sådant förfarande medför osäkerhet om behovet av ytterligare kompletterande nationell reglering på området. Det kan därför inte uteslutas att den nationella myndigheten för cybersäkerhetscertifiering kan komma att ha behov av att meddela ytterligare

kompletterande föreskrifter för vad som ska gälla för självbedömning av överensstämmelse och utfärdande av en EU-försäkran.

En självbedömning av överensstämmelse grundas på – utöver vad som anges i en europeisk ordning för cybersäkerhetscertifiering – även på olika standarder och tekniska krav, m.m. som förutsätter expertkunskap på området. Den nationella myndigheten för cybersäkerhetscertifiering bör därför samråda och samverka med andra berörda myndigheter och andra aktörer, bl.a. i näringslivet, vid framtagande av föreskrifter som meddelas av myndigheten.

Utredningen kan också notera att avsaknaden av fastställda europeiska ordningar som ger utrymme för självbedömning av överensstämmelse av IKT-produkter, -tjänster och -processer medför att myndigheternas resursbehov för att fullgöra sina uppgifter med anledning av en sådan verksamhet i dagsläget är mycket svår att bedöma, bl.a. då det i dag inte går att beräkna eller ens uppskatta i vilken utsträckning som tillverkare och leverantörer kommer att använda sig av möjligheten till självbedömning av överensstämmelse när den möjligheten väl ges. Motsvarande osäkerhet gäller även vad avser ansökan om frivillig respektive obligatorisk cybersäkerhetscertifiering (se nedan).

Frågan om myndigheternas eventuella resursbehov med anledning av införandet av det europeiska ramverket för cybersäkerhetscertifiering behandlas närmare i kapitel 8 respektive 14.

Frågan om vilka bestämmelser för handläggning av ärenden som rör självbedömning av överensstämmelse, dvs. utfärdande av EU-försäkran, behandlas i kapitel 11.

7.4.2 Utfärdande och innehav av europeiska cybersäkerhetscertifikat

Bedömning: Den som utfärdar ett europeiskt cybersäkerhetscertifikat enligt artikel 56.4–6 i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering eller innehar ett sådant certifikat bör åläggas att anmäla detta till den nationella myndigheten för cybersäkerhetscertifiering.

Regeringen eller den myndighet som regeringen bestämmer bör ha möjlighet att meddela föreskrifter om utfärdande av cybersäkerhetscertifikat enligt artikel 56.4–6 och om innehav av sådana certifikat samt om skyldigheten att lämna information enligt artikel 55.1 samt artikel 56.7 och 8 i EU:s cybersäkerhetsakt.

Av artikel 56.1. framgår 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. En sådan certifiering ska vara frivillig om inte annat framgår av nationell rätt eller unionsrätten.

Ett cybersäkerhetscertifikat som avser assuransnivå ”grundläggande” eller ”betydande” får utfärdas av ett organ för bedömning av överensstämmelse på grundval av de kriterier som anges i en europeisk ordning för cybersäkerhetscertifiering.

I artikel 60.1 föreskrivs att ett sådant organ för bedömning av överensstämmelse ska vara ackrediterat av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008, dvs. Swedac, när det gäller ackreditering av organ för bedömning av överensstämmelse som bedriver verksamhet i landet. En ackreditering får dock endast utfärdas under förutsättning att det angivna organet för bedömning av överensstämmelse uppfyller de krav som anges i bilagan till EU:s cybersäkerhetsakt. Om en europeisk ordning för cybersäkerhetscertifiering innehåller särskilda eller ytterligare krav enligt artikel 54.1 f ska endast sådana 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 56.5 följer att en europeisk ordning för cybersäkerhetscertifiering kan föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen endast får utfärdas av ett offentligt organ som 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.

Om ett europeiskt cybersäkerhetscertifikat ska utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a ska certifieringsorganet vid den nationella myndigheten för cybersäkerhetscertifiering vara ackrediterat som ett organ för bedömning av överensstämmelse enligt artikel 60.1.

Av artikel 56.6 följer att om en europeisk ordning för cybersäkerhetscertifiering kräver assuransnivå ”hög” får det europeiska cybersäkerhetscertifikatet endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller av ett organ för bedömning av överensstämmelse efter *förhandsgodkännande* av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt europeiskt cybersäkerhetscertifikat som utfärdas av det organet för bedömning av överensstämmelse.

Den nationella myndigheten för cybersäkerhetscertifiering får även genom en på förhand *allmän delegering* ge uppgiften att utfärda ett sådant europeiskt cybersäkerhetscertifikat till ett organ för bedömning av överensstämmelse. Även i detta fall gäller att om ett europeiskt cybersäkerhetscertifikat ska utfärdas av en nationell myndighet för cybersäkerhetscertifiering ska certifieringsorganet vid den nationella myndigheten för cybersäkerhetscertifiering vara ackrediterad som ett organ för bedömning av överensstämmelse enligt artikel 60.1.

I artikel 56.7 anges att en fysisk eller juridisk person som lämnar in sina IKT-produkter, -tjänster eller -processer för certifiering ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndigheten för cybersäkerhetscertifiering som avses i artikel 58, om denna myndighet är det organ som utfärdar det europeiska cybersäkerhetscertifikatet, eller till det organ för bedömning av överensstämmelse som avses i artikel 60.

Vidare följer av artikel 56.8 att 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, -tjänsten eller -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.

I det offentliggjorda utkastet till europeisk cybersäkerhetsordning för IKT-produkter föreskrivs att denna omfattar endast IKT-produkter på som uppfyller kraven på assuransnivå ”betydande” och ”hög” och att angivna IKT-produkter inte får bli föremål för självbedömning av överensstämmelse med stöd av den föreslagna ordningen.

Den föreslagna regleringen omfattar således att endast IKT-produkter som motsvarar kraven för lägst assuransnivån ”betydande” kan bli föremål för bedömning av överensstämmelse av antingen en nationell myndighet med uppgift att bedöma överensstämmelse, dvs. utfärda ett europeiskt cybersäkerhetscertifikat för IKT-produkter enligt den föreslagna ordningen, eller av ett ackrediterat organ för bedömning av överensstämmelse som uppfyller kraven för bedömning på den angivna assuransnivån.

När det gäller frågan om det föreligger behov av kompletterande nationell reglering för handläggningen och prövningen i ärenden som avser ansökan, utfärdande, underhåll och återkallande av europeiska cybersäkerhetscertifikat som kan komma att utfärdas med stöd att vad som anges i EU:s cybersäkerhetsakt och det nu offentliggjorda utkastet med förslag till europeisk ordning för cybersäkerhetscertifiering av IKT-produkter eller en annan europeisk ordning gör utredningen följande överväganden.

Inledningsvis kan noteras att det offentliggjorda förslaget till europeisk certifieringsordning är ett förslag, vilket innebär att vad som där anges kan komma att ändras i den ordning som slutligen kan komma att fastställas. På motsvarande sätt som när det gäller avsaknaden av en fastställd europeisk ordning för självbedömning av överensstämmelse innebär avsaknaden av en fastställd europeisk ordning för cybersäkerhetscertifiering osäkerhet om behovet av kompletterande nationell reglering på området.

Av samma skäl och på motsvarande sätt som gäller för den som utfärdar en EU-försäkran om överensstämmelse bör utfärdande eller innehav av europeiska cybersäkerhetscertifikat anmälas till den nationella myndigheten för cybersäkerhetscertifiering. Regeringen eller den eller de myndigheter som regeringen bestämmer bör meddela föreskrifter om utfärdande och innehav av europeiska cybersäkerhetscertifikat.

När det gäller vad som anges i artikel 56.5, dvs. att ett europeiskt cybersäkerhetscertifikat i vissa fall endast får utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller ett offentligt organ som är ackrediterat som organ för bedömning av överensstämmelse, behövs inte någon kompletterande reglering. Vilken myndighet som enligt utredningens bedömning ska ha till uppgift att vara nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 behandlas i kapitel 8.

När det gäller regleringen i artikel 56.6 att ett certifikat som kräver högsta assuransnivån endast får utfärdas av en nationell myndighet för cybersäkerhetscertifiering eller av ett organ för bedömning av överensstämmelse efter *förhandsgodkännande* för varje enskilt europeiskt cybersäkerhetscertifikat *eller* genom en på förhand *allmän delegering* av uppgiften till ett organ för bedömning av överensstämmelse, gör utredningen följande överväganden.

Bestämmelsen ger utrymme för medlemsstaterna att i nationell rätt närmare reglera i vilka fall som ett förhandsgodkännande och en delegering ska vara möjlig. Utgångspunkten är att det är fråga om förhandsgodkännande i varje enskilt fall alternativt en allmän delegering av rätten att utfärda ett europeiskt cybersäkerhetscertifikat på högsta assuransnivån. Det är således fråga om cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer som ska motsvara höga eller mycket högt ställda krav på cybersäkerhet och som kan antas komma att användas i bl.a. industriella, samhällsviktiga och säkerhetskänsliga verksamhet.

Utredningen anser att det i första hand bör ankomma på den nationella myndigheten för cybersäkerhetscertifiering att besluta om i vilka fall det är möjligt och lämpligt att i det enskilda fallet överlåta rätten att utfärda ett cybersäkerhetscertifikat på högsta assuransnivån till ett fristående organ för bedömning av överensstämmelse. Det förutsätter emellertid att det aktuella organet är ackrediterat för denna verksamhet, dvs. utöver vad som i allmänhet gäller för själva ackrediteringen även möter de övriga krav som anges i EU:s cybersäkerhetsakt och motsvarande europeiska ordning för cybersäkerhetscertifiering.

Utredningen gör sammantaget bedömningen att det inte föreligger behov av kompletterande lagreglering för utfärdande och innehav av europeiska cybersäkerhetscertifikat. I kapitel 8 lämnas förslag på den myndighet som enligt utredningens bedömning bör ha till uppgift att vara nationell myndighet för cybersäkerhetscertifiering, bl.a. enligt artikel 56.5 och 6.

8 Nationell myndighet för cybersäkerhetscertifiering

8.1 Inledning

Utredningen har enligt kommittédirektivet i uppdrag att föreslå vilken befintlig myndighet som ska få i uppdrag att vara nationell myndighet för cybersäkerhetscertifiering med uppgift att övervaka de skyldigheter som följer av det europeiska ramverket för cybersäkerhetscertifiering och även ta ställning till hur myndighetens organisation kan komma att påverkas. Enligt direktiven kommer det vid myndigheten – som kommer att ha ett särskilt ansvar för utfärdande av certifikat på den högsta assuransnivån – att samlas känslig information om cybersäkerheten i IKT-produkter, -tjänster och -processer. Det är därför viktigt att myndigheten har personal med erfarenhet av och förmåga att bedöma och hantera uppgifter enligt de krav som ställs i offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagen (2018:585). Utredningen ska också utarbeta kompletterande författningsförslag, inklusive om de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering ska tilldelas, i syfte att myndigheten ska kunna utföra de uppgifter som följer av EU:s cybersäkerhetsakt.

8.2 Det europeiska ramverket för cybersäkerhetscertifiering

Nationell myndighet för cybersäkerhetscertifiering

Av artikel 58.1 i EU:s cybersäkerhetsakt framgår att en eller flera nationella myndigheter för cybersäkerhetscertifiering ska fullgöra de uppgifter som framgår av det europeiska ramverket för cybersäkerhetscertifiering, dvs. cybersäkerhetsakten och de olika europeiska

ordningar för cybersäkerhetscertifiering som kommer att antas med stöd av akten (genomförandeakter).

Eftersom uppgifterna enligt EU:s cybersäkerhetsakt är grundläggande för vilken eller vilka myndigheter som kan komma ifråga som nationell myndighet för en eller flera av uppgifter finns skäl att närmare redogöra för vad dessa uppgifter innebär eller kan komma att innebära. Redogörelsen följer i tillämpliga delar strukturen i cybersäkerhetsakten.

Självbedömning av överensstämmelse enligt artikel 53

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. 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.

Cybersäkerhetscertifiering enligt artikel 56.5

I artikel 56.4 anges att de organ för bedömning av överensstämmelse som avses i artikel 60 får utfärda europeiska cybersäkerhetscertifikat på assuransnivå ”grundläggande” eller ”betydande”.

Av artikel 56.5 följer att en europeisk ordning för cybersäkerhetscertifiering kan föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av den ordningen endast kan utfärdas av ett offentligt organ. Ett sådant organ ska vara antingen 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. Det innebär att det endast är den nationella myndigheten för cybersäkerhetscertifiering eller ett annat offentligt ackrediterat organ, dvs. en annan myndighet, som är behörig att utfärda det aktuella certifikatet.

Cybersäkerhetscertifiering enligt artikel 56.6

I artikel 56.6 föreskrivs att om en europeisk ordning för cybersäkerhetscertifiering kräver assuransnivå ”hög” får 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.

När artikel 56.6 är tillämplig, dvs. när en europeisk ordning för cybersäkerhetscertifiering kräver assuransnivå ”hög” är det en nationell myndighet för cybersäkerhetscertifiering som får utfärda ett cybersäkerhetscertifikat på den nivån. Myndigheten har dock möjlighet att på förhand delegera rätten att utfärda certifikatet till ett angivet ackrediterat organ för bedömning av överensstämmelse eller besluta om en allmän delegering av den uppgiften till ett sådant organ för bedömning av överensstämmelse. Det är således den nationella myndigheten för cybersäkerhetscertifiering som har rätt att besluta om vilken aktör som får utfärda ett cybersäkerhetscertifikat på högsta assuransnivån.

Kontroll och övervakning enligt artikel 58 (tillsyn)

I artikel 58 anges vilka uppgifter som nationella myndigheter för cybersäkerhetscertifiering ska ha. En sådan myndighet ska bl.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,

- 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,
- aktivt bistå och stödja de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med förordningen,
- övervaka och kontrollera den verksamhet som bedrivs av de offentliga organ som avses i artikel 56.5,
- 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 förordningen,
- behandla klagomål 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,
- lämna en årlig sammanfattande rapport om den verksamhet som bedrivits enligt leden b, c och d eller enligt punkt 8 till Enisa och europeiska gruppen för cybersäkerhetscertifiering,
- 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 EU:s cybersäkerhetsakt eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och
- övervaka relevant utveckling på området för cybersäkerhetscertifiering.

8.3 Nationell myndighet för cybersäkerhetscertifiering

Förslag: Försvarets materielverk (FMV) ska utses till nationell myndighet för cybersäkerhetscertifiering.

Myndighetens certifieringsorgan ska vara nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a och 56.6 i EU:s cybersäkerhetsakt.

Myndigheten ska i sin verksamhet beakta nationella säkerhetsintressen vid tillämpningen av EU:s cybersäkerhetsakt.

Uppgifterna för en eller flera nationella myndigheter för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt innefattar sammantaget omvärldsbevakning av frågor som rör cybersäkerhet och cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer, samverkan med nationella och internationella aktörer på området, ansvar för cybersäkerhetscertifieringsverksamhet på högsta assuransnivån och tillsynsansvar över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering.

Frågor som rör cybersäkerhetscertifiering inom ramen för cybersäkerhetsaktens tillämpningsområde omfattar IKT-produkter, IKT-tjänster och IKT-processer i vid bemärkelse, dvs. certifiering av produkter, tjänster och processer som finns inom informations- och kommunikationsteknologi inom de flesta verksamhetsområden i samhället. Frågor som rör certifieringsverksamheten kommer att beröra informations- och cybersäkerhetsverksamheten i verksamhet som omfattar samhällsviktiga tjänster och många produkter och tjänster på konsumentmarknaden. Certifierade produkter, tjänster och processer kommer även att finnas i verksamheter inom ramen för säkerhetskänslig verksamhet.

Utgångspunkter

Utgångspunkterna för utredningens överväganden i frågan om vilken myndighet som ska anförtros uppgiften att vara nationell myndighet för cybersäkerhetscertifiering är – utöver de krav som anges i cybersäkerhetsakten – även den nationella utformningen och regleringen av verksamhet inom informations- och kommunikationsteknik i förening med de riktlinjer som anges i utredningsdirektiven.

Uppgifterna som den nationella myndigheten ska ansvara för ställer höga krav på att myndigheten och berörd personal besitter en bred och teknisk kunskap[1] om och erfarenhet av kontroll och certifiering av IKT-produkter, IKT-tjänster och IKT-processer inom flera olika samhällsområden och verksamheter. Även kraven på förmåga till omvärldsbevakning och förmåga till samverkan med nationella och internationella aktörer förutsätter motsvarande kunskap och erfarenhet.

En viktig utgångspunkt för utredningens överväganden i denna del blir att identifiera de uppgifter och ansvarsområden inom området för informations- och cybersäkerhet som aktuella befintliga myndigheter har i dag och som kan bedömas underlätta för den berörda myndigheten att fullgöra de uppgifter som följer av cybersäkerhetsakten.

I detta sammanhang ska beaktas den verksamhet som planeras och är under uppbyggnad i det svenska nationella cybersäkerhetscentret, vilket bl.a. har till uppgift att underlätta samverkan mellan berörda myndigheter på informations- och cybersäkerhetsområdet. Myndigheterna FMV, FRA, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen förbereder för närvarande etablerandet av det nationella cybersäkerhetscentret. Cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige. Centret ska även ge ett utvecklat och samordnat stöd till olika aktörer i offentlig och privat sektor om hur de kan skydda sig mot cyberattacker. Arbetet sker i form av ett gemensamt etableringsprojekt och verksamheten i centret kommer att utvecklas stegvis de kommande åren.

I detta sammanhang bör även beaktas förslaget om att ett europeiskt kompetenscenter för cybersäkerhet ska inrättas och där medlemsstaternas behöriga myndigheter kommer att erbjudas att delta.

En annan utgångspunkt är att uppgifter och ansvar, t.ex. vad gäller tillsyn, inom informations- och cybersäkerhetsområdet i dag är fördelade på flera myndigheter inom olika samhällssektorer, bl.a. gäller det NIS-direktivets tillämpningsområde och verksamhet som omfattas av regleringen om säkerhetsskydd.

När det gäller frågan om förutsättningarna för att etablera en tillsynsfunktion inom ramen för den nationella myndigheten för cyber-

[1] Även juridisk kunskap är viktig i sammanhanget, inte minst då myndigheten kommer att delta i framtagandet av genomförandeakter under cybersäkerhetsakten.

säkerhetscertifiering bör – förutom de krav som anges i EU:s cybersäkerhetsakt – även beaktas bl.a. de principiella uttalanden som regeringen gjort i skrivelsen 2009/10:79 *En tydlig, rättssäker och effektiv tillsyn*.[2]

Uppdraget i denna del innebär att utredningen ska lämna förslag på ett nationellt system med myndighetsansvar för de uppgifter som följer av cybersäkerhetsakten. Utredningen tolkar direktivens anvisning om att förslaget ska utgå från en befintlig myndighet som att de olika uppgifter, roller, och ansvarsområden som enligt cybersäkerhetsakten ska finnas på nationell nivå i och för sig kan fördelas på en eller flera befintliga myndigheter om det är mer ändamålsenligt och effektivt med en sådan lösning.

Inhämtade synpunkter

Utredningen har i skriftlig enkät i juni 2020 givit berörda myndigheter möjlighet att lämna synpunkter på vilken befintlig myndighet som bör vara nationell myndighet för cybersäkerhetscertifiering och om förutsättningarna att organisera certifieringsorgan och tillsynsfunktion i samma myndighet. Utredningen har efter att skriftliga svar lämnats haft möten med berörda myndighetsledningar för att inhämta ytterligare information och synpunkter i dessa två frågor.

Försvarsmakten framhåller att det finns många urvalskriterier som är av betydelse för att bedöma vilken myndighet som bör ges uppgiften att vara certifierande myndighet, bl.a. teknisk kompetens, kompetensförsörjning och förståelse för hotbilden. Myndigheten bedömer att FMV har bäst förutsättningar att bygga och vidmakthålla den förmågan över tiden. FMV har vidare värdefulla erfarenheter från det arbete som bedrivs i dag. Myndigheten anser vidare att det är främst FMV respektive MSB som bör komma ifråga för uppgiften som tillsynsmyndighet. Det är samtidigt tveksamt om man bör samla certifieringsfunktion och tillsynsansvar hos samma myndighet. I nuläget överväger dock fördelarna med att samla båda funktionerna i en myndighet. De två funktionerna måste dock vara autonoma och väl separerade i förhållande till varandra. Om en tvåmyndighetslösning

[2] Se även Tillsynsutredningens delbetänkande Statlig tillsyn – Granskning på medborgarnas uppdrag (SOU 2002:14).

övervägs bedöms MSB vara den myndighet som har bäst förutsättningar att utgöra tillsynsmyndighet.

Försvarets materielverk (FMV) anger att myndigheten ser flera möjliga myndigheter som kan få ansvar för cybersäkerhetscertifiering, även om det finns både för- och nackdelar i samtliga fall. FMV:s huvuduppdrag och kärnverksamhet är att upphandla varor och tjänster för Försvarsmaktens behov. I detta ingår produkter som är, eller kan vara, certifierade. Det finns konstitutionella utmaningar att organisera de uppgifter som följer av EU:s cybersäkerhetsakt, var och en med olika och eventuellt motstridiga verksamhetsmål, inom ramen för samma myndighet. Myndigheten ser en utmaning med att både certifieringsverksamhet och tillsyn skulle hanteras inom ramen för myndighetens organisation. Ifall en sådan konstruktion förordas bör ledning kunna hämtas från hur den militära flyginspektionen i Försvarsmakten är organiserat. Den är en fristående enhet organiserad i Försvarsmaktens Högkvarter och lyder direkt under regeringen i frågor om tillsyn. I övriga frågor lyder militära flyginspektionen under överbefälhavaren. Verksamheten leds av en flygsäkerhetsinspektör.[3] Om tillsynsverksamheten organiseras inom myndigheten enligt en sådan modell kan kravet på oberoende mötas. I sammanhanget kan uppmärksammas alternativet med en nämndmyndighet med myndigheten som värdmyndighet.[4] En sådan organisation skulle i större utsträckning möta krav på oberoende. Myndigheten framhåller även att myndigheten i sin roll som nationell industrisäkerhetsmyndighet sedan många år är medlem i internationella forum för industrisäkerhet, där det drivs gemensamt arbete med att ta fram ramverk inom cybersäkerhet för skydd av säkerhetsskyddsklassificerad information till stöd för industrin. FMV är den myndighet i Sverige som tecknar flest säkerhetsskyddsavtal, såväl nationellt som internationellt, där man i dagsläget har cirka 1 500 säkerhetsskyddsavtal med företag, varav cirka 150 är s.k. nivå 1 avtal som omfattar drygt 2 000 registerkontrollerade anställda i företagen. En möjlig myndighet är även MSB, med sin roll som samordnande myndighet i informations- och cybersäkerhetsfrågor samt med föreskriftsrätt för statliga myndigheter rörande informationssäkerhet. En annan möjlig myndighet

[3] I 21 a § förordningen (2007:1266) med instruktion för Försvarsmakten anges att när flygsäkerhetsinspektören utövar sin tillsynsfunktion över militär luftfart är flygsäkerhetsinspektören inte underställd överbefälhavaren. Motsvarande reglering finns i 21 § angående Försvarsinspektören för hälsa och miljös tillsynsansvar.
[4] 18 § myndighetsförordningen (2007:515).

är PTS som har erfarenhet av tillsynsfrågor och har även en utpekad roll när det gäller den s.k. eIDAS-förordningen, som berör certifieringsområdet.

Försvarets radioanstalt (FRA) framhåller att vid FMV finns redan det nationella certifieringsorganet för it-säkerhet i system och produkter. Myndigheten anser att det därför är lämpligt att FMV utses till nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten. Tillsynsfunktionen måste ha god kännedom om området för tillsynen. Samtidigt är det viktigt att det organ som får till uppgift att utöva tillsyn är självständigt i förhållande till den verksamhet som tillsynen riktas mot. En förutsättning för att en myndighet får både certifierings- och tillsynsansvaret är därför att funktionerna tydligt skiljs åt organisatoriskt inom myndigheten.

Myndigheten för samhällsskydd och beredskap (MSB) anser att uppdraget att vara nationell myndighet för cybersäkerhetscertifiering i första hand bör i sin helhet bör ges till myndigheten. Myndigheten kan skapa positiva synergieffekter och säkerställa att resultatet av tillsynsarbetet kan få direkt nytta i arbetet med att stärka samhällets informations- och cybersäkerhet. Myndigheten arbetar med många verktyg och med ett brett perspektiv på området. Arbetet inkluderar bland annat samordning och operativt arbete i enlighet med NIS-regleringen avseende informationssäkerhet hos leverantörer av samhällsviktiga och digitala tjänster, samt arbetet med offentlig sektor och övrig samhällsviktig verksamhet som bedrivs vid myndigheten. Myndigheten har en god förståelse och inblick i brister och utmaningar på informations- och cybersäkerhetsområdet vilket underlättar ett tillsynsarbete. Myndigheten driver en rad nätverk, har löpande strategisk och operativ omvärldsbevakning, genomför tematiska kartläggningar och tar emot incidentrapporter. Myndigheten driver ett intensivt arbete med att etablera en regelbunden uppföljning av informationssäkerhetsarbetet i offentlig sektor. Allt detta ger myndigheten tillgång till underlag för vad ett tillsynsarbete behöver omfatta. Myndigheten har erfarenhet av att samordna den informationssäkerhetstillsyn som bedrivs inom ramen för NIS-direktivet. Dessutom har myndigheten eget tillsynsansvar inom andra områden. Myndigheten har i och med detta byggt upp kompetens inom tillsyn och är väl insatt i hur tillsyn på informationssäkerhetsområdet bedrivs. Myndigheten har ett stort internationellt engagemang vilket underlättar arbetet som nationell myndighet för cybersäkerhetscertifiering,

eftersom uppgiften förutsätter god förståelse för internationellt standardiseringsarbete samt innebär krav på att vara kontaktpunkt till både EU och Enisa. Myndigheten deltar inom standardiseringsarbetet på internationell och europeisk nivå. Dessutom är myndigheten nationell kontaktpunkt för en rad centrala samarbeten på EU nivå. Uppgiften som nationell myndighet för cybersäkerhetscertifiering förutsätter omfattande samverkan med privata aktörer. Myndigheten har god vana av privat-offentlig samverkan inom området informations- och cybersäkerhet, bl.a. genom forum för informationsdelning om informationssäkerhet.

Polismyndigheten framhåller bl.a. att FMV alternativt det nya nationella cybersäkerhetscentret är huvudkandidater till nationell myndighet för cybersäkerhetscertifiering. Centret, eller den myndighet som centret inryms i, bör få rollen att vara nationell myndighet för cybersäkerhetscertifiering eftersom det krävs specialistkompetenser för att certifiera. Enligt Polismyndigheten kommer centret att ha etablerade kontaktytor mot exempelvis FRA, Säkerhetspolisen och MUST och genom dessa kunna erhålla relevant information om hotbild och sårbarheter i mjukvaruprodukter. Centret kommer också genom ett nära samarbete med den privata sektorn snabbt kunna fånga upp behov, feedback och annat som berör certifieringen.

Post och telestyrelsen (PTS) framhåller att myndigheten har i dag inte en tydlig roll i fråga om certifieringsorgan och tillsynsfunktion. Myndigheten berörs dock av EU:s cybersäkerhetsakt eftersom aktörer som myndigheten utövar tillsyn över kan komma att omfattas av kommande europeiska certifieringsordningar.[5] För myndighetens del blir de europeiska certifieringsordningarna på de områden som myndigheten har ett tillsynsansvar av betydelse inte bara avseende certifieringsordningarna utan även de säkerhetsstandarder som kraven baserar sig på. Certifieringsordningarna och säkerhetsstandarderna blir relevanta vid såväl tillsyn som vid utformning av föreskrifter inom myndighetens tillsynsområden. Myndigheten bedömer att FMV/CSEC är den myndighet som är mest lämpad att vara certifieringsorgan eftersom den myndigheten redan har uppgifter på området och som har en verksamhet som är närmast de uppgifter som ska utföras. FMV/CSEC bör ha bäst förutsättningar och kortast start-

[5] PTS har tillsynsansvar avseende lagen (2003:389) om elektronisk kommunikation, lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, eIDAS-förordningen ((EU) nr 910/2014) och säkerhetsskyddslagen (2018:585).

sträcka för uppdraget. FMV är även den myndighet som i dag har bäst kompetens och flest närliggande uppgifter för rollen som tillsynsmyndighet. Om det går att skapa en tillsynsfunktion på FMV som är tillräckligt avskild och oberoende från såväl verksamheten som certifieringsorganisation som myndighetens övriga verksamhet som berör användning av certifierade produkter bedöms FMV vara mest lämpad även som tillsynsmyndighet. Om bedömningen är att FMV inte bör ha uppgifterna som både certifieringsorgan och tillsynsmyndighet har PTS möjlighet att bygga upp en sådan tillsynsfunktion. Då det inte finns några direkta synergier med befintlig verksamhet på myndigheten skulle tillskott av resurser krävas och en längre startsträcka kan förväntas än om uppgiften läggs på FMV.

Säkerhetspolisen påpekar att den nationella myndigheten för cybersäkerhetscertifiering får ett brett uppdrag. Den myndighet som pekas ut att bli nationell myndighet behöver ha en mycket bred kompetens och hög förmåga inom ett flertal områden, framför allt inom teknik och certifiering av IKT-produkter, tjänster och processer. Det är i nuläget endast FMV/CSEC som, tillsammans med FRA, har den kompetens och förmåga som krävs för att kunna hantera uppdraget som nationell myndighet för cybersäkerhetscertifiering. En förutsättning för att ge en och samma myndighet ansvar både för certifiering och tillsyn är att funktionerna är tydligt åtskilda organisatoriskt. I övrigt ser myndigheten inte att det skulle föreligga några hinder mot att organisera certifieringsorgan och tillsynsfunktion i en och samma myndighet.

Totalförsvarets forskningsinstitut (FOI) påpekar att den framtida omfattningen av den nationella myndighetens arbete är svår att uppskatta. Däremot bör konsekvenserna av att myndigheter i alla medlemsstater säkerställer harmoniserade cybersäkerhetskrav för informations- och kommunikationsteknologi (IKT) inte underskattas. Ansvaret för it-säkerhet på angränsande områden bör övervägas vid val av myndigheter och eventuell fördelning av uppgifter. Cybersäkerhetsaktens tillsynsfunktioner som angränsar tillsyn av säkerhetsskydd bör hanteras av tillsynsansvariga myndigheter. Cybersäkerhetsaktens tillsynsfunktioner som omfattar samhällsviktiga och digitala tjänster bör hanteras av de myndigheter som utövar tillsyn över sådana tjänster eller att möjligheter till samverkande tillsyn mellan dessa tillsynsfunktioner beaktas. För cybersäkerhetsaktens tillsynsuppgifter bör även övervägas hur angränsningar till andra tillsyns-

ansvar kan effektiviseras. Myndigheten föreslår därför att tillsyn som avser certifikat med hög assuransnivå och som inbegriper säkerhetsskyddsklassificerade uppgifter eller informationssystem som gäller säkerhetskänslig verksamhet bör genomföras av de myndigheter som utövar tillsyn på området. Den nationella myndigheten eller myndigheterna bör kunna arbeta på ett sådant sätt så att nationella säkerhetsintressen inte påverkas av rapporteringskraven eller andra aspekter av certifieringsordningarna. En myndighet med ansvar för certifieringsordningen måste ha god förmåga att hantera de informationssäkerhetsrisker som insamlandet av information om it-system innebär samt en förståelse vilka antagonistiska hot som är förknippade med detta. Vidare bör det beaktas i vilken mån tillsynsmyndighetens uppdrag kan omfatta information, informationsdelning, samråd eller angränsa till ärenden om säkra kryptografiska funktioner och informationssäkerhet.

Genomförandet av EU:s cybersäkerhetsakt i andra länder

Utredningen har i syfte att få en bild av hur EU:s cybersäkerhetsakt införs i jämförbara medlemsstater sökt information om bl.a. hur nationella myndigheter för cybersäkerhetscertifiering organiseras. Med hänsyn till den begränsade utredningstid som stått till förfogande och rådande omständigheter i omvärlden har utredningen haft begränsad möjlighet att göra en sedvanlig internationell utblick genom att inhämta uppgifter vid t.ex. myndighetsbesök i utlandet. Även möjligheten till sedvanlig kvalitetssäkring av erhållna uppgifter har påverkats. Utredningen har i första hand eftersökt information på berörda myndigheters officiella webbsidor. I bl.a. Finland[6] och

[6] Den finska regeringen har lämnat en proposition till riksdagen (RP 98/2020 rd) med förslag till lagändringar med anledning av EU:s cybersäkerhetsakt. I lagförslaget utnämns det nationella Cybersäkerhetscentret vid Transport- och kommunikationsverket (Traficom) till nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten, både vad gäller funktionen att bevilja cybersäkerhetscertifikat på högsta assuransnivån och utövandet av tillsyn. Cybersäkerhetsaktens krav på strikt åtskillnad mellan den nationella cybersäkerhetscertifieringsmyndighetens certifieringsverksamhet och samma myndighets tillsynsverksamhet bedöms leda till ett ökat resursbehov och kräva att Traficom omorganiseras. Den finska regeringen anser att de nya uppgifterna kan tilldelas den existerande organisationen, men inte att samma personer ska få bevilja certifikat på assuransnivån hög och samtidigt sköta tillsynsuppgifter rörande anmälningar om överensstämmelse och kontrollorgan.

Nederländerna[7] har förslag lämnats på kompletterande nationell lagstiftning med anledning av EU:s cybersäkerhetsakt.

8.3.1 Förslag på nationell myndighet för cybersäkerhetscertifiering

Mot bakgrund av bl.a. ovan angivna utgångspunkter bedömer utredningen att det finns följande möjliga alternativ för hur ansvaret att lösa de angivna uppgifterna kan organiseras.

- En och samma myndighet får i uppdrag att vara nationell myndighet för cybersäkerhetscertifiering och att etablera tillsynsfunktionen.
- En myndighet får i uppdrag att vara nationell myndighet för cybersäkerhetscertifiering och en annan fristående myndighet får i uppdrag att ansvara för den nationella tillsynsfunktionen.
- En ansvarig sektorsmyndighet får uppdraget att inom sin sektor vara nationell myndighet för cybersäkerhetscertifiering och även ansvara för myndighetens tillsynsfunktionen inom sektorn.

När det gäller frågan om det bör vara en eller flera myndigheter som ska ansvara för angivna uppgifter och verksamhetsområden gör utredningen bedömningen att uppgifterna som avser omvärldsbevakning, samverkan och ansvar för certifieringsverksamheten bör hållas samman i en myndighet, samtidigt som verksamheten förutsätter en nära samverkan med övriga berörda myndigheter med uppgifter och ansvar som berör informations- och cybersäkerhetsområdet. Frågan om den myndighet som ska vara nationell myndighet för cybersäkerhetscertifiering även bör ha ansvar för tillsynen av efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering behandlas i avsnitt 8.4.

[7] Regeringen i Nederländerna har föreslagit en ny lag för genomförande av EU:s cybersäkerhetsakt. Ministeriet för Ekonomi och Klimatpolitik föreslås utses till nationell myndighet för cybersäkerhetscertifiering. Enligt motiven till lagförslaget planerar ministeriet att lägga de uppgifter som följer av cybersäkerhetsakten på landets telestyrelse, Agentschap Telecom (se www.internetconsultatie.nl/uitvoeringswetcyberbeveiligingsverordening, 2020-09-11). Effektivitetsskäl anförs till grund för införandet av samtliga funktioner i en befintlig organisation med erfarenhet av både verkställande arbete och separerad tillsynsverksamhet inom den digitala domänen.

Vilken eller vilka befintliga nationella myndigheter som bör tilldelas ansvaret att fullgöra en eller flera av uppgifterna bör grundas på de uppgifter och verksamhetsområden som aktuella myndigheter redan i dag ansvarar för eller om en myndighet kan bygga upp en ändamålsenlig och kostnadseffektiv verksamhet för att lösa uppgifterna.

Utredningen bedömer att med ovan angivna utgångspunkter bör uppgiften att vara nationell myndighet för cybersäkerhetscertifiering i första hand tilldelas en myndighet som redan arbetar med informations- och cybersäkerhetsfrågor, och om möjligt även bedriver certifieringsverksamhet på området. Detta innebär att det främst är någon av de myndigheter som ingår i samverkansgruppen för informationssäkerhet (SAMFI) som kan komma ifråga för att tilldelas de uppgifter och ansvarsområden som följer av cybersäkerhetsakten.

I kapitel 2 och 5 finns en närmare redogörelse för SAMFI myndigheternas olika roller, uppgifter och ansvarsområden inom ramen för arbetet med att utveckla och stärka informations- och cybersäkerheten i landet. Utöver dessa myndigheter bedriver Totalförsvarets forskningsinstitut (FOI) forsknings- och utvecklingsarbete på området. Det finns även andra myndigheter som i sin verksamhet hanterar informations- och kommunikationssäkerhet, dock bedöms ingen av dessa myndigheter bedriva sådan verksamhet att de bör vara aktuella för sådana uppgifter som ska anförtros den nationella myndigheten för cybersäkerhetscertifiering.

Flera av de nu aktuella myndigheterna har utöver sina huvuduppgifter vissa uppgifter med beröring till informations- och kommunikationssäkerhet. Försvarsmakten, FRA, SÄPO, och Polisen har sina huvudsakliga roller och ansvar inom ramen för Sveriges försvar och säkerhet och bedriver försvarsverksamhet, underrättelse- och säkerhetstjänst samt brottsbekämpning. Ingen av de sist nämnda myndigheterna, inte heller FOI, bedriver dock i dag sådan verksamhet som medför att det framstår som naturligt eller ändamålsenligt att tilldela en eller flera av dessa myndigheter ansvar för en eller flera av de uppgifter som följer genom cybersäkerhetsaktens införande i Sverige. En eller flera av dessa myndigheter kan dock komma att beröras av frågor som rör cybersäkerhetscertifiering, t.ex. inom ramen för den egna verksamheten eller i egenskap av tillsynsmyndighet, vilket ställer krav på samverkan på nationell nivå mellan den myndighet som får ansvar att vara nationell myndighet för cybersäker-

hetscertifiering och andra berörda myndigheter. Frågan om behovet av utökad samverkan mellan myndigheterna behandlas i kapitel 13.

Utredningen bedömer därför att det i första hand är FMV, MSB och PTS som kan komma i fråga som nationell myndighet för cybersäkerhetscertifiering.

Försvarets materielverk (FMV)

FMV:s huvudsakliga uppdrag är att biträda Försvarsmakten i planeringen av materiel- och logistikförsörjningen och med materielsystemkunskap. Myndigheten biträder också med kompetens när det gäller vidmakthållande och upphandling och ansvarar för upphandling av bl.a. varor och tjänster inom materielförsörjningsområdet som inte omfattas av Försvarsmaktens egna upphandlingsansvar.

FMV har genom stärkt internationell samverkan bidragit till att ta fram ett ramverk för stöd till att hantera cyberhot, sårbarheter och motåtgärder, vilket kan användas av säkerhetsexperter inom både stat och näringsliv. Arbetet är ett resultat av ett samarbete inom Multinational Industrial Security Working Group (MISWG) som arbetar med strategier för nationell cybersäkerhet, policyer för nationell industrisäkerhet och bästa praxis i detta sammanhang. Mot bakgrund av att flera av deltagarländerna i MISWG redan har motsvarande nationella modeller uppnås dessutom harmoniering på området.

FMV bedriver i dag 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). FMV ska enligt myndighetens instruktion i sin verksamhet verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat samt vara Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat (CCRA) och motsvarande överenskommelse inom Europa (SOG-IS MRA). FMV ska i sin verksamhet även beakta nationella säkerhetsintressen. FMV/CSEC har inom ramen för CCRA och den europeiska motsvarigheten SOG-IS medverkat i det fortsatta arbetet med att utveckla och effektivisera Common Criteria, där arbetet är inriktat på att främja en ökad harmonisering av kraven på it-säkerhet för specifika produktkategorier.

CSEC behandlade cirka 30 certifieringar under 2019.[8] Parallellt med detta arbete har certifieringsordningen utvecklats vidare i syfte att bli alltmer tydlig och göra arbetet mer effektivt. Vidare har CSEC genomfört tillsyn av två evalueringsföretag med licens att granska it-säkerhet i produkter inom ramen för certifieringsordningen. CSEC gav även stöd till MSB arbetet med att utarbeta säkerhetskrav för bl.a. säkra USB-minnen och krav på säkerhetsfunktioner i databashanterare.

FMV/CSEC har även uppdraget att ansvara för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämplar enligt artikel 30 och 39 i 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.

FMV/CSEC har således mångårig erfarenhet av certifiering inom informations- och cybersäkerhetsområdet och är i dag organiserat inom myndigheten för att möta de krav på oberoende som gäller för ett ackrediterat organ för bedömning.

Utredningen bedömer att FMV:s uppgifter och verksamhet medför att myndigheten har både en omfattande och en djup teknisk kompetens inom olika verksamhetsområden, bl.a. inom området för informations- och cybersäkerhet samt inom området certifiering av it-säkerhet i produkter och system. Myndigheten har mot den bakgrunden förutsättningar för att – utöver själva certifieringsverksamheten – även kunna ansvara för huvuddelen av de övriga uppgifter som följer av cybersäkerhetsakten och europeiska ordningar för cybersäkerhetscertifiering, bl.a. omvärldsbevakning av cybersäkerhet, samverkan med nationella och internationella aktörer samt den certifieringsverksamhet som den nationella myndigheten för cybersäkerhetscertifiering ska ansvara för.

När det gäller frågan om tillsynsverksamhet kan noteras att FMV i dag inte har några formella tillsynsuppgifter. Samtidigt kan noteras att myndigheten är föreslagen att vara tillsynsmyndighet för en betydande del av verksamheter som bedriver säkerhetskänslig verksamhet på försvarsmaterielområdet och som omfattas av regleringen för säkerhetsskydd. I betänkandet *Kompletteringar till den nya säker-*

[8] Exempel på certifieringsuppdrag är brandväggar, säkra skrivare, datadioder, Linux operativsystem och produkter för intrångsdetektering.

hetsskyddslagen (SOU 2018:82) föreslås FMV få ansvar för tillsyn över enskilda verksamhetsutövare inom området försvarsmateriel. Det föreslagna tillsynsområdet bedöms omfatta samtliga företag som levererar varor, tjänster och byggentreprenader samt logistiktjänster kopplade till det militära försvarets förmåga, vilket bedöms omfatta alla leverantörer som myndigheten har tecknat säkerhetsskyddsavtal med. Inom tillsynsområdet finns också leverantörer som tecknat säkerhetsskyddsavtal med andra myndigheter i liknande syften. Andra aktörer som bedriver säkerhetskänslig verksamhet inom området försvarsmateriel kan vara företag som utvecklar koncept för framtida vapensystem eller teknik som väsentligen ska användas i ett militärt sammanhang, utan att det görs på uppdrag av en myndighet. Enligt vad som anges i betänkandet berörs mellan 1 500–2 000 tillsynsobjekt inom tillsynsområdet. Betänkandet är föremål för beredning i Regeringskansliet.

Myndigheten för samhällsskydd och beredskap (MSB)

MSB bedriver redan i dag verksamhet med att utveckla och stödja informations- och cybersäkerheten i samhället (kapitel 5). MSB deltar bl.a. aktivt i standardiseringsarbetet inom området informationssäkerhet. I sitt arbete med Common Criteria ger MSB, i samarbete med FMV, ut rekommendationer för användning av en skyddsprofil eller certifierad produkt. Förvaltningen av en referenslista över rekommenderade skyddsprofiler kommer att ingå i myndighetens löpande arbete för vidareutveckling av stöd inom it-säkerhet.

MSB deltar också i internationella mötesforum samt bedriver omvärldsbevakning kring CC-standarden, både på nationell och internationell nivå, för att i första hand kunna inventera och representera det civila samhällets behov av produktkategorier som är lämpliga att ta fram skyddsprofiler emot.

Myndigheten har också särskilda samordningsuppgifter för verksamhet som omfattas av lagen om samhällsviktiga tjänster (NIS-direktivet). Till det kommer det arbete och de föreskrifter som myndigheten tar fram för statliga myndigheters informationssäkerhetsarbete.

Myndigheten har också teknisk kompetens inom ramen för det arbete som bl.a. bedrivs vid CERT-SE och RAKEL-verksamheterna

samt inom ramen för det stöd man lämnar till ledningsplatser och signalskydd. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Till uppgifterna hör bl.a. att agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade, samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet och vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa. Vid den nationella CSIRT funktionen finns medarbetare med en bred teknisk kompetens inom bland annat it-säkerhet.

MSB ska vidare enligt den nationella handlingsplanen ta fram och förankra en treårig handlingsplan för ett strategiskt och långsiktigt arbete med standardisering avseende systematiskt och riskbaserat informationssäkerhetsarbete. Åtgärden genomförs tillsammans med FMV/CSEC, berörda myndigheter och organisationer.

MSB har dock ingen djupare teknisk kompetens på området för produktcertifieringar och skulle därför behöva bygga upp, etablera och utveckla en sådan verksamhet. Ett alternativ till en sådan åtgärd skulle vara att överföra CSEC:s certifieringsverksamhet och ansvar som nationellt certifieringsorgan för IT-säkerhet till MSB. Frågan om en sådan överföring har tidigare varit föremål för övervägande i NISU 2014-utredningen[9]. Utredningen fann vid den tidpunkten dock inte skäl att förslå någon organisatorisk förändring av CSEC:s verksamhet.

Samtidigt kan noteras att MSB till skillnad från FMV redan i dag bedriver tillsyn inom tilldelade ansvarsområden Myndighetens tillsynsverksamhet bedrivs inom tre delområden som är tillsyn, tillsynsvägledning och marknadskontroll.

Post- och telestyrelsen (PTS)

PTS är en myndighet med ansvar för elektronisk kommunikation och som sådan en mycket central aktör för säkerhetsarbete på detta område De europeiska certifieringsscheman som kan komma att

[9] Informations- och cybersäkerhet – i Sverige Strategi och åtgärder för säker information i staten (SOU 2015:23).

antas inom ramen för cybersäkerhetsakten kan förväntas omfatta all typ av informations- och kommunikationsteknologi (IKT) och som berör all samhällsverksamhet. Samtidigt kan noteras att myndigheten har begränsad erfarenhet av arbete med nu aktuella cybersäkerhetscertifieringar och saknar därmed den tekniska specialistkompetens som krävs på certifieringsområdet.

Utredningen gör bedömningen att PTS nuvarande roll, ansvar och verksamhet på elektronik- och telekommunikationsområdet, som inte innefattar aktuell certifieringsverksamhet, skulle medföra att myndigheten skulle behöva bygga upp en verksamhet med kompetens och teknisk expertis som möter kraven i cybersäkerhetsakten på förmåga till omvärldsbevakning inom cybersäkerhet och cybersäkerhetscertifiering, förmåga till samverkan inom området och förmåga att verka som nationell myndighet för cybersäkerhetscertifiering på högsta assuransnivån.

Försvarets materielverk föreslås utses till nationell myndighet för cybersäkerhetscertifiering

Utredningen kan till en början konstatera att såväl FMV/CSEC, som MSB och PTS har uppgifter och bedriver verksamhet inom området för informations- och kommunikationsteknologi (IKT). Utredningen bedömer samtidigt att finns både fördelar och nackdelar när det gäller vilken av dessa myndigheter som bör anförtros uppdraget att vara nationell myndighet med ansvar för de uppgifter som följer av det europeiska ramverket för cybersäkerhetscertifiering.

Till FMV:s fördel talar att myndigheten genom sitt uppdrag att bl.a. vara nationell myndighet för certifiering av system och produkter inom it-säkerhet redan har en bred och djup kunskap om cybersäkerhetscertifiering och även lång erfarenhet av både omvärldsbevakning av dessa frågor samt internationell och nationell samverkan med andra berörda aktörer på området. Inom myndigheten finns redan organisatoriskt CSEC som ett ackrediterat organ för bedömning enheten av överensstämmelse vid certifiering av system och produkter på området it-säkerhet.

Även om MSB respektive PTS har redovisade uppgifter och ansvar inom informations- och kommunikationsteknologi bedriver ingen av dessa myndigheter verksamhet som innefattar prövning och teknisk bedömning för cybersäkerhetscertifiering, vilket innebär att

CSEC:s verksamhet skulle behöva föras över till en av dessa myndigheter alternativt att motsvarande verksamhet skulle behöva byggas upp vid myndigheten. Även uppgifterna avseende omvärldsbevakning och samverkan på området skulle enligt utredningens bedömning förutsätta att kompetens tillförs och byggs upp för att möta kraven på dessa områden enligt cybersäkerhetsakten. Kraven på organisatoriska förändringar i form av ett överförande av CSEC till en av dessa myndigheter och ett ökat resursbehov för kompetensuppbyggnad bedömer utredningen inte medföra några fördelar i förhållande till att motsvarande verksamhet utvecklas vid FMV.

Sammantaget talar det angivna för – enligt utredningens bedömning – för att FMV bör anförtros uppgiften att vara nationell myndighet för cybersäkerhetscertifiering för med ansvar för omvärldsbevakning, samverkan och certifieringsverksamhet på högsta assuransnivån. Det medför att myndigheten bör få uppdraget att vara den nationella myndigheten för cybersäkerhetscertifiering som anges i artikel 56.5 a, och 56.6. FMV får då i uppgift att vara den nationella myndighet som enligt artikel 56.6 får utfärda cybersäkerhetscertifikat när en europeisk ordning för cybersäkerhetscertifiering som antagits enligt artikel 49 kräver assuransnivå hög. Efter förhandsgodkännande av myndigheten får ett sådant enskilt europeiskt cybersäkerhetscertifikat även utfärdas av ett organ för bedömning av överensstämmelse. Myndigheten får även genom allmän delegering på förhand till ett organ för bedömning av överensstämmelse ge detta tillstånd att utfärda europeiskt cybersäkerhetscertifikat.

Utredningen vill i detta sammanhang framhålla att det europeiska ramverket för cybersäkerhetscertifiering är under införande i medlemsstaterna och någon europeisk ordning för sådan certifiering har ännu inte antagits, även om ett utkast till sådan ordning offentliggjorts under utredningstiden. Det innebär att den framtida omfattningen av certifieringsverksamheten på grundval av en eller flera sådana europeiska ordningar blir svår att bedöma och därför även dess organisatoriska och resursmässiga konsekvenser. Detta innebär enligt utredningen att nu aktuella frågeställningar bör tas upp till ny bedömning när omfattningen och resursbehovet av certifieringsverksamheten närmare kan bedömas.

Utredningens överväganden och förslag när det gäller frågan om FMV även bör ha ansvar för tillsynsfunktion eller om det är lämpligare och mer ändamålsenligt att ansvaret för certifierings- respektive

tillsynsverksamheten fördelas på två olika myndigheter behandlas nedan i avsnitt 8.4.

8.3.2 Certifieringsorganet och krav på oberoende ställning

Förslag: Vid Försvarets materielverk (FMV) 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 EU:s cybersäkerhetsakt är denne inte underställd myndighetschefen.

Bedömning: Certifieringsorganets ekonomiska resurser bör bestämmas i särskild ordning av regeringen.

Med utredningens förslag att FMV ska vara nationell myndighet för cybersäkerhetscertifiering uppkommer även frågan om CSEC, som i dag är en organisatorisk enhet inom myndigheten FMV, har en sådan organisatorisk ställning och arbetsformer att dessa möter de krav som följer av cybersäkerhetsaktens reglering av ackrediterade organ för bedömning av överensstämmelse för bedömning.

I artikel 56.4 anges att de organ för bedömning av överensstämmelse som avses i artikel 60 får utfärda europeiska cybersäkerhetscertifikat som avser assuransnivå ”grundläggande” eller ”betydande” på grundval av de kriterier som anges en europeisk ordning för cybersäkerhetscertifiering, som antagits av kommissionen i enlighet med artikel 49.

Ett europeiskt cybersäkerhetscertifikat får utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a och 56.6 om certifieringsorganet har ackrediterats som ett organ för bedömning av överensstämmelse enligt punkt 1 i artikel 60.

Av artikel 56.5 a följer att ett sådant organ i vissa fall, dvs. när det anges i en europeisk ordning för cybersäkerhetscertifiering, ska vara en nationell myndighet för cybersäkerhetscertifiering under förutsättning att certifieringsorganet vid myndigheten uppfyller ställda krav på ett ackrediterat organ för bedömning av överensstämmelse.

I artikel 60.1 anges 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 dock endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilagan till cybersäkerhetsakten. I punkten 1 i bilagan föreskrivs att 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. 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.

Vidare föreskrivs att ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för att utföra bedömningen av överensstämmelse, inte får utgöras av någon 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 (punkten 4).[10]

Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får inte heller delta direkt i konstruktionen, tillverkningen, marknadsföringen, installationen, användningen eller underhållet av IKT-produkter, IKT-tjänster eller IKT-processer som bedöms, eller företräda de parter som bedriver sådan verksamhet (punkten 5).

Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får inte heller delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömningen av överensstämmelse, särskilt vad gäller konsulttjänster (punkten 5).

En medlemsstat ska även 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 avskild från uppgifter och

[10] 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.

ansvarsområden i förhållande till tillsynsverksamheten och att dessa verksamheter utförs oberoende av varandra. Vidare ska den nationella myndigheten som utövar tillsyn vara oberoende av de enheter som den utövar tillsyn över vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande.

Utredningen kan notera att organisationsenheten CSEC i egenskap av nationellt certifieringsorgan av it-säkerhet redan i dag är organiserat på ett sätt som möter kraven på oberoende ställning inom myndigheten FMV för att möta de krav som anges i internationella överenskommelser och övriga bestämmelser i syfte att vara ett ackrediterad organ för bedömning av överensstämmelse.

Frågan är då om CSEC:s nuvarande organisation och ställning inom FMV kan anses uppfylla de krav som anges i bilagan till EU:s cybersäkerhetsakt. Enligt punkten 19 i bilagan ska ett organ för bedömning av överensstämmelse 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. Utredningen kan konstatera att CSEC är i dag ackrediterad som organ för bedömning av överensstämmelse som utför certifiering av IKT-produkter, IKT-tjänster eller IKT-processer och får därför anses uppfylla kraven i denna punkt.

Vidare anges i punkten 6 i bilagan att när 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.

FMV har föreslagit att det kan finnas skäl att stärka CSEC:s oberoende inom myndigheten för att möta kraven på oberoende och att bl.a. organiseringen av den militära flygsäkerhetsinspektionen i Försvarsmakten kan tjäna som förebild i detta avseende.

Utredningen delar myndighetens bedömning och anser att CSEC:s oberoende inom FMV ska säkerställas genom att det i författning anges att det organ för certifiering som ska finnas i myndigheten, dvs. i nuläget CSEC, i sin certifieringsverksamhet är en oberoende funktion inom myndigheten FMV. Fråga uppkommer om även chefen för certifieringsorganet bör utses av regeringen och om budget och ekonomiska resurser bör bestämmas i särskild ordning.

Utredningen bedömer att vad som anges i punkten 6 (se ovan) i förening med att certifieringsorganets oberoende regleras i den kompletterande nationella författningsregleringen utgör tillräckliga åtgärder för att säkerställa certifieringsorganets oberoende i den nationella myndigheten för cybersäkerhetscertifiering (FMV). Det saknas därför för närvarande skäl att föreslå ytterligare åtgärder, t.ex. att chefen för certifieringsorganet ska utses av någon annan än chefen för myndigheten. Utredningen anser dock att certifieringsorganets ekonomiska resurser bör beslutas i särskild ordning av regeringen. Det innebär sammantaget att certifieringsorganet, dvs. CSEC, bedöms möta angivna krav i bilagan till EU:s cybersäkerhetsakt som oberoende organ för bedömning av överensstämmelse.

I utredningsdirektiven anges att vid Försvarets materielverk finns ett nationellt certifieringsorgan för it-säkerhet i produkter och system och att myndigheten, certifieringsorganet, ska i sin verksamhet beakta nationella säkerhetsintressen. Ett sådant krav bör införas även i den reglering som föreslås av utredningen.

Utredningen noterar att den bestämmelse som redan finns anger att myndigheten, certifieringsorganet, i sin verksamhet ska beakta nationella säkerhetsintressen. Bestämmelsen är enligt sin lydelse begränsad till viss certifieringsverksamhet och det kan råda osäkerhet om bestämmelsens tillämpningsområde. Det bör därför enligt utredningens bedömning införas en motsvarande bestämmelse för myndigheten FMV och dess certifieringsorgan och som ska tillämpas i myndighetens verksamhet som följer av EU:s cybersäkerhetsakt. Det finns därför skäl att införa en sådan bestämmelse i den kompletterande författningsreglering som nu föreslås.

8.4 Tillsyn

8.4.1 Inledning

Utredningen har i kapitel 4 och avsnitt 8.2 redogjort närmare för cybersäkerhetsaktens struktur och olika bestämmelser. Det finns dock skäl att i detta sammanhang inledningsvis översiktligt återge de huvuduppgifter som utredningen bedömer ligger till grund för och därmed blir styrande för hur tillsynsverksamheten lämpligen kan och bör organiseras.

Genom det europeiska ramverket för cybersäkerhetscertifiering fastställs en mekanism för inrättandet av europeiska ordningar för cybersäkerhetscertifiering. Av artikel 58 framgår att en nationell myndighet för cybersäkerhetscertifiering ska ansvara för tillsynen av efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering. I artikel 54 anges att en europeisk ordning för cybersäkerhetscertifiering ska innehålla minst de komponenter och regleringar som anges i den artikeln. I punkten j anges bl.a. att en sådan ordning ska innehålla regler för övervakning av efterlevnaden av IKT-produkter, IKT-tjänster och IKT-processer när det gäller kraven för EU-försäkran om överensstämmelse eller europeiska cybersäkerhetscertifikat, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven. Vidare ska enligt punkten k anges de villkor som ska gälla för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat samt villkor för utvidgning eller inskränkning av tillämpningsområdet för certifiering. Av punkten följer att även bestämmelser om följderna för IKT-produkter, IKT-tjänster och IKT-processer för vilka en EU-försäkran om överensstämmelse har utfärdats eller som har certifierats, men som inte överensstämmer med kraven i ordningen, ska anges.

Kommissionen kommer i unionens löpande arbetsprogram att fastställa strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. Även om något arbetsprogram ännu inte offentliggjorts har Enisa den 2 juli 2020 offentliggjort ett första utkast till en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter som uppfyller kraven för på assuransnivåerna ”betydande” respektive ”hög”. Vidare anges vad som ska gälla vid när vissa bestämmelser inte efterlevs.

Utredningen kan notera att den föreslagna ordningen, utöver att närmare ange vilka krav som ska uppfyllas för att ett cybersäkerhetscertifikat ska kunna utfördas, också innehåller en detaljerad och omfattande reglering av bl.a. olika frågor som kan uppkomma i samband med handläggningen av en ansökan, utfärdande och underhåll av ett certifikat samt vad som gäller ett eventuellt återkallande av certifikatet. Utredningen bedömer att de olika europeiska ordningarna i betydande omfattning kommer att reglera de olika krav som ska gälla vid såväl handläggningen av olika ärenden som omfattas av cybersäkerhetsaktens tillämpningsområde, som grunderna för själva bedömning av överensstämmelse men även vad som ska gälla i form av tillsyn.

Eftersom såväl cybersäkerhetsaktens bestämmelser som bestämmelserna i de europeiska ordningarna för cybersäkerhetscertifiering har direkt effekt och är tillämpliga i en medlemsstat uppkommer frågan i vilken utsträckning det finns utrymme och behov av och förutsättningar för kompletterande nationell reglering på området.

Utredningen kan konstatera att eftersom några europeiska ordningar för cybersäkerhetscertifiering, utöver det nu aktuella utkastet till en sådan ordning, ännu inte formellt antagits eller fastställts föreligger en osäkerhet om vilka krav som kan komma att ställas på den nationella tillsynen för att möta framtida behoven av tillsyn med anledning av de europeiska ordningar som kan komma att antas på området.

Utredningen bedömer dock att cybersäkerhetsaktens olika bestämmelser om tillsyn ger utrymme för att med en tillräcklig grad av säkerhet vid denna tidpunkt kunna lämna förslag om hur den nationella tillsynsverksamheten bör organiseras och utformas. Utredningen gör samtidigt bedömningen, på motsvarande sätt som gäller för kompletterande nationella föreskrifter för cybersäkerhetscertifiering, att utrymmet för berörda myndigheter att meddela ytterligare föreskrifter på tillsynsområdet för närvarande blir begränsat då eventuella myndighetsföreskrifter måste beakta den framtida unionsrättens reglering på området.

8.4.2 Utgångspunkter

Den närmare innebörden av begreppet tillsyn är inte närmare definierad vare sig i EU:s cybersäkerhetsakt eller i den nationella rättsordningen, även om begreppet förekommer på olika verksamhetsområden. En tydlig avgränsning till begrepp som rådgivning vägledning, och utbildning saknas. För att tillsynen ska vara ändamålsenlig och effektiv krävs att det inte råder oklarhet om när en myndighet uppträder i rollen som tillsynsmyndighet, vad som är föremål för tillsyn och hur tillsynen ska gå till.

I samband med att en myndighet lämnar rådgivning uppkommer ofta en risk för att råd lämnas om vad som ska göras snarare än hur något bör göras. Detta medför att råd som tillsynsmyndigheten lämnar kan utmynna i att tillsynsobjektet vidtar åtgärder som senare blir föremål för tillsyn, vilket kan underminera själva syftet med tillsynen som en fristående granskning. Detta väcker också tveksam-

heter vad gäller objektivitet eftersom tillsynsmyndighetens förmåga att upptäcka brister vid en efterföljande tillsyn kan ifrågasättas. Det är således viktigt att tillsynsobjektets tydliga ansvar för åtgärder inte påverkas eller förskjuts i riktning mot tillsynsmyndigheten, vilket det finns en risk för om tillsynsmyndigheten ska utöva tillsyn och lämna råd till samma verksamhetsutövare.

Ett tydliggörande av tillsynsverksamhetens inriktning och syfte skapar också förutsägbarhet och minskar utrymmet för godtyckligheten. Det är därför viktigt att det av regleringen framgår vad tillsynen syftar till och innebörden av denna. Vidare är ramarna för tillsynens omfattning av betydelse för att kunna fastställa hur långt tillsynsmyndigheternas befogenheter sträcker sig. Det finns även behov av att närmare reglera hur tillsynsverksamheten ska bedrivas.

I dag finns heller ingen formell eller författningsreglerad tillsynsstruktur för den verksamhet som det europeiska ramverket för cybersäkerhetscertifiering kommer att omfatta. Det kommer därför att finnas ett behov av att upprätthålla en översiktlig och sammanhållen bild över tillsynsverksamheten för att kunna följa upp, utvärdera och utveckla tillsynen på området.[11]

Utredningen kan konstatera att omfattningen av tillsynsverksamheten är svår att bedöma då det är fråga om lagstiftning som inte tidigare tillämpats vilket medför svårigheter att uppskatta antalet tillsynsobjekt. Det är en förutsättning att tillsynsmyndigheten har en lägesbild över vilka tillsynsobjekt som man har i uppdrag att kontrollera för att kunna bedriva ändamålsenlig och effektiv tillsyn.

Utredningen kan vidare konstatera att eftersom det i dag inte bedrivs någon formell tillsyn av verksamheter på cybersäkerhetsaktens tillämpningsområde är det svårt att få en tydlig bild över tillgången på sak- och tillsynskompetens för den tillsyn som nu införs. Experterna i utredningen har upplyst att det i dag råder brist på kompetent personal för uppgifter, bl.a. tillsyn, som följer av cybersäkerhetsaktens införande. Även om det inom FMV och certifieringsorganet CSEC finns kompetens om certifiering av it-säkerhet i produkter och system medför bristen på kompetens i dagsläget att den blivande tillsynsfunktionen behöver vidta åtgärder för kunna bedriva en ändamålsenlig och effektiv tillsyn, eftersom rekrytering och utbildning kommer att ta tid i anspråk.

[11] Se bl.a. Riksrevisionens rapport Informationssäkerheten i den civila statsförvaltningen (RIR 2014:23).

Frågan är då hur tillsynsverksamheten kan organiseras och utformas med utgångspunkt i bl.a. de krav på tillsynsverksamheten som föreskrivs i cybersäkerhetsakten och i linje med regeringens skrivelse *En tydlig, rättssäker och effektiv tillsyn* (skr. 2009/10:79).[12]

Utredningen redogör nedan för några av de mer principiella utgångspunkter som bör ligga till grund för fortsatta överväganden om organisering och utformning av den tillsynsverksamhet som cybersäkerhetsakten anger ska finnas på nationell nivå i en medlemsstat. I det sammanhanget redogörs även för några av de utredningar som tidigare behandlat frågor om tillsyn på informations- och kommunikationssäkerhetsområdet.

Regeringens skrivelse En tydlig, rättssäker och effektiv tillsyn (skr. 2009/10:79)

I regeringens skrivelse *En tydlig, rättssäker och effektiv tillsyn* (skr. 2009/10:79), lämnas generella bedömningar och görs principiella ställningstaganden av hur en tillsynsreglering bör vara utformad. I skrivelsen framhålls bl.a. betydelsen av enhetlighet i fråga om offentlig tillsyn. Det lämnas samtidigt utrymme för att göra avsteg från de bedömningar som görs i skrivelsen. Ett viktigt skäl för att precisera tillsynsbegreppet anges vara att en tydlig definition gör det enklare att skilja granskandet från främjande verksamhet. Ett tydligt och avgränsat tillsynsbegrepp behöver samtidigt inte hindra att tillsynsmyndigheter även kan ha till uppgift att arbeta främjande och förebyggande för att effektivt uppnå lagstiftningens mål. Det är i allmänhet inte lämpligt att tillsynsmyndigheten ger råd om hur tillsynsobjekten ska agera i specifika ärenden. Ett skäl till det anges vara att det kan uppstå svårigheter om tillsynsmyndigheten tidigare lämnat råd i ärenden som sedan blir föremål för tillsyn. Samtidigt framhålls att inom vissa tillsynsområden kan skäl tala för att, utöver upplysningar om gällande rätt, så kan även rekommendationer och vägledning utgöra del av tillsynen. En annan faktor som tas upp är vilka risker regelöverträdelser kan orsaka. Regelöverträdelser som innebär

[12] Statskontoret framhåller i sin rapport Tänk till om tillsynen betydelsen av att staten ser tillsynen som ett sammanhållet system, där de olika delarna reglering, organisering, styrning, finansiering och ingripandemöjligheter samspelar för att bästa möjliga resultat av verksamheten ska kunna åstadkommas (s. 93).

risker för exempelvis människors liv och hälsa kan påverka såväl behovet av en enhetlig tillsyn som utformning av sanktioner.

I skrivelsen framhålls att det är viktigt att utgå från de förutsättningar som gäller för det specifika tillsynsområdet. Det går inte att bortse från att många tillsynsområden har väsentligt olika förutsättningar som påverkar hur tillsynsregelverket bör utformas för att effektivt bidra till att de materiella reglerna efterlevs och intentionerna i regelverken förverkligas. Faktorer som kan behöva vägas in är bland annat vem som bedriver den verksamhet som tillsynen avser, vilket slag av verksamhet som tillsynen riktas mot, vilka risker regelöverträdelser kan orsaka och hur det materiella regelverk som tillsynen avser är utformat. Vidare påpekas att det måste beaktas att tillsyn är kostnadskrävande och orsakar störningar och påfrestningar för den som kontrolleras.

I skrivelsen framhålls att begreppet tillsyn främst bör användas för verksamhet som avser självständig granskning för att kontrollera om tillsynsobjektet uppfyller krav som följer av lagar och andra bindande föreskrifter. En grundläggande förutsättning för tillsynen är att tillsynsorganet har författningsreglerade möjligheter att ingripa. Tillsynsorganen bör ha rätt att av den objektsansvarige få del av de upplysningar eller handlingar som behövs för tillsynen. Tillsynsorganet bör även ha tillträdesrätt till utrymmen som används i den tillsynspliktiga verksamheten. Tillsynsorganen bör ha möjlighet att begära biträde från Kronofogdemyndigheten. Vidare bör tillsynsorganen ha möjlighet att ålägga den som är tillsynsobjektet ansvar för att utöva egen kontroll av sin verksamhet. Alla ingripanden bör kunna överklagas.

Tillsyn enligt förslag av NISU 2014

Frågan om tillsyn över den statliga sektorns informationssäkerhet behandlades i betänkandet *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23).

Utredningen konstaterade att ett antal myndigheter vid sidan om Försvarsmakten, Säkerhetspolisen och sektorsmyndigheterna har tillsynsansvar inom informationssäkerhetsområdet, bl.a. Datainspektionen, Finansinspektionen och Strålsäkerhetsmyndigheten. Enligt utredningen är detta en krävande uppgift som ställer höga krav på

expertkompetens då tillsynsansvaret omfattar alla aspekter av informationssäkerhet, allt från administrativ säkerhet till it-säkerhet och krypto. Enligt utredningen är det inte rimligt att kräva eller förutsätta att den bredd och djup i kompetens som krävs ska finnas inom varje tillsynsmyndighet. Betydligt effektivare och mer rationellt vore om tillsynen genomförs i samverkan med en utpekad myndighet som har den djupa kompetens som krävs. Då skulle tillsynsmyndigheten ha ansvaret och kunskapen om föremålet för tillsyn, och samtidigt dra fördel av expertmyndighetens djupa fackkunskaper. Detta bidrar till kvalitet och stabilitet i tillsynen och en jämn tillämpning av informationssäkerhetskraven på tillsynsobjekten. En samordning av stöd till tillsynsverksamheten vore också effektivt sett till både ekonomi och säkerhet.

I betänkandet angavs bl.a. att tillsynen över den statliga sektorns informationssäkerhet borde samordnas och förstärkas. MSB borde enligt förslaget utöva tillsyn över myndigheternas informationssäkerhetsarbete. I betänkandet konstateras att ett en sådan tillsynsuppgift föranleder ökad samverkan med myndigheter i det myndighetsråd som föreslogs. Vidare framhölls nödvändigheten av samordning i förhållande till den tillsyn som utövas under säkerhetsskyddslagen för att undvika överlappande tillsynsansvar. Även samordning med den tillsyn inom staten avseende informationssäkerhet som sker genom sektorsansvariga myndigheters försorg borde öka.

Utredningen ansåg angeläget att noga följa utvecklingen och inom en inte alltför avlägsen framtid följa upp frågan, bl.a. med hänsyn till NIS-direktivet.

Utredningen om genomförande av NIS-direktivet

I betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36) analyserade utredningen behovet och utformningen av tillsyn med anledning av NIS-direktivets genomförande i den svenska rättsordningen. I kommittédirektiven till utredningen angavs att befintliga myndigheter borde behålla eller komplettera nuvarande roller. MSB borde mot bakgrund av sitt ansvar att samordna arbetet med samhällets informationssäkerhet få en samordnande roll mellan tillsynsmyndigheterna i syfte att få en samlad bild över EU-direktivets genomförande och tillämpning i Sverige. Detta skulle

dock inte medföra något övertagande av sektorsmyndigheternas ansvar för tillsyn över aktörer eller något mandat att styra hur dessa myndigheter ska använda sina resurser.

Enligt direktiven borde utgångspunkten därför vara att tillsynsmyndigheterna inom de sektorer som omfattas av NIS-direktivet även fortsättningsvis har kvar ansvaret för att kontrollera att aktörerna följer respektive sektors regler om informationssäkerhet. För de sektorer där det i dag saknas tillsyn över informationssäkerhet behövde det övervägas vilken myndighet som kan anförtros den uppgiften. Inriktningen borde enligt kommittédirektiven vara att Post- och telestyrelsen (PTS) gav fortsatt och vid behov kompletterande ansvar för tillsyn av de digitala infrastrukturer som nämnas i bilaga 2 till NIS-direktivet.

I betänkandet redogjordes för myndigheternas olika tillsynsfunktioner inom berörda samhällssektorer. Utredningen föreslog att varje sektor och för de digitala tjänster som omfattas av lagstiftningen ska en tillsynsmyndighet ansvara för att övervaka att regelverket följs. Utredningen föreslog att MSB ska inom ramen för sitt uppdrag ha en samlad bild av NIS-direktivets genomförande och tillämpning i Sverige genom att leda ett samarbetsforum där samtliga tillsynsmyndigheter ska ingå samt ta emot tillsynsmyndighetens bedömning av brister i nätverk och informationssystem. I bedömningen bör ingå brister som upptäcks vid tillsyn men även svårigheter vid tillämpning och tolkning av regelverket.

Utredningen föreslog vidare att MSB ska tillhandahålla tillsynsmyndigheterna det metodstöd för tillsyn som behövs för en effektiv tillsyn enligt det föreslagna regelverket.

Regeringens proposition 2017/18:205 Informationssäkerhet för samhällsviktiga och digitala tjänster

I propositionen 2017/18:205 *Informationssäkerhet för samhällsviktiga och digitala tjänster* framhålls att nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och den inre marknadens funktion. I syfte att genomföra NIS-direktivet i svensk rätt föreslog regeringen en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Den nya lagen innebär bl.a. att vissa leverantörer av samhällsviktiga och digitala tjänster ska vidta

säkerhetsåtgärder till skydd för säkerheten i nätverk och informationssystem och att leverantörerna ska rapportera incidenter som påverkar kontinuiteten i tjänsterna. Vidare anges att den myndighet som regeringen bestämmer ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till den följs, och att myndigheten ska kunna besluta om vitesföreläggande och sanktionsavgift mot den som inte följer lagens bestämmelser. Den nya lagen trädde i kraft den 1 augusti 2018.

Betänkandet En ny säkerhetsskyddslag (SOU 2015:25)

I betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) behandlades frågan om tillsyn av säkerhetsskyddet. Utredningen konstaterade i betänkandet att formerna för tillsynen av säkerhetsskyddet i väsentliga avseenden avviker från hur offentlig tillsyn normalt är ordnad. Utredningen framhöll att tillsynen har ett stort inslag av råd och stöd till verksamhetsutövarna. Samtidigt underströk utredningen att det finns svårigheter med att förena en rådgivande roll med en kontrollerande roll och att det vore olyckligt med en utveckling mot att myndigheter som utövar tillsyn är så restriktiva i sin rådgivning att det innebär ett försämrat säkerhetsskydd. Utredningen stannade för bedömningen att det vid tidpunkten inte fanns tillräckliga skäl för att förändra tillsynens inriktning och genomförande. Utredningen lade däremot fram vissa förslag om ändringar i fråga om placeringen av tillsynsansvaret, bl.a. att MSB skulle ta över tillsynsansvaret för kommuner och landsting från Säkerhetspolisen och även länsstyrelsernas ansvar för enskilda verksamheter som inte ligger under någon annan myndighets tillsynsområde. Förslaget beträffande MSB fick ett blandat mottagande i samband med remitteringen av betänkandet.

Regeringens proposition 2017/18:89 Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag

I propositionen 2017/18:89 *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag* noterades att ansvaret för tillsyn enligt säkerhetsskyddslagen är uppdelat mellan flera myndigheter.

I propositionen framhölls att behovet är stort av ett förbättrat säkerhetsskydd hos såväl offentliga som enskilda verksamhetsutövare.

Den nya säkerhetsskyddslagen utvidgar i viss mån kraven på offentliga aktörer och kommer också på ett tydligare sätt att omfatta enskilda verksamheter. Det är svårt att förutsäga hur många enskilda verksamhetsutövare som kommer att vara skyldiga att tillämpa lagstiftningen. Det kan dock konstateras att antalet verksamheter som har betydelse för Sveriges säkerhet, och som drivs i enskild regi, har ökat i takt med privatiseringen av offentlig verksamhet. Det innebär sammantaget med den snabba digitaliseringen av samhället att det kan antas att verksamheter med central betydelse för Sveriges säkerhet även i framtiden kommer att drivas av enskilda aktörer. Att tillsynen över såväl offentliga som enskilda verksamhetsutövare även framöver fungerar på ett tillfredsställande sätt är därför mycket angeläget.

I propositionen framhölls att en ny säkerhetsskyddslag bör kompletteras med en möjlighet att utfärda sanktioner mot aktörer som brister i sitt säkerhetsskyddsarbete. När det gäller frågan om tillsyn finns anledning att på nytt utreda vilka myndigheter som bör ha uppgifter att utöva tillsyn enligt säkerhetsskyddslagen. Även ett införande av sanktionsmöjligheter medför ett behov av att se över tillsynsstrukturen eftersom det också innebär att tillsynens karaktär behöver förändras från dagens inriktning mot rådgivning och stöd till tillsyn i en mer traditionell mening.

Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82)

I betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) lämnar utredningen förslag på en utökad tillsyn över säkerhetskänslig verksamhet. Utredningen fann att det finns brister när det gäller tillsynsverksamheten och regleringen av tillsynen på säkerhetsskyddsområdet. Utredningen menade att det inte är definierat och avgränsat vad tillsynen syftar till och avser. Ingen myndighet har en samlad bild över tillsynen. Vidare saknas det reglering om hur tillsynsmyndigheterna ska utbyta hotinformation med Säkerhetspolisen och Försvarsmakten. Utredningen bedömde att själva tillsynen hittills har bedrivits i alltför begränsad omfattning. Vidare ansåg utredningen att tillsynsmyndigheterna saknar de befogenheter som krävs för att de ska kunna genomföra en effektiv tillsyn och åstadkomma rättelse. Tillsynskompetensen behöver också öka hos många tillsynsmyndigheter och det behöver skapas en överblick över

vilka tillsynsobjekt som finns inom respektive tillsynsområde. Betänkandet har remissbehandlats och är föremål för beredning i Regeringskansliet. Det ingår utredningens uppdrag att beakta den fortsatta beredningen av betänkandet.

8.4.3 Nationell myndighet med ansvar för tillsyn

Förslag: Försvarets materielverk (FMV) ska vara nationell myndighet för cybersäkerhetscertifiering enligt artikel 58 i EU:s cybersäkerhetsakt. Myndigheten ska fullgöra de tillsynsuppgifter som följer av artikel 58.7.

Bedömning: Regeringen kan meddela de verkställighetsföreskrifter som behövs för genomförandet av tillsynsverksamheten enligt artikel 58.7.

FMV bör organisera tillsynsfunktionen i myndigheten så att kraven på oberoende enligt EU:s cybersäkerhetsakt uppnås.

Utgångspunkter

I artikel 58 i EU:s cybersäkerhetsakt anges att medlemsstaterna bör kunna utse mer än en nationell myndighet med ansvar för att utföra uppgifter som rör kontroll och övervakning av det europeiska ramverket för cybersäkerhetscertifiering. Medlemsstaterna får vid behov använda eller anpassa organisationsstrukturer vid genomförandet av cybersäkerhetsakten.

Cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer med stöd av EU:s cybersäkerhetsakt tar sikte på att förebygga eller minska allvarliga konsekvenser till följd av hot och angrepp mot system för informations- och cybersäkerhet som finns inom alla samhällets områden, bl.a. inom samhällsviktiga verksamheter och säkerhetskänslig verksamhet.

EU:s cybersäkerhetsakt är utformad på ett sätt som ger den verksamhetsansvarige ett stort ansvar och bedömningsutrymme i fråga om såväl regelverkets tillämplighet som att bestämma hur verksamheten ska bedrivas för att möta kraven i regleringen. Det kan medföra utmaningar i fråga om möjligheter att ingripa, som förutsätter

tydlighet om vilka brister som behöver åtgärdas. Ett annat förhållande som är viktigt att beakta är att lagstiftningens karaktär medför att det kan finnas ett stort behov av vägledning och stöd till de verksamheter som har att tillämpa cybersäkerhetsakten och europeiska cybersäkerhetsordningar. Särskilt i förhållande till företag, bl.a. tillverkare och leverantörer, men även organ för bedömning av överensstämmelse, kan finnas ett större behov av råd och stöd vid regelverkets tillämpning. Det behovet kan dessutom komma att öka i de fall europeiska ordningar som föreskriver tvingande cybersäkerhetscertifiering kommer att införas.

Mot den bakgrunden kan det antas att cybersäkerhetsaktens genomslag kan komma att vara beroende av om de myndigheter som har ett särskilt ansvar för certifiering och tillsyn på olika sätt kan i en tillräcklig omfattning vägleda och stödja berörda aktörer i deras verksamhet.

Utredningen anser att till en början bör en förebyggande inriktning i tillsynsarbetet ske. Flera av experterna i utredningen har också framhållit att det är viktigt att tillsynen utgår från samverkan och ger utrymme för en dialog mellan myndighet och den verksamhet som berörs av tillsynen. Det är utredningens bedömning det inom det nu aktuella tillsynsområdet är viktigt att det finns goda förutsättningar för samverkan mellan myndigheter och enskilda verksamheter. Om brister i verksamheten kan medföra åtgärder som till exempel varningar och vitessanktionerade åtgärdsföreläggande, kan det minska benägenheten att på eget initiativ ta upp brister med den myndighet som kontrollerar att kraven på området för cybersäkerhetscertifiering efterlevs. Det kan medföra en risk att sådana inslag skulle kunna medföra att värdefullt erfarenhetsutbyte, till exempel i fråga om säkerhetshot mellan de verksamheter som kontrolleras och den myndighet som utövar tillsynen motverkas.

Även vilken form av verksamhet som tillsynen riktas mot bör beaktas i sammanhanget. De tillsynsobjekt och verksamheter som kan komma att beröras av tillsynen är främst de som utfärdar EU-försäkran om överensstämmelse eller europeiska cybersäkerhetscertifikat, dvs. tillverkare och leverantörer samt organ för bedömning av överensstämmelse av IKT-produkter, -tjänster och -processer. De aktörer som berörs finns inom många olika branscher och verksamhetsområden. Aktörerna utgörs av stora, medelstora och små företag, som i egenskap av tillverkare eller leverantör tillhandahåller an-

givna produkter, tjänster och processer på marknaden. Organ för bedömning kan utgöras av en nationell myndighet eller företag på marknaden. Det rör sig således om aktörer i verksamheter med olika inriktning och karaktär inom en rad olika områden för informations- och cybersäkerhet. Detta talar också för att ha en enhetlig tillsyn i syfte att uppnå stabilitet och samsyn inom tillsynsverksamheten på området.

Inte bara bred och djup kunskap om cybersäkerhetscertifiering och informations- och cybersäkerhetsäkerhet är viktiga komponenter för en tillsynsmyndighet utan även djup och bred erfarenhet av informationssäkerhet inom olika samhällsområden bör tillmätas stor betydelse. Härtill kommer att myndigheten också ska ha tillräcklig kunskap och förståelse för verksamhet som faller inom det europeiska ramverkets tillämpningsområde.

En annan faktor som ska beaktas när man bedömer hur ett tillsynssystem ska utformas är vilka risker som eventuella regelöverträdelser kan komma att medföra. Syftet med det europeiska ramverket för cybersäkerhetscertifiering är att höja nivån på säkerhet och tillit i IKT-produkter, IKT-tjänster och IKT-processer som används bl.a. i nätverk och informationssystem för samhällsviktiga tjänster och digitala tjänster. Möjligheten att kunna utfärda en EU-försäkran eller ett cybersäkerhetscertifikat syftar till att hantera, förebygga och minimera hot och risker i produkter, tjänster och processer.

Eftersom dessa även handlas mellan medlemsstaterna kan eventuella brister och sårbarheter i dessa även få en gränsöverskridande verkan. Det angivna talar för att ett system för tillsynen utöver enhetlighet också bör innefatta en förebyggande inriktning.

I dag finns nationellt flera system för tillsyn av informations- och cybersäkerhet i de verksamheter som kan komma att beröras av cybersäkerhetsaktens tillämpningsområde och verksamheterna har i många fall flera olika tillsynsmyndigheter. Vissa tillsynsmyndigheter utövar redan i dag tillsyn över säkerhet i nätverk och informationssystem medan andra har en annan inriktning på tillsynen. Till följd av bl.a. NIS-direktivet och säkerhetsskyddslagsregleringen finns skillnader i såväl omfattning som utformning av tillsyn av informationssäkerheten i många olika samhällsverksamheter. Även om det europeiska ramverket för cybersäkerhetscertifiering och det nationella tillsynssystemet utformas på ett enhetligt sätt kommer kraven på åtgärder

för olika IKT-produkter, IKT-tjänster och IKT-processer att vara olika inom olika verksamhetsområden och samhällsverksamheter.

Utgångspunkten bör vara att om möjligt eftersträva en enhetlig tillsyn på cybersäkerhetsaktens tillämpningsområde. Detta påverkar också utformningen av själva systemet och hur tillsynen bör bedrivas.

Utredningen kan konstatera att ett system med en tillsynsmyndighet som ansvarar för hela tillsynsverksamheten på området har både för- och nackdelar. Det som talar för ett system med en tillsynsmyndighet är att kunskap cybersäkerhetscertifiering i förening med kunskap om hot, sårbarheter och risker i informations- och cybersäkerhet kan samlas i en myndighet med djup och bred kunskap på området. Detta framstår som särskilt viktigt på de områden för informations- och cybersäkerhet som redan regleras av nationell lagstiftning eller EU-rättsakter och där en bedömning kan behöva göras om tillämpligheten av det europeiska ramverket för cybersäkerhetscertifiering på området.

Det är vidare i detta fall en fördel om normgivning och tillsyn kan hållas samman, vilket även förekommer inom många andra samhällssektorer där aktörerna omfattas av såväl nationella regleringar som EU-rättsakter. Eftersom cybersäkerhetscertifiering utgör den större delen av tillsynsverksamheten är det särskilt viktigt att erfarenheter från sådan verksamhet kan tas tillvara i tillsynsarbetet på ett sätt som även bidrar till att förbättra den inre marknadens funktion.

Det som ytterligare kan anföras mot att utse två eller flera myndigheter att fullgöra tillsynsfunktionen är att uppgifterna och arbetet med tillsyn på cybersäkerhetsaktens tillämpningsområde, särskilt när det gäller säkerhet i IKT-produkter, IKT-tjänster och IKT-processer samt säkerhet i nätverk och informationssystem, kräver bred och djup expertkunskap och erfarenhet från området. Det är redan i dag en besvärande brist på experter med bred och djup kompetens inom det nu aktuella området och att det skulle medföra stora svårigheter att bemanna en tillsynsverksamhet som är uppdelad på två eller flera myndigheter.

Enligt utredningens mening talar det nu angivna för att utgångspunkten för tillsynens utformning ska vara att det ska finnas en tillsynsmyndighet för hela det europeiska ramverket för cybersäkerhetscertifiering.

Eftersom tillsynsfunktionen ska organiseras vid en befintlig myndighet är det en fördel om den myndigheten redan har kunskap och

erfarenhet av cybersäkerhetscertifiering vilket medför att förberedelsetiden för att påbörja tillsynsverksamheten kan reduceras. En effektiv tillsyn kräver även förtroende mellan tillsynsmyndighet och tillsynsobjekten, vilket bygger på långsiktiga relationer samt kunskap och förståelse för verksamheten.

Förslag på myndighet med ansvar för tillsyn

Nästa fråga blir då vilken befintlig myndighet som har förutsättningar och är lämplig att utöva tillsyn när det gäller efterlevnaden av det europeiska ramverket och den kompletterande nationella lagstiftningen på området.

Utredningen har vid kartläggningen och bedömningen av lämplig myndighet för tillsynsfunktionen beaktat om myndigheten i dag har

- kunskap och erfarenhet av certifiering på området för informations- och cybersäkerhet,
- kunskap om sårbarheter, hot och risker inom informations- och cybersäkerhet,
- erfarenhet och ansvar för tillsyn av informations- och cybersäkerhetkunskap, och
- ansvar för att utfärda föreskrifter.

Utredningen kan konstatera att det i dag inte finns någon enhetlig struktur för tillsyn inom de områden som angränsar till cybersäkerhetsaktens tillämpningsområde. På vissa områden finns flera tillsynsmyndigheter med olika ansvar, i andra är ansvaret utpekat och i vissa fall saknas tillsynsmyndighet.

Mot bakgrund av de krav som anges i cybersäkerhetsakten, vad som anges i regeringens skrivelse (skr. 2009/10:79) och vad som framkommit om nu aktuella befintliga myndigheter gör utredningen bedömningen att främst en myndighet som ingår i SAMFI-myndigheternas samverkansgrupp som kan komma ifråga som tillsynsmyndighet.

Fråga uppkommer då om någon de andra s.k. SAMFI-myndigheterna skulle kunna ges rollen som tillsynsmyndighet. Bl.a. utövar SÄPO och MUST/Försvarsmakten utövar i dag tillsyn över informations- och cybersäkerhetsverksamhet inom respektive ansvarsom-

råden. Utredningen kan samtidigt konstatera att tillsynsuppgifterna som följer av det europeiska ramverket för cybersäkerhetscertifiering är av en annan karaktär än de tillsynsuppgifter som dessa myndigheter i dag har, bl.a. vad gäller tillsyn över certifieringsverksamhet, och som förutsätter en djupare kunskap om certifiering av IKT-produkter, IKT-tjänster och IKT-processer inom ett brett område. Ingen av dessa myndigheter har i dag någon sådan uppgift eller verksamhet och ingen av myndigheterna har heller under utredningen angett att de skulle vara lämpliga i den nu aktuella rollen som tillsynsmyndighet enligt cybersäkerhetsakten. Inte heller Polismyndigheten har några sådana uppgifter.

Utöver FMV är det endast MSB, och i viss mån även PTS, som har uppgifter som knyter an till de uppgifter som följer av det europeiska ramverket för cybersäkerhetscertifiering.

PTS bevakar områdena elektronisk kommunikation och post. Begreppet elektronisk kommunikation omfattar telekommunikationer, it och radio. PTS har tillsynsansvar och får meddela föreskrifter på flera olika områden. PTS har tillsyn enligt lagen (2003:389) om elektronisk kommunikation. PTS är även tillsynsmyndighet för digital infrastruktur och digitala tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. PTS är vidare tillsynsmyndighet för betrodda tjänster enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Även enligt säkerhetsskyddslagen (2018:585) har PTS ett tillsynsansvar och får meddela föreskrifter. PTS har även ansvar och uppgifter inom bl.a. området kontanthantering. Även om myndigheten har uppgifter och erfarenhet av informations- och cybersäkerhetsarbete samt har till uppgift att vara tillsynsmyndighet verkar myndigheten främst inom området för elektronisk kommunikation. Om PTS fick uppgiften att vara tillsynsmyndighet skulle myndigheten behöva bygga upp och utveckla en bred och djup teknisk kompetens för tillsyn på cybersäkerhetsaktens tillämpningsområde, vilket även skulle innebära att myndigheten fick ett betydligt bredare uppdrag än vad som är fallet i dag.

MSB:s uppgifter och verksamhet har tidigare beskrivits i kapitel 5. Som tidigare framgår har myndigheten i dag uppgifter och ansvar på informations- och cybersäkerhetsområdet, bl.a. har den ansvar för att utveckla och stödja informations- och cybersäkerheten i samhället Myndigheten har också särskilda uppgifter inom ramen för

den verksamhet som omfattas av lagen om samhällsviktiga tjänster (NIS-direktivet).

Utredningen kan samtidigt konstatera att även om MSB har en bred kompetens inom olika delområden avseende informations- och cybersäkerhet har myndigheten i jämförelse med FMV och certifieringsorganet CSEC inte den breda och djupa tekniska kompetens och erfarenhet på området för cybersäkerhetscertifiering som kan förutsättas behövas för att myndigheten ska kunna utöva en ändamålsenlig och effektiv tillsyn på området för det europeiska ramverket för cybersäkerhetscertifiering.

FMV har genom certifieringsorganet CSEC en djup och bred kompetens och erfarenhet på området för cybersäkerhetscertifiering samt lång erfarenhet av samverkan med nationella och internationella aktörer inom såväl cybersäkerhet som annan kvalificerad teknisk verksamhet på försvars- och säkerhetsområdet. Myndigheten är nu även föreslagen som tillsynsmyndighet för verksamhet som omfattas av säkerhetsskyddslagstiftningen. Sammantaget gör utredningen bedömningen att FMV är den av aktuella myndigheter som i dag framstår som den myndighet som har förutsättningar att på det mest ändamålsenliga och effektiva sättet kunna fullgöra tillsynsuppgifterna.

Samtidigt uppkommer frågan om uppgifterna som nationell myndighet för cybersäkerhetscertifiering med de uppgifter som följer i den rollen går att förena med rollen som ansvarig för tillsyn över det europeiska ramverket för cybersäkerhetscertifiering.

I artikel 58.3 i EU:s cybersäkerhetsakt framhålls att den nationella myndigheten för cybersäkerhetscertifiering ska vara oberoende av de enheter som den utövar tillsyn över, särskilt vad gäller tillsynsobjektet organisation, beslut om finansiering, rättsliga struktur och beslutsfattande.

Av punkten 4 följer att medlemsstaten även 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 och att dessa verksamheter utförs oberoende av varandra.

Utredningen kan konstatera att angivna reglering ställer krav på att såväl certifieringsorganet som myndighetens tillsynsfunktion är organiserade på ett sätt som innebär att de är strikt åtskilda och oberoende av varandra. När det gäller certifieringsorganet i FMV lämnar

utredningen i avsnitt 8.3.2 förslag på åtgärder som syftar till att säkerställa certifieringsorganets oberoende i verksamhet som utförs enligt EU:s cybersäkerhetsakt. EU:s cybersäkerhetsakt ställer utöver det angivna inte några ytterligare krav på tillsynsfunktionens organisering, vilket enligt utredningens bedömning medför att certifieringsorganet och tillsynsfunktionen kan organiseras i myndigheten FMV under förutsättning att verksamheterna är strikt åtskilda och oberoende av varandra.

Av artikel 58 framgår att myndigheten för cybersäkerhetscertifiering har tillsynsuppgifter varför det i denna del inte krävs någon kompletterande nationell reglering. Enligt den nationella förvaltningsmodellen är det myndigheten som organiserar verksamheten i myndigheten om inte annat särskilt anges i författning eller regleringsbrev. Utredningen anser att frågan om hur tillsynsfunktionen inom FMV ska organiseras och formerna för arbetets bedrivande för att möta kraven i EU:s cybersäkerhetsakt bör beslutas av den myndigheten, t.ex. i myndighetens arbetsordning. Det finns därför inte heller i denna del behov av kompletterande nationell reglering.

Myndigheten bör därför utses att ansvara för tillsynsuppgifterna som följer av artikel 58 i EU:s cybersäkerhetsakt.

Utredningen kan samtidigt konstatera att tillsynsmyndigheter inom olika samhällssektorer fortsatt ska ha ansvaret för att kontrollera att myndigheter och andra aktörer följer respektive sektors regler om informations- och cybersäkersäkerhet, också när en fråga uppkommer som berör cybersäkerhetsaktens tillämpningsområde. Det ställer krav på utökad samverkan mellan den nationella myndigheten med ansvar för cybersäkerhetscertifiering och tillsyn och övriga berörda myndigheter på informations- och cybersäkerhetsområdet. Utredningen återkommer till denna fråga i kapitel 13.

8.5 Avgifter

Förslag: I lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska anges att den nationella myndigheten för cybersäkerhetscertifiering får ta ut avgifter för de verksamheter som myndigheten bedriver enligt EU:s cybersäkerhetsakt och den nya lagen.

Regeringen eller den myndighet som regeringen bestämmer bör bemyndigas att meddela närmare bestämmelser om avgiftssystemets utformning.

Bedömning: Det behövs inga kompletterande författningsbestämmelser om FMV:s möjlighet att meddela närmare föreskrifter om avgiftsfinansieringen av dess verksamhet.

Enligt EU:s cybersäkerhetsakt omfattar de nationella cybersäkerhetscertifieringsmyndigheternas uppdrag såväl utfärdande av cybersäkerhetscertifikat enligt artikel 56 som tillsyn enligt artikel 58 över IKT-produkters, -tjänsters och -processers överensstämmelse med kraven i de certifikat som utfärdats inom deras länder.

FMV/CSEC:s verksamhet är i dag både anslags- och avgiftsfinansierad. Motsvarande system bör införas när det gäller finansieringen av den certifieringsverksamhet som den nationella myndigheten för cybersäkerhetscertifiering bedriver enligt EU:s cybersäkerhetsakt. Bemyndigandet att ta ut avgifter bör beslutas genom lag (se SOU 2007:96 s. 143).

Utredningen anser vidare att berörda aktörer bör ersätta kostnaden för tillsynsverksamheten. Detta kan lämpligen ske genom att en tillsynsavgift betalas av enskilda. 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. Dessutom bör den gälla den nationella cybersäkerhetscertifieringsmyndighetens tillsynsverksamhet enligt den nya lagen och föreskrifter som har meddelats i anslutning till lagen samt enligt cybersäkerhetsakten och rättsakter som har meddelats med stöd av den förordningen.

Regeringen eller den myndighet som regeringen bestämmer bör bemyndigas att meddela närmare bestämmelser om avgiftssystemets utformning.

Utredningen noterar att FMV, som utredningen föreslår ska utses till nationell myndighet för cybersäkerhetscertifiering, får i dag ta ut avgifter för sin verksamhet med stöd av 14 § förordningen (2007:854) med instruktion för Försvarets materielverk. Myndigheten har även rätt att meddela föreskrifter om avgifternas storlek. Det behövs därför inga kompletterande författningsbestämmelser i denna del.

Utredningen bedömer att det inte bör införas någon författningsreglerad avgiftsfinansiering av de privata organen 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.

9 Tillsynsbefogenheter och sanktioner

9.1 Inledning

I det föregående kapitlet har utredningen tagit ställning till vilken myndighet som bör utses till nationell myndighet för cybersäkerhetscertifiering samt redogjort för dess tillsynsuppgifter.

Den nationella myndigheten för cybersäkerhetscertifiering ska enligt EU:s cybersäkerhetsakt övervaka och kontrollera efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering. För att kunna utföra sin tillsyn på ett effektivt sätt behöver myndigheten ett antal befogenheter.

Även om det finns ett samförstånd mellan den nationella myndigheten för cybersäkerhetscertifiering och tillsynsobjektet bygger ett legitimt och ändamålsenligt system för tillsyn på att tillsynsmyndigheten har författningsreglerade befogenheter för att kunna genomföra de åtgärder som kan behövas i det enskilda fallet. I artikel 58.8 föreskriver EU:s cybersäkerhetsakt olika minimibefogenheter. Att tillsynsverksamheten är författningsreglerad har även den fördelen att ramarna för tillsynsverksamheten tydliggörs, vilket är ytterligare en fördel när det som i detta fall är fråga om en ny lagstiftning som omfattar många företag, dvs. såväl tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som organ för bedömning av överensstämmelse.

Regelverket om tillsyn på tillämpningsområdet för EU:s cybersäkerhetsakt angränsar till motsvarande bestämmelser i NIS-direktivet och den till direktivet anslutande lagen på området. Det finns i den lagen bestämmelser som ger tillsynsmyndigheterna flera viktiga undersökningsbefogenheter, däribland en rätt att kräva upplysningar av tillsynsobjektet och en tillträdesrätt till lokaler. Det handlar om ny lagstiftning och ett närliggande område. Bestämmelserna är ägnade

att möjliggöra en effektiv tillsyn. En utgångspunkt bör därför vara att de kompletterande nationella bestämmelser som behövs för att befogenheterna som anges i EU:s cybersäkerhetsakt ska kunna tillämpas effektivt är att dessa utformas på motsvarande sätt om inte några särskilda skäl talar emot det. I den mån det finns ett behov av att anpassa reglerna till de särskilda förhållanden som kan finnas på cybersäkerhetsaktens tillämpningsområde ska en sådan anpassning dock ske. Vidare ska vad som anges i regeringens skrivelse *En tydlig, rättssäker och effektiv tillsyn* (skr. 2009/10:79) beaktas vid övervägande om hur tillsynssystemet bör utformas.

I detta kapitel behandlar utredningen de tillsynsbefogenheter som EU:s cybersäkerhetsakt ger den nationella myndigheten för cybersäkerhetscertifiering samt behovet av kompletterande nationell lagstiftning om myndighetens befogenheter. Därefter redogör utredningen för sina överväganden i fråga om ett lämpligt sanktionssystem.

Frågor om sekretess för uppgifter som lämnas i samband med tillsyn till den nationella myndigheten för cybersäkerhetscertifiering behandlas i kapitel 12.

9.2 Undersökningsbefogenheter

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 den förordningen, den nya lagen 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.

Bedömning: Den nationella myndigheten för cybersäkerhetscertifiering bör ha möjlighet att meddela närmare föreskrifter om

1. formerna för lämnandet av information enligt artikel 58.8 a i EU:s cybersäkerhetsakt,
2. kontrollförfarandet vid undersökningar enligt artikel 58.8 b i EU:s cybersäkerhetsakt, och
3. utredningsförfarandet vid tillträde till lokaler artikel 58.8 d i EU:s cybersäkerhetsakt.

9.2.1 Rätten att begära uppgifter

I artikel 58.8 a i EU:s cybersäkerhetsakt anges att en nationell myndighet för cybersäkerhetscertifiering kan 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.

Bestämmelsen innebär att den som står under tillsyn ska på begäran tillhandahålla den nationella myndigheten för cybersäkerhetscertifiering den information som behövs för tillsynen. Uppgiftsskyldigheten gäller för ovan angivna aktörer. Bestämmelsen har direkt effekt och kräver inte kompletterande nationell lagstiftning i fråga om själva rätten att begära nödvändiga uppgifter. När den nationella myndigheten för cybersäkerhetscertifiering begär uppgifter eller information förutsätts den uppge syftet med begäran och precisera vilka uppgifter eller vilken information som ska lämnas.

Den nationella myndigheten för cybersäkerhetscertifiering bör bemyndigas att meddela de föreskrifter som behövs för att uppgiftsskyldigheten enligt artikel 58.8 a ska kunna fullgöras på ett effektivt och ändamålsenligt sätt. En sådan rätt kan lämpligen införas i den nya förordningen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

9.2.2 Rätten att genomföra undersökningar i form av kontroller

Av artikel 58.8 b i EU:s cybersäkerhetsakt framgår att den nationella myndigheten för cybersäkerhetscertifiering får 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. Myndigheten har således möjlighet att genomföra en undersökning och kontrollera att IKT-tillverkare och -leverantörer som utfärdar en EU-försäkran om överensstämmelse eller innehar ett europeiskt cybersäkerhetscertifikat efterlever det europeiska ramverket för cybersäkerhetscertifiering. Motsvarande gäller även organ för bedömning av överensstämmelse.

Bestämmelsen har direkt tillämplighet och påkallar ingen nationell lagstiftning för att genomföras. Det finns emellertid behov, på motsvarande sätt som gäller vid uppgiftsskyldigheten (se avsnitt 9.2.1), av att den nationella myndigheten för cybersäkerhetscertifiering kan meddela förskrifter om kontrollförfarandet vid undersökningarna.

9.2.3 Rätten att få tillträde till lokaler och biträde av Kronofogdemyndigheten

I artikel 58.8 d i EU:s cybersäkerhetsakt anges 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. Bestämmelsen är en förutsättning för att det ska kunna bedrivas en effektiv tillsyn enligt cybersäkerhetsakten. Tillträdesrätten, som omfattar alla lokaler där det bedrivs verksamhet som omfattas av aktens tillämpningsområde, ska dock av integritetsskäl inte gälla bostäder som finns i anslutning till verksamheten.[1] Tillsynsobjekten är tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som är innehavare av cybersäkerhetscertifikat samt organ för bedömning av överensstämmelse. Utredningen noterar att utfärdare av en EU-försäkran utelämnats från bestämmelsens tillämpningsområde.

För att tillsyn ska kunna bedrivas på ett effektivt sätt är det nödvändigt att den myndigheten som utövar tillsyn 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.

Genomförandet av artikel 58.8 d kräver inte kompletterande nationell reglering. Om verksamhetsutövaren däremot vägrar att ge den

[1] I regeringens skrivelse En tydlig, rättssäker och effektiv tillsyn (skr. 2009/10:79, s. 50 f.) anges att tillsynsorgan bör ha tillträdesrätt till alla utrymmen som används i den tillsynspliktiga verksamheten men att av integritetsskäl bör bostäder inkluderas endast om det är nödvändigt för att tillsynsorganet ska kunna bedriva en effektiv tillsyn. För övrigt kan noteras att bestämmelsen i EU:s cybersäkerhetsakt anger just ”lokaler” och inte andra utrymmen.

nationella myndigheten för cybersäkerhetscertifiering tillträde till en lokal eller liknande för undersökning kan tvångsåtgärder behöva användas. Att vidta sådana åtgärder ligger inte inom myndighetens befogenheter. Det finns inte anledning att anta att det kommer finnas risk för hot eller handgripligheter i samband med tillsynen enligt de aktuella bestämmelserna. De eventuella hinder som kan uppstå får i stället antas vara av fysiskt art. Den nationella myndigheten för cybersäkerhetscertifiering bör därför kunna begära biträde av Kronofogdemyndigheten för att få tillgång till en lokal för att kunna kontrollera handlingar, utrustning och verksamheten på plats. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

I likhet med vad som konstaterats ovan bör den nationella myndigheten för cybersäkerhetscertifiering även ha möjlighet att meddela närmare föreskrifter om utredningsförfarandet vid tillträde till lokaler.

9.2.4 Rätten att vidta lämpliga åtgärder

Av artikel 58.8 c framgår att varje nationell myndighet för cybersäkerhetscertifiering ges 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.

Utredningen konstaterar att artikel 58.8 c i EU:s cybersäkerhetsakt enligt sin lydelse förutsätter komplettering i nationell rätt för att genomföras av medlemsstaterna. Utredningen anser att en möjlighet för den nationella myndigheten för cybersäkerhetscertifiering att besluta nödvändiga förelägganden, förenade med vite, utgör lämpliga nationella åtgärder för att säkerställa efterlevnad av regelverket. 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 bör gälla för de krav som följer av den nya lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt och föreskrifter som meddelas i anslutning till lagen.

Nedan motiverar utredningen sitt förslag till lagstiftningsåtgärd i denna del.

Den nationella myndigheten för cybersäkerhetscertifiering bör kunna meddela åtgärdsförelägganden

I linje med vad regeringen i skrivelsen *En tydlig, rättssäker och effektiv tillsyn* uttalat om behovet av att i vissa fall ge en tillsynsmyndighet möjlighet att besluta om förelägganden i enskilda fall (skr. 2009/10:79 s. 44) bör övervägas om det även på tillämpningsområdet för EU:s cybersäkerhetsakt bör finnas en sådan möjlighet för att kunna styra beteendet hos tillsynsobjektet.

När den nationella myndigheten för cybersäkerhetscertifiering konstaterar att det förekommer mindre allvarliga brister i efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering hos tillsynsobjekten kan det i många fall vara tillräckligt att myndigheten påpekar bristerna och att verksamhetsutövaren frivilligt åtar sig att åtgärda dem. Vid mer allvarliga brister kan det dock behövas en möjlighet att meddela formella åtgärdsförelägganden som kan förenas med vite.[2] Sådana förelägganden kan t.ex. behövas när det visar sig att en innehavare av ett europeiskt cybersäkerhetscertifikat eller att den som utfärdat en EU-försäkran om överensstämmelse allvarligt brustit i de skyldigheter som följer av det europeiska ramverket för cybersäkerhetscertifiering eller nationell lagstiftning på området. Möjligheten att meddela åtgärdsförelägganden bör dock inte begränsas till dessa situationer. I stället bör det finnas en sådan möjlighet vid alla slags åsidosättanden av reglerna i ramverket för cybersäkerhetscertifiering och den nya lagen respektive föreskrifter som utfärdas i anslutning till denna lag. Föreläggandets utformning skapar även möjligheter för den nationella myndigheten för cybersäkerhetscertifiering att anpassa ett ingripande efter vad som är behövligt beroende på vilket område det handlar om. Det bör därför finnas en möjlighet att utforma föreläggandet vitt och i princip ansluta till till-

[2] Regeringen har i skrivelsen En tydlig, rättssäker och effektiv tillsyn uttalat att ett tillsynsorgan bör ha en möjlighet att besluta om förelägganden i enskilda fall (skr. 2009/10:79 s. 44). Möjligheten att utforma föreläggandet för att kunna styra beteendet hos den objektsansvarige bör enligt dessa uttalanden vara vitt och i princip ansluta till tillsynens omfattning. Föreläggandets utformning skapar enligt regeringen möjligheter för tillsynsorganet att anpassa ett ingripande efter vad som är behövligt beroende på vilket område det handlar om. Det anges i skrivelsen att ett åtgärdsföreläggande bör kunna förenas med vite.

synens omfattning. Befogenheten att besluta förelägganden innefattar även förbudsföreläggande.

Möjligheten att förena åläggande med vite

Vite som föreläggs med stöd av 3 § lagen (1985:206) om viten (viteslagen) ska fastställas till ett belopp som med hänsyn till vad som är känt om mottagarens ekonomiska förhållanden och omständigheterna i övrigt kan antas förmå den som det riktas mot att följa det föreläggande som är förenat med vitet. Med omständigheterna i övrigt avses bl.a. kostnaderna för föreläggandets fullgörande och omfattningen av de åtgärder som krävs. Beloppet bör vidare bestämmas med hänsyn till hur angeläget det är att föreläggandet följs. Om föreläggandet avser att tillgodose ett betydelsefullt samhällsintresse kan ett högre belopp vara motiverat. Myndigheterna kan emellertid inom ramen för 3 § viteslagen bestämma hur högt eller lågt belopp som helst.

Ett vite bör som huvudregel fastställas till ett bestämt belopp. Om det är lämpligt med hänsyn till omständigheterna får vite dock enligt 4 § viteslagen föreläggas som löpande vite. Vitet bestäms då till ett visst belopp för varje tidsperiod av viss längd under vilken föreläggandet inte har följts eller, om föreläggandet avser en återkommande förpliktelse, för varje gång adressaten underlåter att fullgöra denna. Om ett föreläggande inte följs kan myndigheten behöva upprepa föreläggandet. Det kan i dessa fall vara lämpligt att höja vitesbeloppet.

I 28 § NIS-lagen finns det regler om vitessanktionerade åtgärdsförelägganden för vissa underlåtenheter att leva upp till de krav som ställs i lagen och de föreskrifter som meddelats med stöd av lagen.

Utredningen bedömer att det finns skäl att den nationella myndigheten för cybersäkerhetscertifiering på motsvarande sätt bör ges möjlighet att förena ett åtgärdsföreläggande med vite i det fall tillsynsobjektet underlåtenheter att leva upp till de krav som ställs i EU:s cybersäkerhetsakt, lagen och de föreskrifter som meddelats med stöd av lagen. Som framhållits ovan bör det finnas en möjlighet för myndigheten att vid olika slags åsidosättanden av reglerna i det europeiska ramverket för cybersäkerhetscertifiering och lagen samt föreskrifter som utfärdas med stöd av denna lag meddela ett åtgärdsföreläggande. Utredningen anser att den nationella myndigheten för

cybersäkerhetscertifiering bör ges möjlighet att förena ett föreläggande med vite i de fall ett sådant förfarande är påkallat och med tillämpning av de grundläggande principer som anges i viteslagen.

Det europeiska ramverket för cybersäkerhetscertifiering är på motsvarande sätt som NIS-direktivet och NIS-lagen tillämplig på såväl offentliga aktörer, såsom statliga myndigheter, och på enskilda aktörer. När det gäller vitesföreläggande har det i NIS-lagen inte gjorts något undantag för staten eller andra offentliga aktörer. Bedömningen är att det på det området är godtagbart med vite i förhållande till statliga myndigheter och kommuner. Utredningen ser inga skäl till att en annan ordning bör gälla på cybersäkerhetsaktens tillämpningsområde.

Möjligheten för den nationella myndigheten för cybersäkerhetscertifiering att vitesförelägga den som ska lämna uppgifter eller tillträde till lokal bör dock i första hand ske när det kan befaras att den det gäller inte kommer att följa beslutet att lämna uppgifter eller frivilligt medverka till en kontroll på platsen.

9.2.5 Omedelbar verkställighet och inhibition

Bedömning: Den nationella myndigheten för cybersäkerhetscertifiering får bestämma att ett beslut om föreläggande ska gälla omedelbart. Bestämmelser om omedelbar verkställighet finns emellertid i förvaltningslagen (2017:900) och behöver inte tas in i den nya lagen.

Bestämmelser om inhibition finns i förvaltningsprocesslagen (1971:291) och behöver inte tas in i den nya lagen.

Om den nationella myndigheten för cybersäkerhetscertifiering konstaterat att det finns skäl för att ingripa genom beslut om föreläggande finns det ofta ett behov av att beslutet blir gällande genast. T.ex. då myndigheten ser sig nödgad att besluta om att ett förfarande eller verksamhet inte får fortsätta kan det finnas skäl för omedelbar verkställighet för att förhindra eller minska sårbarheter och risken för skador. Skäl för myndigheten att verkställa ett beslut omedelbart gör sig också gällande beträffande dess beslut att förelägga tillsynsobjektet att lämna tillträde till lokaler och att lämna upplysningar, handlingar och liknande för att tillsynen ska kunna genomföras. I sådana fall kan det vara angeläget att beslutet inte förhalas genom ett över-

klagande. En kompletterande bestämmelse om rätten att bestämma att sådana beslut ska gälla omedelbart behöver emellertid inte införas i den nya lagen. Förvaltningslagen (2017:900) (FL) innehåller nämligen bestämmelser om när myndighetsbeslut får verkställas. Enligt 35 § får ett beslut alltid verkställas omedelbart bl.a. om det gäller endast tillfälligt eller 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. Denna befintliga nationella reglering får i sammanhanget anses fullgod och välavvägd.

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 en tillsynsmyndighet minimeras. Bestämmelser om inhibition finns i 28 § förvaltningsprocesslagen (1971:291) och behöver inte tas in i den nya lagen.

9.3 Tillsynsbefogenheter med stöd av den nya lagen

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

I kapitel 8 har utredningen redogjort för tillsynsuppgifterna för den nationella myndigheten för cybersäkerhetscertifiering. Tillsynen omfattar alltså såväl EU:s cybersäkerhetsakt med anslutande certifieringsordningar som den nationella regleringen.

Utredningen finner följaktligen att de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering har enligt artikel 58.8 i EU:s cybersäkerhetsakt även bör gälla vid tillsyn över att bestämmelserna i den nya lagen och andra föreskrifter som kompletterar lagen följs.

En utgångspunkt bör vara att den nationella myndigheten för cybersäkerhetscertifiering ska kunna få det underlag som behövs för

tillsynen genom kontakter med t.ex. tillverkare och leverantörer på marknaden som har utfärdat en EU-försäkran om överensstämmelse eller innehar ett europeiskt cybersäkerhetscertifikat samt organ för bedömning av överensstämmelse.

9.4 Rätten att återkalla europeiska cybersäkerhetscertifikat

Förslag: Den nationella myndigheten för cybersäkerhetscertifiering ska få återkalla europeiska cybersäkerhetscertifikat som utfärdats av den myndigheten eller 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.

Enligt artikel 58.8 e i EU:s cybersäkerhetsakt får en nationell myndighet för cybersäkerhetscertifiering, i enlighet med nationell rätt, återkalla europeiska cybersäkerhetscertifikat som utfärdats av den myndigheten respektive 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.

Av artikel 56 framgår att de organ för bedömning av överensstämmelse som avses i artikel 60 får utfärda europeiska cybersäkerhetscertifikat i enlighet med vad som anges i denna 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.

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.

Genomförandet av artikel 58.8 i EU:s cybersäkerhetsakt förutsätter kompletterande reglering i nationell rätt. Den av utredningen föreslagna bestämmelsen ger den nationella myndigheten för cybersäkerhetscertifiering motsvarande rätt att återkalla sådana europeiska cybersäkerhetscertifikat som utfärdats av den myndigheten eller ett organ för bedömning av överensstämmelse som ackrediterats enligt artikel 60.1 och som inte längre uppfyller kraven i cybersäkerhetsakten eller en europeisk ordning för cybersäkerhetscertifiering.

9.5 Sanktioner

9.5.1 Inledning

I artikel 58.8 f i EU:s cybersäkerhetsakt anges att varje nationell myndigheter för cybersäkerhetscertifiering ska utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör.

I artikel 65 föreskrivs 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 dessa regler och åtgärder samt ändringar av dessa utan dröjsmål till kommissionen. I EU:s cybersäkerhetsakt saknas dock närmare riktlinjer för vilken typ av sanktioner som bör finnas eller i vilka fall en sanktionsavgift bör tas ut av den som inte efterlever bestämmelserna i ramverket

Enligt utredningsdirektiven ska utredningen analysera behovet av att införa bestämmelser om sanktioner och hur ett sådant regelsystem kan utformas.

9.5.2 Allmänna utgångspunkter

Utredningen ska således överväga vilka former av sanktioner som är nödvändiga och lämpliga för att bidra till ett effektivt genomförande av det europeiska ramverket för cybersäkerhetscertifiering.

De sanktionsverktyg som normalt står till buds för staten är straff och sanktionsavgifter samt vite, förbud och återkallelse av tillstånd. Varken direktiven eller EU:s cybersäkerhetsakt innehåller några begränsningar i fråga om vilken sorts sanktioner som får eller bör övervägas.

Till en början kan noteras att EU:s cybersäkerhetsakt ger den nationella myndigheten för cybersäkerhetscertifiering rätt att begränsa, tillfälligt upphäva eller återkalla bemyndiganden för organ för bedömning av överensstämmelse om dessa inte uppfyller kraven i förordningen.

Vidare får myndigheten återkalla europeiska cybersäkerhetscertifikat om sådana certifikat inte uppfyller kraven i förordningen eller en europeisk ordning för cybersäkerhetscertifiering.

Frågorna om bemyndigande och när en återkallelse bör komma i fråga har behandlats tidigare.

När det gäller behovet av att härutöver införa bestämmelser om straff eller sanktionsavgifter gör utredningen följande överväganden.

9.5.3 Finns behov av straffrättsliga sanktioner?

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

Genom förslagen om att utse en nationell myndighet med ansvar för tillsyn och föreslagna befogenheter införs ett system för tillsyn på cybersäkerhetsaktens tillämpningsområde; bl.a. får myndigheten användbara verktyg för att få till stånd rättelse av brister i arbetet med cybersäkerhetscertifiering.

Det kan mot den bakgrunden, och med hänsyn till möjligheten att införa ytterligare administrativa sanktioner, ifrågasättas om det är nödvändigt med en kriminalisering av överträdelser av det europeiska ramverket för cybersäkerhetscertifiering.

Det är vidare, enligt utredningens bedömning, tveksamt om straff skulle vara den mest effektiva sanktionen när det gäller åsidosättande av EU:s cybersäkerhetsakt och författning som meddelats med stöd av den akten. Aktörer som ska tillämpa regleringen utgörs främst av statliga myndigheter och företag. Straffansvar kan enligt svensk rätt endast träffa fysiska personer. Om straff införs skulle det i många fall vara svårt att identifiera en fysisk person som ansvarig för överträdelsen och att leda i bevis att denna haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet.

Härtill kommer att utredningen om genomförandet av NIS-direktivet (SOU 2017:36) övervägde om straff kunde utgöra en lämplig sanktion för överträdelser av det lagförslag om informationssäkerhet i vissa samhällsviktiga tjänster och digitala tjänster som utredningen lämnade. Utredningen fann dock inte tillräckliga skäl för att föreslå en sådan ordning. Utredningen föreslog i stället att den som gör sig skyldig till mer allvarliga överträdelse av lagens bestämmelser ska påföras en sanktionsavgift, som ska bestämmas till ett belopp som grundas på bl.a. hur allvarlig överträdelsen bedöms vara.

Utredningen gör sammantaget bedömningen att det för närvarande inte finns tillräckliga skäl för att föreslå en kriminalisering för överträdelser av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering. Någon särskild straffbestämmelse bör alltså inte införas i detta läge. I första hand bör man försöka korrigera brister och överträdelser av regelsystemet genom administrativa åtgärder och sanktioner.

9.5.4 Behovet av sanktionsavgift

Utredningen har föreslagit att den nationella myndigheten för cybersäkerhetscertifiering ges möjlighet till administrativa ingripanden i form av åtgärdsföreläggande, meddela förbud och möjlighet att återkalla ett europeiskt certifikat. Sanktionsavgift är en annan administrativ sanktion som riktar sig mot en konstaterad överträdelse av en författningsbestämmelse men ingår inte i det straffrättsliga systemet. En sådan avgift kan också påföras oberoende av om reglerna överträtts uppsåtligen eller av oaktsamhet.

Vid utformningen av sanktionssystemet bör utgångspunkterna vara desamma som när man i andra sammanhang infört sanktionsavgifter i den nationella rättsordningen (jfr t.ex. prop. 2017/18:232 s. 319). Det innebär att bestämmelserna om sanktionsavgift bör utformas i linje med hur sådana avgifter utformats inom andra områden.

Det innebär vidare att regeringens riktlinjer och Sveriges internationella åtaganden, däribland åtagandena enligt Europakonventionen, samt att de rättssäkerhetskrav som ställs på sanktionsavgift ska få genomslag.

En annan utgångspunkt är att systemet bör vara ändamålsenligt och effektivt för att på ett verkningsfullt sätt motverka de brister som det är tänkt att åtgärda.

Ett syfte med sanktionsavgift är att skapa en kännbar ekonomisk sanktion mot juridiska personer och incitament att undvika överträdelser av regelverk. Om sanktionsbeloppet är för lågt kan tillsynsobjektet/den objektsansvarige se avgiften som enbart en kostnad som det går att kalkylera med. När sanktionsavgift tas ut av en myndighet har den ekonomiska aspekten dock inte lika stor betydelse. Det kan vid ny lagstiftning även förekomma viss osäkerhet om hur sanktionssystemet ska tillämpas. Systemet måste därför utformas så att det är förutsebart och samtidigt möta kraven på en rättssäker process, rimlig handläggningstid och möjlighet till domstolsprövning. Frågor om sanktionsavgift bör därför regleras i lag och av lagen ska framgå när, hur och av vem sanktionsavgift får tas ut.

Vidare ska beaktas att ett system med sanktionsavgifter kan kräva ökade resurser hos den nationella myndigheten för cybersäkerhetscertifiering.

Eftersom utredningen föreslår att det införs en möjlighet att utfärda vitessanktionerade åtgärdsförelägganden skulle införandet av sanktionsavgifter leda till att den nationella myndigheten för cybersäkerhetscertifiering i vissa situationer kan välja mellan att genomdriva en åtgärd vid vite eller att i efterhand påföra sanktionsavgift. En fördel med detta är att ingripandemöjligheterna kan anpassas till behovet i det enskilda fallet.

Det ska noteras att det rör det sig om ett nytt, komplext och avgränsat rättsområde. En nackdel är då att sanktionssystemet inte blir

så förutsägbart som är önskvärt.[3] Samtidigt är en sanktionsavgift en skyndsam och tydlig sanktion som kan riktas både offentliga och privata aktörer vid mer allvarliga överträdelser av regelsystemet.

Det kan inte bortses från att risken att drabbas av en ekonomiskt kännbar sanktion bör vara avskräckande och kan bidra till att minska antalet överträdelser av regelsystemet. Bl.a. tvingas mindre seriösa aktörer som ger sig in på marknaden beakta risken att drabbas av sanktioner om reglerna inte följs. En konsekvens av sådana sanktioner bör också bli att konsumenternas förtroende för branschen på sikt kan öka, vilket ligger i det allmännas intresse. Genom att införa en möjlighet för den nationella myndigheten för cybersäkerhetscertifiering att i vissa fall besluta om sanktionsavgift skulle nämligen drivkrafterna för aktörerna att i förebyggande syfte anpassa sin verksamhet efter gällande krav öka. Detta gäller inte minst vid underlåtenhet att åtgärda brister och sårbarheter som borde ha kunnat upptäckas och hanteras innan de orsakat en säkerhetsincident eller på annat sätt uppmärksammats, t.ex. inom ramen för ett tillsynsärende. Utan möjligheten till sanktionsavgift riskerar företagen i princip inte några särskilda konsekvenser för sådan underlåtenhet eftersom tillsynen endast är framåtsyftande. Det finns följaktligen anledning att anta att ett system med sanktionsavgifter är förhållandevis effektivt och även kan ha betydelse för andra staters förtroende för hur det europeiska ramverket för cybersäkerhetscertifiering tillämpas i Sverige. Mer direkta sanktioner än förelägganden vid vite bör även kunna vara mer effektiva i fall där det är systematiska brister som ligger bakom incidenterna.

Utredningen bedömer att enbart möjligheten att återkalla bemyndiganden att utfärda cybersäkerhetscertifikat eller meddela åtgärdsföreläggande eller att återkalla ett certifikat inte är tillräckligt, särskilt med hänsyn till att cybersäkerhetscertifierade produkter, tjänster och processer kan förekomma i verksamheter som utgör samhällsviktig verksamhet och/eller i verksamheter som berör nationell säkerhet.

[3] Systemet med sanktionsavgifter medför högre krav på precision i de regler som kan ligga till grund för uttagande av avgiften. Dvs. det måste vara tydligt och förutsebart hur man ska leva upp till ett krav. Uttryckt med andra ord ska formuleringarna i lagen vara tillräckligt tydliga för att den aktuella sanktionsavgiften ska ha kunnat förutses (jfr Kammarrätten i Jönköpings dom den 22 november 2017 i mål nr 1847-16).

Även om EU:s cybersäkerhetsakt och det utkast till europeisk cybersäkerhetsordning som nu offentliggjorts endast reglerar möjligheten till frivillig certifiering av angivna IKT-produkter på assuransnivå betydande och hög ska beaktas att cybersäkerhetsakten ger möjlighet till att i en europeisk ordning föreskriva om obligatorisk certifiering av produkter, tjänster och processer inom aktens tillämpningsområde. Det ska noteras att Enisa för närvarande arbetar med att ta fram europeiska certifieringsordningar, förutom avseende den angivna för IKT-produkter (se kapitel 4) även för molntjänster (cloud services).[4]

Det kan i detta sammanhang noteras att i propositionen med förslag till kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (prop. 2015/16:72, s. 48 f.) gör regeringen bedömningen att överträdelser av förordningens bestämmelser är svårbedömda och därmed mindre lämpliga för sanktionsavgifter. Regeringen framhöll också att grunden för tillhandahållandet av betrodda tjänster är att inblandade parter hyser tillit till den som tillhandahåller den aktuella tjänsten. Denne kan dessutom förlora sin status som tillhandahållare av kvalificerade tjänster om man inte följer tillsynsmyndighetens föreläggande att vidta rättelse.

Utredningen finner inte skäl att göra någon bedömning av frågan om sanktionsavgift när det gäller överträdelser av den angivna förordningen. Samtidigt ska framhållas att det enligt utredningens bedömning finns betydande skillnader mellan dessa två regelsystem vad gäller syftet och omfattningen av regelsystemens tillämpningsområden. Till skillnad från regleringen av elektronisk signatur och betrodda tjänster, som i och för sig är viktiga tjänster inom olika verksamheter och samhällsområden, är syftet med det europeiska ramverket för cybersäkerhetscertifiering att öka cybersäkerheten elektroniska kommunikationsnät och kommunikationstjänster som har en avgörande betydelse för samhället. Informations- och kommunikationsteknik (IKT) är grunden för komplexa system som stöder viktiga samhällsverksamheter inom sektorer som hälso- och sjukvård, energi, finans och transporter samt bidrar till den inre marknadens funktion. För att minska riskerna i och öka cybersäkerheten måste därför alla nödvändiga åtgärder vidtas i unionen så att nätverks-

[4] Det finns ännu inga formella beslut om att ta fram certifieringsordningar för internet of things (IoT), 5G, e-hälsa, och kontrollsystem för automatisering inom industrin, men detta är områden som kan komma att beröras i framtiden.

och informationssystem, kommunikationsnät, digitala produkter, tjänster och enheter som används av myndigheter, organisationer, företag och privatpersoner skyddas bättre mot cyberhot.

Utredningen anser att förtroendet för och tilliten till att certifierade IKT-produkter, -tjänster och -processer uppfyller ställda krav på cybersäkerhet är grundläggande för legitimiteten och effektiviteten i det europeiska ramverket för cybersäkerhetscertifiering. Överträdelser av regelsystemet, som medför att certifierade produkter, tjänster och processer inte uppfyller förväntad funktionalitet i fråga om cybersäkerhet, innebär risk för att dessa kan komma att finnas i samhällsviktiga informations- och kommunikationssystem och åsamka betydande skador, såväl ekonomiska som allvarliga skador av annan karaktär. Vikten av ett sanktionssystem som har en avskräckande verkan för att inte följa regelsystemet är därför betydande.

Utredningen gör sammantaget bedömningen att även om en prövning av en överträdelse i vissa fall kan innefatta komplexa och svårbedömda frågor, av bl.a. teknisk natur, överväger vikten av att alla aktörer efterlever bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering, inte minst mot bakgrund av vikten av säkra och fungerande ITK-produkter, -tjänster och -processer i samhällsviktiga verksamheter men även då många konsumenter kan komma att utsättas för risker med bristfällig cybersäkerhet i produkter och tjänster. Det bör därför i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt införas en bestämmelse om sanktionsavgift som ett komplement till möjligheten för den nationella myndigheten för cybersäkerhetscertifiering att meddela åtgärdsföreläggande, förbud eller besluta om återkallelse av ett europeiskt cybersäkerhetscertifikat.

9.5.5 Överträdelser som ska leda till sanktionsavgift

Förslag: Sanktionsavgift ska tas ut av den som

1. utfärdar en EU-försäkran om överensstämmelse 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 informera den myndighet eller det organ som avses artikel 56.8 punkt 7 i EU:s cybersäkerhetsakt 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. den som 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 fattat av den nationella myndigheten för cybersäkerhetscertifiering, eller
7. använder ett europeiskt cybersäkerhetscertifikat som blivit återkallat enligt artikel 58.8 e i EU:s cybersäkerhetsakt.

Frånvaron av fastställda europeiska ordningar för cybersäkerhetscertifiering innebär en utmaning att mer uttömmande ange vilka konkreta överträdelser av regelverket som bör komma ifråga för sanktioner. Om det införs krav på obligatorisk cybersäkerhetscertifiering på området ökar dock behovet av ett effektivt sanktionssystem.

Flertalet aktörer som kommer att vara verksamma på marknaden för cybersäkerhetscertifiering är vinstdrivande företag som verkar i konkurrens med varandra. Fråga uppkommer då om behovet av att utforma regleringen så att den ger aktörerna tillräckliga drivkrafter att följa de krav som uppställs. Utgångspunkterna vid övervägande om vilka överträdelser av det europeiska ramverket för cybersäkerhetscertifiering som 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.

Det europeiska ramverket för cybersäkerhetscertifiering utgörs av bestämmelser som återfinns i EU:s cybersäkerhetsakt och i de europeiska ordningar för cybersäkerhetscertifiering som kommer att utfärdas med stöd av akten. Certifieringsverksamheten grundas förutom på dessa bestämmelser även på internationella standarder, bl.a. vad som anges i Common Criteria (CC), samt tekniska standarder och andra kravspecifikationer. Det är således ett omfattade och komplext regelsystem, varför endast mer allvarliga och tydliga och avgränsade överträdelser bör omfattas av sanktionsavgift.

Den nationella myndigheten för cybersäkerhetscertifiering har i uppgift att kontrollera och övervaka efterlevnaden av bestämmelserna i det europeiska ramverket för cybersäkerhetscertifiering, bl.a. att tillverkare och leverantörer uppfyller sina skyldigheter enligt regelverket. För att myndigheten ska kunna fullgöra sitt uppdrag förutsätts att den får kunskap om att en EU-försäkran eller ett europeiskt cybersäkerhetscertifikat utfärdas (se kapitel 7). En IKT-tillverkare eller -leverantör ska enligt artikel 53.3 ge den nationella myndigheten för cybersäkerhetscertifiering tillgång till bl.a. EU-försäkran om överensstämmelse. Cybersäkerhetsakten ålägger också enskilda som ansöker om cybersäkerhetscertifiering och certifikatinnehavare en informationsskyldighet i förhållande till berörda myndigheter och organ (se artikel 56.7 och 8). Till detta kommer att den nationella myndigheten för cybersäkerhetscertifiering har rätt att enligt artikel 58.8 a begära alla uppgifter som är nödvändiga från utfärdare av EU-försäkringar av överensstämmelse, certifikatinnehavare och organ för bedömning av överensstämmelse. Därför finner utredningen inte skäl att föreslå någon anmälningsskyldighet i den nya lagen som kan grunda sanktionsavgift. Om närmare föreskrifter om en anmälningsskyldighet meddelas bör den nationella myndigheten för cybersäker-

hetscertifiering främst förelägga IKT-tillverkaren eller -leverantören att fullgöra skyldigheten, eventuellt vid äventyr av vite.

Av EU:s cybersäkerhetsakt och den aktuella europeiska ordningen för cybersäkerhetscertifiering framgår vidare de skyldigheter som gäller för den som utfärdar en EU-försäkran eller innehar ett europeiskt cybersäkerhetscertifikat.

Utredningen anser att en tillverkare eller leverantör som gör sig skyldig till en överträdelse 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 påföras en sanktionsavgift, bl.a. om en tillverkare eller leverantör tillhandhåller en IKT-produkt, -tjänst eller -process i strid mot vad som gäller enligt cybersäkerhetsakten och europeiska ordningar för cybersäkerhetscertifiering eller vid bristande fullgörelse av skyldigheten att lämna uppgifter och information enligt artiklarna 54 m och 55 eller någon annan skyldighet som följer av en europeisk ordning för cybersäkerhetscertifiering eller lagen med kompletterande bestämmelser till cybersäkerhetsakten eller föreskrifter som utfärdats med stöd av den lagen. Den som lämnar oriktiga uppgifter till den nationella myndigheten för cybersäkerhetscertifiering i samband med tillsyn bör också kunna påföras sanktionsavgift.

En sanktionsavgift bör dock bara komma i fråga för mer allvarliga överträdelser. Det bör för övrigt sakna betydelse om en skada faktiskt har inträffat eller inte.

9.5.6 Vem ska påföras sanktionsavgiften?

I EU:s cybersäkerhetsakt saknas närmare bestämmelser om 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. Även statliga myndigheter kan påföras sanktionsavgift.

9.5.7 Sanktionsavgift ska alltid tas ut

Förslag: Regleringen av sanktionsavgifter ska bygga på strikt ansvar. Det ska vara obligatoriskt att ta ut sanktionsavgift när en bestämmelse i cybersäkerhetsakten och den nya lagen som kan föranleda avgift har överträtts.

Huvudregeln vid användande av sanktionsavgift är att avgiftsskyldigheten ska bygga på strikt ansvar. Det behöver då inte bevisas att handlandet varit avsiktligt eller oaktsamt, vilket medför att system med sanktionsavgifter anses vara effektiva (se t.ex. prop. 2017/18:232 s. 324). För att inte den fördelen ska gå förlorad bör berörd aktör ha ett strikt ansvar för sådana överträdelser som kan föranleda att sanktionsavgift tas ut. Det är också svårt att se att överträdelser i normalfallet kan bero på annat än uppsåt eller oaktsamhet (jfr regeringens riktlinjer för att använda sanktionsavgift, prop. 1981/82:142 s. 24 och 25). Utredningen anser att det inte finns skäl att avvika från denna grundprincip när det gäller överträdelser av det europeiska ramverket för cybersäkerhetscertifiering. Den ordning som föreslås bygger således på strikt ansvar, utan krav på uppsåt eller oaktsamhet. Det är tillräckligt för att kunna ta ut en sanktionsavgift att en överträdelse har ägt rum.

Bestämmelser om sanktionsavgifter är vanligen obligatoriska, men den motsatta lösningen förekommer. Å ena sidan 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). Å andra sidan kan reglerna om cybersäkerhetscertifiering vara komplexa, och obligatoriskt beslutande om sanktionsavgifter kan lägga en stor börda på myndigheten med ansvar för tillsyn.[5]

Utredningen anser att övervägande skäl ändå talar för att det på det nu aktuella området bör vara obligatoriskt att besluta om sanktionsavgift när förutsättningarna för det är uppfyllda. Detta minskar utrymmet för skönsmässiga bedömningar av den nationella myndigheten för cybersäkerhetscertifiering och är dessutom bäst förenligt med förslaget om sanktionsavgift för mer allvarliga överträdelser av regelverket.

[5] Liknande resonemang har förts i betänkandet om Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82).

En sådan utformning innebär också att det inte bör införas ett krav på att ett beslut om sanktion alltid ska föregås av ett åtgärdsföreläggande. Den nationella myndigheten för cybersäkerhetscertifiering bör dock ha möjlighet att under vissa förutsättningar sätta ned eller avstå från att ta ut en sanktionsavgift (se avsnitt 9.5.10).

9.5.8 Den nationella myndigheten för cybersäkerhetscertifiering ska besluta om sanktionsavgift

Beslut om sanktionsavgift fattas som huvudregel av en tillsynsmyndighet eller av domstol efter ansökan från tillsynsmyndigheten.

Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En domstol brukar anses mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva subjektiva rekvisit eller andra svårbedömda rekvisit (se t.ex. prop. 2017/18:205 s. 68).

En tillsynsmyndighet har genom tillsynsansvaret en god inblick i verksamheten och torde bli väl förtrogen med det europeiska ramverket för cybersäkerhetscertifiering. Den nationella myndigheten för cybersäkerhetscertifiering bör ha, eller genom t.ex. kompetensutveckling kunna skaffa sig, goda förutsättningar att upptäcka och bedöma överträdelser av bestämmelserna (jfr resonemangen i SOU 2013:38 s. 546).

En fördel med en ordning där myndigheten med ansvar för tillsyn fattar beslutet om sanktionsavgift är även att handläggningen blir snabbare eftersom en domstol inte måste involveras i hanteringen. Erfarenheter av sanktionsavgifter från andra områden talar för att systemet används betydligt mer när myndigheterna själva kan fatta beslutet jämfört med situationer där myndigheterna måste ansöka hos domstol. Erfarenheten visar dessutom att det är ovanligt att sanktionsavgiftsbeslut som meddelas av en myndighet överklagas och att ändringsfrekvensen är låg i de fall som överklagas (se SOU 2014:83 s. 105).

Med hänsyn till det anförda bör det, enligt utredningens mening, vara den nationella myndigheten för cybersäkerhetscertifiering som bestämmer om sanktionsavgift ska tas ut i det enskilda fallet och hur hög avgiften i så fall ska vara.

9.5.9 Sanktionsavgiftens storlek

Förslag: En sanktionsavgift ska bestämmas till lägst 10 000 kronor och högst 15 miljoner kronor.

Sanktionsavgifter kan vara utformade som på förhand bestämda belopp eller beloppsintervall, som gäller oavsett vem som begått överträdelsen, eller vara kopplade till årsomsättning i näringsverksamhet. Det viktiga är att sanktionsavgifterna är effektiva, proportionerliga och avskräckande.

Överträdelser av det europeiska ramverket för cybersäkerhetscertifiering bedöms som tidigare angetts kunna påverka samhällsviktig verksamhet och även leda till allvarlig skada för Sveriges säkerhet. Därför bör maximibeloppet sättas så högt att det får en avskräckande effekt.[6] Systemet får inte heller bli verkningslöst för de som väljer att använda sig av det.

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.

Med hänsyn till att de aktörer som omfattas av bestämmelserna är både myndigheter och företag är det inte lämpligt att koppla sanktionsavgiften till omsättning, utan att ett system med bestämda beloppsintervall är att föredra (jfr bedömningarna i prop. 2017/18:205 s. 70 och 71 samt SOU 2018:82 s. 442 f.).

För att sanktionsavgifterna ska vara effektiva, proportionerliga och avskräckande bör intervallet för sanktionsavgiften vara förhållandevis stort. Den nationella myndigheten för cybersäkerhetscerti-

[6] Dessutom bör beaktas att bristande efterlevnad av regelverket för europeisk cybersäkerhetscertifiering, i tillämpliga fall, kan föranleda ingripanden mot själva certifikatet, såsom återkallelse. Vidare kan överträdelser straffas av marknaden i sig då en grund för en affärsverksamhet att tillhandahålla cybersäkerhetscertifierad IKT torde bygga på att inblandade parter hyser tillit till att tillverkaren och leverantören uppfyller uppställda krav (jfr resonemanget i prop. 2015/16:72 s. 48 f.).

fiering 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. NIS-lagen eller vad som föreslagits i betänkandet *Komplettering till säkerhetsskyddslagen* (SOU 2018:82) vid överträdelser av säkerhetsskyddslagstiftningen, dvs. högst tio (10) miljoner kronor. En sådan avgift har av regeringen bedömts utgöra en effektiv, proportionell och avskräckande sanktion mot allvarliga överträdelser (jfr prop. 2017/18:205 s. 71). En jämförelse kan även göras med betänkandet *Organisation och samordning av marknadskontroll* (SOU 2020:49) där det föreslagits att en marknadskontrollmyndighet ska kunna ta ut en sanktionsavgift på mellan 15 000 kronor och 15 miljoner kronor. Det högre spannet motiveras av att brister i överensstämmelse med produktrelaterade krav i värsta fall kan innebära stora risker för människors liv och hälsa, och även för miljön. Utredningen noterar att marknadskontrollen har flera likheter med området för europeisk cybersäkerhetscertifiering.

Mot bakgrund av det ovan angivna, och med beaktande av förekomsten av stora globala aktörer på IKT-marknaden, gör utredningen bedömningen att det högsta sanktionsbeloppet bör bestämmas till 15 miljoner kronor. Den nedersta gränsen kan 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. T.ex. om 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 IKT som kan skada samhällsviktig verksamhet bör bedömas strängare.

9.5.10 Sanktionsavgiftens storlek i det enskilda fallet

Förslag: När sanktionsavgiftens storlek ska bestämmas ska hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den avgiftsskyldige tidigare begått en överträdelse och de kostnader som den avgiftsskyldige undvikit 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 eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

När storleken på sanktionsavgiften ska bestämmas i det enskilda fallet bör hänsyn tas till alla relevanta omständigheter. Det är inte möjligt att i den nya lagen ange samtliga relevanta omständigheter som kan behöva beaktas i enskilda fall. Vi bedömer dock att lagen bör innehålla en bestämmelse som anger omständigheter som särskilt bör beaktas.

De omständigheter som är särskilt viktiga att beakta och som alltså bör tas in i lagen är den skada eller risk för skada som uppstått till följd av överträdelsen, om den avgiftsskyldige tidigare begått en överträdelse och de kostnader som den avgiftsskyldige undvikit till följd av överträdelsen. En försvårande omständighet vid bedömningen av skadan eller risken för skada är om överträdelsen medför sårbarhet eller risk för skada på bl.a. samhällsviktig verksamhet och/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.

Vissa omständigheter kan det finnas anledning att beakta i mildrande riktning. Att en verksamhet aktivt samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelser kan vara en sådan omständighet samt om verksamheten snabbt har vidtagit rättelse (jfr t.ex. 15 kap. lagen om bank- och finansieringsrörelse och prop. 2016/17:22 s. 220 och 221).

Att avgiftsskyldigheten bygger på strikt ansvar innebär att det behöver finnas en möjlighet för den nationella myndigheten för cybersäkerhetscertifiering att underlåta att besluta om sanktionsavgift. Det bör därför införas en bestämmelse som ger myndigheten utrymme att jämka eller avstå från att ta ut avgiften i fall där det inte framstår som rimligt och proportionerligt att ta ut avgift, t.ex. när överträdelsen skulle kunna anses ursäktlig. 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. Det är däremot inte oskäligt att ta ut en sanktionsavgift när överträdelsen exempelvis berott på att en aktör inte känt till reglerna eller överträdelsen berott på dålig ekonomi, tidsbrist eller bristande rutiner.

9.5.11 Hinder mot sanktionsavgift

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.

Enligt Europakonventionen och EU:s stadga om de grundläggande rättigheterna finns en rätt att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. dubbelbestraffningsförbudet. Som regeringen har konstaterat i flera lagstiftningsärenden får begreppet straff i den mening som avses i Europakonventionen anses omfatta vite (se prop. 2007/08:107 s. 24 och 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 bör anses vara när det inleds en domstolsprocess angående frågan om utdömande av vite (jfr prop. 2016/17:22 s. 228).

Ett föreläggande om vite bör därför inte hindra ett senare 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. Dock ska obligatoriskt uttagande av sanktionsavgift inte möjliggöra att ett åtgärdsföreläggande beslutas därefter och vite utdöms om den ansvarige trots sanktionsavgift och föreläggande ändå inte vidtar rättelse.

9.5.12 Förfarandet vid beslut om sanktionsavgift

Förslag: 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.

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.

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

Beslut om administrativa sanktionsavgifter är en särskilt ingripande åtgärd. I likhet med vad som gäller enligt bl.a. NIS-lagen bör sådana beslut därför delges den betalningsskyldige enligt delgivningslagen (2010:1932). En bestämmelse om detta bör tas in i den nya lagen.

Enligt NIS-lagen gäller att sanktionsavgift inte får beslutas om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom

två år från överträdelsen. I propositionen angav regeringen att en sådan gräns bör finnas på grund av sanktionsavgiftens ingripande natur (prop. 2017/18:205 s. 74). Man har även anslutit sig till detta resonemang i betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82). 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 att två år är en rimlig sådan gräns. En bestämmelse med motsvarande innebörd som i den nyss nämnda lagen bör alltså införas i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Liksom i andra liknande fall bör bevisbördan för att kommunikation har skett ligga på tillsynsmyndigheten (jfr prop. 2017/18:205 s. 74).

För att regleringen om sanktionsavgifter ska bli tillräckligt handlingsdirigerande och effektiv bör den avgift som den nationella myndigheten för cybersäkerhetscertifiering beslutat kunna drivas in utan att det krävs något domstolsavgörande. Det bör därför föreskrivas 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. Det bör vidare föreskrivas att myndigheten ska lämna den obetalda avgiften för indrivning om avgiften inte betalas inom denna tid.

I allmänhet gäller för den här typen av avgifter att de preskriberas i den utsträckning verkställighet inte har skett inom fem år. Det saknas anledning att införa annan preskriptionstid än den som i allmänhet används. Preskriptionstiden bör därför vara fem år.

Sanktionsavgiften bör tillfalla staten.

10 Organ för bedömning av överensstämmelse

10.1 Inledning

I detta kapitel behandlas frågan om behovet av kompletterande nationella bestämmelser när det gäller ackreditering av organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt och förutsättningar för att överlämna uppgiften att utfärda cybersäkerhetscertifikat till sådana organ enligt artiklarna 56.4, 56.5 b, 56.6 eller 60.3 i cybersäkerhetsakten. Vidare behandlas anmälningsförfarandet för ackrediterade organ för bedömning av överensstämmelse till kommissionen enligt artikel 61.

10.2 Bakgrund

Ackreditering är en term som ibland används som synonym för certifiering eller registrering.[1] I rättslig mening innebär ackreditering att ett företag, en organisation eller en person får ett opartiskt och internationellt accepterat godkännande av att ha kompetens, system och rutiner för att utföra vissa bestämda uppgifter inom provning, kontroll eller certifiering. Ackrediteringen meddelas av ett särskilt ackrediteringsorgan (en myndighet) efter genomförd utvärdering av en aktör. Närmare bestämt är alltså ackrediteringsorganet ett tredjepartsorgan som bedömer och kompetensprövar certifieringsorgan, besiktningsorgan, kontrollorgan och laboratorier. Ackreditering syftar till att bedöma och säkerställa att tillämpliga krav[2] på aktö-

[1] Att ackreditera betyder att ”ge fullmakt åt” någon, Svenska Akademins ordlista (2015).
[2] Kraven avser teknisk kompetens, kapacitet och oberoende.

rerna uppfylls. Som huvudregel ska också ackreditering ligga till grund för utnämning av s.k. anmälda organ.[3]

Gemensamma bestämmelser för ackreditering inom EU finns 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. Regleringen innebär att ett nationellt ackrediteringsorgan förklarar att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, ytterligare krav.

Begreppet ackreditering definieras i artikel 2 i förordningen som en förklaring från ett nationellt ackrediteringsorgan om att ett organ för bedömning av överensstämmelse[4] uppfyller kraven i harmoniserade standarder och, i förekommande fall, eventuella ytterligare krav. Sådana krav kan vara bl.a. de som fastställs i sektorsspecifika program för att utföra specifika bedömningar av överensstämmelse.[5]

För att säkerställa att ackrediteringsorganet som utför ackreditering också är oberoende och kompetent att utföra ackreditering har ett antal internationella procedurer och standarder fastställts i medverkan av ackrediteringsorgan i olika stater. Kraven på de organ som ackrediterats har också fastställts i standarder.

Det krävs vidare att varje medlemsstat måste ha ett nationellt ackrediteringsorgan, som ska handha ackreditering avseende såväl obligatorisk som frivillig provning och kontroll. Den nationella ackrediteringen ska vara fri från kommersiell konkurrens och bedrivas som en icke-vinstdrivande aktivitet. Detta gäller oberoende av om ackrediteringen sker på harmoniserade eller icke-harmoniserade områden. Ackrediteringsorganen får inte bedriva verksamhet som konkurrerar med de organ som ackrediteras. Inte heller ska olika länders nationella ackrediteringsorgan aktivt konkurrera med varandra.

[3] För vissa produkter krävs att en bedömning görs av en tredje part; ett till Europeiska kommissionen anmält organ som bedömts kompetent. Kommissionen administrerar en databas med uppgifter om anmälda organ kallad Nando (New Approach Notified and Designated Organisations). Genom Nando går det att ta reda på vilket organ som har tilldelats ett visst nummer och vilka uppgifter organet har befogenhet att utföra.
[4] Överensstämmelse innebär uppfyllande av ett krav.
[5] I cybersäkerhetsaktens allmänna bestämmelser hänvisas till relevanta definitioner i förordning (EG) nr 765/2008 i fråga om ackreditering och bedömning av överensstämmelse.

10.3 Bestämmelser i EU:s cybersäkerhetsakt om ackreditering av organ för bedömning av överensstämmelse

Det europeiska ramverket för cybersäkerhetscertifiering syftar till en harmonisering av regler för cybersäkerhetscertifiering. Regelverket avser vidare att öka cybersäkerheten och den inre marknadens funktion, t.ex. vad avser fri rörlighet på den inre marknaden. För att kunna uppnå detta måste de krav som ställs på ackrediterade organ för bedömning av överensstämmelse och de regler som ska gälla för dessas verksamhet vara så enhetliga som möjligt inom unionen.

Av artikel 56.4 i EU:s cybersäkerhetsakt följer att de organ för bedömning av överensstämmelse som avses i artikel 60 ska utfärda europeiska cybersäkerhetscertifikat som avser assuransnivå ”grundläggande” eller ”betydande” på grundval av de kriterier som ingår i en europeisk ordningen för cybersäkerhetscertifiering.

I artikel 60.1 föreskrivs att 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.

I artikel 60.2 föreskrivs att om ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet 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 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.

Ackrediteringen som avses i artikel 60.1 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 som anges i artikel 60.

I bilagan till EU:s cybersäkerhetsakt framgår att de organ för bedömning av överensstämmelse som önskar bli ackrediterade ska uppfylla bl.a. 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.

Förutom det ovan angivna ställs även krav på bl.a. kompetens och teknisk expertis hos organen för bedömning av överensstämmelse (se bilaga 3). De organ för bedömning av överensstämmelse som an-

ges i artikel 60.1 ska således utöver de krav som gäller för ackrediteringen enligt regelverket för ackreditering även uppfylla de krav som följer av EU:s cybersäkerhetsakt och de krav som kan tillkomma i europeiska ordningar för cybersäkerhetscertifiering.

10.4 Gällande reglering om ackreditering och bedömning av överensstämmelse

Lagen (2011:791) om ackreditering och teknisk kontroll innebär att svensk rätt anpassas till förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter när det gäller ackreditering och CE-märkning. Lagen och tillhörande förordning 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. I lagen finns också regler om att organ ska ge Styrelsen för ackreditering och teknisk kontroll (Swedac) tillträde för tillsyn. Av 7 § i den lagen framgår att bedömning av organ som begär att få bli utsett och anmält för uppgifter i samband med bedömning av överensstämmelse enligt harmoniserad unionslagstiftning (anmält organ) ska ske genom ackreditering, om inget annat är föreskrivet.

Ett organ som vill bli ackrediterat måste lämna en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen och förordningen om ackreditering och teknisk kontroll och de föreskrifter som Swedac har utfärdat för det aktuella området. Organet måste även uppfylla de sektorsspecifika myndighetsföreskrifter eller andra krav som organet ska arbeta i enlighet med.

Efter att en verksamhet ackrediterats genomför Swedac regelbundet granskningar av att kraven som ställs på kompetens och arbetsrutiner uppfylls.

Swedac har meddelat föreskrifter och allmänna råd om ackreditering som tillämpas på organ som beviljats eller ansöker om ackreditering hos Swedac.[6] Ett organ som omfattas av föreskrifterna ska på Swedacs begäran ge tillträde till lokaler, upplysningar och hand-

[6] STAFS 2015:8.

lingar i den utsträckning som behövs för tillsyn enligt 19 § lagen (2011:791) om ackreditering och teknisk kontroll.

Swedac har meddelat föreskrifter och allmänna råd om ackreditering av organ som certifierar produkter: STAFS 2013:5. Dessa föreskrifter tillämpas på organ som är eller ansöker om att bli ackrediterade av Swedac för certifiering av produkter. En förutsättning för ackreditering för certifiering är att den ansökande kan visa att kraven i den internationella standarden ISO/IEC 17065:2012 uppfylls. Föreskrifterna kompletterar Swedacs föreskrifter och allmänna råd (STAFS 2015:8) om ackreditering.

I Sverige är det Swedac som efter kompetensbedömning anmäler svenska organ till kommissionen. Swedac ansvarar även för att föra in information om svenska anmälda organ i kommissionens informationssystem Nando.

Förhållandet till standarder

Swedacs koppling till standardiseringsfrågorna sammanhänger med dess roll som organ för den nationella ackrediteringen, som bygger på standarder. Swedac måste som ackrediteringsorgan följa standarden ISO/IEC 17011 för sin egen verksamhet (och i sitt ackrediteringsarbete tillämpas andra ISO-, ISO/IEC- eller SS-EN-standarder).

Att Swedac och ackrediteringsorgan i olika länder arbetar enligt samma standarder underlättar ömsesidiga godkännanden av kompetensen hos ackrediterade organ. Detta i sin tur underlättar internationell handel eftersom certifikat som utfärdats av ett ackrediterat organ i ett land erkänns i ett annat land och ingen ytterligare kontroll behöver ske. Det är särskilt viktigt för små och medelstora företag eftersom dessa normalt har större svårigheter än större företag att hantera olika länders krav på teknisk kontroll.

Påverkan på gällande reglering

Swedac utfärdar inte några egna föreskrifter med krav som organ för bedömning för överensstämmelse ska leva upp till, utan andra myndigheter tar fram regler som Swedac sedan applicerar när man granskar sina kunder och deras efterlevnad av föreskrifterna. Här är det alltså inte själva produkterna som granskas. Det sker ett sam-

arbete med utfärdande myndighet och Swedac gör i sin verksamhet närmast en tolkning av föreskrifterna i respektive fall. Möjligheten att påverka utformningen av kraven ligger främst i att Swedac vid remittering får yttra sig över samtliga tekniska föreskrifter.

Swedac anger att myndigheten fortsättningsvis kommer att ackreditera evalueringsorganisationer och certifieringsorgan mot redan befintliga kontrollordningar. Swedac noterar att Enisa fått i uppgift att evaluera ackrediteringsbara certifieringsordningar som aktörer därefter kommer att kunna certifiera sig mot. Swedac kommer, när certifieringsordningarna är klara, att ackreditera certifieringsorgan mot certifieringsordningarna.

Swedac har tidigare utfärdat flera föreskrifter för ackreditering inom området it-säkerhet, vilka kompletterat de allmänna reglerna om ackreditering. Mot bakgrund av cybersäkerhetsaktens ikraftträdande utfärdade Swedac föreskriften STAFS 2019:3 om upphävande av Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd (STAFS 2007:20) om evalueringsorganisationer som utvärderar IT-säkerhet samt föreskrifter och allmänna råd (STAFS 2007:21) om ackreditering av organ som certifierar IT-säkerhet. Nämnda föreskrifter upphörde att gälla efter december 2019.

Att Swedac upphävt sina tidigare föreskrifter om certifieringsorgan och evalueringsorganisationer på it-säkerhetsområdet, vilka bl.a. byggt på CCRA, beror på att ackrediteringsorganet i och med cybersäkerhetsakten inte längre anser sig ha mandat att reglera området. Man vill således undvika dubbelreglering. Swedac får för övrigt inte ta fram egna certifieringsordningar. Nationella certifieringsordningar kan likväl tas fram, om än den dominerande uppfattningen bland experter är att merparten av ordningarna för cybersäkerhetscertifiering kommer att antas på EU-nivå. Tillkommer en certifieringsordning på aktuellt område evaluerar Swedac huruvida ordningen är ackrediterbar eller inte. Det finns ingen nationell rätt som reglerar krav avseende ackreditering och certifiering på IKT-området, utan kundkrav på informationssäkerhet är vanligast förekommande. Swedac har även gett ut dokument om vägledning för ackrediterade verksamheters informationssäkerhetsarbete. Dokumenten ger också vägledning till de krav som ställs vid bedömning av informationssäkerhet.

10.5 Behovet av kompletterande bestämmelser

Förslag: I lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska det upplysningsvis anges att bestämmelser om ackreditering av organ för bedömning av överensstämmelse finns i förordning (EG) nr 765/2008 och i lagen (2011:791) om ackreditering och teknisk kontroll.

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

I och med att EU:s cybersäkerhetsakt anger att organen för bedömning av överensstämmelse ska vara ackrediterade enligt förordning (EG) nr 765/2008 finns det inget behov av att i den nya lagen ange att ackreditering ska ske på det sättet. Däremot bör det i lagen införas en upplysningsbestämmelse om var det finns bestämmelser om ackreditering.

I bilagan till EU:s cybersäkerhetsakt finns emellertid bestämmelser om vilka krav som organ för bedömning av överensstämmelse som önskar bli ackrediterade ska uppfylla (se ovan). Som framgår finns det i lagen om ackreditering och teknisk kontroll bestämmelser inom det område som cybersäkerhetsakten omfattar. Den lagen har dock införts för att genomföra förordningen om ackreditering och lagen täcker inte hela aktens tillämpningsområde. Det kan finnas behov av kompletterande reglering avseende ackreditering och dessa bestämmelser bör till följd av cybersäkerhetsaktens införande samlas i den nya lagen med kompletterande bestämmelser till den akten.

Regeringen eller den myndighet regeringen utser ska bemyndigas att meddela de ytterligare föreskrifter om ackreditering som kan behövas.

Gränsdragningen mellan myndigheten för cybersäkerhetscertifiering och Swedac vid tillsyn över ackrediterade organ för överensstämmelse

I utredningsdirektiven anges att utredningen bör – för att undvika att den nationella myndigheten för cybersäkerhetscertifiering tilldelas uppgifter som redan utförs av Styrelsen för ackreditering och teknisk kontroll (Swedac) – kartlägga hur förhållandet mellan den myndigheten och Swedac ska se ut, i vilka fall de två myndigheterna

ska samarbeta och vilket behov av kompletterande nationella bestämmelser som behövs. Det är viktigt att i detta arbete beakta de kostnader, den tid och andra aspekter som en dubbel granskning av såväl Swedac som den nationella myndigheten för cybersäkerhetscertifiering kommer att innebära för den som blir granskad.

Utredningen bedömer att när det gäller Swedacs uppgifter och ansvar för såväl ackreditering som tillsyn av organ för bedömning av överensstämmelse framgår detta av gällande reglering om ackreditering i förening med de ytterligare krav som anges i EU:s cybersäkerhetsakt och framtida genomförandeakter. Motsvarande gäller för den nationella myndigheten för cybersäkerhetscertifiering när det gäller tillsyn enligt EU:s cybersäkerhetsakt. Myndigheterna ska därför samverka och samråda vid tillsyn över ett tillsynsobjekt för att undvika att oklarhet uppstår om vad tillsynen av respektive myndighet omfattar och för att reducera kostnaderna för tillsynsobjektet.

10.6 Överlämnande av förvaltningsuppgifter till organ för bedömning av överensstämmelse

Bedömning: I artiklarna 56.4, 56.6, 58.7 e och 60.3 i EU:s cybersäkerhetsakt överlämnas certifieringsuppgifter, dvs. förvaltningsuppgifter, till privaträttsliga organ för bedömning av överensstämmelse. Denna reglering är att likställa med lag och innebär att det inte behövs kompletterande nationella bestämmelser till stöd för att överlämna dessa förvaltningsuppgifter till privaträttsliga organ.

Överlämnande av förvaltningsuppgift

När det gäller frågan om det föreligger behov av nationella kompletterande bestämmelser för att den nationella myndigheten för cybersäkerhetscertifiering ska kunna överlämna, men även kunna återta, uppgiften att utfärda cybersäkerhetscertifikat till privaträttsliga subjekt i form av organ för bedömning av överensstämmelse gör utredningen följande överväganden.

Enligt 12 kap. 4 § andra stycket regeringsformen får överlämnande av en förvaltningsuppgift ske endast med stöd av lag. Av artikel 56.4

i EU:s cybersäkerhetsakt följer att ett privat organ för bedömning av överensstämmelse som avses i artikel 60 får utfärda europeiska cybersäkerhetscertifikat på assuransnivå grundläggande och betydande. Utfärdande av cybersäkerhetscertifikat enligt EU:s cybersäkerhetsakt bör ses som en förvaltningsuppgift som även kan innefatta myndighetsutövning, eftersom certifikatet, särskilt när det är fråga om obligatorisk cybersäkerhetscertifiering, utgör en förutsättning för att en enskild tillverkare eller leverantör ska kunna tillhandhålla IKT-produkten eller IKT-tjänsten på den inre marknaden. Bestämmelsen rör således rättigheter och skyldigheter för enskild som är att jämställa med lag. Därför behövs ingen kompletterande nationell reglering i detta fall.

Krav på bemyndigande

När artikel 56.6 är tillämplig, dvs. när en europeisk ordning för cybersäkerhetscertifiering kräver assuransnivå hög, är det en nationell myndighet för cybersäkerhetscertifiering som får utfärda ett cybersäkerhetscertifikat på den nivån. Myndigheten har dock möjlighet att på förhand delegera rätten att utfärda certifikatet till ett angivet ackrediterat organ för bedömning av överensstämmelse eller besluta om en allmän delegering av den uppgiften till ett sådant organ för bedömning av överensstämmelse. Av denna bestämmelse framgår således att den nationella myndigheten för cybersäkerhetscertifiering får överlämna till ett privat organ för bedömning av överensstämmelse att utfärda angivna certifikat. Det behövs i detta fall därför ingen kompletterande nationell reglering.

Enligt artikel 58.7 e får en nationell myndighet för cybersäkerhetscertifiering i tillämpliga fall utfärda bemyndiganden enligt artikel 60.3 för kontrollorgan att utföra certifieringsuppgifter och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organet inte uppfyller kraven enligt EU:s cybersäkerhetsakt.

I artikel 60.3 anges att om en europeisk ordning 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.

Som framgår ovan får således enligt artikel 60.3 i EU:s cybersäkerhetsakt endast de organ för bedömning av överensstämmelse som uppfyller de krav som anges i de europeiska ordningarna för cybersäkerhetscertifiering eller ytterligare krav enligt artikel 54.1 f bemyndigas av den nationella myndigheten för cybersäkerhetscertifiering att utföra uppgifter inom ramen för sådana ordningar.

Ett beslut om överlämnande av uppgifterna kan också återkallas om certifikat utfärdas i strid mot gällande föreskrifter eller om den fysiska eller juridiska person som anförtrotts uppgiften på annat sätt visar sig olämplig att fullgöra denna. Den nationella myndigheten för cybersäkerhetscertifiering som genom ett bemyndigande beslutar att överlämna en uppgift till ett organ för bedömning av överensstämmelse bör vara den myndighet som även återkallar sitt bemyndigande, t.ex. när ett organ för bedömning av överensstämmelse inte längre uppfyller de villkor som anges i en europeisk ordning för cybersäkerhetscertifiering eller ytterligare krav enligt artikel 54.1 f.

Av de ovan angivna bestämmelserna framgår att den nationella myndigheten för cybersäkerhetscertifiering får både utfärda bemyndiganden och återkalla sådana bemyndiganden när angivna förutsättningar föreligger. Bestämmelserna, som är direkt tillämpliga, behöver ingen kompletterande nationell reglering.

10.7 Anmälan av organ för bedömning av överensstämmelse som har ackrediterats

För varje europeisk ordning för cybersäkerhetscertifiering ska den nationella myndigheten för cybersäkerhetscertifiering enligt artikel 61 i EU:s cybersäkerhetsakt anmäla till kommissionen de organ för bedömning av överensstämmelse som har ackrediterats och, i tillämpliga fall, bemyndigats i enlighet med artikel 60.3 att utfärda europeiska cybersäkerhetscertifikat på angivna assuransnivåer enligt artikel 52. Myndigheten ska även, utan onödigt dröjsmål, anmäla till kommissionen eventuella ändringar. Kommissionen ska senast ett år efter ikraftträdandet av en europeisk ordning för cybersäkerhetscertifiering offentliggöra en förteckning över de organ för bedömning av överensstämmelse som har anmälts enligt den ordningen i Europeiska unionens officiella tidning.

Myndigheten får lämna in en begäran till kommissionen om att stryka ett organ för bedömning av överensstämmelse, som anmälts av den myndigheten, från förteckningen. Kommissionen ska då 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.

Kommissionen får anta genomförandeakter för att fastställa förutsättningar, format och förfaranden för anmälningar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.

Utredningen bedömer att det i denna del inte behövs någon kompletterande nationell reglering, utan det följer av EU:s cybersäkerhetsakt hur och av vem en anmälan till kommissionen ska göras.

11 Handläggning och rättsmedel

11.1 Inledning

I detta kapitel redogör utredningen till en början för grundläggande förvaltningsrättsliga bestämmelser och principer som kan bli aktuella vid svenska myndigheters handläggning av ärenden. Utredningen behandlar sedan vilka handläggningsregler som blir tillämpliga för berörda myndigheter i samband med ansökan om respektive utfärdande av cybersäkerhetscertifikat, i den nationella cybersäkerhetscertifieringsmyndighetens tillsynsverksamhet samt vid klagomål och när beslut fattats. Därefter utreds vad som gäller för ärendehandläggningen hos privata organ för bedömning. Utredningen drar fortlöpande slutsatser om behovet av kompletterande nationella förfaranderegler. Slutligen hanterar utredningen frågan om överklagande som ett effektivt rättsmedel.

Enligt utredningsdirektiven ska utredningen lämna förslag till författningsbestämmelser som kompletterar EU:s cybersäkerhetsakt och bl.a. analysera om det bör införas nationella bestämmelser om självbedömning av överensstämmelse och om organ för bedömning av överensstämmelse. Direktiven anger vidare att utredningen ska ta ställning till i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i EU:s cybersäkerhetsakt. Cybersäkerhetsakten innehåller nämligen regler om rätt för enskilda att ge in klagomål och skyldigheter för certifikatutfärdare och den nationella myndigheten för cybersäkerhetscertifiering att handlägga inkomna klagomål (artikel 63). Vidare ger cybersäkerhetsakten enskilda rätt till ett effektivt rättsmedel mot organet eller myndigheten som fattat ett beslut eller underlåtit att vidta åtgärder med anledning av ett klagomål (artikel 64).

Det europeiska ramverket för cybersäkerhetscertifiering innebär att IKT-tillverkare och -leverantörer får utfärda EU-försäkran om

överensstämmelse eller ansöka om cybersäkerhetscertifiering. Självbedömning av överensstämmelse görs hos tillverkaren eller leverantören medan ansökan om certifiering riktas till antingen en myndighet eller ett privaträttsligt organ för bedömning av överensstämmelse. I det sammanhanget uppkommer fråga om vilka bestämmelser som gäller vid hantering av en ansökan, framför allt om denna avser certifiering. Vidare kommer den nationella myndigheten för cybersäkerhetscertifiering att hantera ärenden inom ramen för sin tillsynsverksamhet, vilket också aktualiserar frågan om tillämpliga handläggningsregler.

11.2 Myndigheters ärendehandläggning

11.2.1 Regler i förvaltningslagen

Förvaltningslagens (2017:900) (FL) generella tillämpningsområde omfattar i princip all ärendehandling hos förvaltningsmyndigheterna. Vissa av lagens bestämmelser gäller också faktiskt handlande hos myndigheterna. Eftersom en ansökan om cybersäkerhetscertifikat hos den nationella myndigheten för cybersäkerhetscertifiering eller myndighetens tillsynsåtgärd i normalfallet innebär handläggningsåtgärd hos myndighet redogörs för tillämpliga bestämmelser i lagen.

Av 1 § FL framgår att den lagen gäller för handläggning av ärenden hos förvaltningsmyndigheter och därför blir lagen tillämplig i samband med den ärendehandläggning som följer av det europeiska ramverket för cybersäkerhetscertifiering eller den kompletterande nationella lagstiftningen.

Förvaltningsmyndighet avser de myndigheter vars uppgift är att sköta offentliga förvaltningsuppgifter. Utanför FL:s tillämpningsområde faller normalt sådana organ som formellt är organiserade i privaträttsliga former, t.ex. bolag.

Förfarandereglerna i FL gäller som huvudregel i alla ärenden, inte bara i ärenden som avser myndighetsutövning[1] mot enskild. Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från FL ska emellertid den bestämmelsen tillämpas (4 §). Det

[1] Myndighetsutövning avser situationer då myndigheter ensidigt fattar beslut eller vidtar andra åtgärder som ytterst utgör ett uttryck för samhällets makt över medborgarna och som får bestämda positiva eller negativa rättsverkningar för enskilda (jfr prop. 2016/17:180 s. 47 ff.). Begreppet har emellertid utmönstrats ur FL.

kan här noteras att regler om handläggning vid t.ex. ansökan om cybersäkerhetscertifikat finns i EU:s cybersäkerhetsakt och kan antas finnas i framtida europeiska ordningar för cybersäkerhetscertifiering.

Till skillnad från annan förvaltningsverksamhet, dvs. det som vanligen brukar betecknas som faktiskt handlande, avslutas ärendehandläggningen med ett beslut av något slag. Ett beslut innefattar regelmässigt ett uttalande från en myndighet som är avsett att ha vissa verkningar för den som beslutet är riktat mot.[2] Faktiskt handlande karaktäriseras i stället av att myndigheten i praktiken vidtar en viss faktisk åtgärd. Uttrycket handläggning innefattar alla åtgärder som en myndighet vidtar från det att ett ärende inleds till dess att det avslutas. Såväl utomstående som myndigheten själv kan ta initiativ till att ett sådant förfarande inleds.[3] När ett ärende väl inletts är myndigheten skyldig att göra någon form av prövning av den fråga som aktualiseras (se prop. 2016/17:180 s. 23 f.).

Svensk förvaltningsrätt kräver en effektiv handläggning i förhållande till enskilda som innebär att förvaltningsärenden ska avgöras utan oskälig fördröjning. Myndigheterna är skyldiga att handlägga ärendena så enkelt, snabbt och kostnadseffektivt som möjligt utan att rättssäkerheten eftersätts. Det ska vidare finnas tillräcklig möjlighet för enskilda att vidta effektiva rättsliga åtgärder mot långsam handläggning (se prop. 2016/17:180 s. 105 ff. och 9 § FL).

Det finns också en allmän serviceskyldighet för myndigheter som kommer till uttryck i 6 § FL. Enligt bestämmelsen ska en myndighet se till att kontakterna med enskilda blir smidiga och enkla. Kraven på smidighet och enkelhet avser den enskildes rätt till ett positivt bemötande från myndighetens sida. Kravet på enkelhet innebär också att den enskilde inte behöver ha någon särskild sakkunskap innan denne kontaktar en myndighet i en viss fråga. Myndigheten ska även lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Den ska vidare ges utan onödigt dröjsmål.

[2] När en myndighet lämnar upplysningar och råd med stöd av den allmänna bestämmelsen som serviceskyldighet i 6 § FL ger myndighetens besked dock inte uttryck för beslut i förvaltningsrättslig mening, även om informationen kan påverka mottagarens handlande.
[3] En enskild kan inleda ett ärende hos en myndighet genom en ansökan, anmälan eller annan framställning (19 §). Myndigheters möjligheter att på eget initiativ ta upp ärenden till behandling eller att inleda ett ärende hos en annan myndighet är inte reglerade i FL.

Av allmänna förvaltningsrättsliga principer som intagits i svensk lag följer att i princip vem som helst kan göra en framställning till en myndighet, som då är skyldig att behandla den. En myndighet är enligt FL och inom ramen för sin allmänna serviceskyldighet skyldig att lämna enskilda råd och bl.a. hjälpa den enskilde till rätta med en ofullständig framställning och hur man gör en ansökan och vidarebefordra felsända handlingar till rätt myndighet.[4] Myndigheten anses vidare vara skyldig att informera om handläggningen och resultatet av en framställning som gjorts och vid behov samverka med andra myndigheter. En myndighet som får in en framställning från en enskild anses också vara skyldig att lämna någon form av svar som inte får dröja längre än nödvändigt (prop. 1985/86:80 s. 59 och prop. 2016/17:180 s. 66 f.).

Enligt 8 § FL ska en myndighet inom sitt verksamhetsområde samverka med andra myndigheter. Syftet är att samverkan mellan myndigheter ska leda till att förvaltningen generellt ska bli så enhetlig och effektiv som möjligt, men bestämmelsen utgör också ett led i regleringen av myndigheternas serviceskyldighet gentemot allmänheten och underlättar enskildas kontakter med myndigheterna.

Krav på handläggningen av ärenden enligt FL inbegriper bl.a. rätt till partsinsyn (10 §), en huvudregel om kommunikationsskyldighet (25 §), dokumentation (27 och 31 §§), motiveringsskyldighet (32 §) samt underrättelse om beslut och överklagandemöjlighet (33 och 34 §§). En myndighet har vidare ett ansvar att se till att ärendet blir utrett i den omfattning som dess beskaffenhet kräver (23 §).

Myndigheter har för övrigt befogenhet och skyldighet att enligt 37–39 §§ FL ändra egna beslut, t.ex. på grund av att uppenbar felaktighet uppkommit till följd av förbiseende (rättelse) eller då det framkommit nya relevanta omständigheter i ärendet.[5] Genom denna möjlighet kan ett onödigt överklagande i vissa fall undvikas. En myndighet får även ändra ett beslut som överklagats om vissa förutsättningar är uppfyllda.

[4] För övrigt rymmer den allmänna serviceskyldigheten inom svensk förvaltningsrätt att en myndighet ska tillhandahålla de formulär och blanketter som behövs för verksamheten, t.ex. för att underlätta inlämningen av klagomål.

[5] Det förfarande som beskrivs som ändring av beslut beskrevs i den förra förvaltningslagen som omprövning.

11.2.2 Ärendehandläggning hos nationella myndigheter

Bedömning: I den mån det europeiska ramverket för cybersäkerhetscertifiering inte innehåller avvikande bestämmelser är förvaltningslagen (2017:900) tillämplig på berörda myndighets handläggning av ärenden. Det behövs inga kompletterande nationella regler om ärendehandläggningen hos myndigheterna.

Utredningen behandlar i denna del behovet av kompletterande nationella bestämmelser vid handläggningen av ärenden enligt det europeiska ramverket för cybersäkerhetscertifiering.

Förhållandet mellan det europeiska ramverket för cybersäkerhetscertifiering och förvaltningslagen

Ett ärende om ansökan av cybersäkerhetscertifikat kan ha stor betydelse för den sökande och röra rättigheter och skyldigheter för enskild. Utredningen bedömer att ärenden vid en myndighet som avser ansökan om utfärdande av ett europeiskt cybersäkerhetscertifikat med stöd av EU:s cybersäkerhetsakt och antagna europeiska ordningar för cybersäkerhetscertifiering i första hand ska handläggas och prövas enligt de bestämmelser som följer av dessa författningar. FL är subsidiär i förhållande till denna unionsrätt (se 4 §). I de fall det europeiska ramverket för cybersäkerhetscertifiering inte reglerar en viss fråga bör emellertid nationella handläggningsbestämmelser tillämpas.

Utredningen kan notera att EU:s cybersäkerhetsakt inte innehåller några uttryckliga regler om handläggning av t.ex. ansökan om certifikat. Mot denna bakgrund och i avsaknad av annan reglering, eftersom någon europeisk ordning för cybersäkerhetscertifiering ännu inte fastställts, föreligger osäkerhet i vilken mån någon kompletterande nationell reglering behövs på området. Som ovan anges gäller emellertid FL subsidiärt och bör därför tillämpas när annan reglering inte finns i fråga om berörda myndigheters hantering av ansökningar om cybersäkerhetscertifiering.

Det innebär således att FL kompletterar de handläggningsregler som kan återfinnas i det euroepiska ramverket för cybersäkerhetscertifiering, bl.a. vid handläggning hos den nationella myndigheten för cybersäkerhetscertifiering och dess certifieringsorgan. FL gäller

på motsvarande sätt även för andra offentliga organ för bedömning av överensstämmelse som bemyndigats enligt EU:s cybersäkerhetsakt att utfärda certifikat (jfr artikel 56.5 b och 56.6). Det kan noteras att organen för bedömning av överensstämmelse visserligen har att tillämpa standarder som innehåller vissa handläggningsförfaranden, men FL är inte subsidiär i förhållande till dessa (se 4 § FL) så länge detta inte särskilt anges i författning. Inte heller bedöms dessa organs interna förfarandedokument äga företräde framför FL. Den nationella myndigheten för cybersäkerhetscertifiering och offentliga organ för bedömning av överensstämmelse ska alltså följa FL:s regler i samband med att de tar emot en ansökan om cybersäkerhetscertifiering så länge inga avvikande förfaranderegler införts genom det europeiska ramverket för cybersäkerhetscertifiering.

Utredningen bedömer att det inte föreligger behov av kompletterande nationella bestämmelser om handläggningen av ärenden hos den nationella myndigheten för cybersäkerhetscertifiering eller ett offentligt organ för bedömning av överensstämmelse.

För det fall en nationell myndighet har till uppgift att tillverka eller leverera en IKT-produkt, -tjänst eller -process som omfattas av det europeiska ramverket för cybersäkerhetscertifiering, och fråga uppkommer om självbedömning av överensstämmelse, blir FL:s subsidiärt gällande handläggningsregler tillämpliga i myndigheten verksamhet. Utredningen bedömer att det inte heller i dessa fall finns behov av kompletterande nationell reglering.

Vad som anförts ovan i fråga om handläggningsregler gäller också vid den nationella cybersäkerhetscertifieringsmyndighetens tillsyn.

Den nationella myndigheten för cybersäkerhetscertifiering bör dock vid behov kunna meddela kompletterande verkställighetsföreskrifter om t.ex. vad en ansökan ska omfatta och vad som i övrigt ska gälla för handläggningen och prövningen av ett sådant ärende. Myndigheten bör även bemyndigas att meddela de föreskrifter som behövs för motsvarande handläggning av ansökan hos ett offentligt organ för bedömning av överensstämmelse som utfärdar ett europeiskt cybersäkerhetscertifikat enligt artiklarna 56.4, 56.5 b, 56.6 eller 60.3 (se nedan).

Frågan om vilka regler för handläggning som bör gälla i samband med klagomål enligt artiklarna 58.7 f och 63 behandlas i avsnitt 11.5.

11.3 Ärendehandläggning hos privata organ för bedömning av överensstämmelse

Förslag: Finner ett privaträttsligt 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.

Bedömning: Det finns för närvarande inte skäl att införa en bestämmelse om att förvaltningslagen (2017:900) ska vara tillämplig på privata ackrediterade organ för bedömningen av överensstämmelse när ett sådant organ handlägger ett ärende enligt EU:s cybersäkerhetsakt eller den nya kompletterande lagen.

Handläggning av ärenden

Utredningens analys och överväganden om behov av kompletterande föreskrifter för överlämnande av uppgiften att utfärda certifikat till ett organ för bedömning av överensstämmelse redogörs för i avsnitt 10.6.

I frågan om vilka regler som bör gälla för handläggningen av en ansökan om utfärdande av certifikat hos ett privat organ för bedömning av överensstämmelse, samt behovet av omprövning av sådana beslut, gör utredningen följande överväganden.

När de privata organen utför bedömning av överensstämmelse enligt det europeiska ramverket för cybersäkerhetscertifiering fattar de beslut som rör enskildas rättigheter och skyldigheter. T.ex. innefattar organens beviljande av eller avslag på ansökan om cybersäkerhetscertifiering myndighetsutövning.

Utgångspunkten är att det är fråga om privaträttsliga subjekt, huvudsakligen i form av juridiska personer som t.ex. ett aktiebolag. I likhet med vad som konstaterats i föregående avsnitt bör i första hand unionsrättsliga författningar[6] som reglerar frågor om organens ärendehandläggning, dvs. de regler som anges i det europeiska ramverket för cybersäkerhetscertifiering och som är tillämpliga på organen

[6] Såsom EU:s cybersäkerhetsakt (t.ex. skyldigheten i artikel 63.2 att underrätta klaganden om förfarandets fortskridande) och europeiska ordningar för cybersäkerhetscertifiering.

(se avsnitt 11.5 för en närmare redogörelse av klagomålshanteringen). Då de privata organen för bedömning av överensstämmelse inte utgör myndigheter i förvaltningslagens mening – även om de anförtrotts offentliga förvaltningsuppgifter som innefattar myndighetsutövning – är den lagen dock inte tillämplig på organens handläggning av ärenden. Däremot är lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter tillämplig. I denna lag – som gäller subsidiärt – regleras främst hur beslut överklagas, överklagandetiden, rättidsprövning och avvisning av för sent inkomna överklaganden. Därutöver bör det finnas förfaranden för ärendehantering på grundval av tillämplig standard för ackrediteringen och övriga standarder som tillämpas.

Det kan noteras att privata organ för bedömning av överensstämmelse inte har någon formell allmän serviceskyldighet som följer av förvaltningslagen. Samtidigt bör utgångspunkten för dessa organs verksamhet vara att iaktta motsvarande serviceskyldighet i sin verksamhet, även om det inte finns någon formell skyldighet i detta avseende. Detta särskilt mot bakgrund av att det är fråga om nya författningsbestämmelser på ett i vissa avseenden mycket komplext sakområde och att det är frågan om en överlämnad förvaltningsuppgift som i vissa fall även innefattar myndighetsutövning.

När offentliga förvaltningsuppgifter som innefattar myndighetsutövning överlämnas åt privaträttsliga organ brukar det i allmänhet anges i en särskild författning att vissa av FL:s bestämmelser ska tillämpas vid handläggningen av ärenden. De allmänna förvaltningsrättsliga principer som gäller för myndigheternas handläggning är bara i begränsad utsträckning direkt tillämpliga i de privaträttsliga organens verksamhet. Några exempel är dock principerna om legalitet, objektivet och saklighet som har sin grund i regeringsformen (1 kap. 1 och 9 §§ RF). Många av de specialförfattningar som avser privaträttsliga organs ärendehandläggning innehåller regleringar som avviker från vad som gäller enligt FL. Avvikande reglering finns t.ex. när det gäller handläggningstiden och verkställighet av beslut (se prop. 2017/18:235 s. 124 ff.).

Det kan i och för sig framstå som naturligt och konsekvent att samma krav på rättssäkerhet vid handläggningen av förvaltningsärenden upprätthålls oberoende av om uppgiften utförs av en myndighet eller överlämnats för att fullgöras av ett privaträttsligt organ. Tidigare utredningar har emellertid bedömt att det inte finns tillräck-

liga belägg för en ordning helt grundad på FL med samma förfaranderegler för privaträttsliga organ (se bl.a. prop. 2016/17:180 s. 27). FL:s bestämmelser är utformade på ett sätt som inte alltid lämpar sig att tillämpas av privaträttsliga organ. Om det för handläggningen av en viss förvaltningsuppgift finns ett särskilt framträdande behov av att säkerställa att lagens förfaranderegler följs, bör detta kunna ske genom särskilda föreskrifter som meddelas för den verksamheten (se prop. 2016/17:180 s. 27).

I propositionen *Följdändringar till ny förvaltningslag* (2017/18:235) bedömde regeringen att hänvisningar till andra bestämmelser i FL än bestämmelserna om utredningsansvaret i 23 § och om dokumentation av beslut i 31 § inte borde göras i uppräkningar som avser privaträttsliga organs ärendehandläggning. När det gäller bestämmelsen om utredningsansvaret konstaterade regeringen att det fick förutsättas att privaträttsliga organ redan vid sin ärendehandläggning utredde ärenden som rörde enskilda i den utsträckning som krävdes. Därför ansågs det både lämpligt och rimligt att de privaträttsliga organen skulle vara skyldiga att följa FL:s bestämmelser om utredningsansvaret. Med hänsyn till rättssäkerhetens krav framstod det enligt regeringen också som angeläget att skyldigheten att dokumentera skriftliga beslut skulle gälla för de privaträttsliga organen på samma sätt som för myndigheterna.[7]

I lagrådsremissen *En anpassning av bestämmelser om kontroll i livsmedelskedjan till EU:s nya kontrollförordning*[8] anges att vissa bestämmelser i FL bör tillämpas när ett organ med delegerade uppgifter, eller en fysisk person som har delegerats uppgifter, utför offentlig kontroll eller annan offentlig verksamhet. För att en överprövande instans ska kunna ta ställning till om ett överklagat beslut är korrekt och för att enskilda ska kunna ta till vara sin möjlighet att överklaga ett beslut bör vissa bestämmelser i FL tillämpas. Det gäller att ett beslut ska vara motiverat (32 §), att den enskilde ska underrättas om beslutet (33 §) och hur ett överklagande går till (34 §). Vidare anges att bestämmelserna om legalitet, objektivitet och proportionalitet (5 §), partsinsyn (10 §), jäv (16–18 §§), utredningsansvar (23 §), när

[7] I t.ex. växtskyddslagen (1972:318) föreskrivs att enskilda kontrollorgan ska tillämpa flera av förvaltningslagens bestämmelser (11 a §). Jfr även 7 kap. 10 § lagen om offentliga uppköpserbjudanden på aktiemarknaden där ett organ med representativa företrädare för näringslivet som utför förvaltningsuppgifter ska tillämpa ett tiotal bestämmelser i förvaltningslagen.

[8] Europaparlamentets och rådets förordning (EU) 2017/625 om offentlig kontroll och annan offentlig verksamhet för att säkerställa tillämpningen av livsmedels- och foderlagstiftningen och av bestämmelser om djurs hälsa och djurskydd, växtskydd och växtskyddsmedel.

man får lämna uppgifter muntligt (24 §), kommunikation (25 §), dokumentation av uppgifter (27 §), dokumentation av beslut (31 §), rättelse av skrivfel och liknande (36 §), samt vem som får överklaga ett beslut (42 §) bör tillämpas.

Utredningen har övervägt om det finns behov av att införa dessa bestämmelser i FL i den nya lagen för de privata kontrollorganens ärendehandläggning. Den lagrådsremiss som hänvisas till ovan avser livsmedelskontroll genom privaträttsliga kontrollorgan på uppdrag av bl.a. Livsmedelsverket. Även om det finns likheter med detta och det nu aktuella området föreligger också skillnader, bl.a. ska det ackrediterade organet för bedömning av överensstämmelse som verkar i enlighet med EU:s cybersäkerhetsakt följa regler om handläggning enligt vad som anges i internationella standarder. Vidare är cybersäkerhetscertifieringen frivillig eller obligatorisk och kontrollorganen verkar på en konkurrensutsatt marknad

Med hänsyn till att det redan finns en viss ordning för ärendehandläggning genom det europeiska ramverket för cybersäkerhetscertifiering och standarder som ackrediterade organ för bedömning av överensstämmelse ska tillämpa,[9] samt då en författningsreglering av privaträttsliga organs ärendehandläggning utifrån FL ska vara motiverad av ett särskilt framträdande behov, bedömer utredningen att det för närvarande inte föreligger tillräckligt starka skäl att, utöver en omprövningsskyldighet (se nedan), föreslå en ordning med formaliserade regler för handläggningen hos de privata kontrollorganen. Till detta kommer att det finns möjlighet att vända sig till den nationella myndigheten för cybersäkerhetscertifiering för tillsynsåtgärder avseende certifieringen och klaga på fattade beslut (se nedan). Samtidigt vill utredningen framhålla att frågan om ytterligare reglering av ärendehandläggningen hos de privata kontrollorganen bör övervägas när ytterligare erfarenheter erhållits av cybersäkerhetsaktens tillämpning.

[9] För övrigt gäller förvaltningslagen för CSEC och andra offentliga organ för bedömning av överensstämmelse.

Omprövning

Ett privat organ för bedömning av överensstämmelse bör ha en motsvarande ärendehantering och ett klagomålsförfarande som gäller för ett offentligt organ för bedömning av överensstämmelse och som grundas på bl.a. tillämplig standard för ackreditering av sådana organ.[10]

I detta sammanhang kan noteras att när det gäller möjlighet till omprövning har FMV/CSEC inrättat ett sådant internt förfarande.[11] Det kan noteras att den verksamheten i stor utsträckning grundas på de internationella arrangemangen CCRA respektive SOG-IS MRA samt att denna handläggningsordning kan komma att behöva anpassas efter de europeiska ordningar för cybersäkerhetscertifiering som införs.

Det kan i detta sammanhang noteras att det i t.ex. fordonslagen (2002:574) finns en regel om att ackrediterade besiktningsorgan ska vidta omprövning i vissa fall. Besiktningsorganen är även skyldiga att rapportera betydelsefulla iakttagelser till föreskrivande myndigheter. Utöver detta föreskriver lagen inget om besiktningsorganens ärendehandläggning. Lagrådet yttrade i prop. 2001/02:130 (s. 189) att det särskilt kunde övervägas huruvida den ordning för omprövning efter klagomål som AB Svensk Bilprovning iakttog borde regleras i författning. Bolaget använde nämligen som kvalitetssystem standarden ISO 17020 (tidigare EN45004) som angav möjligheten till omprövning av resultatet av t.ex. en kontrollbesiktning. Regeringen hänvisade till detta kvalitetssystem och framhöll att behovet av andra regler om ärendehandläggning än sådana som angav vad som skulle kontrolleras var relativt litet. I den efterföljande propositionen 2009/10:32 befarade regeringen emellertid att det inte var möjligt att under den då gällande ordningen ha uppsikt över att besiktningsorganen verkligen tillämpade godtagbara omprövningsmöjligheter, bl.a. då systemet skulle fungera för många olika aktörer och ISO-standardens regler-

[10] Skyldigheten för organ för bedömning av överensstämmelse (inbegripet testlaboratorier) att inrätta ett klagomålsförfarande är ett vanligt inslag i standarder som används för ackreditering (t.ex. EN-ISO/IEC 17065, EN-ISO/IEC 17021-1 och EN-ISO/IEC 7025). Jfr även p. 19 i bilagan till EU:s cybersäkerhetsakt. Se även den nederländska regeringens utkast till förklaring av lagen om genomförande av cybersäkerhetsakten (MvT Uitvoeringswet Cyberbeveiligingsverordening), s. 10, 2020-05-01. Motsvarande notering har gjorts av det nederländska Ministeriet för Ekonomi och Klimatpolitik i sina överväganden till förslaget till ny nationell lag om genomförandet av EU:s cybersäkerhetsakt, samtidigt som man finner att civilrätt gäller för bedömningsorganens hantering av klagomål. Någon författningsreglering av klagomålsförfarandet vid organen för bedömning av överensstämmelse föreslogs därför inte.

[11] Till en början dokumenterar och utreder certifieringsorganet alla klagomål mot dess certifieringsaktiviteter.

ing av omprövningsmöjligheten var ganska vag och övergripande till sin karaktär (s. 73). Man ansåg därför att det fanns ett starkt behov av att författningsreglera en omprövningsskyldighet, utformad med ledning av förvaltningslagen.

Mot den bakgrunden, och då ärenden avseende cybersäkerhetscertifiering är av mycket teknisk karaktär, får behovet, som ovan framgår, av formella regler om ärendehandläggningen i dessa fall minska (jfr prop. 2001/02:130 s. 93). Det finns dock skäl att i författning reglera de ackrediterade bedömningsorganens skyldighet att ompröva ett tidigare beslut i ett certifieringsärende. En enskild bör därför ges möjlighet att i första hand få organen för bedömning av överensstämmelse att ompröva beslutet. Den regel om omprövningsskyldighet som behövs kan lämpligen utformas med ledning av den generella regeln om omprövningsskyldighet som finns i förvaltningslagen. Enligt 38 § i den lagen ska en myndighet ändra ett beslut som den har meddelat som första instans om den 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 beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild part.[12]

11.4 Effektiva rättsmedel

11.4.1 Inledning

Enligt artikel 63.1 i EU:s cybersäkerhetsakt ska fysiska och juridiska personer ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller till den berörda nationella myndigheten för cybersäkerhetscertifiering. Myndigheten eller organet till vilket klagomålet lämnats in ska underrätta den klagande om hur förfarandet fortskrider och beslut som fattas (se artiklarna 58.7 f och 63.2). Vidare ska klaganden informeras om sin rätt till effektiva rättsmedel enligt artikel 64.

[12] Skyldigheten för en myndighet att ändra ett beslut gäller inte om det föreligger särskilda skäl mot det, t.ex. då en myndighet kommer fram till att ett överklagat beslut är oriktigt bara på en av flera punkter och att den punkten är mindre betydelsefull i sammanhanget. Det förhållandet att bara väsentliga oriktigheter behöver beaktas innebär att myndigheterna ges stöd för att avstå från att besluta om ändring i dessa fall (se prop. 1985/86:80 s. 79 och prop. 2016/17:180 s. 236).

Enskilda ska enligt artikel 64 ha rätt till ett effektivt rättsmedel inför behörig nationell domstol mot den myndighet eller det organ som nämnts ovan och som fattat ett beslut, samt när det gäller underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till myndigheten eller organet.

Enligt utredningsdirektiven torde rätten till effektiva rättsmedel beträffande den nationella cybersäkerhetscertifieringsmyndighetens befogenheter i artikel 58.8 för svensk del bäst tillgodoses genom en rätt för enskilda att överklaga myndighetens tillsynsbeslut till allmän förvaltningsdomstol.

I direktiven anges att bestämmelserna i de ovanstående frågorna behöver bli föremål för närmare analys, bl.a. i vilken utsträckning det behövs kompletterande bestämmelser till rättsmedel för enskilda som regleras i EU:s cybersäkerhetsakt och vad avser utövandet av den nationella cybersäkerhetscertifieringsmyndighetens tillsynsbefogenheter.

Utredningen behandlar dessa frågor dels i ett avsnitt som rör frågan om klagomål, dels i ett avsnitt som behandlar frågan om överklagande av beslut.

11.4.2 Klagomål

Bedömning: Det behövs ingen särskild författningsreglering av certifieringsorganens handläggning av klagomål.

Enskildas rätt att enligt artikel 63.1 i EU:s cybersäkerhetsakt lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller den berörda nationella myndigheten för cybersäkerhetscertifiering kräver inga lagstiftningsåtgärder.

Det behövs inga särskilda författningsbestämmelser om hur den nationella myndigheten för cybersäkerhetscertifiering ska behandla klagomål.

Utredningen behandlar till en början frågan om det finns behov av kompletterande nationella bestämmelser till regleringen i EU:s cybersäkerhetsakt om rätten att lämna klagomål till berörda myndigheter och organ för bedömning av överensstämmelse. Därefter tar utredningen ställning till om det behövs särskild författningsreglering för handläggningen av inkomna klagomål.

Av artiklarna 58.7 f och 63.1 i EU:s cybersäkerhetsakt följer att 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 för behandling. Myndigheten ska då i lämplig utsträckning undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen. Klagomål ska i övriga fall lämnas till utfärdaren av ett europeiskt cybersäkerhetscertifikat. Även dessa organ för bedömning av överensstämmelse är skyldiga att handlägga inkomna klagomål (se artikel 63.2).

Utgångspunkter

Med klagomål avses vanligen missnöje som uttrycks av enskilda och som inte avser överklagande eller någon annan formellt reglerad åtgärd. Syftet med en klagomålsfunktion är dels att skapa tilltro, dels att säkerställa att det finns en fristående instans som den som anser sig vara utsatt för felaktig behandling kan vända sig till med klagomål. Klagomål lämnas vanligen till en tillsynsmyndighet. Att enskilda kan framföra klagomål till en tillsynsmyndighet är ägnat att öka förtroendet för och därmed legitimiteten i den verksamhet som tillsynen avser.

Utredningen anser att begreppet anmälan i och för sig i stället för klagomål i vissa fall tydligare skulle särskilja förfarandet från överklagande. I den fortsatta framställningen används emellertid begreppet klagomål då detta används i EU:s cybersäkerhetsakt, även om den som ger in klagomål beskrivs inte bara som ”den klagande” utan även som ”anmälaren”. Någon nyansskillnad mellan begreppen klagomål och anmälan är – såvitt kan förstås – dock inte avsedd. Med enskild förstås för övrigt fysisk eller juridisk person.

Rätten att ge in klagomål kan även ses som ett rättsmedel. Vad den enskilde kan uppnå genom att ge in ett klagomål skiljer sig från vad denne kan uppnå genom en domstolsprövning och kan inte jämställas med rätten att överklaga ett beslut fattat av berörd myndighet eller organ för bedömning av överensstämmelse. Artiklarna 58.7 f

och 63 i EU:s cybersäkerhetsakt bör därför inte ges någon annan innebörd än att en fysisk eller juridisk person ska tillförsäkras en rätt att framföra klagomål till, i tillämpliga fall, den nationella myndigheten för cybersäkerhetscertifiering eller utfärdaren av ett europeiskt cybersäkerhetscertifikat.

Uppgiften för behöriga nationella myndigheter för cybersäkerhetscertifiering att enligt artikel 58.7 f ”behandla” relevanta klagomål inbegriper, som berörts ovan, viss handläggning. Denna handläggningsskyldighet beskrivs alltså något mer preciserat än klagomålshanteringen enligt artikel 63.2. I avsnitt 14.2.2 nedan redogör utredningen för relevanta nationella bestämmelser om handläggning av klagomål.

Det kan noteras att de europeiska ordningarna för cybersäkerhetscertifiering också kan antas behandla frågor om hantering av klagomål. T.ex. förskriver den föreslagna EUCC-ordningen att övervakning av överensstämmelse mellan en IKT-tillverkares eller leverantörs ansökan och kraven i aktuellt cybersäkerhetscertifikat ska ske bl.a. genom möjligheten att hantera klagomål. Vidare anger ordningen att underlåtenhet att fullgöra skyldigheterna enligt EU:s cybersäkerhetsakt att hantera av klagomål kan medföra en avvikelse från gällande reglering (se s. 39 i utkastet till EUCC). Dessutom ska noteras att mekanismen för inbördes granskning bl.a. ska utbyta bästa praxis om hanteringen av klagomål (se kapitel 13).

Närmare om gällande reglering

Som framgår ovan gäller FL för myndigheternas handläggning av ärenden, inbegripet klagomålsärenden, i den mån det europeiska ramverket inte reglerar frågan. När det gäller klagomålshantering kan konstateras att EU:s cybersäkerhetsakt innehåller handläggningsregler som ska följas av såväl den nationella myndigheten för cybersäkerhetscertifiering som offentliga och privata organ för bedömning av överensstämmelse. Dessutom torde ytterligare sådana förfaranderegler kunna tillkomma inom det europeiska ramverket för cybersäkerhetscertifiering. Vidare kan noteras att handläggningsförfarandet enligt cybersäkerhetsakten uppvisar flera likheter med FL i fråga om utredningsansvar, skyndsamhetskrav och underrättelseskyldighet (jfr artiklarna 58.7 f och 63.2).

Den nationella myndigheten för cybersäkerhetscertifiering har alltså inte någon skyldighet grundat på klagomålet att vidta tillsynsåtgärder eller att alltid närmare undersöka sakförhållandena. Tvärtom har tillsynsmyndigheten enligt cybersäkerhetsakten, precis som enligt svensk tillsynstradition, ett tydligt utrymme att själv avgöra vilka tillsynsärenden som ska drivas och på vilket sätt det ska ske. Det framgår inte heller uttryckligen av cybersäkerhetsakten att tillsynsmyndigheten måste fatta ett formellt beslut i varje klagomåls- eller tillsynsärende.

Följaktligen finner utredningen ingen anledning att föreslå kompletterande bestämmelser om myndigheternas klagomålshantering.

En skillnad är emellertid att en tillsynsmyndighets beslut att inte vidta någon åtgärd med anledning av ett klagomål inte är överklagbart enligt svensk rättspraxis (RÅ 2010:29), medan cybersäkerhetsakten ger 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.

Även om FL inte är tillämplig på de privata kontrollorganens handläggning av ansökningar om utfärdande av cybersäkerhetscertifikat och andra ärenden skiljer sig dessa organs praktiska hantering av klagomål dock inte i någon större utsträckning från vad som bör gälla för en myndighet. EU:s cybersäkerhetsakt nämner emellertid inte rätten till omprövning uttryckligen.

Det ska samtidigt noteras att ett klagomål för rättelse av ett organs beslut i fråga om certifikat kan röra enskildas rättigheter och skyldigheter och därför myndighetsutövning. Lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter blir därför tillämplig (se avsnitt 11.4.3).

Vidare ger rätten till klagomål enligt artikel 63 i EU:s cybersäkerhetsakt möjligheten att genom en anmälan uppmärksamma den nationella myndigheten för cybersäkerhetscertifiering på upplevda felaktigheter i handläggningen av en ansökan eller annat förfarande vid ett sådant organ, vilket ger en klagande möjlighet att få sitt klagomål prövat även som ett tillsynsärende vid den myndigheten. Dessa möjligheter får, sammantaget med den ovan föreslagna omprövningsskyldigheten,[13] anses utgöra tillräcklig reglering för att en klagande ska kunna tillvarata sin rätt.

[13] Det kan noteras att omprövning t.ex. kan komma i fråga efter klagomål.

Av artikel 64 i EU:s cybersäkerhetsakt ska enskilda ges rätt till effektiva rättsmedel inför domstol som kan inbegripa överklagande av beslut fattade av såväl en nationell myndighet som organ för bedömning av överensstämmelse, även i fråga om underlåtenhet att vidta åtgärder med anledning av ett klagomål. I viss utsträckning kan dock även en formell rätt till omprövning anses utgöra ett effektivt rättsmedel. Sammantaget bedömer utredningen att ytterligare förslag om reglering av klagomålshanteringen inte är motiverade.

11.4.3 Överklagande

Förslag: Beslut enligt EU:s cybersäkerhetsakt och motsvarande europeiska ordningar för cybersäkerhetscertifiering, den nya lagen eller föreskrifter som meddelats i anslutning till lagen ska kunna överklagas till allmän förvaltningsdomstol. Detta gäller även för beslut som fattas av privata organ för bedömning av överensstämmelse.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Rätt till överklagande enligt artikel 64.1

I artikel 64.1 i EU: cybersäkerhetsakt anges att enskilda ska ha rätt till effektiva rättsmedel avseende beslut som har fattats av en myndighet för cybersäkerhetscertifiering eller det organ för bedömning av överensstämmelse som avses i artikel 63.1 eller om myndigheten eller organet underlåter att vidta en åtgärd med anledning av ett klagomål enligt artikel 63.1. Som exempel på beslut anges beslut som innebär felaktigt utfärdande eller icke-utfärdande av europeiska cybersäkerhetscertifikat eller erkännande av ett sådant certifikat som innehas av fysiska eller juridiska personer.

Av artikel 64.2 framgår, i den svenska versionen av EU:s cybersäkerhetsakt, att förfaranden enligt artikeln ska inledas vid domstolarna i den medlemsstat där myndigheten eller organet som det rättsmedlen avser är beläget. I den engelska versionen uttrycks samma bestämmelse enligt följande: “Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the

authority or body against which the judicial remedy is sought is located."

Utredningen kan notera att innebörden av vad som anges skiljer sig åt på så sätt att enligt den svenska översättningen ska ett förfarande *inledas* vid domstolarna medan tolkningen av den engelska översättningen snarare ger vid handen att ett förfarande *ska väckas* vid en domstol. Den svenska översättningen ger således intryck av att ett överklagande *måste* inledas medan den engelska lydelsen kan tolkas som att en *talan ska ske vid en domstol*, dvs. ger utrymme för att ett beslut först kan överklagas till en myndighet och att den klagande sedan får överklaga den myndighetens beslut till en domstol i medlemsstaten. Utredningen anser att tolkningen av den engelska lydelsen är mer förenlig med vad som rimligen bör avses med innebörden av begreppet "rätt till effektiva rättsmedel" och lägger därför denna tolkning till grund för fortsatta överväganden om hur kravet på rätt till effektiva rättsmedel kan tillgodoses.

De beslut av en myndighet och organ för bedömning av överensstämmelse som – enligt utredningens bedömning – främst kan komma ifråga är beslut efter ansökan om att utfärda ett europeiskt cybersäkerhetscertifikat enligt artikel 56.4–6 eller att avslå en sådan ansökan, t.ex. på grund av att IKT-produkten inte bedöms möta kraven i det europeiska ramverket för cybersäkerhetscertifiering. Ett sådant beslut kan meddelas av antingen den nationella myndigheten för cybersäkerhetscertifiering eller ett offentligt eller privat organ för bedömning av överensstämmelse. Även beslut om vidmakthållande av ett sådant certifikat eller att återkalla certifikatet kan bli aktuellt. Även beslut av tillsynsmyndigheten om t.ex. föreläggande vid vite att vidta åtgärder eller om återkallelse av certifikat kan bli aktuella.

Frågan uppkommer om alla beslut som fattas av en myndighet eller av ett organ för bedömning av överensstämmelse bör kunna överklagas av den det berör och, i sådana fall, hur instansordningen bör utformas för att möta kraven i artikel 64 på effektiva rättsmedel.

I denna fråga gör utredningen följande övervägande.

I artikel 64.1 a EU:s cybersäkerhetsakt föreskrivs att fysiska och juridiska personer, utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol, ska ha rätt till effektiva rättsmedel avseende beslut som fattas av den myndighet eller det organ som avses i artikel 63.1, t.ex. när besluten avser ett

felaktigt utfärdande, icke-utfärdande eller erkännande av ett europeiskt cybersäkerhetscertifikat.[14] Motsvarande rätt gäller avseende underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till myndigheten eller organet (punkten b).

Utredningen konstaterar att artikel 64.1 b, till skillnad från punkten a, inte förutsätter att klagomålet rör beslut om europeiska cybersäkerhetscertifikat. Bestämmelsen kan sålunda tänkas omfatta klagomål rörande t.ex. EU-försäkringar om överensstämmelse.

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till en förvaltningsrätt som första instans. När det gäller beslut som fattas enligt en EU-förordning är utgångspunkten att rätten att överklaga följer av förvaltningslagen. Enligt FL tillkommer talerätt den som beslutet angår, om beslutet gått denne emot (se 41 och 42 §§). I praktiken innebär detta i normalfallet att det är den som beslutet riktas mot, t.ex. certifikatinnehavare eller den som ansöker om certifikat.[15]

Mot bakgrund av det angivna anser utredningen att myndighetsbeslut som rör utfärdande av EU-försäkran om överensstämmelse och europeiska cybersäkerhetscertifikat eller innehav av ett sådant certifikat ska kunna överklagas till allmän förvaltningsdomstol. FL är alltså tillämplig på överklagandeförfarandet. Ett överklagande av ett beslut ska därmed göras skriftligen till den högre instans som ska pröva överklagandet (överinstansen). Överklagandet ska dock ges in till den myndighet eller det organ som meddelat beslutet.

När det gäller frågan om i vilken utsträckning som beslut av den nationella myndigheten för cybersäkerhetscertifiering bör kunna överklagas gör utredningen följande överväganden.

I enlighet med artikel 58.8 i cybersäkerhetsakten ska de nationella myndigheterna för cybersäkerhetscertifiering kunna ålägga utfärdare av EU-försäkringar om överensstämmelse, utfärdare och innehavare av europeiska cybersäkerhetscertifikat samt organ för bedömning av överensstämmelse att lägga fram nödvändiga uppgifter, vidta undersökningsåtgärder för att kontrollera överensstämmelse med kraven i det europeiska ramverket för cybersäkerhetscertifiering samt kräva att överträdelser av regelverket omedelbart upphör. Med anledning

[14] Också beslut om t.ex. avvisning av eller avslag på klagomål bör omfattas.
[15] Det kan dock inte uteslutas att ett beslut skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om talerätt.

av detta föreslås i kapitel 8 att den nationella myndigheten för cybersäkerhetscertifiering ska kunna besluta om förelägganden och förbud, i förekommande fall i förening med vite, samt sanktionsavgift. En tillsynsmyndighets beslut om förelägganden, inbegripet beslut för att kunna fullgöra tillsynen, och sanktioner måste kunna överklagas. Sådana överklaganden ska ställas till allmän förvaltningsdomstol varvid tillsynsmyndigheten är motpart i domstolen.[16]

Även i övrigt följer av EU:s cybersäkerhetsakt att den nationella myndigheten för cybersäkerhetscertifiering ska fatta vissa beslut som måste kunna överklagas. Det rör t.ex. beslut enligt artikel 58.7 e att återkalla bemyndiganden för organ för bedömning av överensstämmelse och beslut enligt 58.8 e att återkalla vissa europeiska cybersäkerhetscertifikat.[17] För övrigt kan Swedacs beslut om ackreditering också överklagas hos allmän förvaltningsdomstol.

Som tidigare berörts är enligt svensk rättspraxis en tillsynsmyndighets beslut att inte vidta någon åtgärd med anledning av ett klagomål normalt inte överklagbart. Dock ska enskilda enligt EU:s cybersäkerhetsakt ha rätt till effektiva rättsmedel även avseende underlåtenhet att vidta åtgärd med anledning av ett klagomål.[18] Detta talar för att akten ger den enskilde en generell rätt att klaga på berörd myndighets underlåtelse med anledning av ett klagomål, även om en sådan underlåtelse normalt inte medför några rättsligt bindande följder för den som har lämnat in klagomålet.[19]

Utredningen har övervägt att i den nya lagen ange beslut som inte ska vara överklagbara. En sådan kartläggning utifrån det europeiska ramverket för cybersäkerhetscertifiering, och med beaktande av att ytterligare relevanta beslutsbefogenheter kan tillkomma genom de europeiska certifieringsordningarna, låter sig emellertid svårligen göras. Vad gäller frågan om hur underlåtenhet att handlägga klagomål enligt artikel 64 bör – enligt utredningens mening – denna överlämnas till rättstillämpningen att avgöra.

[16] Med hänsyn till erfarenheterna från andra områden där tillsynsmyndigheter får besluta om sanktionsavgift kan det förväntas att överklagande bara kommer att ske i begränsad omfattning.
[17] Vidare kan det nationella ackrediteringsorganet besluta att återkalla ackrediteringen av ett organ för bedömning av överensstämmelse.
[18] Artikel 64 kan alltså möjliggöra för enskilda att klaga på mottagarens underlåtenhet att vidta åtgärder med anledning av ingivet klagomål
[19] Något uttryckligt krav i cybersäkerhetsakten på att rätten enligt artikel 64.1 b till effektivt rättsmedel ska avse den som ett beslut rör framgår inte.

Inledningsvis kan det antas att överklagande sker i begränsad omfattning.[20] Även om det finns ett visst behov av specialisering för den som ska hantera dessa mål, framstår det som lämpligt att samma ordning som gäller för överklagande enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska gälla även enligt den nya lagen. De beslut som berörda myndigheter meddelar bör därför få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten (se 40 § förvaltningslagen [2017:900]). Kammarrättens avgörande ska inte kunna överklagas.

Formerna för överklagande av den nationella cybersäkerhetscertifieringsmyndighetens tillsynsbeslut, vilken överklagandefrist som ska gälla, vem som har talerätt m.m., bör i övrigt inte avvika från förvaltningslagens bestämmelser. Det finns därför inte skäl att föreslå några särskilda bestämmelser om detta. Av tydlighetsskäl kan dock framhållas att den nationella myndigheten för cybersäkerhetscertifiering har ställning som motpart i ett mål hos domstolen som gäller överklagande av tillsynsbeslut.

Det som ovan anförts om rätten till effektiva rättsmedel gäller även för beslut av privata organ för bedömning av överensstämmelse, dock med följande undantag. I stället för förvaltningslagen ska lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter tillämpas på överklagade beslut av de privata organen för bedömning av överensstämmelse (överklagandelagen). I lagen – som gäller subsidiärt och tillämpas på överklagade beslut av bolag och andra enskilda organ, som enligt särskilda bestämmelser får överklagas till bl.a. förvaltningsmyndighet – regleras hur beslut överklagas, överklagandetiden, rättidsprövning och avvisning av försent inkomna överklaganden. Av 2 § samma lag följer att ett överklagande ska ges in till det organ som ska pröva överklagandet.[21]

Det krävs emellertid uttryckligt författningsstöd för att ett beslut av ett privaträttsligt organ ska kunna överklagas. För att överklagandelagen ska bli tillämplig förutsätts därför att det finns särskilda bestämmelser som medger att det enskilda organets beslut överklagas

[20] Bl.a. med hänsyn till att användningen av europeisk cybersäkerhetscertifiering inom den närmsta tiden är frivillig.
[21] Denna myndighet ska pröva om överklagandet har kommit in i rätt tid. Överklagandetiden är tre veckor från den dag då klaganden fick del av beslutet.

till regeringen, till en förvaltningsdomstol eller till en förvaltningsmyndighet.

De uppgifter som kontrollorganen utför kan, som ovan berörts, utmynna i beslut som får verkningar för en enskild och därmed påverka dennes situation på ett inte obetydligt sätt. Sådana beslut är överklagningsbara enligt allmänna förvaltningsrättsliga principer (jfr 41 § förvaltningslagen och prop. 2016/17:180, s. 248 och 251 f.).

Mot denna bakgrund, och då samma argument som anförts ovan gör sig gällande även här, finner utredningen att det i den nya lagen bör införas en bestämmelse som anger att även beslut som fattas av privata organ för bedömning av överensstämmelse får överklagas till allmän förvaltningsdomstol.

Utredningen har övervägt behovet av en ordning med en s.k. överklagandemyndighet[22] som första instans. Också i det fallet gör sig behovet av kompetens och specialisering gällande. Den nationella myndigheten för cybersäkerhetscertifiering hade därmed kunnat komma i fråga som överklagandemyndighet. Utredningen anser att de föreslagna åtgärderna innebär tämligen generösa möjligheter till både omprövning och överklagande. Vidare ska en klagande, i tillämpliga fall, kunna vända sig till den nationella cybersäkerhetscertifieringsmyndigheten i fråga om tillsynsåtgärder. Sammantaget med målet att undvika onödig tidsutdräkt finner utredningen inte anledning att inrätta en instansordning med även en överklagandemyndighet.

[22] En myndighet – inte domstol – som ska pröva överklagandet.

12 Sekretess

Förslag: Det ska införas en bestämmelse om tystnadsplikt i den föreslagna lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt med innebörden 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.

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

Det ska införas en bestämmelse som upplyser om att den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Det ska även införas en bestämmelse i bilagan till offentlighets- och sekretessförordningen som medför att sekretess enligt 9 § offentlighets- och sekretessförordningen (2009:641) gäller uppgift om enskilds affärs- eller driftförhållanden i verksamhet vid FMV som består i utredning och tillsyn enligt EU:s cybersäkerhetsakt och lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

12.1 Inledning

Utredningen ska enligt utredningsdirektiven analysera om nuvarande sekretessbestämmelser för offentliga organ och bestämmelser om tystnadsplikt för privata aktörer behöver anpassas, eller ny lagstiftning föreslås, med anledning av regleringen i EU:s cybersäkerhetsakt om tystnadsplikt och konfidentialitet hos organen för bedömning av överensstämmelse.

I detta kapitel analyseras om bestämmelserna i offentlighets- och sekretesslagen (2009:400) (OSL) innebär ett tillräckligt skydd för de uppgifter som kan komma att lämnas till myndigheter samt offentliga eller privata organ för bedömning av överensstämmelse med anledning av det europeiska regelverket för cybersäkerhetscertifiering.

12.2 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 hos ett ackrediterat organ för bedömning av överensstämmelse.

När det gäller frågan om behov av reglering av sekretess och säkerhet i verksamhet som avser cybersäkerhetscertifiering kan noteras att 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 kan innebära extra cybersäkerhetsrisker eftersom sårbarheter i sådana tredjepartskomponenter även kan påverka IKT-produkternas, IKT-tjänsternas och IKT-processernas säkerhet.

Om sådana beroendeförhållanden identifieras, dokumenteras och offentliggörs kan det medföra ökade risker och skador för tillverkare och användare av IKT-produkter, IKT-tjänster och IKT-processer och negativt påverka riskhantering av cybersäkerhet, bl.a. genom att ge möjlighet till att påverka förfaranden för att hantera och avhjälpa sårbarheter.

Både en EU-försäkran och ett utfärdat europeiskt cybersäkerhetscertifikat grundas på bl.a. känslig information och uppgifter om den aktuella produktens, tjänstens eller processens konstruktion och funktionalitet Ofta finns därför ett berättigat behov av att informationen och uppgifterna skyddas av sekretess, bl.a. av konkurrens- och säkerhetsskäl. Tillverkare och leverantörer av IKT-produkter, IKT-tjänster och IKT-processer bör därför ges möjlighet att få ett fullgott sekretesskydd för känslig information kring produkterna, tjänsterna eller processerna som lämnas till den nationella myndigheten för cybersäkerhetscertifiering eller ett ackrediterat organ för

bedömning av överensstämmelse. Det är viktigt för att kunna säkerställa att dessa produkter, tjänster och processer skyddas i högsta möjliga grad, bl.a. för att motverka möjligheten till och förekomsten av cyberattacker. Möjligheten till sekretess bör finnas under IKT-produktens, IKT-tjänstens och IKT-processens hela livstid.

12.3 Allmänt om sekretess

I offentlighets- och sekretesslagen (2009:400) (OSL) regleras i stort sett all sekretess i det allmännas verksamhet. Sekretess innebär ett förbud att röja en uppgift, vare sig det sker genom utlämnande av en handling eller genom att röja uppgiften muntligen eller på annat sätt (3 kap. 1 § OSL).

Sekretessen innebär dels handlingssekretess, dels tystnadsplikt. Till den del sekretessen avser handlingssekretess innebär den en begränsning av enskilds rätt att få del av allmänna handlingar enligt 2 kap. tryckfrihetsförordningen. Till den del sekretessen avser tystnadsplikt innebär sekretessen en begränsning av yttrandefriheten i vissa angivna fall enligt regeringsformen och Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Förbudet mot att röja eller utnyttja en uppgift gäller för myndigheter och personer som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning, uppdrag, tjänsteplikt eller liknande grund (2 kap. 1 §).

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter och inom en myndighet, om det där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra. Sekretess gäller också i förhållande till utländska myndigheter och mellanfolkliga organisationer (8 kap. 1–3 §§ OSL). I vissa fall måste dock myndigheter kunna utbyta uppgifter för att kunna utföra sina uppgifter.[1] Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser.

En grundläggande princip i OSL är att sekretesskydd inte automatiskt följer med en uppgift som omfattas av sekretess när den

[1] Med myndighet avses ett organ inom den statliga och kommunala förvaltningen. Med myndighet jämställs i OSL också andra organ där det kan förekomma allmänna handlingar. Statliga aktiebolag, ekonomiska föreningar, stiftelser och andra privaträttsliga organ är dock bara skyldiga att tillämpa OSL om organet i fråga finns angivet i bilagan till den lagen och i sådana fall bara i den verksamhet som anges i bilagan (2 kap. 4 § OSL).

lämnas till en annan myndighet. Sekretess gäller för uppgiften hos den mottagande myndigheten endast om det följer av en s.k. primär sekretessbestämmelse som är tillämplig hos den mottagande myndigheten eller av en bestämmelse om överföring av sekretess (7 kap. 2 § OSL). Då den senare typen av bestämmelse bara kan tillämpas på uppgifter som en myndighet fått från en annan myndighet finns det inte någon sekretess enligt OSL som härvid kan överföras från enskilda.[2]

12.4 Uppgifter som lämnas till myndigheter

12.4.1 Uppgifter som kan behöva sekretesskydd

De fysiska och juridiska personer som ansöker om certifiering av sina IKT-produkter, -tjänster eller -processer har en skyldighet att göra alla uppgifter som är nödvändiga för cybersäkerhetscertifieringen tillgängliga för berört organ för bedömning av överensstämmelse (artiklarna 54.1 h och 56.7 i EU:s cybersäkerhetsakt). En inte obetydlig del av de uppgifter som därmed kommer att utbytas med stöd av EU:s cybersäkerhetsakt utgörs av uppgifter om ägarförhållanden och liknande. En tillverkare eller leverantör ska även enligt artikel 55 lämna kompletterande cybersäkerhetsinformation för sin certifierade IKT.

Vidare är innehavare av europeiska cybersäkerhetscertifikat enligt artikel 56.8 i EU:s cybersäkerhetsakt 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 – som även kan vara ett privat organ för bedömning av överensstämmelse – ska i sin tur överlämna mottagen information till den berörda nationella myndigheten för cybersäkerhetscertifiering.

Dessutom kommer enskilda, som utfärdare av EU-försäkringar om överensstämmelse, certifikatinnehavare och privata organ för bedömning av överensstämmelse, att behöva lämna uppgifter som är

[2] För övrigt kan det vara möjligt att överföra sekretess i flera led.

nödvändiga för den tillsyn som utförs av den nationella myndigheten för cybersäkerhetscertifiering enligt artikel 58.7 och 8.[3]

Följaktligen kommer både nationella myndigheter för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse att erhålla uppgifter om certifikatsökande, certifikatinnehavare och utfärdare av EU-försäkringar om överensstämmelse (IKT-tillverkare och -leverantörer). Också det nationella ackrediteringsorganet kommer att få uppgifter från organ som ansöker om ackreditering enligt cybersäkerhetsakten.

Till följd av skyldigheten att lämna uppgifter som rör utfärdande av EU-försäkran om överensstämmelse och europeiska cybersäkerhetscertifikat till den nationella myndigheten för cybersäkerhetscertifiering kommer skyddsvärda uppgifter från såväl tillverkare och leverantörer som organ för bedömning av överensstämmelse att finnas hos berörda myndigheter och kontrollorgan. Det kan t.ex. vara fråga om nyupptäckta cybersäkerhetssårbarheter i certifierad IKT som används i samhällsviktig verksamhet. Organen kommer även att förfoga över ytterligare information från enskilda vid utförandet av sin kontrollverksamhet, t.ex. avseende tester och underlag för provning samt certifieringsorganets bedömning av dessa underlag (se vidare avsnitt 12.4.2). När det gäller kompletterande cybersäkerhetsinformation som tillverkare och leverantörer ska lämna enligt artikel 55 (främst till slutanvändare) ska visserligen informationen tillgängliggöras elektroniskt. Samtidigt kan för sådana uppgifter finnas behov av sekretess. Det föreskrivna tillgängliggörandet torde inte innebära att all kompletterande cybersäkerhetsinformation måste offentliggöras.

I de fall IKT-produkter genomgår en s.k. sammansatt produktevaluering kan känslig information även komma att delas mellan involverade evalueringsföretag (jfr den föreslagna EUCC-ordningen som föreskriver ett strukturerat förfarande för hur en sådan informationsdelning ska ske).[4] Det är fråga om uppgifter som typiskt sett även kan vara av intresse för aktörens konkurrenter och som skulle

[3] Nationella myndigheter för cybersäkerhetscertifiering ska i sin tillsynsverksamhet kunna ta emot uppgifter direkt från enskilda. I avsnitt 12.6–7 behandlas sekretesskydd för uppgifter som den nationella myndigheten för cybersäkerhetscertifiering fått från andra myndigheter, såväl svenska som utländska. Också informationsutbyte med mellanfolkliga organisationer kommer att förekomma.

[4] Enisa ska tillhandahålla en mall för en teknisk rapport för sammansättning.

kunna skada dess verksamhet om de röjs. Fråga uppstår därmed om intresset av att uppgifterna omfattas av sekretess.

I följande avsnitt redogör utredningen för relevanta sekretessbestämmelser i unionsrätten och nationell rätt. Därefter tar utredningen ställning till om det finns behov av kompletterande nationell sekretessreglering.

12.4.2 Gällande sekretessreglering

Uppgifter som offentliga organ för bedömning av överensstämmelse får i sin certifieringsverksamhet

Krav på konfidentialitet och tystnadsplikt hos organ för bedömning av överensstämmelse i EU:s cybersäkerhetsakt

I punkten 16 i bilagan till EU:s cybersäkerhetsakt finns närmare bestämmelser om vad som ska gälla avseende sekretess hos organ för bedömning av överensstämmelse. I denna punkt anges att ett sådant organ som önskar bli ackrediterat ska bevara konfidentialitet och iaktta tystnadsplikt avseende all den information som organen[5] 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.[6] Det ställs även krav på att organ för bedömning av överensstämmelse ska ha dokumenterade förfaranden som möter kraven på konfidentialitet och tystnadsplikt.[7] Vidare anges att immateriella rättigheter ska skyddas.

Utredningen konstaterar att även offentliga organ för bedömning av överensstämmelse ska ackrediteras enligt EU:s cybersäkerhetsakt (se artiklarna 56.5 b och 60.1–2) och att kraven i nämnda bilaga därmed även gäller för det nationella certifieringsorganet (CSEC).

[5] Inbegripet organens personal, kommittéer, dotterbolag, underleverantörer och eventuella anslutna organ eller personal vid externa organ som ett organ för bedömning av överensstämmelse anlitar.
[6] Utredningen noterar att den engelska översättningen av sekretessbestämmelsen anger att organen ”shall maintain confidentiality” medan organen enligt den svenska översättningen ska ”underhålla” konfidentialitet.
[7] Förutom kraven i punkten 16 hindrar inget i bilagan utbyte av teknisk information och vägledning om gällande regler mellan organ för bedömning av överensstämmelse och en person som önskar certifieras. För övrigt anges i punkten 9 att om underleverantörer eller utomstående konsulter anlitas ska det finnas ett skriftligt avtal som reglerar sekretess och intressekonflikter.

Närmare om europeiska ordningar för cybersäkerhetscertifiering

En europeisk ordning för cybersäkerhetscertifiering kan innehålla föreskrifter om skydd för känslig information (jfr den föreslagna EUCC-ordningen). 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. I den föreslagna EUCC-ordningen föreskrivs att alla parter som är involverade i tillämpningen av ordningen ska respektera konfidentialiteten hos uppgifter som erhållits vid utförandet av aktuella uppgifter i syfte att skydda bl.a. enskildas affärshemligheter och immateriella rättigheter under IKT-produktens livscykel. Dessutom anges att personuppgifter ska skyddas i enlighet med GDPR[8].

Enligt den föreslagna EUCC-ordningen är vidare utgångspunkten att all information som mottagits från organen för bedömning av överensstämmelse (inbegripet både certifieringsorgan och tillhörande evalueringsföretag), tillverkarna eller leverantörerna ska användas endast för certifieringens syfte och anses vara konfidentiella av de nationella myndigheterna för cybersäkerhetscertifiering. Undantag från detta aktualiseras om annat avtal träffas eller om ett informationsflöde krävs på grund av en särskild reglering i den angivna europeiska ordningen.[9]

Sekretess i uppdragsverksamhet för enskilds räkning

Sekretess gäller för uppgift som avser provning, bestämning av egenskaper eller myckenhet, värdering, vetenskaplig, teknisk, ekonomisk eller statistisk undersökning eller annat sådant uppdrag som myndigheten utför för en enskilds räkning, om det måste antas att uppdraget har lämnats under förutsättning att uppgiften inte röjs (31 kap. 12 § OSL). Sekretessen gäller dock inte om intresset av allmän kännedom om förhållande som rör människors hälsa har sådan vikt att uppgiften bör lämnas ut.

[8] Denna skyldighet gäller till slutet av den angivna lagringstiden för all certifieringsinformation, såvida röjande inte är nödvändigt med hänsyn till det allmännas intresse eller följer av domstolsbeslut.
[9] Enisa kan ge vägledning om hur man kan säkerställa säkerheten för information baserad på arbetsflöden i samband med de aktiviteter som beskrivs i EUCC-ordningen.

Denna bestämmelse är tillämplig på information som ett offentligt certifieringsorgan får tillgång till under licensierings- och certifieringsuppdrag som utförs för enskilds räkning och där uppdraget lämnas till certifieringsorganet under förutsättning att informationen hålls hemlig.

Sekretessen gäller endast just uppgift som avser själva provningen, i praktiken uppgifter som ingår i de underlag (evidence) som ingår i evalueringen och som lämnas till certifieringsorganet, samt certifieringsorganets bedömning av dessa underlag. Sekretessen gäller alltså inte generellt för enskilds affärs- eller driftförhållanden[10].

Begäran om att uppgift ska hållas hemlig bör göras av den som lämnar uppgiften men en bedömning ska också göras internt inom certifieringsorganet. Skriftlig dokumentation och andra handlingar som tas fram inom certifieringsorganet ska bedömas utifrån denna aspekt och vid behov hanteras som sekretesskyddade handlingar.

Övrigt

Uppgifter om enskildas ekonomiska förhållanden kan i vissa fall behöva sekretesskydd (se nedan). Begreppet ekonomiska förhållanden innefattar bl.a. affärs- och driftförhållanden. Affärs- eller driftförhållanden inbegriper i sin tur uppgifter om förvärv, överlåtelser, upplåtelser eller användning av egendom, tjänster eller annat. Vidare omfattas bl.a. affärshemligheter av mera allmänt slag, marknadsundersökningar, marknadsplaneringar, prissättningskalkyler och planer rörande reklamkampanjer. Även förhandlingar och andra affärshändelser omfattas av begreppet.[11] Också uppgift om namnet på den som det begärs uppgifter om kan omfattas.

Begreppet har en vidsträckt betydelse och täcker i praktiken det som ligger inom ramen för en affärsverksamhet. Det handlar i första hand om uppgifter som typiskt sett kan vara av intresse för konkurrenter och som skulle kunna skada verksamheten om de blev kända.

Sekretess enligt 31 kap. 16 § OSL gäller för uppgift om en enskilds affärs- eller driftförhållanden när denne i annat fall än som av-

[10] Sekretess för sådana uppgifter finns i 30 kap. 23 och 27 §§ när det gäller skydd i verksamhet som avser tillsyn m.m. i fråga om näringslivet. 31 kap. OSL reglerar sekretess till skydd för enskild i annan verksamhet med anknytning till näringslivet, och 16 § avser affärsförbindelser med myndigheter (se nedan).

[11] Jfr prop. 2018/19:150 s. 70, prop. 1979/80:2 del A s. 145, HFD 2015 ref. 11 med där angivna hänvisningar.

ses i 31 kap. 1 § första stycket, 2–4 och 12 §§, har trätt i affärsförbindelse[12] med en myndighet, om det av särskild anledning kan antas att den enskilde lider skada om uppgiften röjs.

Denna bestämmelse är tillämplig för uppgifter som ett offentligt certifieringsorgan får tillgång till genom en affärsförbindelse. För certifieringsorganet gäller detta främst information som evalueringsföretag, sponsorer och utvecklare begär att certifieringsorganet ska hålla hemlig.

Certifieringsorganet ska bedöma om en inkommen eller en upprättad handling innehåller uppgifter som ska skyddas enligt denna bestämmelse och därmed hanteras som sekretessbelagd. På motsvarande sätt ska handlingar som tas fram inom certifieringsorganet bedömas utifrån denna aspekt och hanteras som sekretessreglerade om de anses innehålla uppgifter som skyddas av sekretess.

Skydd för uppgifter som lämnas vid upptäckt av sårbarheter och tillsyn

En myndighets verksamhet för inspektion, kontroll eller annan tillsyn[13]

Sekretess gäller för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjs (17 kap. 1 § OSL). Bestämmelsen är tillämplig på all information där validiteten av en granskning skulle påverkas om informationen var känd på förhand.

Sekretess gäller också för uppgift som ingår i eller utgör underlag för kunskapsprov eller psykologiskt prov under en myndighets överinseende, om det kan antas att syftet med provet motverkas om uppgiften röjs (17 kap. 4 § OSL). Denna bestämmelse är tillämplig för sådan information som tas fram inom certifieringsorganet och som avser tester och prov för att bedöma kunskapsnivå och tilldela status som evaluerare eller certifierare. Bestämmelsen är tillämplig på all information där validiteten av ett prov skulle påverkas om informatio-

[12] Uttrycket affärsförbindelser avser sådana transaktioner av ekonomisk natur som avses i 19 kap. 1 § och 3 § OSL.

[13] Det bör noteras att tillsynsbegreppet i OSL är vitt. Det omfattar i stort sett alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Den typ av uppgifter som det i första hand handlar om att sekretessbelägga med stöd av bestämmelsen är uppgifter som typiskt sett kan vara av intresse för konkurrenter och som skulle skada verksamheten om de blev kända.

nen var känd på förhand. Inom ramen för sin rapporteringsskyldighet enligt artikel 56.7 i EU:s cybersäkerhetsakt och den nationella cybersäkerhetscertifieringsmyndighetens tillsyn enligt artikel 58.8 kan bl.a. IKT-tillverkare och -leverantörer även behöva lämna uppgifter som rör deras ekonomiska verksamhet. Enligt 30 kap. 23 § första stycket 1 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 för uppgift om en enskilds affärs- eller driftförhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs. Bestämmelsen hade alltså kunnat vara tillämplig på tillsynsverksamheten vid den nationella myndigheten för cybersäkerhetscertifiering i förhållande till enskilda, om regeringen föreskriver det.

Regeringen har i 9 § offentlighets- och sekretessförordningen (2009:641) och i bilagan till förordningen meddelat föreskrifter om i vilken utsträckning sekretess enligt 30 kap. 23 § första stycket OSL gäller. I bilagan listas bl.a. planering och tillsyn hos FMV vid uppbyggnad och kontroll av företags säkerhetsskydd, utredning hos FMV för bedömning av företag inför framtida materielleveranser samt utredning, planering och stödverksamhet hos Försvarets materielverk med avseende på exportstödjande verksamhet (punkterna 91, 95, 132).

Försvarssekretess

Förutom ovan nämnda bestämmelser kan bl.a. bestämmelsen om försvarssekretess i 15 kap. 2 § OSL vara tillämplig i vissa situationer. Försvarssekretess kan exempelvis aktualiseras hos organen för bedömning av överensstämmelse och hos den nationella myndigheten för cybersäkerhetscertifiering. Försvarssekretess gäller 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. Berörd myndighet kan t.ex. komma att hantera uppgifter om sårbarheter som sammantaget ger en sådan bild av samhällets infrastruktur att det kan antas utgöra en sådan fara för Sveriges säkerhet om de röjs att försvarssekretess gäller.

12.4.3 Slutsatser

Utredningen konstaterar att det finns sekretessbestämmelser i OSL som kan aktualiseras i offentliga certifieringsorgans verksamhet. Ovan nämnda nationella bestämmelser är, i likhet med flertalet sekretessbestämmelser i OSL, försedda med s.k. raka skaderekvisit. Det innebär att utgångspunkten är att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. Om uppgiften typiskt sett måste betraktas som känslig omfattas den dock normalt av sekretess (och får då inte utan särskilt lagstöd lämnas ut eller röjas muntligen).

Enligt utredningen tillgodoser konstruktionen med ett rakt skaderekvisit i de relevanta sekretessbestämmelserna allmänhetens berättigade intresse av insyn i kontrollorganens och den nationella cybersäkerhetscertifieringsmyndighetens verksamhet, eftersom harmlösa uppgifter får lämnas ut. Samtidigt tillgodoser bestämmelserna tillverkares och leverantörers berättigade intresse av diskretion, eftersom uppgifter inte får röjas om det kan antas leda till skada.

Utredningen finner att punkten 16 i bilagan till EU:s cybersäkerhetsakt, i förening med 31 kap. 12 § OSL, är tillämplig på uppgifter som enskilda lämnar till offentliga certifieringsorgan i dess certifieringsverksamhet. Utredningen anser att bestämmelsen i 32 kap. 12 § OSL, med sitt raka skaderekvisit, ger ett väl avvägt skydd. Befintlig nationell sekretessreglering bedöms, sammantaget med kraven på konfidentialitet och tystnadsplikt i bilagan till EU:s cybersäkerhetsakt – som avser all information som erhållits vid utförandet av certifieringsuppgifterna, och enligt vilken absolut sekretess råder – säkerställa att uppgifter som organen får vid bedömningen av överensstämmelse enligt EU:s cybersäkerhetsakt inte obehörigen röjs. Eftersom det således får anses finnas ett fullgott sekretesskydd för uppgifter som samlas hos organen behövs i denna del ingen förändring av bestämmelserna i OSL. Samtidigt kan noteras att bilagan till cybersäkerhetsakten lämnar utrymme för nödvändigt informationsutbyte som är författningsreglerat. Privata kontrollorgan är alltså inte förhindrade att t.ex. lämna erforderliga uppgifter till tillsynsverksamheten vid den nationella myndigheten för cybersäkerhetscertifiering.

Som framgår ovan finns flera sekretessbestämmelser i OSL som kan aktualiseras i den nationella cybersäkerhetscertifieringsmyndighetens verksamhet för att skydda känsliga uppgifter från enskilda

som erhålls vid tillämpningen av EU:s cybersäkerhetsakt. För att sekretess ska gälla enligt 30 kap. 23 § OSL krävs dock att regeringen meddelar föreskrifter som närmare anger vilka uppgifter som omfattas av sekretessen. Utredningen noterar att regleringen i bilagan till offentlighets- och sekretessförordningen är begränsad beträffande FMV. Denna bestämmelse är varken tillämplig i certifierings- eller tillsynsverksamheten vid FMV som den nationella myndigheten för cybersäkerhetscertifiering kommer att bedriva. När det gäller sekretesskyddet för uppgifter som den nationella myndigheten för cybersäkerhetscertifiering kan komma att behandla i sin verksamhet inom ramen för cybersäkerhetsaktens tillämpningsområde bedömer utredningen att detta behöver kompletteras när det gäller uppgifter om enskilds affärs- eller driftförhållanden. För att tillförsäkra ett fullgott sekretesskydd föreslår utredningen därmed att offentlighets- och sekretessförordningen (2009:641) ska kompletteras så att sekretess gäller för uppgift om enskilds affärs- eller driftförhållanden i verksamhet som består i utredning och tillsyn enligt EU:s cybersäkerhetsakt och lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Det är vidare oklart i vilken utsträckning Enisa kommer att behandla sekretesskyddade uppgifter från bl.a. enskilda. Det kan dock noteras att det finns ett förbud för Enisa att för tredje part röja uppgifter som byrån behandlar eller mottar, om det begärts att uppgifterna ska behandlas konfidentiellt. Vidare omfattas Enisas anställda och experter av tystnadsplikt. Enisa ska i sina interna verksamhetsregler fastställa hur reglerna om konfidentialitet ska tillämpas praktiskt (se artikel 27).

12.5 Uppgifter som lämnas till privata organ för bedömning av överensstämmelse

Vad som redogjorts för ovan under avsnitt 12.4.1 om vilka uppgifter som kan komma att samlas hos offentliga organ för bedömning av överensstämmelse gäller också för privata kontrollorgan. Uppgifter som enskilda lämnar enligt det europeiska regelverket för cybersäkerhetscertifiering kan alltså vara av sådan karaktär som motiverar sekretesskydd.

Den som i privat verksamhet disponerar över uppgifter och information bestämmer själv om utlämnande av den till andra, med de begränsningar som följer av lagstiftning och åtaganden som vilar på civilrättslig grund.

Enligt nuvarande bestämmelser i OSL kommer privata organ för bedömning av överensstämmelse som utför uppgifter enligt EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhet – inbegripet förvaltningsuppgifter – inte att omfattas av OSL, eftersom den lagen, med vissa undantag, inte är tillämplig utanför den offentliga sektorn.

Inom flera olika verksamhetsområden gäller dock tystnadsplikt enligt lag för privata aktörer, och som ofta är reglerad som ett förbud mot att obehörigen röja vissa uppgifter. Det finns också tystnadsplikter i privat verksamhet som inte har någon motsvarighet i det allmännas verksamhet, utan skyddar information som lämnas till personer i olika slag av förtroendeställning. I dessa fall har obehörighetsrekvisitet sammanfattningsvis tolkats som att ett utlämnande av uppgifter får ske bl.a. om den som uppgiften rör har lämnat sitt samtycke, om uppgifter lämnas vidare till personer inom den berörda verksamheten som behöver dem för verksamheten eller om uppgifterna enligt lag eller annan författning ska lämnas ut, exempelvis till en tillsynsmyndighet (se t.ex. prop. 2002/03:139 s. 479).[14]

Författningsreglerad tystnadsplikt, oavsett om den följer av OSL eller av bestämmelser om tystnadsplikt för den privata sektorn, utgör en inskränkning av yttrandefriheten enligt regeringsformen och är som regel förenad med straffansvar. Den som bryter mot tystnadsplikten kan därmed dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Fråga uppkommer om det finns behov av kompletterande nationell reglering om tystnadsplikt för de privata organen för bedömning av överensstämmelse.

De i bilagan till cybersäkerhetsakten uppställda kraven på konfidentialitet och tystnadsplikt för organ för bedömning om överensstämmelse, som utredningen behandlat i avsnitt 12.4.2, är också direkt

[14] Det finns i svensk rätt flera bestämmelser om tystnadsplikt där obehörighetsrekvisitet används. Den praxis som finns rörande dessa bestämmelser bör i fråga om rekvisitets innebörd kunna tjäna som ledning även vid tolkningen och tillämpningen av den nu föreslagna bestämmelsen.

tillämpliga för privata kontrollorgan.[15] Dessa krav för ackreditering måste uppfyllas för att ett organ för bedömning av överensstämmelse ska kunna verka enligt EU:s cybersäkerhetsakt. Sekretesskraven får anses vara förhållandevis långtgående, såväl när det gäller sekretessens föremål och räckvidd som dess styrka.[16] Det kan dock inte uteslutas att uppgifter som kommer fram vid certifieringsverksamhet i enlighet med EU:s cybersäkerhetsakt kan komma att hanteras av en vidare krets av personer än de som omfattas av nämnda bilaga och 2 kap. 1 § OSL.

Som ovan berörts är brott mot tystnadsplikt normalt förenat med straffansvar. Straffansvaret gäller var och en som har skyldighet att hemlighålla en uppgift enligt lag eller annan författning, förutsatt att straffansvaret inte har reglerats särskilt. Straffansvaret enligt brottsbalken förutsätter dock att tystnadsplikten har sin grund i just svensk författning (se Ulväng m.fl., Brotten mot allmänheten och staten, 2 uppl. 2014, s. 276).[17] EU:s cybersäkerhetsakt kan alltså inte grunda straffansvar för brott mot tystnadsplikten.

Mot bakgrund av det anförda bedömer utredningen att det finns behov av att införa en nationell bestämmelse om tystnadsplikt för de privata organen för bedömning av överensstämmelse. Tystnadsplikten gäller uppgifter som lämnas till organen. Tystnadsplikt ska även gälla för sådana uppgifter som framkommer i verksamhet som organen bedriver och som rör certifieringsverksamheten. Närmare bestämt innebär utredningens förslag att en enskild i ett privat organ för bedömning av överensstämmelse inte obehörigen får röja eller utnyttja uppgifter om enskilds personliga och ekonomiska förhållanden. Den förslagna formuleringen omfattar t.ex. ett företags drifts- och affärsförhållanden. Förslaget innebär därmed att fler uppgifter kommer att omfattas av straffsanktionerade regler. Därför bör det i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt även införas en upplysning om att den som bryter mot tystnadsplikten kan dömas för brott.

En möjlighet för de privata organen för bedömning av överensstämmelse att bryta sekretessen i förhållande till behöriga nationella

[15] Vidare kan, som tidigare berörts, europeiska ordningar för cybersäkerhetscertifiering innehålla bestämmelser om hur organen för bedömning av överensstämmelse ska bevara sina uppgifter.
[16] Också provningslaboratorier omfattas.
[17] Därmed omfattas inte åsidosättanden av tystnadsplikter som avtalats mellan exempelvis arbetsgivare och arbetstagare (vilka däremot kan sanktioneras på annat sätt än genom straffansvar, t.ex. genom skadeståndsskyldighet).

myndigheter, och då författning kräver att uppgifter lämnas, har intagits i bilagan till EU:s cybersäkerhetsakt. Detta undantag ligger i linje med svensk rätt på området (se ovan) och möjliggör nödvändigt informationsutbyte (se vidare avsnitt 12.6). 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.

12.6 Informationsutbyte mellan medlemsstaternas myndigheter

12.6.1 Uppgifter som delas

Av artikel 58.7–9 i EU:s cybersäkerhetsakt framgår att nationella myndigheter för cybersäkerhetscertifiering ska

- 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.

12.6.2 Gällande sekretessreglering

EU:s cybersäkerhetsakt

I EU:s cybersäkerhetsakt finns inte några bestämmelser som närmare reglerar frågan om sekretess för uppgifter och information som lämnas mellan medlemsstaternas myndigheter eller mellan en sådan

myndighet och kommissionen eller Enisa.[18] I artikel 27 finns dock en sekretessbestämmelse för uppgifter som lämnas till Enisa. Av bestämmelsen framgår att Enisa inte ska röja uppgifter som den behandlar eller mottar för tredje part, om det i en motiverad ansökan har begärts att uppgifterna helt eller delvis ska behandlas konfidentiellt. Enisa ska i sina interna verksamhetsregler fastställa hur reglerna om konfidentialitet ska tillämpas praktiskt. Av artikel 28 framgår att förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos Enisa.

Utrikessekretess

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. Skadebegreppet ska inte ges en alltför vid innebörd, utan det måste röra sig om någon olägenhet för landet.[19]

När det gäller uppgifter som fås från en annan stat eller en mellanfolklig organisation kan avsändarens uppfattning i sekretessfrågan inte avgöra om uppgiften ska hållas hemlig, men avsändarens intresse av sekretess kan ha betydelse för sekretessprövningen i det enskilda fallet. Generellt är utrymmet för öppenhet enligt bestämmelsen mer begränsat när det gäller uppgifter som fås från en EU-institution eller annan medlemsstat än uppgifter i handlingar som upprättats i Sverige (jfr prop. 1994/95:112 s. 29).

Utrikessekretessen är en s.k. primär sekretessbestämmelse som en myndighet ska tillämpa på grund av att bestämmelsen omfattar vissa uppgifter som finns hos myndigheten till följd av att dess räckvidd inte har begränsats och därför gäller inom hela den offentliga

[18] I den föreslagna EUCC-ordningen anges emellertid att utbyte av information får ske om det är nödvändigt för ett effektivt genomförande av certifieringsordningen, särskilt för inbördes granskning. Informationsutbyte får också ske för att åstadkomma effektivt samarbete mellan de involverade myndigheterna och organen för bedömning av överensstämmelse, för hantering av nyupptäckta sårbarheter samt för handläggning av klagomål. Information som utbyts konfidentiellt mellan behöriga myndigheter respektive mellan berörda myndigheter och kommissionen får dock inte lämnas ut till allmänheten utan föregående godkännande av ursprungsmyndigheten.

[19] Att mindre och tillfälliga störningar eller irritationer inom ett annat lands ledning inte kan uteslutas om uppgifter lämnas ut bör alltså inte alltid leda till sekretess (se prop. 1979/80:2 Del A s. 131).

sektorn. Det kan tilläggas att det är få uppgifter som är så känsliga att de behöver omfattas av sekretess oavsett hos vilken myndighet de befinner sig (se prop. 2008/2009:15 s. 285).

Sekretess i det internationella samarbetet på grund av en bindande EU-rättsakt

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 bestämmelsens 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.

Uppgiftens innehåll, art eller karaktär saknar betydelse för bestämmelsens tillämplighet. Bestämmelsen är t.ex. tillämplig i fråga om uppgifter om enskilda, om de finns hos myndigheten på grund av ett reglerat internationellt samarbete. Ett sådant exempel är en uppgift som kommit in från en utländsk myndighet och som härrör från en utredning eller ett annat ärende där. Detsamma gäller om uppgiften på annat sätt samlats in av den svenska myndigheten i syfte att vidarebefordras till en annan stat eller en mellanfolklig organisation, i enlighet med t.ex. en biståndsskyldighet.

En förutsättning för att sekretess ska gälla är att ett röjande av uppgiften kan antas försämra Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten.[20] Uttrycket ”möjlighet att delta i” syftar främst på möjligheten att få del av information i enlighet med EU-rättsakten eller avtalet, dvs. dra nytta av samarbetet. Bestämmelsen gäller normalt bara om det finns en tydlig sekretessbestämmelse i den aktuella rättsakten (se prop. 2012/13:192 s. 35).[21]

[20] Myndigheten är i det enskilda fallet skyldig att göra en självständig bedömning av vilka konsekvenser ett röjande kan antas få för det fortsatta samarbetet.

[21] Om det inte gör det, så kommer en tillämpning av sekretessbestämmelserna normalt inte att aktualiseras, även om det inte utesluts av bestämmelsernas ordalydelse. I sådana fall torde det främst vara uppgiftens art och anknytning till det internationella samarbetet som medför att skaderekvisitet är uppfyllt vilket enligt förarbetena innebär att det ligger närmare till hands att tillämpa bestämmelsen om utrikessekretess i 15 kap. 1 § OSL (se ovan).

EU:s cybersäkerhetsakt är en sådan bindande EU-rättsakt som avses i 15 kap. 1 a § OSL. Akten innehåller förutom sekretessbestämmelsen i punkten 16 i bilagan sekretessbestämmelsen i artikel 27 som reglerar sekretessen för uppgifter som lämnas till Enisa.[22] Av artikel 27 framgår som sagt att Enisa inte får röja uppgifter som den behandlar eller mottar för tredje part, om det i en motiverad ansökan har begärts att uppgifterna helt eller delvis ska behandlas konfidentiellt.[23]

Utredningen noterar att det i EU:s cybersäkerhetsakt inte finns någon bestämmelse som anger – förutom vad som gäller enligt punkten 16 i bilagan – att medlemsstaterna ska säkerställa skyddet av konfidentiella uppgifter som erhålls vid tillämpningen av cybersäkerhetsakten.

Av vad som anges i artikel 58 kan förutses att det kommer att förekomma informationsutbyte mellan såväl medlemsstaternas myndigheter som mellan dessa och kommissionen och Enisa.

Fråga uppkommer då om det är möjligt att i avsaknad av en uttrycklig sekretessbestämmelse att tillämpa 15 kap. 1 a § OSL. Eftersom det finns en sekretessbestämmelse för uppgifter hos Enisa finns – enligt utredningens bedömning – förutsättningar att tillämpa 15 kap. 1 a § på uppgifter som inhämtas och lämnas till Enisa. Vad gäller uppgifter som inhämtas med stöd av cybersäkerhetsakten och en europeisk ordning för cybersäkerhetscertifiering och som lämnas eller inhämtas från en myndighet i en medlemsstat eller kommissionen bör – enligt utredningens mening – även sådana uppgifter omfattas av samma paragraf om det i en europeisk ordning finns en reglering av sekretessen. Även i avsaknad av en sådan reglering torde paragrafen kunna tillämpas enligt sin ordalydelse, i annat fall bör 15 kap. 1 § kunna tillämpas på uppgifterna (se ovan).

En bedömning av om sekretesskydd föreligger ska, som framgår ovan, göras i varje enskilt fall. Enligt utredningen utgör nu nämnda sekretessbestämmelser i EU:s cybersäkerhetsakt en sådan sekretessreglering som kan medföra att skaderekvisitet enligt 15 kap. 1 a § OSL uppfylls om uppgifter som mottagits eller inhämtats lämnas ut.

Sekretessen enligt 15 kap. 1 a § OSL gäller alltså för den myndighet som fått uppgift från ett utländskt organ, dvs. den nationella myndigheten för cybersäkerhetscertifiering. Om en myndighet mottagit

[22] EU:s cybersäkerhetsakt väcker frågan om aktuella samarbeten kommer att förutsätta sekretesskydd hos andra myndigheter.
[23] Jfr även kravet i artikel 59.2 på beaktande av konfidentialitet vid nationella cybersäkerhetscertifieringsmyndigheters inbördes granskning.

uppgiften från annat håll gäller emellertid inte bestämmelsen hos den mottagande myndigheten. Där kan t.ex. utrikessekretessen i 15 kap. 1 § OSL aktualiseras i stället.[24] Utrikes- och försvarssekretess (se avsnitt 12.4.2 och 12.7.4) gäller hos alla myndigheter.

De sekretessbrytande bestämmelserna i 10 kap. 15–27 §§ och 28 § första stycket OSL får inte tillämpas när det gäller en uppgift som omfattas av sekretess enligt 15 kap. 1 a § OSL. Det kan noteras att bestämmelsen om s.k. nödvändigt utlämnande i 10 kap. 2 § OSL inte omfattas av undantaget i 15 kap. 1 a § (se mer on nödvändigt utlämnande under avsnitt 12.7.3).

Sekretess för uppgift om en enskilds ekonomiska eller personliga förhållanden på grund av avtal med mellanfolklig organisation

Som berörts ovan kommer uppgifter som nationella myndigheter för cybersäkerhetscertifiering erhåller om certifikatsökande och IKT-tillverkare och -leverantörer att delas med andra medlemsstaters myndigheter och kommissionen.[25] Det kan bl.a. vara fråga om ekonomiska förhållanden.

Enligt 30 kap. 24 § OSL gäller, i den mån riksdagen godkänt avtal om det med främmande stat eller mellanfolklig organisation, sekretess hos statlig myndighet i verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt, för sådan uppgift om enskilds ekonomiska eller personliga förhållanden som myndigheten förfogar över på grund av avtalet.

Eftersom bestämmelsen saknar skaderekvisit är det fråga om s.k. absolut sekretess. Det innebär att det inte behöver göras någon skadebedömning.

I bestämmelsen anges vidare att de sekretessbrytande bestämmelserna i 10 kap. 15–27 §§ och 28 § första stycket OSL inte får tillämpas i strid med vad som avtalats.

Bestämmelsen omfattar både uppgifter som myndigheten har fått från utlandet och uppgifter som myndigheten har inhämtat i Sverige

[24] Det kan påpekas att berörd myndighet, vid behov av konsultation med andra myndigheter, bör beakta vilket sekretesskydd som kan aktualiseras för uppgifterna hos den mottagande myndigheten.
[25] Jfr artiklarna 56.7, 56.8 och 58.7–9.

med stöd av avtalet. I begreppet avtal anses ingå bl.a. rättsakter som gäller till följd av Sveriges medlemskap i EU, dvs. förordningar och direktiv m.m. som utfärdats av EU:s institutioner.

För att bestämmelsen ska bli tillämplig krävs att den aktuella rättsakten innehåller en klausul om att uppgifterna inte får lämnas vidare i det aktuella fallet. Regleringen måste således vara tillräckligt specifik för att anses som en sådan sekretessklausul. De sekretessbestämmelser i EU:s cybersäkerhetsakt som angetts ovan gör sig gällande även här.

Frågan är om den svenska verksamheten i dessa fall utgör sådan utredning eller annan verksamhet som faller inom tillämpningsområdet för 30 kap. 24 § OSL. I förarbetena till regleringen uttalas att information om företagskriser, planerade företagsöverlåtelser och liknande förhållanden kan sägas utgöra planering eller utredning med avseende på näringslivet och alltså täcks av begreppen i paragrafen.

Det kan vidare konstateras att de nationella myndigheterna för cybersäkerhetscertifiering kommer att behöva utföra utredning i form av att samla in och ställa samman information för att kunna uppfylla sin rapporteringsskyldighet till Enisa (artikel 58.7 g). EU:s cybersäkerhetsakt binder medlemsstaternas nationella myndigheter för cybersäkerhetscertifiering till ett samarbete och informationsutbyte kring cybersäkerhetscertifieringen av IKT-produkter, -tjänster och -processer där varje medlemsstat utför en del i den utredning som utförs inom ramen för samarbetet. Utredningen anser att den verksamhet i form av insamlande och vidarebefordran av uppgifter om certifikatsökande och certifikatinnehavare omfattas av tillämpningsområdet för 30 kap. 24 § OSL. En förordning är en sådan bindande EU-rättsakt som avses i paragrafen. I likhet med vad som anförts ovan bedömer utredningen att artikel 27 och punkten 16 i bilagan till EU:s cybersäkerhetsakt[26] utgör sådan sekretessreglering som gör det möjligt att tillämpa bestämmelsen. De uppgifter om enskilds affärs- eller driftförhållanden som nämnda aktörer kommer att förfoga över till följd av cybersäkerhetsakten omfattas därmed.

[26] Jfr även artikel 59.2.

12.6.3 Slutsatser

Mot bakgrund av vad som anförts ovan gör utredningen bedömningen att de uppgifter som berörda myndigheter kan komma att erhålla vid tillämpningen av artikel 58.7–9 i EU:s cybersäkerhetsakt[27] som utgångspunkt omfattas av sekretess enligt 15 kap. 1 a § OSL. Vidare kan genom bestämmelsen i 30 kap. 24 § OSL uppgifter om enskildas ekonomiska förhållanden skyddas – och båda bestämmelser ger ett starkt sekretesskydd i form av absolut sekretess – men behövligt sekretesskydd uppnås alltså redan genom 15 kap. 1 a § OSL.[28]

I sammanhanget förtjänar även att 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). Då EU-förordningar jämställs med lag vid tillämpningen av OSL utgör sekretess således inget hinder för det informationsutbyte som enligt artikel 58.7–9 i cybersäkerhetsakten ska ske mellan de nationella myndigheterna för cybersäkerhetscertifiering.

12.7 Informationsutbyte mellan svenska myndigheter

12.7.1 Inledning

I många fall måste myndigheter kunna utbyta information för att kunna utföra sina uppgifter. I Sverige kommer bl.a. den nationella myndigheten för cybersäkerhetscertifiering, offentliga organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet att dela uppgifter med varandra med anledning av EU:s cybersäkerhetsakt. Fråga kan vara om sekretessbelagda uppgifter som myndigheterna behöver i sin certifierings-, tillsyns- eller ackrediteringsverksamhet. Det kan noteras att den nationella myndigheten för cybersäkerhetscertifiering vid sin tillsyn över efterlevnaden av kraven i certifikat som utfärdats i Sverige även ska samarbeta med andra berörda marknadsövervakningsmyndigheter (artikel 58.7 a). Uppgifter kommer vidare att utbytas mellan myndigheter som framför allt in-

[27] Jfr även artikel 56.8 sista meningen.
[28] OSL:s uppbyggnad innebär att en myndighet kan få beakta flera olika sekretessbestämmelser i ett och samma ärende. Av förarbetena till lagen framgår att vid konkurrens mellan flera olika tillämpliga sekretessbestämmelser är det den bestämmelse som ger det starkaste skyddet för uppgiften som får fälla utslaget (se prop. 2008/09:150, s. 286, jfr prop. 1979/80:2 Del A s. 70).

går i SAMFI, men även med andra berörda myndigheter. T.ex. kan tänkas att information lämnas till FOI som underlag för testning och liknande.

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. Sekretessbrytande bestämmelser finns även i andra författningar som OSL hänvisar till, eller som en uppgiftsskyldighet varvid 10 kap. 28 § OSL blir tillämplig. Det finns också bestämmelser om överföring av sekretess till myndigheter.[29]

12.7.2 Sekretessgräns inom den nationella myndigheten för cybersäkerhetscertifiering

Vad som föreskrivs om sekretess mot andra myndigheter och om uppgiftslämnande och överföring av sekretess gäller, som nämns i avsnitt 12.3.1, också mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra (8 kap. 2 § OSL).

Utredningen kan konstatera att tillsyns- och certifieringsverksamheterna vid den nationella myndigheten för cybersäkerhetscertifiering kommer att tillämpa delvis olika sekretessbestämmelser. T.ex. är 31 kap. 12 § bara tillämplig på certifieringsverksamheten, medan sekretessen enligt 30 kap. 24 § OSL är tillämplig på tillsynsverksamheten (avsnitt 12.6.2).[30] Uppgifter som enskilda lämnar till certifieringsorganet vid den nationella myndigheten i certifieringsärenden kommer emellertid inte att samlas in och bearbetas av organet inom ramen för myndighetens tillsynsverksamhet. Dessa uppgifter kommer därför inte att omfattas av tillsynssekretess. Vidare ska enligt EU:s cybersäkerhetsakt det nationella certifieringsorganet organiseras på ett sådant sätt att det förhåller sig självständigt i förhållande till den nationella myndighetens tillsynsverksamhet. Detta medför att det uppstår en sekretessgräns mellan de olika verksamhetsgrenarna inom den nationella myndigheten för cybersäkerhetscertifiering. Där-

[29] Det finns emellertid ingen sekretess enligt OSL som kan överföras från enskilda, utländska myndigheter eller mellanfolkliga organisationer. Den myndighet som mottar uppgifter direkt från sådana aktörer kan alltså inte tillämpa en sekundär sekretessbestämmelse.
[30] Däremot kan t.ex. sekretessen enligt 17 kap. 1 § OSL för myndigheters förberedelser för granskning gälla för både FMV och CSEC.

med ska bestämmelserna i OSL om uppgiftsutlämnande och överföring av sekretess tillämpas på samma sätt som mellan myndigheter.

Utredningen har tidigare i avsnitt 8.3.2 framhållit vikten av att den nationella myndigheten för cybersäkerhetscertifiering organiserar sin verksamhet på ett sätt som säkerställer oberoendet för det nationella certifieringsorganet och därigenom även säkerställer att det finns en tydlig sekretessgräns mellan de olika verksamhetsgrenarna.

I avsnitt 12.7.5 behandlas det nationella certifieringsorganets möjligheter att i vissa fall kunna lämna information till den nationella cybersäkerhetscertifieringsmyndigheten.

12.7.3 Sekretessbrytande bestämmelser

Nedan följer en redogörelse för de sekretessbrytande bestämmelser i OSL som är av intresse när det gäller förutsättningar att lämna ut uppgifter om rapporterade cybersäkerhetssårbarheter och om affärs- och driftförhållanden. Även överföring av sekretess berörs.

Nödvändigt utlämnande

Sekretess enligt 10 kap. 2 § OSL hindrar 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 (ett visst åliggande). Bestämmelsen kan vara tillämplig i fall där någon av de övriga sekretessbrytande reglerna inte gäller, men ska tillämpas restriktivt. Bara bedömningen att effektiviteten i myndighetens handlande sätts ned genom en föreskriven sekretess får inte leda till att sekretessen åsidosätts.

Tillsyn eller revision

Enligt 10 kap. 17 § OSL hindrar inte sekretess 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.

Det kan även förekomma informella kontakter mellan myndigheter i samband med en tillsyns- eller revisionsverksamhet. Ett vanligt förekommande fall torde vara att en myndighet tar kontakt med sin tillsynsmyndighet. Även sådana kontakter faller in under begreppet tillsyn eller revision. En förutsättning är dock att kontakten tas just därför att den ena myndigheten utövar tillsyn över eller revision hos den andra (prop. 1979/80:2 Del A s. 317).

T.ex. offentliga organ för bedömning av överensstämmelse ska lämna de nödvändiga uppgifter som den nationella myndigheten för cybersäkerhetscertifiering begär för fullgörandet av sin tillsyn. Eftersom uppgiftsskyldigheten följer av författning likställd med lag är det möjligt för myndigheter att i detta fall lämna ut sekretesskyddade uppgifter med stöd av 10 kap. 28 § första stycket OSL (se nedan).

Det är möjligt att lämna uppgifter även om det inte begärs av den granskande myndigheten. Så kan exempelvis ske i samband med att information om nyupptäckta cybersäkerhetssårbarheter lämnas.

Generalklausulen

Enligt den s.k. generalklausulen (10 kap. 27 § OSL) får en sekretessbelagd uppgift 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 tillkom mot bakgrund av att sekretess inte bör hindra myndigheter från att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför intresset av att uppgifterna inte lämnas ut. Generalklausulen kan inte tillämpas om utlämnandet strider mot lag eller förordning eller föreskrift som har meddelats med stöd av GDPR. Bestämmelsen är subsidiär i förhållande till andra sekretessbrytande bestämmelser och ska alltså inte tillämpas om någon annan sekretessbrytande bestämmelse kan tillämpas.

Vid prövningen av en utlämnandefråga enligt generalklausulen ska en avvägning göras mellan den mottagande myndighetens behov

av uppgifterna och det intresse som sekretesskyddet typiskt sett tillgodoser. Ytterligare omständigheter som är av betydelse är uppgifternas art och i vilket syfte de ska användas.

Sekretess vid uppgiftsskyldighet

Sekretess hindrar inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Sekretessbrytande bestämmelser finns också i anslutning till berörda sekretessbestämmelser (10 kap. 28 § OSL).[31]

Som tidigare nämnts medför EU:s cybersäkerhetsakt skyldighet för bl.a. offentliga organ för bedömning av överensstämmelse att lämna uppgifter till den nationella myndigheten för cybersäkerhetscertifiering.

12.7.4 Reglerna om partsinsyn och kommunikation

I förvaltningslagen (2017:900) (FL) finns ett antal handläggningsregler som är av betydelse för bl.a. utredningens förslag om förelägganden. En sådan regel är rätten till partsinsyn som kommer till uttryck i 10 §. Bestämmelsen innebär att den som är part i ett ärende har rätt att ta del av allt material som har tillförts ärendet med de begränsningar som följer av 10 kap. 3 § OSL. Bestämmelserna i 10 kap. 3 § första stycket reglerar vad som ska gälla vid konflikt mellan partsinsyn och sekretess (prop. 2016/17:180 s. 54). Enligt bestämmelserna hindrar inte sekretess att en enskild eller en myndighet som är part i ett mål eller ärende hos domstol eller annan myndighet, och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. En sådan handling eller ett sådant material får dock inte lämnas ut till parten i den utsträckning det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att en sekretessbelagd uppgift i materialet inte röjs. I sådana fall ska myndigheten på annat sätt lämna parten upplysning om vad materialet innehåller i den utsträckning det behövs för att parten ska kunna ta till vara sin rätt och det kan ske utan allvarlig skada för det intresse som sekretessen ska skydda.

[31] Med föreskrift i lag likställs EU-förordningar (se t.ex. prop. 2006/07:6 s. 32).

Det är enligt utredningens bedömning rimligt att anta att ärenden om föreläggande kan komma att innehålla sekretessbelagda uppgifter. Man kan dock tänka sig att många ärenden kommer att inrymma uppgifter av mer teknisk karaktär. Även om en inte obetydlig del av uppgifterna i ärendena kan antas vara mindre känsliga kan det i vissa ärenden finnas uppgifter som är så känsliga att de inte under några förhållanden bör komma parten till del. Sådana uppgifter kan omfattas av t.ex. försvarssekretess enligt 15 kap. 2 § OSL om de rör nationell säkerhet. Det kan vara fråga om uppgifter vars röjande medför att kritiska samhällsfunktioner äventyras och att verksamheter av betydelse för Sveriges säkerhet hotas.

Bestämmelsen i 10 kap. 3 § första stycket OSL om kravet på synnerlig vikt balanserar partsinsynen och skyddsintresset i den typ av ärenden som kan bli aktuella enligt EU:s cybersäkerhetsakt och anslutna författningar.

Sammantaget anser utredningen att det inte framkommit tillräckliga skäl för att med stöd av 10 kap. 3 § OSL tredje stycket göra undantag från bestämmelsens första stycke.

Partsinsynen i ärenden om föreläggande bör därför gälla så som den kommer till uttryck i 10 § FL. På motsvarande sätt gäller underrättelseskyldigheten i 25 § FL, om krav på handläggande myndighet att underrätta part och ge denne tillfälle att yttra sig över aktuellt material innan myndighetens beslutsfattande, med de begränsningar som följer av 10 kap. 3 § OSL. Förhållandet till sekretess motiverar av samma skäl som anförts ovan inte undantag från den förvaltningsrättsliga bestämmelsen om kommunikation.

12.7.5 Slutsatser

Utredningen konstaterar att det finns flera sekretessbrytande bestämmelser som kan tillämpas för att uppgifter som omfattas av sekretess ska kunna delas mellan myndigheter i samband med tillsyn[32] och rapportering av sårbarheter. Detta gäller alltså även inom den nationella myndigheten för cybersäkerhetscertifiering, mellan dess certifieringsverksamhet och tillsynsverksamhet. Undantagsreglerna kan tillämpas även på det nationella ackrediteringsorganets tillsyns-

[32] Motsvarande gäller i förhållande till kontrollverksamheten vid det nationella certifieringsorganet. Uppgifter vid certifieringsorgan rör emellertid även andra sekretessbestämmelser än de här nämnda (se avsnitt 16.3.5–7, 16.4.5 och 16.4.6).

verksamhet över offentliga organ för bedömning av överensstämmelse respektive när myndigheten får uppgifter i samband med ansökan om ackreditering.

Det bör noteras att de sekretessbrytande bestämmelserna i 10 kap. 15–27 §§ och 28 § första stycket OSL inte kan tillämpas om sekretess gäller enligt 15 kap. 1 a § (se 15 kap. 1 a § tredje stycket och avsnitt 12.6.2.). Motsvarande begränsning aktualiseras i fråga om 30 kap. 24 § OSL. För sådana uppgifter, som bl.a. nationella myndigheter kommit att förfoga över till följd av gränsöverskridande samarbete, kvarstår då den möjlighet till vidare informationsutbyte som bestämmelsen i 10 kap. 2 § OSL om nödvändigt utlämnande ger. Även om denna bestämmelse ska tillämpas restriktivt torde den vara tillräcklig i sammanhanget.

Utredningen kan notera att det finns behov av informationsutbyte såväl mellan nationella myndigheter som mellan dessa myndigheter och deras självständiga verksamheter. Offentliga organ för bedömning av överensstämmelse, vilka fått uppgifter från certifikatinnehavare om nyupptäckta sårbarheter, ska enligt EU:s cybersäkerhetsakt vidarebefordra potentiellt känslig information till den nationella myndigheten för cybersäkerhetscertifiering. Vidare behöver sådana organ lämna information till den nationella myndigheten för cybersäkerhetscertifiering och det nationella ackrediteringsorganet i samband med ansökan om certifiering respektive ackreditering. Av EU:s cybersäkerhetsakt följer att det hos certifieringsorganen råder sekretess för erhållna uppgifter, dvs. krav på konfidentialitet och tystnadsplikt (jfr avsnitt 12.4.2). Cybersäkerhetsakten medger dock undantag från dessa krav i de fall då uppgifter måste lämnas enligt unionsrätten eller medlemsstaternas nationella rätt. Vidare kan noteras att 10 kap. 17 § OSL medger att t.ex. det nationella certifieringsorganet lämnar uppgift till den nationella myndigheten för cybersäkerhetscertifiering om uppgiften behövs där för tillsyn över organet. Det finns således redan tillräckligt författningsstöd för att sekretess inte ska hindra offentliga certifieringsorgan att vid behov lämna uppgifter till berörda nationella myndigheter.

12.8 Behandling av personuppgifter

Bedömning: I EU:s dataskyddsförordning finns rättslig grund för den nationella myndighetens för cybersäkerhetscertifiering och offentliga kontrollorgans personuppgiftsbehandling inom ramen för deras granskande verksamhet. Utredningen förutsätter att myndigheterna ser över sina respektive regleringar avseende behandling av personuppgifter för att säkerställa att de täcker in sådan personuppgiftsbehandling som kan komma att aktualiseras med anledning av EU:s cybersäkerhetsakt och den föreslagna lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

12.8.1 EU:s dataskyddsförordning

För att myndigheter ska kunna utbyta information med varandra krävs alltså både att informationen inte är sekretessbelagd eller att sekretessen kan brytas, och att bestämmelser om behandling av personuppgifter hos myndigheterna ger stöd för att uppgifterna får behandlas. Dataskyddsregleringen innebär vissa begränsningar av informationsutbyte i de fall personuppgifter berörs. Enligt skäl (74) till EU:s cybersäkerhetsakt ska akten inte påverka tillämpningen av förordning (EU) 2016/679 (EU:s dataskyddsförordning). EU:s dataskyddsförordning utgör grunden för generell personuppgiftsbehandling inom EU. I svensk rätt kompletteras förordningen av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning samt i sektorspecifika registerförfattningar som i stor utsträckning reglerar svenska myndigheters personuppgiftsbehandling

EU:s dataskyddsförordning gäller i princip för all automatiserad behandling, samt i vissa fall manuell behandling, av personuppgifter. Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person. Typiska personuppgifter är personnummer, namn och adress. Ett bolagsnummer är ofta inte en personuppgift men kan vara det om det handlar om ett enmansföretag. Personuppgiftsbehandling innefattar alla former av åtgärder med personuppgifter, exempelvis insamling, användning, utlämnande, spridning eller förstöring. Förordningen hindrar dock inte myndigheter att lämna ut allmänna handlingar enligt offentlighetsprincipen. En myndighet

är inte skyldig att lämna ut allmänna handlingar på elektronisk väg men om det sker gäller dataskyddsförordningen för sådant utlämnande.

Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom avtal (artikel 28.3 i EU:s dataskyddsförordning).

För att en myndighets behandling av personuppgifter ska vara laglig måste det finnas en rättslig grund för behandlingen. Personuppgifter får endast behandlas om minst ett av det villkor som anges i artikel 6.1 a–f i EU:s dataskyddsförordning är uppfyllt. Dessa villkor utgör den rättsliga grunden för personuppgiftbehandlingen. Uppräkningen av vad som kan utgöra rättslig grund för behandling av personuppgifter i artikel 6.1 är uttömmande. Av intresse för myndigheters verksamhet är artikel 6.1 e) som gäller när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. I förarbetena till dataskyddslagen uttalar regeringen att alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse (prop. 2017/18:105, s. 56 f.).

12.8.2 Personuppgifter vid europeisk cybersäkerhetscertifiering

Den nationella myndigheten för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och det nationella ackrediteringsorganet kan komma att behandla personuppgifter, t.ex. organisationsnummer för enskild näringsverksamhet eller namn på fysiska företrädare, inom ramen för sin tillsyns-, certifierings- respektive ackrediteringsverksamhet.[33] EU:s dataskyddsförordning ställer då krav på att myndigheten har rättslig grund för behandling av uppgifterna.[34] Genom utpekandet som nationell myndighet för cybersäkerhetscertifiering i den föreslagna förordningen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ges myndigheten i upp-

[33] Informationsutbyte mellan nationella ackrediteringsorgan behandlas primärt i förordning (EG) 765/2008. Inom ramen för den förordningen är EU:s dataskyddsförordning tillämplig i fråga om behandling av personuppgifter (jfr skäl 31).
[34] Observera att detta inte gäller för de privata organen för bedömning av överensstämmelse.

drag att utföra uppgifter som är av allmänt intresse. Detsamma gäller för offentliga organ för bedömning av överensstämmelse. Det innebär att den rättsliga grunden i artikel 6.1 e i EU:s dataskyddsförordning för behandling av personuppgifter kommer att vara tillämplig.

Om det ingår behandling av personuppgifter i hanteringen är bestämmelserna om personuppgiftsbiträden tillämpliga och personuppgiftsbiträdesavtal ska upprättas.

Myndigheternas hantering av personuppgifter sker med stöd av EU:s dataskyddsförordning. Utredningen bedömer att det finns stöd för den behandling av personuppgifter som utredningens förslag kan medföra i det generella dataskyddsregelverket. Utredningens förslag med mer långtgående befogenheter kan dock leda till att personuppgifter kommer att hanteras i större utsträckning. Utredningen förutsätter därför att berörda myndigheter ser över sin hantering av personuppgifter för att säkerställa att den täcker in den personuppgiftsbehandling som kan aktualiseras med anledning av EU:s cybersäkerhetsakt och den föreslagna lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

13 Övriga frågor

13.1 Inledning

I detta kapitel behandlas behovet av ökad samverkan mellan berörda aktörer, Europeiska gruppen för cybersäkerhetscertifiering, nationella ordningar för cybersäkerhetscertifiering, inbördes granskning och marknadsfrågor.

13.2 Behovet av samverkan

Det europeiska ramverk för cybersäkerhetscertifiering som nu införs ställer krav på nära samarbete och samverkan mellan såväl berörda nationella myndigheter som mellan nationella myndigheter och berörda organ inom Europeiska unionen, främst kommissionen och Enisa. Den nationella myndigheten för cybersäkerhetscertifiering bör även t.ex. delta aktivt i den europeiska gruppen för cybersäkerhetscertifiering i syfte att uppnå en effektiv tillämpning av förordning (artikel 58.6).

Myndigheten ska vidare samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering samt med andra berörda myndigheter och aktörer i näringslivet, bl.a. för att utbyta information om IKT-produkter, IKT-tjänster och IKT-processer som eventuellt avviker från kraven i förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering samt övervaka relevant utveckling på området cybersäkerhetscertifiering (artikel 58.7 h och i).

Berörda myndigheter och aktörer samverkar redan i dag inom ramen för SAMFI-myndigheternas verksamhet och de forumgrupper som drivs av Myndigheten för samhällsskydd och beredskap. Myndigheterna samverkar också inom ramen för det cybersäkerhetscenter som ska etableras under 2020 (kapitel 5).

Utredningen bedömer att det finns ett behov av ökat informationsutbyte och övrig samverkan mellan berörda nationella myndigheter och mellan dessa myndigheter och andra berörda aktörer inom främst näringslivet. Behovet av ökad samverkan uppkommer också när det gäller hur den svenska representationen i den Europeiska gruppen för cybersäkerhetscertifiering kan säkerställas för att kunna tillvarata nationella intressen i detta sammanhang.

13.2.1 Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

I artikel 62.1 i EU:s cybersäkerhetsakt anges att en europeisk grupp för cybersäkerhetscertifiering (nedan kallad gruppen) ska inrättas. Gruppen ska bestå av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller företrädare för andra berörda nationella myndigheter. Intressenter och berörda tredje parter får bjudas in att delta i gruppens möten och delta i dess arbete.

Gruppen ska ha i uppgift att bl.a. ge råd till och bistå kommissionen i arbetet med att säkerställa ett konsekvent genomförande och tillämpning av det europeiska ramverket för cybersäkerhetscertifiering. Det gäller bl.a. frågor som rör unionens löpande arbetsprogram, strategisamordning, utarbetandet av de europeiska ordningarna för cybersäkerhetscertifiering och frågor om cybersäkerhetscertifiering. Gruppen ska även uppmana Enisa att utarbeta förslag till certifieringsordning enligt artikel 48.2, och ska också ge råd till, bistå och samarbeta med Enisa när det gäller utarbetande av förslag till certifieringsordning enligt artikel 49. Gruppen ska också lämna yttrande över förslag till certifieringsordning som utarbetats av Enisa enligt artikel 49 samt lämna förslag till kommissionen avseende översyn och underhåll av befintliga europeiska ordningar för cybersäkerhetscertifiering.

Gruppen ska vidare undersöka utvecklingen på området för cybersäkerhetscertifiering och utbyta information och god praxis om ordningar för cybersäkerhetscertifiering. Den ska vidare underlätta anpassningen av europeiska ordningar för cybersäkerhetscertifiering med internationellt erkända standarder, bl.a. genom att se över befintliga europeiska ordningar för cybersäkerhetscertifiering och lämna rekommendationer till Enisa om att samarbeta med relevanta inter-

nationella standardiseringsorganisationer för att åtgärda brister eller luckor i de befintliga internationellt erkända standarderna.

Gruppen ska även verka för att underlätta samarbetet mellan nationella myndigheter för cybersäkerhetscertifiering, bl.a. i form av utbyte av information och kapacitetsuppbyggnad, vilket bör ske genom att fastställa metoder för ett effektivt informationsutbyte i frågor som rör cybersäkerhetscertifiering.

Till gruppens uppgifter hör även att ge 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.

Kommissionen vara ordförande i gruppen med stöd av Enisa och kommissionen ska även tillhandahålla ett sekretariat för gruppen arbete.

13.2.2 Behovet av nationell strategi och medverkan i Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

Förslag: En strategi för att tillvarata nationella intressen när det europeiska ramverket för cybersäkerhetscertifiering utvecklas bör tas fram.

Bedömning: Det finns behov av ökad samverkan mellan berörda myndigheter, offentliga aktörer, näringslivsorganisationer och företag för att säkerställa att svenska intressen kan representeras och tillvaratas när det europeiska ramverket för cybersäkerhetscertifiering utvecklas.

I artikel 58.6 i EU:s cybersäkerhetsakt framhålls att det är lämpligt att de nationella myndigheterna för cybersäkerhetscertifiering deltar i den Europeiska gruppen för cybersäkerhetscertifiering. De nationella myndigheterna ska även samarbeta med andra myndigheter, bl.a. 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 samt övervaka relevant utveckling på området cybersäkerhetscertifiering.

Utredningen kan konstatera att det europeiska ramverket för cybersäkerhetscertifiering som nu införs genom cybersäkerhetsakten och anknutna europeiska ordningar för cybersäkerhetscertifiering ställer ökade krav på informationsutbyte och samverkan mellan såväl berörda nationella myndigheter som mellan nationella myndigheter och unionens olika ansvariga organ, bl.a. kommissionen och Enisa. Den Europeiska gruppen för cybersäkerhetscertifiering är i detta sammanhang ett viktigt instrument för att säkerställa att det europeiska ramverk för cybersäkerhetscertifiering som nu införs får en ändamålsenlig och effektiv tillämpning.

Uppgiften att vara nationell representant i den Europeiska gruppen för cybersäkerhetscertifiering bör ges till den föreslagna nationella myndigheten för cybersäkerhetscertifiering.[1]

Utredningen vill betona vikten av att det nationella informationsutbytet och samverkan utvecklas för att möta ökade krav och behov av samverkan och för att säkerställa att svenska intressen kan representeras och tillvaratas ramen för det europeiska ramverket för cybersäkerhetscertifiering. Det är viktigt att det finns en adekvat nationell representation i gruppen för att tillvarata svenska nationella intressen i det fortsatta arbetet med att utforma europeiska ordningar för cybersäkerhetscertifiering. Det ställer även krav på en utbyggd och väl fungerande samverkan mellan berörda myndigheter, bl.a. FMV, MSB och Swedac men även med övriga SAMFI-myndigheter, berörda näringslivsorganisationer och företag. Det finns redan etablerade samverkansformer på cybersäkerhetsområdet i form av bl.a. SAMFI-myndigheternas samverkan. Det kan emellertid föreligga behov av ökad samverkan när det europeiska ramverket för cybersäkerhetscertifiering införs och får genomslag. Uppgiften att ta fram organisation och arbetsformer för hur en sådan utvecklad samverkan kan ske bör i första hand lämnas till berörda myndigheter med ansvarsområden inom cybersäkerhetsaktens tillämpningsområde.

Utredningen bedömer samtidigt att det finns behov av en samlad nationell strategi för arbetet med att tillvarata nationella intressen när det europeiska ramverket för cybersäkerhetscertifiering utvecklas. Utredningen föreslår att regeringen överväger att initiera ett arbete med att ta fram en sådan strategi. I det arbetet bör berörda myndigheter, andra offentliga aktörer och näringslivet ges möjlighet att delta.

[1] FMV representerar redan i dag nationella intressen i ECCG.

13.3 Nationell ordning för cybersäkerhetscertifiering

Av artikel 57.1 framgår 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. Befintliga certifikat som utfärdats enligt nationella ordningar för cybersäkerhetscertifiering och som omfattas av en europeisk ordning för cybersäkerhetscertifiering ska dock förbli giltiga tills de löper ut (punkten 3).

Medlemsstaterna får inte heller införa nya nationella ordningar för cybersäkerhetscertifiering av de IKT-produkter, IKT-tjänster och IKT-processer som omfattas av en befintlig europeisk ordning. för cybersäkerhetscertifiering. De nationella ordningar som inte omfattas av en europeisk ordning för cybersäkerhetscertifiering får dock kvarstå.

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.

13.3.1 Förslaget till europeisk ordning för cybersäkerhetscertifiering av IKT-produkter

Som utredningen tidigare redogjort för har Enisa på begäran av kommissionen i enlighet med artikel 48.2[2] utarbetat ett förslag till certifieringsordning som syftar till att fungera som en efterföljare till det befintliga SOG-IS-systemet. Utkastet, som publicerades i juli 2020, baseras på Common-Criteria och syftar till en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter (EUCC). EUCC gäller för certifiering av cybersäkerheten hos IKT-produkter på grundval av Common Criteria, CEM (the Common Methodology for Information Technology Security Evaluation) och standarderna ISO/IEC 15408 respektive ISO/IEC 18045. Ordningen ska täcka varje typ av IKT-produkt som tillhandhålls på den inre marknaden, med villkoren att produkten omfattar åtminstone ett funktionellt

[2] Certifieringsordningen ingår således inte i unionens löpande arbetsprogram.

säkerhetskrav i enlighet med CC del 2 och strävar efter att nå assuransnivåerna ”betydande” eller ”hög”. Ordningen innehåller vidare övergångsregler. Certifikat som utfärdas med stöd av ordningen ska erkännas i alla EU-medlemsstater och är giltiga i fem år och kan förnyas. Ordningen tillåter vidare sammansatt certifiering.

EUCC identifierar, i enlighet med artikel 54.1 o cybersäkerhetsakten, ett antal nationella certifieringsordningar som omfattar samma typ eller kategorier av IKT, säkerhetskrav, utvärderingskriterier, utvärderingsmetoder och assuransnivåer. Bland de nationella ordningar som identifieras finns den svenska ordningen för certifiering och evaluering av it-säkerhetsprodukter och skyddsprofiler, som i dag tillämpas av certifieringsorganet CSEC vid FMV.

13.3.2 Nationella ordningen för certifiering av it-säkerhet i system och produkter

Förslag: FMV bör ges i uppdrag att analysera behov av en fortsatt ordning för certifiering av it-säkerhet i system och produkter.

FMV med certifieringsorganet CSEC ska i sin verksamhet verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat samt vara Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat (CCRA) och motsvarande överenskommelse inom Europa (SOG-IS MRA). I kapitel 5 finns en närmare beskrivning av FMV/CSEC:s verksamhet och den nationella ordningen för certifiering av it-säkerhet i system och produkter.

Som framgår ovan identifierar EUCC i enlighet med artikel 54.1 o i cybersäkerhetsakten ett antal nationella certifieringsordningar som omfattar bl.a. samma typ eller kategorier av IKT.

Mot bakgrund av det ovan angivna uppkommer frågan vilken påverkan införandet av EUCC, om förslaget skulle genomföras i dess nuvarande lydelse, kan få på den svenska nationella ordningen för certifiering av it-säkerhet i system och produkter.

Det ska i detta sammanhang noteras att organisationen och verksamheten vid FMV/CSEC: främst är utformad för att möta krav som anges i de olika internationella överenskommelser och standarder som ligger till grund för certifieringsverksamheten. Certifierings-

organets organisation och verksamhet regleras i styrdokument som är utfärdade av myndigheten. Såväl organiseringen av som själva certifieringsverksamheten ska möta de krav som anges i bl.a. CCRA och SOG-IS MRA (se kapitel 5).

Som framgår ovan medför utfärdandet av en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer att motsvarande nationella certifieringsordning, och de förfaranden som tillämpas ska upphöra att ha verkan från den tidpunkt som den europeiska ordningen träder i kraft.

Även när en sådan europeisk ordning införs kan det finnas IKT-produkter, IKT-tjänster och IKT-processer som inte omfattas av denna ordning, vilket innebär att det kan finnas behov av att certifiera produkter och tjänster enligt en annan certifieringsordning och tillhörande förfarande.

Mot bakgrund av att det i utkastet till EUCC anges att ett antal nationella certifieringsordningar, bl.a. den certifieringsordning som tillämpas av FMV/CSEC, avser samma typ eller kategorier av IKT, säkerhetskrav, utvärderingskriterier, utvärderingsmetoder och assuransnivåer för certifiering och evaluering av it-säkerhetsprodukter och skyddsprofiler, föreligger behov av en djupare analys av i vilken utsträckning som det fortsättningsvis finns behov av en nationell ordning för certifiering av it-säkerhet i system och produkter. FMV bör därför få i uppdrag att närmare analysera denna fråga i samverkan med andra berörda myndigheter och övriga berörda aktörer, bl.a. näringslivsorganisationer och företag.

I detta sammanhang ska noteras att utredningen har i uppdrag att även analysera behov av godkännande och/eller krav på certifiering av produkter, tjänster och processer inom nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet. Dessa frågor har som tidigare angetts beröringspunkter med hur man på det nationella planet kan organisera och utforma en verksamhet för cybersäkerhetscertifiering som dels möter kraven i det europeiska ramverket för cybersäkerhetscertifiering och som dels tillgodoser behovet av en samlad nationell ordning för certifiering av IKT-produkter, -tjänster och -processer som inte omfattas av det europeiska ramverket och som samlat kan bedrivas på ett ändamålsenligt och effektivt sätt.

Utredningen kommer att återkomma till denna fråga i slutbetänkandet.

13.4 Inbördes granskning

Av artikel 59 i EU:s cybersäkerhetsakt framgår att de nationella myndigheterna för cybersäkerhetscertifiering ska omfattas av inbördes granskning i syfte att uppnå likvärdiga standarder i hela unionen för EU-försäkringar om överensstämmelse och europeiska cybersäkerhetscertifikat.

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.

Den inbördes granskningen ska omfatta en bedömning

- av om den verksamhet som bedrivs av nationella myndigheter för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat enligt artikel 56.5 a och 56.6 är strikt åtskilda från tillsynsverksamhet enligt artikel 58 och att dessa verksamheter utförs oberoende av varandra,
- 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,
- 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,
- av förfarandena för övervakning, bemyndigande och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse, och
- av om personalen vid de myndigheter eller organ som utfärdar certifikat med assuransnivån ”hög” i enlighet med artikel 56.6 har lämplig sakkunskap.

Den inbördes granskningen ska utföras av kommissionen och minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater. Enisa ska ges möjlighet att delta i granskningen, som ska utföras minst vart femte år.

Kommissionen får anta genomförandeakter med en plan för den inbördes granskningen. I genomförandeakten ska anges kriterier för

sammansättningen av gruppen som ska utföra granskningen, den metod som ska användas, tidsplanen, frekvensen och övriga uppgifter som behövs för granskningen. Kommissionen ska ta hänsyn till synpunkterna från den Europeiska gruppen för cybersäkerhetscertifiering (se nedan) när en genomförandeakt antas. En genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 66.2.

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.

Den föreslagna nationella myndigheten för cybersäkerhetscertifiering, dvs. FMV, kan komma att omfattas av det angivna granskningsförförandet, dvs. bli föremål för inbördes granskning enligt artikel 59. Eftersom granskningen regleras genom bestämmelserna om inbördes granskning i cybersäkerhetsakten krävs därför ingen ytterligare reglering på området.

När det gäller uppgiften att i egenskap av nationell myndighet för cybersäkerhetscertifiering delta i granskningen av andra medlemsstaters myndigheter bör myndigheten ha i uppgift att kunna delta i en sådan granskning. Myndigheten kan behöva samverka med Swedac om granskningen berör ackrediterade organ för bedömning av överensstämmelse.

13.5 Marknadsfrågor

I direktiven anges att utredningen ska även beakta de konsekvenser som bl.a. införandet av det europeiska ramverket för cybersäkerhetscertifiering kan få när det gäller internationell handel med tredjeland samt hur det påverkar erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

Utredningen kan notera att det europeiska ramverket för cybersäkerhetscertifiering är en unionsrättslig författning som är direkt tillämplig i medlemsstaterna. Det innebär att det kommer att finnas en särskild reglering med krav på cybersäkerhet för IKT-produkter, IKT-tjänster och IKT-processer som tillhandhålls på den inre marknaden. Bedömningen av vilken påverkan införandet av detta regelverk kan få på internationell handel, särskilt med tredje land, inne-

fattar komplexa frågeställningar som bl.a. rör regelgivning och marknadspåverkan.

Utredningen kan konstatera att det mot bakgrund av den tid som funnits tillgänglig för utredningsarbetet i denna första del inte funnits förutsättningar eller varit möjligt att genomföra en djupare analys av dessa frågor. Frågorna behandlas dock i viss utsträckning i Kommerskollegiums rapport *The Cyber Effect – the implications of IT security regulation on international trade*[3] (se nedan).

Utredningen bedömer att vad som anges i rapporten i dessa frågor kan utgöra utgångspunkten för fortsatt analys i det fortsatta arbetet. Det finns därför skäl att redan i detta delbetänkande översiktligt redogöra för några av de slutsatser som redovisas i rapporten och som kan belysa vilken påverkan som det europeiska ramverket för cybersäkerhetscertifiering kan ha på internationell handel och handel med tredje land.

13.5.1 Påverkan på internationell handel

I rapporten *The Cyber Effect – the implications of IT security regulation on international trade* framhålls att syftet med denna är att redogöra för konceptet it-säkerhet, beskriva hur it-säkerhet i informations- och kommunikationsteknologi (IKT) kan regleras samt belysa vilken inverkan denna reglering har på produkternas marknadstillträde och internationell handel. I rapporten diskuteras om en ökad harmonisering av regler för it-säkerhet i IKT är möjlig, särskilt mot bakgrund av att befintliga regleringsstrategier främst präglas av nationella intressen och i mindre utsträckning av försök till samordning och internationella åtaganden. I rapporten konstateras att reglering av it-säkerhet i IKT är ett komplext område som inte följer samma struktur och logik som varureglering generellt. Rapporten pekar också på att politiska beslut avseende it-säkerhetsreglering har en betydande påverkan inte endast på säkerhet utan även på internationell handel.

I rapporten framhålls att beslutsfattare och myndigheter som ska ta ställning till it-säkerhetsreglering behöver ha förståelse för att samhällets funktion vilar på ett stort antal strukturer som är sammankopplade och beroende av varandra, och där det är omöjligt att skilja

[3] Kommerskollegiums rapport *The Cyber Effect – the implications of IT security regulation on international trade*, 2018.

cyberrymden från t.ex. sektorer som livsmedel, hälsa och transport. Cyberrymden kan ses som ett tunt nät som går igenom alla sektorer och som gör att sektorerna kan fungera och kommunicera med varandra. Man bör i detta sammanhang uppmärksamma att levnadssätt och sättet att handla varor baseras på globala snarare än på lokala förhållanden, vilket också måste tas i beaktande vid reglering av IKT som tillverkas, säljs och installeras runt om i världen.

I rapporten noteras att det finns flera olika möjligheter som kan att bidra till en höjd it-säkerhet. En metod är att ställa krav på IKT genom lagstiftning. It-säkerhetsregler för IKT skiljer sig dock från annan varureglering eftersom dessa regler inte bara måste beakta hälsa, säkerhet och miljö, utan också samhällets infrastruktur, den personliga integriteten och nationell säkerhet.

I rapporten framhålls att myndigheter och regelgivare i enskilda länder antar egna metoder och strategier för att hantera it-säkerhet. Myndigheter inför ofta specifika, nationella regler som kompletterar, eller som fungerar som ett alternativ till, befintliga internationella standarder. Detta motiveras med att det finns särskilda nationella säkerhetsbehov. Dessa nationella standarder eller certifieringskrav leder till att företag måste genomgå certifieringar i flera länder, vilket leder till ökade kostnader. Vidare framhålls att de åtgärder som myndigheter vidtar när det gäller it-säkerhet karakteriseras av specifika nationella behov med säkerhet som prioritet, snarare än åtgärder som följer internationella standarder och åtaganden om beaktar handel och marknadstillträde. Denna utveckling, där åtgärder för nationell säkerhet prioriteras på bekostnad av handel och varors marknadstillträde, är dock – enligt rapporten – inte förvånande eftersom det får anses naturligt att vilja dölja hemligstämplad eller skyddsvärd information från utomstående. Men konsekvensen av sådana nationella regler, som när det gäller it-säkerhet ofta är icke-transparenta, blir densamma som för reglering inom andra områden, dvs. en fragmentering av regleringar som riskerar att skapa handelshinder. Följden blir att värdet av öppna processer och transparenta regleringar som gör att företag har en möjlighet att påverka regleringar, t.ex. inom standardisering, minskar. Detta påverkar även möjligheten att förstå och jämföra vilka regler som gäller på olika marknader.

I rapporten noteras att myndigheterna kan anta olika strategier för att höja it-säkerheten i produkter. En strategi är att utarbeta tekniska föreskrifter med bindande krav på egenskaper i IKT, vilket i

och för sig kan medföra att tekniska utvecklingen snabbt gör reglerna föråldrade. En annan strategi som används mer utbrett är att ta fram regler för bedömning av överensstämmelse, dvs. hur IKT ska certifieras. Även om det finns internationella standarder och ordningar för cybercertifiering är kraven i dessa relativt generiska. Detta leder till att olika länder tar fram egna nationella krav som kompletterar internationella standarder. Detta innebär att kraven för en och samma IKT-produkt kan skilja sig åt i olika länder, beroende av hur myndigheterna ser på risker och sårbarheter i sitt land. En konsekvens av att nationella särkrav ökar är en risk för tekniska handelshinder.

I rapporten görs noteringen att antalet tekniska handelshinder som rör it-säkerhet och som diskuteras inom Världshandelsorganisationen (WTO) har blivit fler på senare år. Det blir också allt vanligare att ekonomiska sanktioner eller hot om sanktioner, relaterade till it-säkerhet, lyfts upp på förhandlingsbordet när ledare för större länder möts. Denna utveckling är en tydlig signal på att it-säkerhet även blivit en fråga för handelspolitiken. Även om ett antal handelshinder avseende it-säkerhet har diskuterats inom WTO, så har inga av dessa hinder tagits upp till tvistlösning. Enligt rapporten är skälet för detta förmodligen att nationell säkerhet är en känslig och svår fråga att hantera från ett rättsligt perspektiv. Denna situation leder dock till att de företag som möter hinder inte får någon rättelse utan är tvungna att anpassa sina produkter till de nationella kraven.

I rapporten påpekas att även om det inte saknas internationellt samarbete om gemensamma standarder och ordningar som ska bidra till ökad samstämmighet inom it-säkerhet, och som medfört olika länder ömsesidigt godkänner certifikat inom vissa områden är problemet att olika marknader tillämpar dessa standarder olika, bl.a. genom att lägga till egna krav som ett komplement till internationella standarder. Detta innebär att samarbete i och för sig kan bidra till höjd it-säkerhet, men att arbetet inte nödvändigtvis bidrar till en fungerande gränsöverskridande handel med IKT. En fragmenterad global marknad, där olika länder skyddar sig själv genom nationella regler, kan också leda till mindre säkra produkter och tjänster. Detta genom att resurser som skulle ha kunnat användas för god regleringssed som är accepterad och gångbar internationellt används för att ta fram olika nationella särlösningar.

I rapporten konstateras att beslutsfattare har successivt blivit mer medvetna om den ökande fragmenteringen av regler på it-säkerhets-

området och att de inser att situationen kräver kraftiga och skyndsamma åtgärder, vilket medför nya politiska initiativ och förslag på lagstiftning med syfte att öka internationell harmonisering. En ökad internationell harmonisering skulle kunna leda till större öppenhet och transparens, och befrämja internationell handel. Om utformningen av regler för it-säkerhetsregler flyttas från slutna till öppna grupper skulle det ge olika intressenter större insyn i regleringsprocessen och en möjlighet att påverka utfallet. En ökad harmonisering skulle också göra så att företag kunde slippa onödiga kostnader förknippade med anpassning till olika och duplicerande krav på skilda marknader. På detta sätt skulle krav på it-säkerhet också bli mer tillgängliga och lättbegripliga för företagen. Ökad harmonisering skulle därutöver ha potential att sänka kostnaden för samhället och konsumenterna som betalar för it-säkerheten.

I rapporten framhålls att inom EU utgör eIDAS-förordningen (förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden), NIS-direktivet (direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen) och cybersäkerhetsakten politiska initiativ och viktiga rättsakter som påverkar IKT.

I rapporten påpekas att även om cybersäkerhetsakten har som målsättning att bidra till mer harmoniserade ordningar för bedömning av överensstämmelse, dvs. för cybersäkerhetscertifiering av IKT, är samtidigt många it-säkerhetsexperter tveksamma till värdet av omfattande och dyra produktcertifieringar. En certifiering gör nämligen inte en produkt säker, dvs. en certifiering avlägsnar nödvändigtvis inte alla sårbarheter, eftersom riskerna framför allt är knutna till den miljö där IKT används. Omfattande certifieringar kan således generera ett högt marknadsvärde men samtidigt medföra leverantörer och konsumenter får stå för kostnaderna.

I rapporten noteras vidare att produktcertifiering är komplext, tidskrävande och dyrt varför antalet certifieringar är relativt få i förhållande till antalet IKT och produktutvecklingsprocesser som borde genomgå certifiering för att skapa säkerhet i samhället i stort. Som en konsekvens av detta har det skett en förändring av regelstrategier mot att i stället för att säkra själva produkten har fokus skiftat till att säkra den it-infrastruktur där produkten används. I praktiken innebär detta att man ställer krav på de plattformar som används för att skicka information och där IKT används. Detta kan omfatta it-infra-

strukturer inom en viss sektor eller mellan ett antal myndigheter. Detta tillvägagångssätt avskaffar inte behovet av produktreglering men den höjer säkerheten i stort, genom att metoden från första början tar hänsyn till risker som finns och kan kvarstå hos kommersiella produkter trots certifiering. Fördelen med en strategi som fokuserar på it-infrastruktur är att myndigheterna kan hitta ett mer systematiskt och harmoniserat sätt att effektivt adressera it-säkerhet på nationell nivå och samtidigt kunna godta kommersiella varor som är certifierade enligt internationella standarder. På detta sätt finns det förbättrade möjligheter att höja it-säkerheten utan att skapa nya tekniska handelshinder. Eftersom denna metod kräver investeringar i ny infrastruktur är det nödvändigt att utvärdera kostnader och fördelar utifrån sektorsspecifika risker. För att en sådan strategi för it-infrastruktur ska fungera måste produktkraven avseende certifiering baseras på internationella standarder. Om myndigheterna tillämpar eller gör andra regionala standarder bindande, t.ex. inom EU, kan det leda till att företag drabbas av duplicerande och dyra certifieringar, dvs. riskerar handelshinder.

I rapporten framhålls att företag som tillfrågats har betonat att IKT-marknaden är global och att det således krävs internationellt accepterade lösningar för reglering. Representanter för näringslivet har framfört att initiativ som strävar efter harmonisering av regler måste beakta skillnader som finns mellan olika sektorer.

I rapporten framhålls att angivna aspekter motiverar en noggrann analys av nya regelinitiativ avseende it-säkerhet. Den huvudsakliga slutsatsen i rapporten är att det finns ett stort behov att öka kunskapen om it-säkerhet i samhället. Analysen tyder på att det inte är de enskilda handelshindren som nödvändigtvis behöver stå i fokus, utan avsaknaden av tillit för olika strategier för regelgivning som kan reducera onödiga kostnader och medföra ökad säkerhet.

I rapporten framhålls sammanfattningsvis vikten av att beslutsfattare förstår både omfattningen och effekterna av cyberhot, bl.a. de beroendeförhållanden som finns mellan samhällets infrastruktur (nationell säkerhet) och handel (handelspolitik) när man genomför åtgärder för att höja it-säkerheten. För att finna en relevant metod för att reglera it-säkerhet i IKT bör man först analysera möjliga hot (t.ex. konfidentialitet, tillgång, integritet), motiv (t.ex. pengar, makt, ideologi), intressenter, mål (medborgare, företag, statliga sektorn, länder) och verktyg (ransomware- utpressningsprogram/virus, phishing

– nätfiske, tailgating – obehörig passering, DoS attacker-överbelastningsattacker). En sådan undersökning skulle bättre underbygga beslut om vilka åtgärder och krav som är relevanta och försvarbara för att säkra information. Genom att tekniken utvecklas, utvecklas också användarmiljön och de variabler som påverkar it-säkerhet i IKT. Det är därför viktigt att förstå att lagstiftning inom it-säkerhet har mindre effekt än på många andra regleringsområden. Den snabba it-utvecklingen och de ökande cyberhoten leder till att vissa länder kan förbjuda eller begränsa sin import av IKT från andra länder, vilket innebär att länderna sluter sina gränser för handel. Olika länder kan också använda sig av ekonomiska sanktioner eller hot om sanktioner och exportkontrollåtgärder. En avgörande faktor för marknadstillträde och internationell handel med IKT är att öka förtroendet mellan både länder och regelgivare samt för olika regelalternativ.

Utredningen bedömer att det finns skäl att återkomma till dessa frågor även i fortsatta arbete med analys av behovet av certifiering eller godkännande av informations- och kommunikationssystem i säkerhetskänslig verksamhet.

13.5.2 Sveriges medlemskap i CCRA

Utredningen ska enligt direktiven i sitt arbete analysera och beakta de åtaganden som följer av Sveriges medlemskap i bl.a. CCRA. I denna fråga gör utredningen följande bedömning.

När en europeisk ordning för cybersäkerhetscertifiering införs uppkommer frågan om verkan för certifikat som utfärdats eller utfärdas enligt en annan certifieringsordning, t.ex. CCRA, och som inte omfattas av tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och en europeisk ordning för cybersäkerhetscertifiering. I det offentliggjorda utkastet till EUCC lämnas förslag på övergångsregler som ska gälla när denna ordning införs. Som ovan framgår har ett certifikat som utfärdats av en ordning som sedan kommit att omfattas av det europeiska ramverket för cybersäkerhetscertifiering fortsatt verkan till dess certifikatet löper ut. Ett certifikat som utfärdats, t.ex. enligt CCRA, och som inte omfattas av ramverkets tillämpningsområde bör därför äga fortsatt giltighet i enlighet med vad som anges i den ordningen. Utredningen bedömer att en analys av konsekvenserna

av de åtaganden som följer av Sveriges medlemskap i CCRA, när en europeisk ordning för cybersäkerhetscertifiering införs, bör bli föremål för en djupare analys och har inte varit möjlig inom ramen för den utredningstid som stått till förfogande. Utredningen återkommer till denna fråga i sitt slutbetänkande.

14 Konsekvensbeskrivning

14.1 Inledning

I utredningens uppdrag ingår att analysera konsekvenserna av lämnade förslag i enlighet med 14–15 a §§ kommittéförordningen (1998:1474). Eftersom utredningen lämnar författningsförslag ska konsekvensanalysen också göras i enlighet med 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

I utredningsdirektiven anges att utredningen ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredningen föreslå hur dessa ska finansieras. Utredningen ska särskilt ange konsekvenserna för företag i form av kostnader och ökade administrativa bördor samt personella konsekvenser för berörda myndigheter. Vidare ska beaktas de konsekvenser som genomförandet av EU:s cybersäkerhetsakt kan få när det gäller internationell handel med tredje land och erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

I detta kapitel redovisas utredningens bedömning av konsekvenserna av de förslag utredningen lämnar. Förslagen syftar framför allt till att anpassa svensk lagstiftning till bestämmelserna i EU:s cybersäkerhetsakt och säkerställa att unionsrätten får avsedd effekt. EU:s cybersäkerhetsakt är direkt tillämplig i medlemsstaterna. Det ska därför inledningsvis konstateras att de konsekvenser som uppstår för samhället och de aktörer som berörs huvudsakligen är en direkt följd av den bakomliggande EU-akten och inte av utredningens förslag. De konsekvenser som följer av de direkt tillämpliga bestämmelserna i EU:s cybersäkerhetsakt är för närvarande svårbedömda.

I vissa delar går utredningens förslag längre än vad som krävs enligt cybersäkerhetsakten eller uppställer särskilda krav för tillämp-

ningen av bestämmelser i akten. Utredningens bedömning av konsekvenserna av de förslagen redovisas också nedan.

14.2 Utgångspunkter

Det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförandeakter som antas, är unionsrättsliga författningar som är direkt tillämpliga i medlemsstaterna. Vissa bestämmelser i EU:s cybersäkerhetsakt förutsätter att medlemsstaterna inför kompletterande nationell reglering för genomförandet av akten.

Utredningens förslag syftar till att uppfylla kraven i EU:s cybersäkerhetsakt och att bidra till ett ändamålsenlig 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). De författningsbestämmelser som nu föreslås syftar till att komplettera ramverkets bestämmelser så att de – såvitt nu kan bedömas – kan få fullt genomslag.

14.3 De som berörs av förslagen

Förslagen ska bidra till att säkerställa att målsättningen med ramverket uppnås, dvs. bidra till en ökad cybersäkerhet för IKT-produkter, IKT-tjänster och IKT-processer som tillhandahålls på unionsmarknaden.

Utredningens förslag berör framför allt den statliga myndighet som utredningen föreslår ska utses till nationell myndighet för cybersäkerhetscertifiering och de ekonomiska aktörer som utfärdar EU-försäkran om överensstämmelse eller europeiska cybersäkerhetscertifikat eller innehar ett sådant certifikat. Förslagen berör även myndigheter som samverkar med den nationella myndigheten för cybersäkerhetscertifiering samt Kronofogdemyndigheten och domstolar.

Det går dock inte att bedöma hur många fysiska eller juridiska personer som berörs av förslagen i egenskap av ekonomiska aktörer, bl.a. då omfattningen av frivillig eller krav på obligatorisk cybersäkerhetscertifiering för närvarande inte är kända.

Även andra aktörer som använder informations- och kommunikationsteknik kan förväntas beröras av förslagen. Med hänsyn till syftena med regelverket bedöms förslagen i förlängningen även ha en positiv påverkan för sådana myndigheter, företag och konsumenter som inte direkt berörs av förslagen.

14.4 Konsekvenser för myndigheter

Allmänt

Utredningen bedömer 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. Konsekvenserna för den nationella myndigheten för cybersäkerhetscertifiering och övriga berörda aktörer är i huvudsak en följd av införandet av EU:s cybersäkerhetsakt och inte av utredningens förslag. Eftersom det inte går att bedöma i vilken omfattning som berörda aktörer kommer att använda sig av möjligheten till EU-försäkran om överensstämmelse eller utfärda europeiska cybersäkerhetscertifikat påverkar detta 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 tillkommande resurser för vissa grundläggande funktioner hos den nationella myndigheten för cybersäkerhetscertifiering.

Utredningen har vid utformningen av förslagen, bl.a. när det gäller uppgifter för och organisering av den myndigheten tagit hänsyn till de alternativ som kan förväntas vara mest ändamålsenliga och kostnadseffektiva. De förslag till framför allt samverkan och samordning mellan berörda myndigheter som utredningen presenterar bedöms i kostnadsavseende vara marginella.

Konsekvenser av förslaget att utse en nationell myndighet för cybersäkerhetscertifiering

I enlighet med utredningsdirektiven föreslår utredningen att den nationella myndigheten för cybersäkerhetscertifiering organiseras vid en befintlig myndighet. För den föreslagna myndigheten innebär förslaget nya uppgifter och ett utökat ansvar som följer direkt av EU:s cybersäkerhetsakt och de genomförandeakter som kan komma att antas. Myndigheten får uppgifter som rör omvärldsbevakning, samverkan, ansvar för cybersäkerhetscertifiering på högsta assuransnivån och tillsynsansvar över det europeiska ramverket för cybersäkerhetscertifiering. I uppdraget ingår även att representera Sverige i ECCG och därmed delta i framtagandet av nya europeiska certifieringsordningar (genomförandeakter).

För att myndigheten ska kunna fullgöra sina skyldigheter enligt EU:s cybersäkerhetsakt ska berörda aktörer, dvs. den som utfärdar en EU-försäkran om överensstämmelse eller som utfärdar eller innehar europeiska cybersäkerhetscertifikat, lämna uppgifter till myndigheten. Det innebära ett ökat administrativt arbete och därtill hörande kostnader för myndigheten. Som en följd av att myndigheten tilldelas nya befogenheter och sanktionsmöjligheter finns behov av att initialt utbilda personal och ändra vissa arbetsformer. Inledningsvis bedöms dock kostnaderna för detta vara begränsade.

Utredningen föreslår vidare att berörda myndigheter i ökad utsträckning ska samverka i frågor som rör det europeiska ramverket för cybersäkerhetscertifiering. I dag sker samverkan mellan berörda myndigheter huvudsakligen inom ramen för SAMFI-myndigheternas samverkan men också inom ramen för etableringen av det nationella cybersäkerhetscentret som ska ske 2020. Den föreslagna regleringen om ökad samverkan med anledning av införandet av det europeiska ramverket syftar till att tillvarata nationella intressen och effektivisera myndigheternas arbete, bl.a. genom att öka möjligheten till informationsutbyte. Utredningen bedömer att förslaget i denna del inte får några ekonomiska effekter för myndigheterna.

Utredningen föreslår vidare att när den nationella myndigheten för cybersäkerhetscertifiering respektive Swedac utövar tillsyn över ackrediterade organ för bedömning av överensstämmelse ska myndigheterna samordna kontrollen och åtgärderna om de riktar sig mot samma ekonomiska aktör. Förslaget syftar främst till att underlätta

för ekonomiska aktörer och begränsa antalet myndighetskontakter och bedöms inte medföra ekonomiska konsekvenser.

Konsekvenser av den nationella cybersäkerhetscertifieringsmyndighetens befogenheter

Utredningens förslag om kompletterande bestämmelser avseende den nationella myndighetens befogenheter bedöms inte medföra några ekonomiska konsekvenser i sig. Ett tydligt regelverk när det gäller befogenhet kan förväntas leda till att myndigheten utnyttjar sina tilldelade befogenheter i större utsträckning, vilket leder till en effektivare tillsyn, och därigenom även rättvisa konkurrensvillkor. Genom möjligheten att överklaga myndighetens beslut bedömer utredningen att ett fullgott skydd för enskildas rättigheter säkerställs.

Konsekvenser av sanktionsbestämmelser

I artikel 65 i EU:s cybersäkerhetsakt anges att medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av det europeiska ramverket för cybersäkerhetscertifiering och ska vidta alla nödvändiga åtgärder för att se till att bestämmelserna tillämpas. För att den nationella myndigheten för cybersäkerhetscertifiering ska kunna beivra regelöverträdelser innehåller den föreslagna lagen bestämmelser om möjlighet att påföra en ekonomisk aktör en sanktionsavgift vid överträdelser. Förslaget innebär att en avgift ska kunna beslutas oavsett om överträdelsen har skett uppsåtligen eller av oaktsamhet, dvs. avgiftsskyldigheten baseras på strikt ansvar. Att det föreslagna sanktionsavgiftssystemet bygger på strikt ansvar underlättar för myndighetens bedömning i fråga om att ta ut sanktionsavgift. Genom att myndigheterna själva får besluta om sanktionsavgift kan förslaget antas leda till ett effektivare och enklare sanktionsförfarande. Förslaget bedöms ha positiva effekter för myndighetens möjligheter till effektiv tillsyn utan att påverka kostnaderna i någon större utsträckning. Kostnader kan antas tillkomma för delgivning av beslut om sanktionsavgift.

Konsekvenser av bestämmelser om avgifter vid certifiering och tillsyn

Enligt EU:s cybersäkerhetsakt omfattar de nationella cybersäkerhetscertifieringsmyndigheternas uppdrag såväl utfärdande av cybersäkerhetscertifikat enligt artikel 56 som tillsyn enligt artikel 58 över IKT-produkters, -tjänsters och -processers överensstämmelse med kraven i de certifikat som utfärdats inom deras länder.

FMV:s certifieringsverksamhet är i dag både anslags- och avgiftsfinansierad. Motsvarande system bör införas när det gäller finansieringen av den certifieringsverksamhet som den nationella myndigheten för cybersäkerhetscertifiering bedriver enligt EU:s cybersäkerhetsakt.

Utredningen anser vidare att berörda aktörer bör ersätta kostnaden för tillsynsverksamheten. Detta ska ske genom att en tillsynsavgift betalas av enskilda. Tillsynsavgiften ska 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 utfärdare av EU-försäkringar om överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och berörda organ för bedömning av överensstämmelse. Utredningens förslag om att ta ut en avgift av en ekonomisk aktör avser att finansiera tillsynsverksamhetens kostnader. Förslaget bedöms dock inte få någon större påverkan på myndighetens ekonomiska resurser.

Konsekvenser för Försvarets materielverk (FMV)

Utredningen föreslår att Försvarets materielverk (FMV) utses till nationell myndighet för cybersäkerhetscertifiering enligt artikel 58.1 i EU:s cybersäkerhetsakt, vilket medför flera nya uppgifter och ansvarsområden för myndigheten. Vidare föreslås att FMV ska fullgöra uppgifterna enligt artikel 56.5 och 6, vilket innebär delvis nya uppgifter och ansvarsområden.

Kravet i EU:s cybersäkerhetsakt att verksamheten hos de nationella cybersäkerhetscertifieringsmyndigheterna som beviljar cybersäkerhetscertifikat på assuransnivån hög ska vara strikt åtskild från samma myndighets tillsynsverksamhet medför att viss del av verksamheten hos FMV behöver omorganiseras. De nya uppgifterna kan tilldelas den existerande organisationen, men samma personer kan inte bevilja certifikat på assuransnivån hög och sköta tillsynsuppgifter rörande anmälningar om överensstämmelse och bedömnings-

organ. Uppgifterna bedöms dock inte ha några direkta konsekvenser för samarbetet eller arbetsfördelningen med andra myndigheter.

Verksamheten hos FMV respektive CSEC förutsätter planering av organisation och arbetssätt, upprättande av anvisningar för beviljande av certifikat på högsta assuransnivån, process för bemyndigande av organen för bedömning av överensstämmelse och tillsynsorganisation. Vidare krävs informationsspridning, utbildning av personal och samverkan med berörda aktörer. Vissa av uppgifter bedöms kunna lösas genom en omorganisering av resurserna samtidigt som ytterligare resurser måste tillföras.

När det gäller FMV/CSEC:s uppgifter och ansvarsområden för certifieringsverksamheten enligt EU:s cybersäkerhetsakt är det svårt att bedöma omfattningen av verksamheten till följd av den nya regleringen. CSEC:s beredskap att bevilja certifikat på assuransnivå hög bör dock säkerställas. CSEC:s arbete med att driva en nationell certifieringsordning för säkerhet i it-produkter och system är i dag anslagsfinansierad, medan själva certifieringen av it-produkter är avgiftsfinansierad. Kostnaderna för det tillkommande arbetet bedöms initialt bli av mindre omfattning och kan förväntas rymmas inom ramen för redan tilldelat anslag för denna verksamhet. Behovet av personella resurser beror på flera olika faktorer, bl.a. införandet av europeiska certifieringsordningar. Resursbehovet är också beroende av i vilken omfattning berörda aktörer ansöker om cybersäkerhetscertifikat och antalet organ för bedömning av överensstämmelse.

Tillsynsfunktionen vid FMV ska enligt EU:s cybersäkerhetsakt ha tillräckliga resurser för att på ett effektivt sätt kunna utföra tillsyn och uppnå målen med det europeiska ramverket för cybersäkerhetscertifiering. Detta innebär att tillsynsfunktionen ska ha de personella, tekniska och ekonomiska resurser som behöves för att på ett effektivt sätt kunna utföra sin uppgift. Som ovan anges bygger ramverket för cybersäkerhetscertifiering på en europeisk ordning för cybersäkerhetscertifiering som ännu inte fastställts, vilket medför betydande svårigheter att bedöma organisering och behovet av resurser för tillsynsfunktionen. Ramverket ger samtidigt utrymme för att reglera om cybersäkerhetscertifieringen ska vara obligatorisk eller frivillig, vilket innebär svårigheter att bedöma omfattningen av verksamheten och resursbehovet.

Sammantaget bedöms FMV:s uppgifter som nationell myndighet för cybersäkerhetscertifiering inledningsvis behöva resursförstärk-

ning, främst i form av personalförstärkning. Myndigheten uppger att tillkommande uppgifter och ansvarsområden som nationell myndighet för cybersäkerhetscertifiering medför ett ökat personalbehov som beräknas initialt uppgå till 10–12 heltidsanställda, främst för administrativa, juridiska och tekniska uppgifter. Vidare har myndigheten angett behov av lokaler och administrativt stöd för denna verksamhet. Myndigheten har dock inte angett någon kostnadsberäkning för angivet resursbehov.

Frågan om ytterligare resurser bör fortlöpande övervägas när utvecklingen av den europeiska cybersäkerhetscertifieringen kan överblickas.

Styrelsen för ackreditering och teknisk kontroll (Swedac)

Styrelsen för ackreditering och teknisk kontroll (Swedac) är nationellt ackrediteringsorgan. Ett organ som vill bli ackrediterat måste lämna in en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning samt föreskrifter som Swedac meddelat. Ackrediteringsverksamheten vid Swedac finansieras av kundernas avgifter, som ska täcka samtliga kostnader för ackrediteringen. Frågan om behov av ytterligare resurser för Swedac med anledning av införandet av det europeiska ramverket och åtföljande krav och behov av ackreditering är på motsvarande sätt som anges ovan svår att i dagsläget bedöma. Eftersom verksamheten när det gäller ackreditering är avgiftsfinansierad bör denna verksamhet inte kräva ytterligare finansiella resurser. Jämfört med de uppgifter myndigheten utför i dag skiljer sig ansvaret enligt EU:s cybersäkerhetsakt åt endast i mindre omfattning. Förändringarna följer direkt av förordningen och beror inte på utredningens förslag.

Kronofogdemyndigheten

Bestämmelserna om sanktionsavgifter kan komma att öka antalet ärenden hos Kronofogdemyndigheten något. Även förslaget om att myndigheten 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.

Domstolar

Utredningens förslag i processuella frågor och om överklagande av beslut som meddelas av organ för bedömning av överensstämmelse och av myndigheten för cybersäkerhetscertifiering innebär en ny reglering. 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.

De befogenheter som följer av EU:s cybersäkerhetsakt innebär att tillsynsfunktionen hos den nationella myndigheten för cybersäkerhetscertifiering får besluta om åtgärder som i vissa fall är ingripande för enskilda. De beslut som myndigheten fattar med stöd av den nya lagen är bl.a. beslut om förelägganden, förbud eller om återkallelse av ett certifikat. Utredningen bedömer att sådana beslut kan antas komma att leda till överklaganden av besluten, i vart fall innan vägledande praxis etableras på området. En viss måltillströmning till allmän förvaltningsdomstol kan därför väntas. Omfattningen av måltillströmningen är dock svår att uppskatta. Även mål gällande sanktionsavgifter kan förväntas överklagas. Utredningens förslag innebär att den initiala prövningen av om sanktionsavgift ska utgå ska göras av den nationella myndigheten för cybersäkerhetscertifiering. Det är rimligt att anta att antalet överklagade beslut om sanktionsavgift kommer att medföra en viss måltillströmming till domstolarna, men även här är omfattningen svår att bedöma.

Sammantaget bedöms utredningens förslag innebära en måltillströmning i de allmänna förvaltningsdomstolarna och därigenom något ökade kostnader. Kostnadsökningen bör finansieras genom ökade anslag i den mån den inte ryms inom de befintliga.

Konsekvenser för näringslivet och företag

Allmänt

Eftersom det europeiska ramverket för cybersäkerhetscertifiering är under införande är det svårt att bedöma några omedelbara konsekvenser för näringslivet och företagen av detta regelsystem och de nationella kompletterande regler som nu föreslås, bl.a. mot bakgrund av att det ännu inte fastställts någon europeisk ordning för cybersäkerhetscertifiering. På sikt kan dock införandet av ramverket komma att påverka såväl företag som tillverkar eller levererar angivna produkter och tjänster som företag som använder sig av dessa.

De aktörer som ansöker om europeisk cybersäkerhetscertifiering kan komma att variera i antal beroende på utvecklingen av de europeiska certifieringsordningarna. Dessa kan komma att inkludera bl.a. tillverkare, importörer eller användarorganisationer för olika grupper av IKT-produkter, leverantörer av molntjänster, mjukvaruutvecklare och leverantörer av IKT-infrastruktur. Såväl tillverkare som leverantörer kan vara belägna i Sverige, annan medlemsstat eller tredje land.

Antalet företag och därmed de totala kostnaderna för företag som kommer att ha sina IKT-produkter, -tjänster och -processer certifierade i enlighet det europeiska ramverket för cybersäkerhetscertifiering kan därför för närvarande inte uppskattas. Även en bedömning av behovet av och efterfrågan på cybersäkerhetscertifierad IKT-produkter, -tjänster och-processer är svår att göra.

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. De föreslagna bestämmelserna 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.

Förslaget om att utse en nationell myndighet för cybersäkerhetscertifiering med ansvar för uppgifterna enligt EU:s cybersäkerhetsakt i stället för att ansvaret fördelas på flera myndigheter bedöms både förenkla och begränsa de ekonomiska aktörernas kontakter med myndigheter.

Förslaget om att berörda myndigheter så långt det är möjligt ska samverka när det berör frågor om cybersäkerhetscertifiering för-

väntas ha positiva effekter för de ekonomiska aktörerna. De ekonomiska aktörerna gynnas av att myndigheterna i större utsträckning kan lämna information mellan sig och samverka runt kontroller. Det kan antas vara särskilt positivt för mindre företag som inte har samma resurser att lägga på den administrativa delen av verksamheten som större aktörer.

Konsekvenser av sanktionsbestämmelser

Utredningens förslag om sanktionsbestämmelser ger den nationella myndigheten för cybersäkerhetscertifiering möjlighet att besluta om sanktionsavgifter för överträdelse av regelsystemet. För ekonomiska aktörer som följer gällande krav leder förslaget inte till några ökade kostnader. För de aktörer som inte följer gällande regler innebär förslaget ekonomiska konsekvenser och kan medföra ökade kostnader eftersom sanktionsavgifter ska kunna tas ut utan krav på uppsåt eller oaktsamhet. Det föreslås ingen begränsning av storleken på sanktionsavgifterna i förhållande till den ekonomiska aktörens årsomsättning vilket kan leda till att mindre aktörer riskerar relativt sett högre avgifter.

Förslaget om sanktionsavgift tydliggör för ekonomiska aktörer vilka sanktioner som kan bli aktuella vid överträdelser och under vilka förutsättningar avgift kan beslutas. Eftersom en sanktionsavgift kan uppgå till höga belopp beroende på bl.a. överträdelsens allvar kan förslaget även förväntas leda till en bättre regelefterlevnad. Detta stärker på sikt företagens konkurrenskraft och skapar bättre och mer rättvisa spelregler för företagandet.

Konsekvenser för konsumenter och andra användare

På motsvarande sätt som det föreligger svårigheter att bedöma konsekvenserna av införandet av europeiska ramverket för cybersäkerhetscertifiering för företagen är det förenat med betydande osäkerhet att bedöma vilka konsekvenser, såväl ekonomiska som andra sådana, som det kan ha för enskilda och större konsumentgrupper. Cybersäkerhetscertifiering är förenat med kostnader varför cybersäkerhetscertifierade konsumentprodukter och -tjänster kan antas komma att avspegla sig i priset på sådana produkter och tjänster.

Detta ska dock vägas mot de kostnader som kan uppkomma på grund av brister i säkerheten i dessa produkter och tjänster.

14.5 Konsekvenser för samhället

Syftet med det europeiska ramverket för cybersäkerhetscertifiering är att förbättra medborgarnas och företagens cybersäkerhet. EU:s cybersäkerhetsakt 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.

14.6 Konsekvenser för internationell handel med tredje land

I avsnitt 13.5 redogör utredningen för analys och slutsatser som det europeiska ramverket för cybersäkerhetscertifiering kan få för internationell handel med tredje land samt hur det påverkar erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

Utredningen lämnar en närmare analys av dessa frågor i slutbetänkandet.

14.7 Övriga konsekvenser

Följande områden berörs inte av förslagen (15 § kommittéförordningen):

- 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 som behöver redovisas i detta sammanhang.

15 Författningskommentar

15.1 Förslaget 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.

Övervägandena finns i avsnitt 6.3.

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 läsas fristående från den. Hänvisningen till EU:s cybersäkerhetsakt är dynamisk. Det innebär att hänvisningen avser cybersäkerhetsakten i den vid varje tidpunkt gällande lydelsen. På det sättet säkerställs att ändringar i cybersäkerhetsakten får genomslag i lagen och att den nationella rättstillämpningen vid varje tid överensstämmer med kraven i akten.

Av *andra stycket* framgår upplysningsvis att termer och uttryck i lagen har samma betydelse som i EU:s cybersäkerhetsakt. En lista med definitioner finns i artikel 2 i cybersäkerhetsakten.

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.

Övervägandena finns i kapitel 8.

Medlemsstaterna ska enligt artikel 58.1 i EU:s cybersäkerhetsakt utse en eller flera nationella myndigheter för cybersäkerhetscertifiering. Myndigheternas uppgifter som rör cybersäkerhetscertifiering framgår i huvudsak av artiklarna 53.4, 56.5–7, 58.9 och 62.2. Nationella myndigheter för cybersäkerhetscertifiering har vidare ansvar för att kontrollera och övervaka efterlevnaden av cybersäkerhetsakten och de genomförandeakter som kan komma att antas med stöd av den (tillsyn). Tillsynsuppgifterna följer av artikel 58.7. Det kan tilläggas att i uppgifterna ingår att handlägga inkomna klagomål enligt artiklarna 58.7 f och 63.

Av artikel 63.1 i EU:s cybersäkerhetsakt följer att fysiska och juridiska personer ska ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat och till den berörda nationella myndigheten för cybersäkerhetscertifiering i de fall klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse enligt artikel 56.6.

I paragrafen anges att regeringen ska utse en nationell myndighet för cybersäkerhetscertifiering.

Av *första punkten* framgår att den nationella myndighet för cybersäkerhetscertifiering som utses av regeringen ska fullgöra de uppgifter som följer av EU:s cybersäkerhetsakt.

Med stöd av *andra punkten* ska myndigheten även utöva tillsyn över den nya lagen och föreskrifter som har meddelas med stöd av lagen.

Ackreditering av organ för bedömning av överensstämmelse

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.

Övervägandena finns i avsnitt 10.5.

I artikel 60.1 i EU:s cybersäkerhetsakt anges att organ 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 EU:s cybersäkerhetsakt och bilagan till akten. I punkten 19 i bilagan anges vidare att organen för bedömning av överensstämmelse ska uppfylla de krav som anges i relevant standard som harmoniserats enligt förordning (EG) nr 765/2008.

Bestämmelsen i *första 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.

Av artikel 60.2 i EU:s cybersäkerhetsakt följer att om ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artiklarna 56.5 a och 56.6 ska certifieringsorganet vid denna nationella myndighet ackrediteras som ett organ för bedömning av överensstämmelse enligt artikel 60.1.

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.

Med stöd av bestämmelsen i *andra stycket* blir det möjligt 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.

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.

Övervägandena finns i avsnitt 9.3.

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 andra föreskrifter som kompletterar lagen följs.

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.

Övervägandena finns i avsnitt 9.2.

I artikel 58.8 i EU:s cybersäkerhetsakt anges ett antal minimibefogenheter som den nationella myndigheten för cybersäkerhetscertifiering ska ha vid utövandet av sin tillsyn. Merparten av dessa bestämmelser har s.k. direkt effekt och kräver därför inte kompletterande nationell reglering.

Enligt artikel 58.8 a i EU:s cybersäkerhetsakt får varje nationell myndighet 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.

I artikel 58.8 b i EU:s cybersäkerhetsakt ges den nationella myndigheten för cybersäkerhetscertifiering rätt att genomföra undersökningar för att kontrollera att utfärdare av en EU-försäkran om överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och organ för bedömning av överensstämmelse fullgör sina skyldigheter enligt det europeiska ramverket för cybersäkerhetscertifiering.

I artikel 58.8 c i EU:s cybersäkerhetsakt anges att varje nationell myndighet för cybersäkerhetscertifiering ska vidta lämpliga åtgärder, i enlighet med nationell rätt, för att säkerställa att utfärdare av en EU-försäkran om överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och organ för bedömning av överensstämmelse uppfyller kraven i EU:s cybersäkerhetsakt eller en europeisk ordning för cybersäkerhetscertifiering.

I artikel 58.8 d i EU:s cybersäkerhetsakt ges den nationella myndigheten för cybersäkerhetscertifiering rätt att i samband med en undersökning även få tillgång till alla lokaler hos innehavare av ett europeiskt cybersäkerhetscertifikat eller organ för bedömning av överensstämmelse i syfte att genomföra utredningar i enlighet med unionsrätten eller medlemsstaternas processrätt. Rätten att få tillgång till en lokal för undersökning och kontroll på plats hos en berörd aktör gäller dock inte utfärdare av en EU-försäkran om överensstämmelse. Enligt utredningens mening bör rätten till tillträde till lokal inte gälla om lokalen utgör en bostad.

Genom paragrafens *första och andra stycke* kompletteras artikel 58.8 c i EU:s cybersäkerhetsakt. Utredningen anser att föreslagen möjlighet för den nationella myndigheten för cybersäkerhetscertifiering att besluta nödvändiga förelägganden, förenade med vite, utgör lämpliga nationella åtgärder för att säkerställa efterlevnad av regelverket. 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 fri-

villigt lämna information eller rätta till bristerna och således efterkomma myndighetens påpekanden. Om bristerna i efterlevnaden av regelverket bedöms som allvarliga kan det bli aktuellt att meddela ett åtgärdsföreläggande vid äventyr av vite. Befogenheten att besluta förelägganden innefattar även förbudsföreläggande.

Av *andra stycket* följer att den nationella myndigheten för cybersäkerhetscertifiering även har möjlighet att vitesförelägga en enskild att lämna företräde till en lokal. Det är alltså myndigheten som avgör i vilka fall ett föreläggande ska förenas med vite. Det bör dock endast ske när det kan befaras att den det gäller inte kommer att följa beslutet att lämna uppgifter eller frivilligt medverka till en kontroll på platsen.

Den nationella myndigheten för cybersäkerhetscertifiering har möjlighet att besluta om att ett förfarande eller verksamhet inte får fortsätta. Det kan i dessa fall finnas skäl för myndigheten att förordna att beslutet ska gälla omedelbart, t.ex. för att förhindra eller minska sårbarheter och risken för skador. En uttrycklig bestämmelse om rätten att bestämma att ett myndighetsbeslut ska gälla omedelbart behöver inte införas (se 35 § förvaltningslagen och avsnitt 9.2.5).

I *tredje stycket* anges att den nationella myndigheten för cybersäkerhetscertifiering kan få biträde av Kronofogdemyndigheten för att få tillgång till en lokal för att kunna kontrollera handlingar, utrustning och verksamheten på plats. Myndigheten måste då begära handräckning av Kronofogdemyndigheten för att vid behov få tillträde till ett utrymme. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

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.

Överväganden finns i avsnitt 9.4.

Av artikel 58.8 e i EU:s cybersäkerhetsakt framgår att en nationell myndighet för cybersäkerhetscertifiering får i enlighet med nationell rätt återkalla europeiska cybersäkerhetscertifikat som utfärdats av en

myndighet för cybersäkerhetscertifiering eller av ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6, om sådana certifikat inte uppfyller kraven i förordningen eller en europeisk ordning för cybersäkerhetscertifiering.

Paragrafen, som anger förutsättningarna för att kunna återkalla angivna certifikat, kompletterar artikel 58.8 e i EU:s cybersäkerhetsakt.

Av paragrafen framgår att den nationella myndigheten för cybersäkerhetscertifiering får återkalla europeiska cybersäkerhetscertifikat när de förutsättningar som anges i artikel 58.8 e föreligger. En sådan återkallelse förutsätter att myndigheten, i enlighet med förvaltningslagen, fattar ett beslut.

Om cybersäkerhetscertifikatet avser en IKT-produkt, IKT-tjänst eller IKT-process som omfattas av en obligatorisk cybersäkerhetscertifiering medför beslutet om återkallelse att produkten eller tjänsten eller processen inte längre får tillhandahållas på den inre marknaden som en cybersäkerhetscertifierad IKT-produkt, IKT-tjänst eller IKT-process enligt EU:s cybersäkerhetsakt och en europeisk ordning för cybersäkerhetscertifiering.

Om det är fråga om återkallelse av ett frivilligt cybersäkerhetscertifikat kan produkten eller tjänsten eller processen fortsatt tillhandahållas på denna marknad under förutsättning att tillverkaren eller leverantören tar bort all märkning och vidtar de övriga åtgärder som krävs för att säkerställa att en köpare eller nyttjare av produkten eller tjänsten eller processen inte missleds att tro att produkten eller tjänsten har ett giltigt cybersäkerhetscertifierad enligt EU:s cybersäkerhetsakt och en europeisk ordning för cybersäkerhetscertifiering.

En tillverkare eller leverantör som i strid mot angivna bestämmelser ändå tillhandhåller en IKT-produkt, IKT-tjänst eller IKT-process kan göra sig skyldig till överträdelse av regelverket och därför påföras en sanktionsavgift enligt 7 §.

7 § Den nationella myndigheten för cybersäkerhetscertifiering ska ta ut en sanktionsavgift av den som

1. utfärdar en EU-försäkran om överensstämmelse 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 europeiska 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.

Överväganden finns i avsnitt 9.5.4–8.

Enligt artikel 65 i EU:s cybersäkerhetsakt ska medlemsstaterna fastställa regler om sanktioner för överträdelser av bestämmelserna i förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

I paragrafen anges de överträdelser av regelverket som kan föranleda att en sanktionsavgift ska påföras den som gjort sig skyldig till överträdelsen. Det krävs inte att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen. Det innebär att det föreligger ett strikt ansvar för visade överträdelser. Av 9 § framgår att den nationella myndigheten för cybersäkerhetscertifiering ska beakta olika försvårande och förmildrande omständigheter vid prövningen av avgiftens storlek.

Enligt *punkten 1* kan den som utfärdar en EU-försäkran om överensstämmelse enligt artikel 53.2 utan att fastställda krav på cybersäkerhet i EU:s cybersäkerhetsakt och motsvarande europeisk ordning för cybersäkerhetscertifiering är uppfyllda påföras en sanktionsavgift.

I *punkten 2* anges att den som lämnar oriktiga eller ofullständiga uppgifter vid ansökan om cybersäkerhetscertifieringen enligt artikel 56.7 i EU:s cybersäkerhetsakt kan påföras en sanktionsavgift. En sådan avgift bör dock inte påföras om uppgifterna är av mindre betydelse för prövningen och bedömningen av överensstämmelse. Det är först när den felaktiga uppgiften eller utlämnandet av uppgiften eller informationen riskerar att medföra en felaktig bedömning av överensstämmelsen med bl.a. de säkerhetskrav som gäller för bedömningen som en sanktionsavgift kan bli aktuell.

Av *punkten 3* följer att den som 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 kan påföras en sanktionsavgift. Sådan information ska delges skyndsamt i de fall en sårbarhet kan drabba tredje part. När en underlåtenhet att informera om sårbarheter och oriktigheter bör föranleda en sanktionsavgift måste bedömas från fall till fall. Det är först när underlåtenheten ökar risken för sårbarhet eller skada som avgiften bör tas ut.

I *punkten 4* anges att den som utfärdat en EU-försäkran om överensstämmelse eller som innehar ett cybersäkerhetscertifikat och som underlåter att lämna kompletterande säkerhetsinformation enligt artikel 55 kan påföras en sanktionsavgift. På motsvarande sätt som enligt punkten 4 bör avgiften bara tas ut när det föreligger en ökad risk för sårbarhet eller skada.

Av *punkten 5* följer att den som bryter mot villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat samt villkor för inskränkning eller utvidgning av tillämpningsområdet för certifiering enligt regelsystem kan påföras en sanktionsavgift.

Av *punkten 6* framgår att den som överträder ett förbud som meddelats med stöd av 4 § i lagen kan påföras en sanktionsavgift. Denna bestämmelse anger att även lagens bestämmelser och de föreskrifter som meddelas med stöd av lagen utgör viktiga handlingsregler för ett effektivt genomförande av det europeiska ramverket för cybersäkerhetscertifiering.

I *punkten 7* anges att den som använder ett europeiskt cybersäkerhetscertifikat som blivit återkallat enligt artikel 58.8 e ska påföras en sanktionsavgift. Det är viktigt att respekten för regelsystemet upprätthålls och den som fortsatt använder ett cybersäkerhetscertifikat som blivit återkallat riskerar att tilliten och förtroendet för utfärdade certifikat urholkas. I dessa fall torde förmildrande eller ursäktliga omständigheter vara mer sällsynta varför utrymmet för att efterge eller jämka en avgift är mer begränsat.

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

Övervägandena finns i avsnitt 9.5.9.

I paragrafen fastställs minimi- och maxbelopp för sanktionsavgift. Hur avgiften ska bestämmas i det enskilda fallet regleras i 9 §. Den nationella myndigheten för cybersäkerhetscertifiering beslutar om sanktionsavgiftens storlek.

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

Övervägandena finns i avsnitt 9.5.10.

I paragrafen regleras vilka omständigheter som särskilt ska beaktas när den nationella myndigheten för cybersäkerhetscertifiering bestämmer sanktionsavgiftens storlek. Av paragrafen framgår att särskild hänsyn ska tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den avgiftsskyldige tidigare begått en överträdelse och de kostnader som den avgiftsskyldige undvikit till följd av överträdelsen. En försvårande omständighet vid bedömningen av skadan eller risken för skada är om överträdelsen medför sårbarhet eller risk för skada på bl.a. samhällsviktig verksamhet och/eller säkerhetskänslig verksamhet. Även det förhållandet att överträdelsen medför skada eller risk för skada hos större konsumentgrupper bör beaktas vid bedömningen av avgiftens storlek.

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.

Övervägandena finns i avsnitt 9.5.10.

Paragrafen innehåller en bestämmelse om nedsättning av en sanktionsavgift eller att avstå från att ta ut avgiften.

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.

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.

Övervägandena finns i avsnitt 9.5.11.

Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner.

Om ett 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. En överträdelse kan bli föremål för både åtgärdsföreläggande vid äventyr av vite, så länge ingen ansökan om utdömande av vitet görs, och sanktionsavgift.

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.

Övervägandena finns i avsnitt 9.5.12.

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

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.

Övervägandena finns i avsnitt 9.5.12.

Paragrafen innehåller bestämmelser om betalning och indrivning av sanktionsavgifter.

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.

Övervägandena finns i avsnitt 9.5.12.

Paragrafen innehåller en bestämmelse om när en beslutad sanktionsavgift inte längre behöver betalas.

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).

Övervägandena finns i avsnitt 12.5.

Paragrafen innehåller bestämmelser om tystnadsplikt för den som befattat sig med ett ärende som gäller cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Det kan förekomma att uppgifter i ett ärende om europeisk cybersäkerhetscertifiering hanteras av personer utanför det allmännas verksamhet som inte omfattas av regleringen i OSL. Vissa organ för bedömning av överensstämmelse kan nämligen vara organiserade i privaträttsliga former.

Tystnadsplikten innebär enligt *första stycket* att sådana personer 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 upplysningsbestämmelse om detta.

I *tredje stycket* finns en upplysning om att OSL tillämpas i stället för första styckets regler om tystnadsplikt när det gäller den allmänna verksamhet som bl.a. nationella myndigheter och offentliga organ för bedömning av överensstämmelse bedriver.

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 föreskrifter om avgiftssystemets utformning enligt första stycket.

Övervägandena finns i avsnitt 8.5.

Paragrafen gör det möjligt att införa ett avgiftssystem för att finansiera verksamheterna vid den nationella myndigheten för cybersäkerhetscertifiering. Avgiftsfinansieringen är främst avsedd att ersätta kostnader som uppkommer i samband med att myndigheten utför tillsyn och certifiering. Den nationella myndigheten för cybersäkerhetscertifiering ges således möjlighet att begära ersättning för kostnaderna för utförd kontrollåtgärd från ekonomiska aktörer. Avgifter får tas ut för tjänster som myndigheten tillhandahåller i sin certifieringsverksamhet samt av dem som prövas eller är föremål för tillsynsåtgärd. Möjligheten att ta ut avgift bör omfatta alla berörda utfärdare av EU-försäkringar om överensstämmelse respektive europeiska cybersäkerhetscertifikat samt innehavare av europeiska cybersäkerhetscertifikat. Den ska gälla de verksamheter som den nationella cybersäkerhetscertifieringsmyndigheten bedriver enligt EU:s cybersäkerhetsakt och den nya lagen.

I det *tredje stycket* bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela närmare bestämmelser om avgiftssystemets utformning.

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.

Övervägandena finns i avsnitt 11.3.

I paragrafen finns en bestämmelse som föreskriver en skyldighet för privata organ för bedömning av överensstämmelse att ompröva ett beslut när det är uppenbart oriktigt på grund av nya omständigheter eller av någon annan anledning. Bestämmelsen är utformad med ledning av motsvarande bestämmelser i förvaltningslagen.

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.

Övervägandena finns i avsnitt 11.4.3.

I paragrafen regleras rätten att överklaga beslut av den nationella myndigheten för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse. Detta gäller även beslut av privata organ för bedömning av överensstämmelse. I fråga om förfarandet vid överklagande av de privata kontrollorganens beslut finns bestämmelser i lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter.

Klagoberättigade är var och en som beslutet har gått emot.

Ikraftträdande

Artiklarna 58, 60, 61, 63, 64 och 65 i EU:s cybersäkerhetsakt ska tillämpas från och med den 28 juni 2021. Denna lag bör därför gälla från samma tidpunkt.

Referenser

Offentliga tryck

Propositioner och skrivelser

Prop. 2018/19:150, *Skärpta åtgärder mot penningtvätt och finansiering av terrorism*.

Prop. 2017/18:235, *Följdändringar till ny förvaltningslag*.

Prop. 2017/18:232, *Brottsdatalag*.

Prop. 2017/18:205, *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

Prop. 2017/18:89, *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*.

Prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*.

Prop. 2015/16:72, *Kompletterande bestämmelser till EU:s förordning om elektronisk identifiering*.

Prop. 2014/15:109, *Försvarspolitisk inriktning – Sveriges försvar 2016–2020*.

Prop. 2012/13:192, *Sekretess i det internationella samarbetet*.

Prop. 2012/13:143, *Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna*.

Prop. 2010/11:80, *Ny lag om ackreditering och teknisk kontroll*.

Prop. 2008/2009:15, *Offentlighets- och sekretesslag*.

Prop. 2006/07:6, *Kompletterande bestämmelser till EG-förordningen om konsumentskyddssamarbete*.

Prop. 2002/03:139, *Reformerade regler för bank- och finansieringsrörelse*.

Prop. 1994/95:112, *Utrikessekretess m.m.*

Prop. 1981/82:142, *om ändring i brottsbalken (ekonomiska sanktioner vid brott i näringsverksamhet)*.

Prop. 1979/80:2, *med förslag till sekretesslag m.m.*

Skr. 2016/17:213, *Nationell strategi för samhällets informations- och cybersäkerhet*.

Skr. 2009/10:79, *En tydlig, rättssäker och effektiv tillsyn*.

Lagrådsremisser

Regeringens lagrådsremiss *En anpassning av bestämmelser om kontroll i livsmedelskedjan till EU:s nya kontrollförordning* (2020-07-02).

Statens offentliga utredningar

SOU 2018:82: *Kompletteringar till den nya säkerhetsskyddslagen*.

SOU 2017:36: *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

SOU 2015:25: *En ny säkerhetsskyddslag*.

SOU 2015:23: *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*.

SOU 2014:83: *Sanktionsväxling – effektivare sanktioner på exportkontrollområdet*.

SOU 2013:38: *Vad bör straffas?*

SOU 2010:25: *Översyn av verksamhet och organisation på informationssäkerhetsområdet*.

SOU 2009:71: *EU, Sverige och den inre marknaden – En översyn av horisontella bestämmelser inom varu- och tjänsteområdet*.

SOU 2007:96: *Avgifter*.

SOU 2002:14: *Statlig tillsyn – Granskning på medborgarnas uppdrag*.

SOU 1997:57: *I medborgarnas tjänst*.

Departementspromemorior

Ds 2019:8: *Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*.

Ds 2017:66: *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*.

Rapporter

MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten, och Säkerhetspolisen (mars 2020): *Samlad informations- och cybersäkerhetshandlingsplan 2019–2022*.

Kommerskollegiums rapport (2018): *The Cyber Effect – the implications of IT security regulation on international trade*, uppdaterad 2019-09-25.

Riksrevisionens granskningsrapport RiR 2016:8 (maj 2016): *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerheten i staten*.

MSB (mars 2016): *Nationell handlingsplan för samhällets informationssäkerhet*, Slutrapport.

Riksrevisionen granskningsrapport RIR 2014:23 (november 2014): *Informationssäkerheten i den civila statsförvaltningen*.

EU-institutioners dokument

Bilagor till Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén, Kommissionens arbetsprogram 2020: *En ambitiösare union*, COM(2020) 37 final, 2020-01-29.

Europeiska kommissionen: *Förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum*, COM(2018) 630 final, 2018-09-12.

Gemensam förklaring från Europeiska rådets ordförande, Europeiska kommissionens ordförande och Nordatlantiska fördragsorganisationens generalsekreterare, 2016-07-08 och 2018-07-10.

Rådets slutsatser *om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser*, 10085/18, 2018-06-26.

Europeiska kommissionen: *Förslag till Europaparlamentets och rådets förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden*, COM(2018) 225 final, 2018-04-17.

Europeiska unionens råd: *Handlingsplan för genomförandet av rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*, 15748/17, 2017-12-12.

Europeiska unionens råd: *Slutrapport om den sjunde omgången av ömsesidiga utvärderingar om det praktiska genomförandet och verkan av europeisk politik för förebyggande och bekämpning av it-brottslighet*, 12711/1/17 REV 1, 2017-10-09.

Europeiska ekonomiska och sociala kommittén (mars 2018): *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*.

Europeiska unionens råd: *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17, 2017-10-09.

Europeiska kommissionen: *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final, 2017-09-13.

Europeiska kommissionen (september 2017): *Europeans' attitudes towards cybersecurity*, särskild Eurobarometer 464a.

Europeiska kommissionen/Europeiska utrikestjänsten: *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*, JOIN(2017) 450 final, 2017-09-13.

Europeiska unionens råd: *Slutsatser om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet*, 9916/17, 2017-06-07.

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén (KOM(2017) 228 slutlig) *om halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden: En ansluten digital inre marknad för alla*.

Europeiska kommissionen/Europeiska utrikestjänsten: *Gemensam ram för att motverka hybridhot – Europeiska unionens insatser*, JOIN(2016) 18 final, 2016-04-06.

Europeiska unionens råd: *EU cybersecurity roadmap*, 8901/17, 2017-05-11.

Gemensamt meddelande till Europaparlamentet och rådet (JOIN(2017) 450 slutlig): *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*.

Europeiska unionens råds slutsatser den 15 november 2016 (doknr 13967/1/16 REV 1) *om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch*.

Europeiska kommissionen: *En strategi för en inre digital marknad i Europa*, COM(2015) 192 final, 2015-05-06.

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén (KOM(2016) 410 slutlig): *Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch*.

Europeiska kommissionen (den 28 april 2015): *Europeiska säkerhetsagendan*, COM(2015) 185 final.

Europeiska unionens råd: *Rådets slutsatser om cyberdiplomati*, 6122/15, 2015-02-11.

Gemensamt meddelande från Europeiska kommissionen och Europeiska avdelningen för yttre åtgärder (JOIN(2013) 1 slutlig): *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd*.

Meddelande från Kommissionen till Europaparlament och rådet (KOM(2009) 277): *Förvaltning av Internet – framtida åtgärder*.

Övriga handlingar

ENISA (december 2019): *Standardisation in support of the cybersecurity certification*.

ENISA (januari 2019): *Threat Landscape Report 2018, 15 Top Cyberthreats and Trends*, final version 1.0, ETL 2018.

Europeiska revisionsrätten (mars 2019): *Utmaningar för en ändamålsenlig EU politik för cybersäkerhet*, Briefingdokument.

T. Renard och A. Barrinha: Europeiska säkerhets- och försvarsakademin: *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 2018-11-23.

Europaparlamentets utredningstjänst (september 2018): *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643.

NIS Cooperation Group (2018): *Cybersecurity Incident Taxonomy*, 2018-04.

Europol (2017): *Internet Organised Crime Threat Assessment 2017*.

ENISA (september 2017): *Overview of cybersecurity and related terminology*, version 1.

Cybersecurity law overview – a report by Mannheimer Swartling, april 2017.

Europeiska cybersäkerhetsorganisationen (Ecso, juni 2016): *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*.

ENISA (december 2015): *Definition of Cybersecurity: Gaps and overlaps in standardization*, version 1.0.

SIS: *Terminologi för informationssäkerhet*, teknisk rapport SIS-TR 50:2015, 2015-10-27.

ENISA (december 2014): *Security Guide for ICT Procurement: ICT Procurement Security Guide for Electronic Communications Service Providers*.

FOI MEMO 5100: *Analys av informations- och cybersäkerhet i NRFB*, 2014-11-06.

Ulväng m.fl. (2014): *Brotten mot allmänheten och staten*, 2 uppl.

CEN/CENELEC/ETSI Cyber Security Coordination Group (CSCG): *White Paper No. 01, Recommendations for a Strategy on European Cybersecurity Standardisation*, version 01.08, 2014-02-10.

Kommittédirektiv 2019:73

Cybersäkerhet – genomförandet av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet

Beslut vid regeringssammanträde den 31 oktober 2019

Sammanfattning

En särskild utredare ska föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till. Syftet är att säkerställa att den kompletterande nationella reglering som behövs finns på plats när hela förordningen börjar tillämpas den 28 juni 2021. Utredaren ska också överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet.

Utredaren ska bl.a.

- undersöka vilka kompletterande nationella föreskrifter, exempelvis processuella bestämmelser och bestämmelser om sanktioner, som förordningen kräver eller Sverige bör införa,
- föreslå vilken befintlig myndighet som ska få i uppdrag att vara tillsynsmyndighet,
- analysera om, och i så fall föreslå vilka kompletterande bestämmelser som bör införas dels om självbedömning av överensstämmelse med de krav som ställs i certifieringsordningar och dels om organ för bedömning av överensstämmelse i den svenska regleringen,

- bedöma 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 och föreslå hur ett sådant system skulle kunna utformas, och
- lämna sådana författningsförslag som i övrigt behövs och är lämpliga.

Uppdraget ska i den del som avser anpassningar med anledning av EU-förordningen redovisas senast den 1 juni 2020. I den del som avser regler för verksamheter som är av betydelse för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

Den nya regleringen – cybersäkerhetsakten

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

Förordningen är uppdelad i två delar. Den första delen gäller fastställandet av mål, uppgifter och organisatoriska frågor som rör Enisa. Denna del kräver enligt regeringens bedömning ingen särskild kompletterande nationell reglering från medlemsstaternas sida. Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering. 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 förordningen vad minimiinnehållet i sådana ordningar bör vara. Förordningen anger också väsentliga funktioner och uppgifter för Enisa inom cybersäkerhetscertifiering. Kommissionen kommer att utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. De europeiska certifieringsordningarna kommer sedan att utarbetas av Enisa, med hjälp av expertråd och i nära samarbete med den europeiska gruppen för cybersäkerhetscertifiering (ECCG), som också har inrättats genom förordningen. Gruppens uppgifter regleras i förordningen och består bl.a. i att ge råd till och bistå kommissionen vad gäller cybersäkerhetscertifiering och utarbetande av de europeiska ordningarna för cybersäkerhetscertifiering. En annan uppgift för gruppen är att underlätta anpassningen av de europeiska ordningarna till internationellt erkända standarder och att, 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. Kommissionen ska, med stöd från Enisa, vara ordförande i gruppen. Kommissionen antar sedan de europeiska ordningarna för cybercertifiering genom genomförandeakter.

En europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster och IKT-processer, dvs. på vilken nivå produkten, tjänsten eller processen har utvärderats: ”grundläggande”, ”betydande” eller ”hög”. Varje europeiskt cybersäkerhetscertifikat kan avse någon av assuransnivåerna medan EU-försäkran om överensstämmelse endast kan avse assuransnivån ”grundläggande”. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering. 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. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ”grundläggande” ska försäkra att motsvarande säkerhetskrav är uppfyllda, inbegripet säkerhetsfunktioner, och att utvärderingen har skett 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. Om en europeisk ordning för cybersäkerhetscertifiering ger möjlighet till självbedömning av överensstämmelse bör det vara tillräckligt att tillverkaren eller leverantören har gjort en självbedömning av IKT-produktens, IKT-tjänstens eller IKT-processens överensstämmelse med certifieringsordningen. 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. 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. En europeisk ordning för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer beroende på hur stringent och djupgående den aktuella utvärderingsmetoden är.

Enligt förordningen ska övervakning, tillsyn och verkställighetsuppgifter framför allt ligga hos medlemsstaterna. Medlemsstaterna ska utse en eller flera tillsynsmyndigheter, så kallade nationella myndigheter för cybersäkerhetscertifiering. Myndigheten eller myndigheterna kommer bl.a. att få i uppdrag att övervaka och kontrollera organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse. Ett organ för bedömning av överensstämmelse är ett organ som utför bedömning av överensstämmelse, bl.a. genom kalibrering, provning, certifiering och kontroll.

Förordningens bestämmelser ska inte påverka tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsrättsakter. Förordningen ska heller inte påverka medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Den delen av förordningen som rör cybersäkerhetscertifiering kommer att kräva anpassningar och kompletterande författningsbestämmelser på nationell nivå.

Uppdraget att genomföra EU:s cybersäkerhetsakt

Allmänna riktlinjer för uppdraget

Cybersäkerhetsakten kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen. I dag bestämmer en producent själv om en produkt, tjänst eller process ska certifieras och i så fall vilket certifieringsorgan som ska utföra certifieringen. Utgångspunkten kommer att vara att certifieringen även i framtiden ska vara frivillig, oavsett om en europeisk ordning för cybersäkerhetscertifiering finns på plats eller inte. Detta är dock upp till varje medlemsstat att bestämma. Den största skillnaden är att när en sådan europeisk ordning för cybersäkerhetscertifiering finns på plats, får inte längre nationella cybersäkerhetscertifieringar utföras inom det område som täcks av den europeiska ordningen för cybersäkerhetscertifiering. Förordningen innebär också att när en europeisk ordning för cybersäkerhetscertifiering ska användas reglerar förordningen vilka krav som ställs på certifieringen, certifieringsorganen och de leverantörer och producenter som innehar ett sådant certifikat. Det finns därför ett behov av att ta fram en nationell reglering som kompletterar förordningen.

Utredaren ska därför

- lämna förslag till författningsbestämmelser som kompletterar cybersäkerhetsakten.

Vilken myndighet ska vara nationell myndighet för cybersäkerhetscertifiering?

Cybersäkerhetsakten föreskriver att varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium som ansvariga för tillsynsuppgifterna. Alternativt kan medlemsstaten, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i denna andra medlemsstat (artikel 58).

Flertalet av cybersäkerhetsaktens bestämmelser om nationella myndigheter för cybersäkerhetscertifiering gäller direkt och medför inga krav på eller behov av kompletterande nationella bestämmelser. Medlemsstaterna ska dock underrätta kommissionen om vilka myn-

digheter som utsetts och, om fler än en myndighet utsetts, vilka uppgifter de olika myndigheterna ska ha. Myndigheterna kommer bl.a. även att ha en roll när det gäller utfärdandet av europeiska cybersäkerhetscertifikat (på nivån ”hög”), och då måste medlemsstaterna säkerställa att denna verksamhet är avskild från uppgifterna som myndigheten ska utföra som tillsynsmyndighet och att den utförs av oberoende enheter.

Vissa andra frågor är i och för sig reglerade i förordningen men tillåter ytterligare nationell reglering. Detta gäller exempelvis regleringen om tillsynsmyndighetens befogenheter i artikel 58.8. Det är vidare upp till medlemsstaterna att inom vissa angivna ramar reglera bl.a. tillsynsmyndighetens organisation och se till att myndigheten har tillräckliga resurser.

Vid tillsynsmyndigheten kommer det att samlas känslig information om cybersäkerheten i vissa produkter, tjänster och processer eftersom myndigheten kommer att ha ett särskilt ansvar för utfärdande av certifikat enligt den högsta assuransnivån. Det är därför viktigt att myndigheten har personal med erfarenhet av och förmåga att bedöma och hantera uppgifter enligt de krav som ställs i offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagen (2018:585). Sveriges certifieringsorgan för it-säkerhet som är lokaliserat vid Försvarets materielverk, CSEC, ska enligt sin instruktion i sin verksamhet beakta nationella säkerhetsintressen. Ett sådant krav bör därför införas även i den reglering som föreslås av utredaren.

Styrelsen för ackreditering och teknisk kontroll (Swedac) har i dag vissa av de uppgifter som den nationella myndigheten för cybersäkerhetscertifiering ska ha. Enligt sin instruktion ska Swedac bl.a. ansvara för frågor om teknisk kontroll, vilket inkluderar ackreditering och frågor i övrigt om bedömning av överensstämmelse. Swedac ska särskilt ansvara för ordningar för bedömning av överensstämmelse/teknisk provning och kontroll. Detta inbegriper att i EU, internationellt och nationellt verka för öppna och harmoniserade tekniska kontrollordningar, ackrediteringssystem och normer för ömsesidigt godtagande av resultat från provningar, certifieringar och andra bevis om överensstämmelse som undanröjer tekniska handelshinder samt upprätthålla och vidareutveckla öppna, kostnadseffektiva och behovsanpassade ordningar för teknisk kontroll och bedömning av överensstämmelse. Swedac är även nationellt ackrediteringsorgan i enlighet med 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 anmäler och utövar tillsyn över organ som enligt lagen (2011:791) om ackreditering och teknisk kontroll ska anmälas för uppgifter i samband med bedömning av överensstämmelse enligt bestämmelser som gäller inom EU.

För att undvika att den nationella myndigheten för cybersäkerhetscertifiering tilldelas uppgifter som redan utförs av Swedac bör utredaren kartlägga hur förhållandet mellan den nationella myndigheten för cybersäkerhetscertifiering och Swedac ska se ut, i vilka fall de två myndigheterna ska samarbeta och vilket behov av kompletterande nationella bestämmelser som behövs. Det är viktigt att utredaren i detta arbete beaktar de kostnader, den tid och andra aspekter som en dubbel granskning av såväl Swedac som den nationella tillsynsmyndigheten kommer att innebära för den som blir granskad.

Utredaren ska därför

- föreslå vilken befintlig myndighet som ska få i uppdrag att vara nationell tillsynsmyndighet för cybersäkerhetscertifiering,
- ta ställning till hur myndighetens organisation påverkas,
- kartlägga vilket förhållande den nationella myndigheten för cybersäkerhetscertifiering ska ha till Swedac och hur uppgifterna ska fördelas dem emellan för att undvika såväl överlappande granskningar som luckor i tillsynen, samt
- utarbeta nödvändiga kompletterande författningsförslag, inklusive om de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering ska tilldelas, i syfte att myndigheten ska kunna utföra de uppgifter som följer av förordningen.

Ska det införas kompletterande bestämmelser om sanktioner?

Cybersäkerhetsakten innehåller i artikel 65 bestämmelser om att medlemsstaterna ska fastställa regler om sanktioner vid överträdelser av den delen av förordningen som reglerar ett ramverk för cybersäkerhetscertifiering och för överträdelser av europeiska ordningar för cybersäkerhetscertifiering. Medlemsstaterna ska också vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I artikel 58.8 finns en

lista över de befogenheter som de nationella myndigheterna för cybersäkerhetscertifiering måste ha. I punkt f anges att myndigheterna ska utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör. Medlemsstaterna ska vidare enligt artikel 65 anmäla dessa regler och åtgärder samt eventuella ändringar som berör dem till kommissionen utan dröjsmål. I förordningen saknas dock närmare bestämmelser om hur detta ska gå till och vilka som ska kunna drabbas av sanktioner. Till detta kommer också att det föreslagna systemet är frivilligt. Om sanktionerna för att bryta mot ett system som inte är obligatoriskt är för långtgående finns det risk för att aktörer inte kommer att använda sig av den europeiska cybersäkerhetscertifieringen eller att de vänder sig till länder med mildare sanktionssystem. Samtidigt får det europeiska systemet inte bli tandlöst för dem som trots allt väljer att använda sig av det. Det finns därför behov av att analysera och ta ställning till i vilken utsträckning överträdelser av förordningen bör bli föremål för sanktioner i Sverige.

Utredaren ska därför

- analysera vilka kompletterande bestämmelser om sanktioner som Sverige behöver eller bör införa,
- lämna sådana författningsförslag som behövs och är lämpliga.

Processuella frågor och rätten att klaga

Av artikel 58.8 i förordningen framgår det att utövandet av tillsynsmyndighetens befogenheter ska vara föremål för lämpliga skyddsåtgärder, bl.a. effektiva rättsmedel. Enligt artikel 58.8 d ska tillsynsmyndigheten ha befogenhet att få tillgång till lokaler hos organ för bedömning av överensstämmelse eller hos innehavare av ett europeiskt cybersäkerhetscertifikat i enlighet med unionsrätten eller nationell processrätt. Fysiska och juridiska personer ska, enligt förordningen, 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, till den behöriga nationella myndigheten för cybersäkerhetscertifiering (artikel 63.1). Vidare ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel mot den myndighet eller de organ som nämnts ovan och som fattat ett beslut, och när det

gäller underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till myndigheten eller organet (artikel 64.1). Detta torde för svensk del bäst tillgodoses genom en rätt för enskilda att överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol.

Behovet av kompletterande nationella bestämmelser i de ovanstående frågorna behöver bli föremål för närmare analys.

Utredaren ska därför

- analysera i vilken utsträckning det behövs kompletterande bestämmelser om utövandet av tillsynsmyndighetens befogenheter,
- ta ställning till i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i förordningen, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Hur ska förordningens bestämmelser om organ för bedömning av överensstämmelse och självbedömning av överensstämmelse genomföras?

Förordningen reglerar även organ för bedömning av överensstämmelse, som bl.a. kan utfärda europeiska cybersäkerhetscertifikat. I bilagan till förordningen finns närmare bestämmelser med krav på dessa organ, bl.a. om upprätthållande av konfidentialitet och tystnadsplikt. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorganet – i Sveriges fall är det Swedac. I fall där ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som organ för bedömning av överensstämmelse.

En europeisk ordning för cybersäkerhetscertifiering kan också ge tillverkare eller leverantörer möjlighet att göra en självbedömning av överensstämmelse. Detta tillåts endast i förhållande till produkter, tjänster och processer där de uppfyllda säkerhetskraven är ställda på en lägre nivå. I förordningen finns bestämmelser om hur detta ska gå till (artikel 53). Där anges också att detta är frivilligt att utfärda, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

Utredaren ska därför

- föreslå hur bestämmelserna om kraven på organen för överensstämmelse ska genomföras,
- analysera om nuvarande sekretessbestämmelser för offentliga organ och bestämmelser om tystnadsplikt för privata aktörer behöver anpassas eller ny lagstiftning föreslås, med anledning av förordningens reglering om tystnadsplikt och konfidentialitet hos organen för överensstämmelse, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Frivillighet

Cybersäkerhetscertifieringen ska enligt förordningen vara frivillig, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt (artikel 56.2). Förordningen ger dock kommissionen i uppdrag att regelbundet bedöma effektiviteten hos och användningen av de antagna europeiska ordningarna för cybersäkerhetscertifiering och huruvida en specifik europeisk ordning för cybersäkerhetscertifiering ska göras obligatorisk genom unionsrätten i syfte att säkerställa en adekvat cybersäkerhetsnivå 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. Kommissionen ska sedan på grundval av bedömningen fastställa om produkter, tjänster eller processer ska omfattas av en obligatorisk certifieringsordning.

Som tidigare nämnts upphör de nationella ordningarna för cybersäkerhetscertifiering och tillhörande förfaranden att gälla så fort det finns europeiska motsvarigheter. Befintliga certifikat kommer dock att förbli giltiga till dess att de löper ut. Medlemsstaterna förbinder sig också att inte införa nya nationella ordningar, som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering, och ska meddela kommissionen och ECCG om alla avsikter att utarbeta nya nationella ordningar för cybersäkerhetscertifiering. Detta regleras i förordningen och kommer att påverka såväl innehavare av befintliga certifikat som de certifieringsorgan som i dag utfärdar certifikat enligt andra ordningar. Verksamheter måste anpassas till det nya systemet,

och branschen måste hålla sig uppdaterad om de förslag till europeiska ordningar för cybersäkerhetscertifiering som utarbetas.

Utredaren ska därför

- hålla sig uppdaterad om hur arbetet med att utarbeta europeiska ordningar för cybersäkerhetscertifiering fortgår, och
- lämna sådana författningsförslag som behövs och är lämpliga.

Certifiering på den högsta assuransnivån

I Sverige finns i dag vid Försvarets materielverk ett nationellt certifieringsorgan för it-säkerhet i produkter och system, CSEC. CSEC ska i sin verksamhet beakta nationella säkerhetsintressen och verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Dessutom är CSEC Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat, Common Criteria Recognition Arrangement (CCRA), och motsvarande överenskommelse inom Europa, Senior Officials Group Information Systems Security – Mutual Recognition Arrangement (SOG-IS MRA), (5 § förordningen [2007:854] med instruktion för Försvarets materielverk). Detta innebär att CSEC representerar och tar tillvara landets intressen inom organisationerna. Som nationellt certifieringsorgan ansvarar CSEC för att ta fram och utveckla regler för granskning av it-säkerhet i produkter och system enligt Common Criteria, CC. CSEC licensierar företag som utför granskningar enligt dessa regler samt utövar tillsyn över dessa företag. Produkter som certifierats av CSEC används bl.a. av Försvarsmakten. CC erkänns internationellt av världens ledande länder inom it-säkerhet och anses obligatoriskt för it-produkter i kritiska infrastrukturer i flera länder. CSEC har även som uppdrag att samverka internationellt med andra certifieringsorgan och säkerhetsmyndigheter.

CCRA och SOG-IS MRA tillåter endast statliga certifieringsorgan, vilket medför att det i dag bara är CSEC som utfärdar certifikat enligt den standarden i Sverige. Med cybersäkerhetsakten tillåts privata certifieringsorgan endast att utfärda certifikat på nivån ”grundläggande” eller ”betydande”. För nivån ”hög” är det den nationella myndigheten för cybersäkerhetscertifiering som är behörig. Myndigheten kan dock delegera detta till ett organ för bedömning av överensstämmelse genom en allmän delegering på förhand av uppgiften eller efter

förhandsgodkännande av varje enskilt europeiskt cybersäkerhetscertifikat.

Utredaren ska därför

- föreslå hur certifiering på assuransnivån ”hög” ska genomföras i Sverige och utreda om detta kan och bör regleras genom författning. Utredaren ska ha som utgångspunkt att CSEC ska ha en roll då det gäller denna typ av certifiering.

Uppdraget att överväga om det bör införas krav på certifiering och godkännande till skydd för Sveriges säkerhet

Särskilda krav på säkerhet måste kunna ställas på nät- och informationssäkerhet för att skydda nationell säkerhet. Åtgärder för att skydda nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget). Av artikel 1.2 cybersäkerhetsakten framgår även att förordningen inte ska påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på strafflagstiftningens område.

Säkerhetsskyddslagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). För informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig dels om förberedande åtgärder inför driftsättning av sådana informationssystem, dels om säkerhetskrav som kontinuerligt ställs på informationssystemen. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. Bestämmelserna innebär att det är verksamhetsutövaren som ansvarar för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

Det finns anledning att överväga om ytterligare krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs

för att upprätthålla skyddet av sådana verksamheter. En möjlighet kan vara att införa krav på att produkter, tjänster och processer inom nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt särskilda certifieringsordningar som ställer krav anpassade för användning i säkerhetskänslig verksamhet. En kompletterande eller alternativ möjlighet är att införa krav på godkännande från en utpekad myndighet innan en sådan produkt, tjänst eller process tas i drift i säkerhetskänslig verksamhet.

Utredaren ska därför:

- bedöma om det finns anledning att införa särskilda krav på att produkter, tjänster och processer som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt särskilda certifieringsordningar utformade för säkerhetskänslig verksamhet,
- överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana produkter, tjänster och processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet,
- göra en internationell jämförelse av lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för produkter, tjänster och processer som ingår i ett nätverks- eller informationssystem i länder som utredaren bedömer vara av intresse,
- lämna förslag, förenliga med EU-rätten, på hur ett sådant regelverk skulle kunna se ut, inklusive vilken eller vilka myndigheter som skulle ansvara för uppgiften och vilka sanktioner en sådan reglering bör förenas med,
- lämna nödvändiga författningsförslag som behövs och är lämpliga.

Utredningen har i denna del att förhålla sig till betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) som för närvarande bereds i Regeringskansliet.

Övriga frågor

Utredaren är fri att inom de ramar som anges i de allmänna riktlinjerna ta upp och belysa även andra frågeställningar som är relevanta för uppdraget.

Om utredaren kommer fram till att det krävs eller är lämpligt med kompletterande nationella bestämmelser i andra delar ska sådana kunna föreslås.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt ange konsekvenserna för företag i form av kostnader och ökade administrativa bördor samt personella konsekvenser för berörda myndigheter.

Utredaren ska även beakta de konsekvenser som förordningens genomförande kan få när det gäller internationell handel med tredjeland och erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

Kontakter och redovisning av uppdraget

Utredaren ska hålla Regeringskansliet (Försvarsdepartementet) informerat om det löpande arbetet.

Vid genomförandet av uppdraget ska utredaren hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet (exempelvis arbetet med betänkandet Kompletteringar till den nya säkerhetsskyddslagen, SOU 2018:82), utredningsväsendet och inom EU. Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från myndigheter, näringslivet och andra som kan vara berörda av de aktuella frågorna.

Uppdraget ska redovisas i den del som avser anpassningar med anledning av EU-förordningen senast den 1 juni 2020. I den del som avser regler till skydd för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

(Försvarsdepartementet)

Kommittédirektiv 2020:57

Tilläggsdirektiv till Cybersäkerhetsutredningen (Fö 2019:01)

Beslut vid regeringssammanträde den 14 maj 2020

Förlängd tid för en del av uppdraget

Regeringen beslutade den 31 oktober 2019 kommittédirektiv om att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till samt att överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet (dir. 2019:73). Enligt direktiven skulle utredaren redovisa den del av uppdraget som avser anpassningar med anledning av cybersäkerhetsakten senast den 1 juni 2020.

Utredningstiden förlängs för en del av uppdraget. Den del av uppdraget som avser anpassningar med anledning av cybersäkerhetsakten ska i stället redovisas senast den 31 augusti 2020.

(Försvarsdepartementet)

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 fleråriga 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.

Statens offentliga utredningar 2020

Kronologisk förteckning

1. Översyn av yrket personlig assistent – ett viktigt yrke som förtjänar bra villkor. S.
2. Skärpta regler om utländska månggiften. Ju.
3. Hållbar slamhantering. M.
4. Vägen till en klimatpositiv framtid. M.
5. Fler ruttjänster och höjt tak för rutavdraget. Fi.
6. En begriplig och trygg sjukförsäkring med plats för rehabilitering. S.
7. Brott mot djur – Skärpta straff och ett mer effektivt sanktionssystem. N.
8. Starkare kommuner – med kapacitet att klara välfärdsuppdraget. Fi.
9. Kunskapsläget på kärnavfallsområdet 2020. Steg för steg. Var står vi? Vart går vi? M.
10. Stärkt lokalt åtgärdsarbete – att nå målet Ingen övergödning. M.
11. Kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar. Ju.
12. Nya kapitaltäckningsregler för värdepappersbolag. Fi.
13. Att kriminalisera överträdelser av EU-förordningar. N.
14. Framtidens teknik i omsorgens tjänst. S.
15. Strukturförändring och investering i hälso- och sjukvården – lärdomar från exemplet NKS. S.
16. Ett effektivare regelverk för utlänningsärenden med säkerhetsaspekter. Ju.
17. Grönt sparande. Fi.
18. Framtidens järnvägsunderhåll. I.
19. God och nära vård. En reform för ett hållbart hälso- och sjukvårdssystem. S.
20. Skatt på modet – för att få bort skadliga kemikalier. Fi.
21. Sveriges museum om Förintelsen. + Holocaust Remembrance and Representation. Documentation from a Research Conference. Ku.
22. Motorfordonspooler – på väg mot ökad delning av motorfordon. Fi.
23. Hälso- och sjukvård i det civila försvaret – underlag till försvarspolitisk inriktning. S.
24. Tillsammans för en välfungerande sjukskrivnings- och rehabiliteringsprocess. S.
25. Ett nationellt biljettsystem för all kollektivtrafik. I.
26. En sjukförsäkring anpassad efter individen. S.
27. Högre växel i minoritetspolitiken. Stärkt samordning och uppföljning. Ku.
28. En mer likvärdig skola – minskad skolsegregation och förbättrad resurstilldelning. U.
29. En ny myndighet för att stärka det psykologiska försvaret. Ju.
30. En moderniserad arbetsrätt. A.
31. En ny mervärdesskattelag. Del 1 och 2. Fi.
32. Grundpension. Några anslutande frågor. S.
33. Gemensamt ansvar – en modell för planering och dimensionering av gymnasial utbildning. Del 1 och 2. U.
34. Stärkt kvalitet och likvärdighet i fritidshem och pedagogisk omsorg. U.
35. Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen. Fi.
36. Ett nationellt sammanhållet system för kunskapsbaserad vård – ett system, många möjligheter. S.

37. Ett nytt regelverk för arbetslöshetsförsäkringen. A.
38. Ökad trygghet för visselblåsare. A.
39. Kärnavfallsrådets yttrande över SKB:s Fud-program 2019. M.
40. En gemensam utbildning inom statsförvaltningen. Fi.
41. Kommuner som utförare av tjänster åt Arbetsförmedlingen – en analys av de rättsliga förutsättningarna. A.
42. En annan möjlighet till särskilt stöd. Reglering av kommunala resursskolor. U.
43. Bygga, bedöma, betygssätta – betyg som bättre motsvarar elevernas kunskaper. U.
44. Grundlagsskadestånd – ett rättighetsskydd för enskilda. Ju.
45. Ett ändamålsenligt skydd för tryck- och yttrandefriheten. Ju.
46. En gemensam angelägenhet. Vol. 1 och 2. Fi.
47. Hållbar socialtjänst. En ny socialtjänstlag. Del 1 och 2. S.
48. Skatt på engångsartiklar. Fi.
49. Enhetlig och effektiv marknadskontroll. UD.
50. Enklare skatteregler för enskilda näringsidkare. Fi.
51. En ny lag om konsumentskydd vid köp och vissa andra avtal. Ju.
52. Rutavdrag för äldre. Fi.
53. Personuppgiftsbehandling vid antalsberäkning inför klinisk forskning. N.
54. En långsiktigt hållbar migrationspolitik. Ju.
55. Innovation genom information. I.
56. Det demokratiska samtalet i en digital tid. Så stärker vi motståndskraften mot desinformation, propaganda och näthat. Ku.
57. Ett särskilt hedersbrott. Ju.
58. EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering. Fö.

Statens offentliga utredningar 2020

Systematisk förteckning

Kunskapsläget på kärnavfallsområdet 2020. Steg för steg. Var står vi? Vart går vi? [9]

Stärkt lokalt åtgärdsarbete – att nå målet Ingen övergödning. [10]

Kärnavfallsrådets yttrande över SKB:s Fud-program 2019. [39]

Näringsdepartementet

Brott mot djur – Skärpta straff och ett mer effektivt sanktionssystem. [7]

Att kriminalisera överträdelser av EU-förordningar. [13]

Personuppgiftsbehandling vid antalsberäkning inför klinisk forskning. [53]

Socialdepartementet

Översyn av yrket personlig assistent – ett viktigt yrke som förtjänar bra villkor. [1]

En begriplig och trygg sjukförsäkring med plats för rehabilitering. [6]

Framtidens teknik i omsorgens tjänst. [14]

Strukturförändring och investering i hälso- och sjukvården – lärdomar från exemplet NKS. [15]

God och nära vård. En reform för ett hållbart hälso- och sjukvårdssystem. [19]

Hälso- och sjukvård i det civila försvaret – underlag till försvarspolitisk inriktning. [23]

Tillsammans för en välfungerande sjukskrivnings- och rehabiliteringsprocess. [24]

En sjukförsäkring anpassad efter individen. [26]

Grundpension. Några anslutande frågor. [32]

Ett nationellt sammanhållet system för kunskapsbaserad vård – ett system, många möjligheter. [36]

Hållbar socialtjänst. En ny socialtjänstlag. Del 1 och 2. [47]

Utbildningsdepartementet

En mer likvärdig skola – minskad skolsegregation och förbättrad resurstilldelning. [28]

Gemensamt ansvar – en modell för planering och dimensionering av gymnasial utbildning. Del 1 och 2. [33]

Stärkt kvalitet och likvärdighet i fritidshem och pedagogisk omsorg. [34]

En annan möjlighet till särskilt stöd. Reglering av kommunala resursskolor. [42]

Bygga, bedöma, betygssätta – betyg som bättre motsvarar elevernas kunskaper. [43]

Utrikesdepartementet

Enhetlig och effektiv marknadskontroll. [49]