**Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cyberresiliensförordningen**

**PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL**

I denna proposition föreslås det att det stiftas en ny lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering samt att lagen om marknadskontrollen av vissa produkter, cybersäkerhetslagen, lagen om tjänster inom elektronisk kommunikation och lagen om verkställighet av böter ändras.

Syftet med propositionen är att utfärda nationella bestämmelser som kompletterar och preciserar en EU-förordning som gäller cyberresiliens, det vill säga den så kallade cyberresiliensakten eller cyberresiliensförordningen. Cyberresiliensförordningen fastställer övergripande minimikrav på informationssäkerhet för produkter med digitala element, det vill säga utrustning och programvara som kan anslutas till internet eller annan utrustning. De föreslagna bestämmelserna gäller marknadskontroll av cyberresiliensförordningen, anmälan av och tillsyn över organ för bedömning av överensstämmelse samt administrativa påföljder.

Syftet med propositionen är också att komplettera den nationella lagstiftningen om europeiska ordningar för cybersäkerhetscertifiering för tillämpningen av EU:s så kallade cybersäkerhetsakt. De föreslagna bestämmelserna gäller uppgifter och befogenheter för den nationella myndigheten för cybersäkerhetscertifiering samt organ för bedömning av överensstämmelse.

Syftet med propositionen är också att komplettera det nationella genomförandet av EU:s så kallade cybersäkerhetsdirektiv till den del det gäller registreringsuppgifter om domännamn samt registrarer på den miniminivå som förutsätts i direktivet. Kompletteringarna gäller behandling och utlämnande av uppgifter om domännamn.

Transport- och kommunikationsverket åläggs som nya uppgifter marknadskontroll av cyberresiliensförordningen och utnämnande av och tillsyn över organ för bedömning av överensstämmelse. I fråga om AI-system med hög risk är marknadskontrollmyndighet den myndighet som är behörig med stöd av lagen om tillsyn över vissa system för artificiell intelligens. Transport- och kommunikationsverket ska även i fortsättningen vara nationell myndighet för cybersäkerhetscertifiering.

Ett smidigt och effektivt genomförande av cyberresiliensförordningen för att förbättra informationssäkerheten hos enheter och program ingår i de prioriterade åtgärderna i genomförandeplanen för Finlands cybersäkerhetsstrategi. Finlands nya cybersäkerhetsstrategi för åren 2024–2035 har godkänts som ett principbeslut av statsrådet i oktober 2024. Enligt regeringsprogrammet för statsminister Petteri Orpos regering stärks cybersäkerheten och samarbetet kring cybersäkerhet mellan myndigheterna och näringslivet, regeringen förbättrar informationssäkerheten inom kritiska sektorer, och i samband med genomförandet av EU-lagstiftningen undviks ytterligare nationell reglering.

Lagarna avses huvudsakligen träda i kraft den 1 juni 2026. Till de delar lagarna hänför sig till det nationella genomförandet av EU:s cybersäkerhetsdirektiv avses de dock träda i kraft så snart som möjligt. Det föreslås att tillämpningen av den föreslagna lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering i fråga om vissa bestämmelser tillämpas på graderat sätt på ett sätt som motsvarar början för tillämpningen av cyberresiliensförordningen.

---

**INNEHÅLL**

## MOTIVERING

# 1 Bakgrund och beredning

## 1.1 Bakgrund

Bakgrunden till beredningen av propositionen utgörs av Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen). Förordningen har trätt i kraft den 10 december 2024 och tillämpningen av den börjar under åren 2026–2027, dock i huvudsak den 11 december 2027. Genom denna förordning föreslås de nationella bestämmelser som behövs för att tillämpa förordningen.

Bakgrunden till förslaget utgörs av utvecklingen inom cyberresiliensförordningen, som har lett till att enheter och programvaror allt oftare utsätts för cyberattacker. Cyberattackerna orsakar avsevärda kostnader såväl för dem som attackerats som för utomstående, till exempel genom att personuppgifterna äventyras. Utmaningen med produkterna är en låg datasäkerhetsnivå, sårbarheter och brister i dataskyddsuppdateringarna samt bristfällig kunskap om produkternas säkerhetsegenskaper och begränsad tillgång till information om dessa. Målet med förordningen är att ingripa i dessa utmaningar och säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel och att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element.

Inom Europeiska unionen eller på nationell nivå i Finland finns det inte sedan tidigare något övergripande regelverk som fastställer cybersäkerhetskrav för alla produkter med digitala element.

Beredningen av propositionen har därtill berott på det i myndighetsverksamheten observerade behovet av nationell kompletterande reglering för att kunna tillämpa 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 i uppgifterna för den nationella myndigheten för cybersäkerhetscertifiering. Denna uppgift har i Finland tilldelats Transport- och kommunikationsverket i lagen om tjänster inom elektronisk kommunikation (917/2014). Bestämmelserna om certifieringsramverket för cybersäkerhet i cybersäkerhetsakten har blivit tillämpliga i huvudsak i juni 2021. Tillämpningen av cyberresiliensförordningen förutspås öka myndighetsuppgifterna i anknytning till cybersäkerhetscertifieringen jämfört med nuläget.

Finlands cybersäkerhetsstrategi har uppdaterats i enlighet med regeringsprogrammet för statsminister Orpos regering så att det motsvarar den förändrade verksamhetsmiljön. Finlands nya cybersäkerhetsstrategi för åren 2024–2035 godkändes som ett principbeslut av statsrådet den 10 oktober 2024. Efter att cybersäkerhetsstrategin har godkänts har man berett en genomförandeplan för den, där utvecklingsåtgärder fastställs för att uppnå målen med strategin. Ett smidigt och effektivt genomförande av cyberresiliensförordningen för att förbättra informationssäkerheten hos enheter och programvaror ingår i de prioriterade åtgärderna i genomförandeplanen för Finlands förnyade cybersäkerhetsstrategi.

## 1.2 Beredning

### 1.2.1 Beredningen av EU-rättsakten

Kommissionen gav den 15 september 2022 förslaget till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (COM(2022)454). Kommissionen gjorde en konsekvensbedömning av förslaget (SWD (2022) 292 final). Kommissionen ordnade ett offentligt samråd om initiativet på våren 2022. Förhandlingarna om förslaget fördes i rådets horisontella cyberarbetsgrupp till centrala delar under år 2023.

Statsrådet överlämnade U-skrivelsen U 83/2022 rd om förslaget till förordning till riksdagen. Kommunikationsutskottet gav utlåtandet KoUU 39/2022 rd om ärendet. Stora utskottet instämde enligt StoURS 147/2022 rd med statsrådets ståndpunkt i enlighet med kommunikationsutskottets utlåtande. Ingen kompletterande skrivelse gavs om ärendet.

Finland understödde förslagets mål om att på marknaden släppa ut produkter som är säkrare i cybermiljön, vars säkerhetsegenskaper förutsätts vara av hög nivå och vars säkerhetsegenskaper och -krav är mer transparenta för de konsumenter och företag som använder dessa. Genom förslaget ansågs det vara möjligt att förbättra dataskyddet för alla aktörer i samhället. Finland ansåg att förbättring av säkerheten för nätanslutna enheter och programvaror är ett avsevärt utvecklingsobjekt inom cybersäkerhetssektorn.

Finland ansåg det vara värt att understödja att ansvaret för produkternas säkerhet i cybermiljön hänförs i högre grad än för närvarande från användaren till tillverkaren, oberoende av var man tillverkar de produkter som släpps ut på den inre marknaden. Finland har ansett att en riskbaserad approach i påvisandet av överensstämmelse och marknadskontrollen i princip är värd att understödja. Finland ansåg också att det var viktigt att förfarandena bildar en tydlig helhet i förhållande till övriga författningar och att kraven inte orsakar någon extra administrativ börda.

Beredningen av cybersäkerhetsakten har beskrivits i regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den (RP 98/2020 rd, s. 12–13). Cybersäkerhetsakten har varit i kraft i huvudsak från och med juni 2019. Cybersäkerhetsakten har ändrats genom Europaparlamentets och rådets förordning (EU) 2025/37, genom vilken dataskyddstjänster fogades till dess tillämpningsområde. Ändringarna påverkar inte direkt behovet av nationell reglering som kompletterar förordningen.

Med anledning av det förslag som ledde till utfärdandet av ändringsförordning (EU) 2025/37 och kommissionens förslag till cybersolidaritetsakt överlämnade statsrådet U-skrivelsen U 20/2023 rd till riksdagen. Med anledning av skrivelsen gav grundlagsutskottet utlåtandet GrUU 6/2023 rd, i vilket anmärkningarna dock främst gäller förslaget till cybersolidaritetsakt. I enlighet med specialutskottens ståndpunkter instämde stora utskottet i statsrådets ståndpunkt och riktade statsrådets uppmärksamhet på de konstitutionella omständigheter som nämnts i grundlagsutskottets utlåtande.

Enligt Finlands ståndpunkt kunde målen för den föreslagna ramen för certifiering av betrodda leverantörer anses vara värda att understödjas i den mån som regleringen syftar till att öka förtroendet för den digitala inre marknaden, minska företagens kostnader för certifiering och förbättra kvaliteten och säkerheten i cybersäkerhetstjänster.

EU:s cybersäkerhetsdirektiv (NIS 2-direktivet) och beredningen av dess nationella genomförande beskrivs i avsnitt 1.2 i regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) RP 57/2024 rd.

1.2.2 Beredningen av regeringens proposition

Propositionen har beretts som ett tjänsteuppdrag vid kommunikationsministeriet. Beredningen av propositionen har gjorts i samarbete med Transport- och kommunikationsverket.

Under beredningen ordnades samråd om ordnandet av myndighetsuppgifterna i fråga om marknadskontrollen och kontrollen av anmälda organ samt myndighetssamråd om sambanden mellan övervakningen enligt förordningen om artificiell intelligens och cyberresiliensförordningen.

Kommunikationsministeriet ordnade den 6 maj 2024 ett samråd om utseendet av de anmälda organen och ordnandet av de myndighetsuppgifter som gäller tillsynen över dessa. I samrådet framfördes synpunkter på att myndighetsuppgifterna i anknytning till utseendet och övervakningen av de anmälda organen ska ordnas centraliserat och effektivt. I samrådet framfördes synpunkter på att effektiv myndighetsverksamhet är betydelsefullare för en ekonomisk aktör än frågan om i samband med vilken myndigheten uppgiften ordnas.

Kommunikationsministeriet ordnade den 7 maj 2024 ett samråd om ordnandet av den myndighetsuppgift som gäller marknadskontrollen enligt cyberresiliensförordningen. I samrådet ansågs det vara viktigt att den myndighetsuppgift som gäller marknadskontrollen ordnas effektivt. I samrådet ansågs det vara viktigt att marknadskontrollmyndigheten är sakkunnig och förmår ge de ekonomiska aktörerna handledning och rådgivning kring tillämpningen av cyberresiliensförordningen. I samrådet ansågs det vara allmänt motiverat att marknadskontrolluppgiften samlas till en myndighet för att undvika överlappningar i myndighetsuppgifterna.

Kommunikationsministeriet ordnade den 11 december 2024 ett samråd för myndigheterna om sambanden mellan förordningen om artificiell intelligens och cyberresiliensförordningen och om det samordnande av marknadskontrollen som förordningen förutsätter. I samrådet framfördes synpunkter på att de myndigheter som övervakar förordningen om artificiell intelligens i fråga om cyberresiliensförordningen inte ska tilldelas andra marknadskontrolluppgifter än sådana som gäller AI-system. Under beredningen har en bedömningspromemoria utarbetats om alternativen för att ordna marknadskontrollen. Det centrala innehållet i bedömningspromemorian beskrivs i avsnitt 5.1.1.

Propositionen var på remiss på finska mellan den 17 juni och den 12 augusti 2025 och på svenska mellan den 26 juni och den 21 augusti 2025. Propositionen var på remiss hos Ålands landskapsregering i sex veckor mellan den 1 september och den 13 oktober 2025. Sammanlagt 33 utlåtanden togs emot om propositionen. Ett sammandrag av utlåtandena har utarbetats om remissvaren. Remissvaren behandlas till centrala delar nedan i avsnitt 6.

Beredningsunderlaget till regeringens proposition är tillgängligt på Statsrådets projektportal under projektkoden LVM014:00/2024 (länk: https://valtioneuvosto.fi/sv/projektet?tunnus=LVM014%3A00/2024).

## 2 EU-förordningens syften och huvudsakliga innehåll

### 2.1 Cyberresiliensförordningen

#### 2.1.1 Målsättning och tillämpningsområde

Det allmänna målet med cyberresiliensförordningen är att skapa förhållanden för utveckling av säkra produkter med digitala element och säkerställa att enheter och programvaror har mindre sårbarheter och att tillverkarna tar säkerhetsaspekter på allvar under produktens livscykel. Ett ytterligare mål är att öka synligheten för produkternas dataskyddsegenskaper för enhetsanvändarna. Syftet med förslaget är att skapa ett ramverk för säkerhetskraven, främja transparensen i säkerhetsegenskaperna och möjliggöra att produkterna används säkert.

För att uppnå målen skapas genom förordningen ett regleringsramverk, som harmoniserar säkerhetskraven för produkter med digitala element på EU:s inre marknad.

Förordningen innehåller bestämmelser om de minimikrav som ska ställas på produkter med digitala element och deras tillverkare, distributörer och importörer samt om påvisande och övervakning av överensstämmelsen med kraven. Cyberresiliensförordningens tillämpningsområde är horisontellt. Med stöd av artikel 2.1 i förordningen tillämpas den på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät.

Enligt artikel 3.1 i förordningen avses med produkt med digitala element en programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat. Definitionerna av fjärrbehandling av data, programvara, hårdvara, komponent, rimligen förutsebar användning och anslutning i anknytning till tillämpningsområdet preciseras i artikel 3 i förordningen.

Enligt skäl 11 till förordningen bör sådana lösningar för fjärrbehandling av data definieras som all databehandling på distans för vilken programvaran har utformats och utvecklats av tillverkaren av den berörda produkten med digitala element eller för dennes räkning, och vars avsaknad skulle innebära att produkten med digitala element inte skulle kunna utföra en av sina grundläggande funktioner. Detta tillvägagångssätt säkerställer att tillverkarna på lämpligt sätt säkrar sådana produkter i sin helhet, oavsett om uppgifterna behandlas eller lagras lokalt på användarens enhet eller på distans av tillverkaren. Samtidigt omfattas fjärrbehandling eller fjärrlagring av denna förordnings tillämpningsområde endast i den mån det är nödvändigt för att en produkt med digitala element ska kunna utföra sina funktioner. Sådan fjärrbehandling eller fjärrlagring omfattar situationer där en mobilapplikation kräver tillgång till ett programmeringsgränssnitt eller en databas som tillhandahålls genom en tjänst som utvecklats av tillverkaren. I ett sådant fall omfattas tjänsten av denna förordnings tillämpningsområde som en lösning för fjärrbehandling av uppgifter. Enligt skäl 12 till förordningen utgör molnlösningar lösningar för fjärrbehandling av data i den mening som avses i denna förordning endast om de uppfyller definitionen som fastställs i denna förordning. Till exempel omfattar denna förordning molnaktiverade funktioner som tillhandahålls av en tillverkare av enheter för smarta hem som gör det möjligt för användare att fjärrkontrollera enheten. Å andra sidan omfattas webbplatser som inte stöder funktionen hos en produkt med digitala element, eller molntjänster som utformats och utvecklats utanför en tillverkares ansvar för en produkt med digitala element, inte av denna förordnings tillämpningsområde.

Det finns uttömmande bestämmelser om avgränsningarna av förordningens tillämpningsområde i punkterna 2–7 i dess artikel 2. Förordningen tillämpas inte på medicinsk utrustning enligt förordningarna (EU) 2017/745 och (EU) 2017/246 och inte heller på fordon som omfattas av tillämpningsområdet för (EU) 2019/2114. Dessutom tillämpas förordningen inte på luftfartyg som certifierats med stöd av förordning (EU) 2018/1139 och inte heller på fartygsutrustning enligt direktiv 2014/90/EU. Dessutom tillämpas förordningen inte på produkter som tillverkats uteslutande för ändamål som gäller den nationella säkerheten och landsförsvaret och inte heller på produkter som tillverkats uteslutande för att behandla sekretessbelagda information. Tillämpningsområdet omfattar inte heller reservdelar vars syfte är att användas för att ersätta komponenter som ingår i en produkt med digitala element och som tillverkats enligt samma specifikationer som de ursprungliga komponenterna. Enligt förslaget har kommissionen befogenhet att anta delegerade akter som gäller avgränsning av vissa produkter utanför tillämpningsområdet och ändring av bilagorna III och IV, vilket beskrivs i avsnitt 2.1.9.

Förordningens allmänna tillämpningsområde gäller tillhandahållande på marknaden, det vill säga att en produkt eller programvara släpps ut på EU-marknaden. En del av skyldigheterna enligt förordningen avgränsas till utsläppande på marknaden, det vill säga den tidpunkt när produkten första gången tillhandahålls på marknaden inom EU. Utsläppande på marknaden och tillhandahållande på marknaden definieras i artikel 3.21 och artikel 3.22 i förordningen.

### 2.1.2 Produkters överensstämmelse med kraven

Med stöd av artikel 6 i cyberresiliensförordningen får produkter med digitala element tillhandahållas på marknaden endast om de uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I, om de processer som införs av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Med stöd de i del I i bilaga I fastställda väsentliga cybersäkerhetskraven ska produkterna planeras, utvecklas och produceras så att deras cybersäkerhetsnivå står i rätt proportion till riskerna. En produkt ska bland annat tillhandahållas med en säker standardkonfiguration och utan information om sårbarheter som kan utnyttjas.

För att uppfylla de väsentliga cybersäkerhetskrav som fastställs i del II i bilaga I ska tillverkarna införa processer som gäller behandling av sårbarheter. Av tillverkarna förutsätts bland annat att sårbarheter i en produkt identifieras och dokumenteras och att sårbarheter avhjälps till exempel genom att tillhandahålla dataskyddsuppdateringar, om det är möjligt, samt att test av en produkts dataskydd görs regelbundet.

I enlighet med artikel 7 i förordningen avses med viktiga produkter en produkt med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III till förordningen. Av viktiga produkter förutsätts ett förfarande för bedömning av överensstämmelse av högre nivå än för andra produkter. I enlighet med artikel 8 i förordningen avses med kritiska produkter en produkt med digitala element som har kärnfunktionen hos en produktkategori som anges bilaga IV till förordningen. För kritiska produkter ska man för att visa överensstämmelse inhämta ett cybersäkerhetscertifikat som minst är av assuransnivå ”betydande” i enlighet med cybersäkerhetsakten, under förutsättning att det finns en omfattande tillämplig certifieringsordning som godkänts med stöd av cybersäkerhetsakten för produktkategorin och som är tillgänglig för tillverkarna. Kommissionen har getts befogenhet att anta delegerade akter i fråga om de viktiga och kritiska produkter som fastställs i III och IV, vilket beskrivs nedan i avsnitt 2.1.9.

Med stöd av artikel 11 i cyberresiliensförordningen ska, som avvikelse från artikel 2.1 tredje stycket b i förordning (EU) 2023/988, kapitel III avsnitt 1 (ekonomiska aktörers skyldigheter), kapitlen V och VII (marknadskontroll, kommissionens roll och samordning av tillsyn av genomförandet) och kapitlen IX–XI (internationellt samarbete, finansieringsbestämmelser och slutbestämmelser) i den förordningen tillämpas på produkter med digitala element med avseende på aspekter och risker eller riskkategorier som inte omfattas av cyberresiliensförordningens tillämpningsområde. En ytterligare förutsättning är att särskilda säkerhetskrav som föreskrivits annanstans i unionens harmoniseringslagstiftning inte tillämpas på produkterna.

Artikel 12 i cyberresiliensförordningen innehåller specialbestämmelser om AI-system med hög risk som omfattas av tillämpningsområdet. AI-system med hög risk enligt artikel 6 i förordningen om artificiell intelligens ska anses uppfylla de cybersäkerhetskrav som föreskrivs i artikel 15 i förordningen om artificiell intelligens, då kraven enligt cyberresiliensförordningen är uppfyllda och detta har visats i enlighet med artikel 12 i cyberresiliensförordningen. Artikel 52 i cyberresiliensförordningen innehåller en specialbestämmelse om marknadskontrollen av AI-system med hög risk, vilket beskrivs i avsnitt 2.1.6.

### 2.1.3 Kraven på ekonomiska aktörer och förvaltare av programvara med fri och öppen källkod

#### 2.1.3.1 Tillverkare

Det finns bestämmelser om de centrala skyldigheterna för tillverkare i artiklarna 13 och 14 i cyberresiliensförordningen.

*Tillverkares skyldigheter (artikel 13)*

Med stöd av artikel 13 i cyberresiliensförordningen ska tillverkarna när en produkt med digitala element släpps ut på marknaden säkerställa att den har utformats, utvecklats och producerats i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I i del I. Tillverkarna ska bedöma cybersäkerhetsriskerna i anknytning till produkten och beakta resultaten som en del av planeringen, utvecklingen, produktionen, leveransen och administreringen av produkten. Riskbedömningen ska dokumenteras, den ska uppdateras vid behov under stödtiden och dokumentation ska redogöra för om kraven enligt punkt 2 i del I till bilaga I till förordningen tillämpas på produkten, och om ja, på vilket sätt och hur kraven genomförs utifrån riskbedömningen. I bedömningen ska också anges hur tillverkaren tillämpar bilaga I del I punkt 1 och de krav på sårbarhetshantering som anges i bilaga I del II. Tillverkaren ska inkludera en bedömning av cybersäkerhetsriskerna i den tekniska dokumentation som krävs med stöd av artikel 31 och bilaga VII och om de väsentliga cybersäkerhetskraven inte är tillämpliga på en viss produkt med digitala element motivera detta i den tekniska dokumentationen. Mikroföretag och små företag får tillhandahålla alla delar av den tekniska dokumentation som anges i kommissionen genomförandeakt med användning av ett förenklat formulär (artikel 33.5).

Med stöd av artikel 13 i cyberresiliensförordningen ska tillverkarna dessutom systematiskt dokumentera relevanta cybersäkerhetsaspekter som rör produkterna med digitala element, inbegripet sårbarheter de får kännedom om och all relevant information som tillhandahålls av tredje part. Tillverkarna ska fastställa stödperioden och säkerställa att sårbarheter som gäller produkten och dess komponenter under stödtiden behandlas effektivt i enlighet med del II i bilaga I. Stödperioden ska fastställas för att överensstämma med den förväntade livslängden, dock för minst fem år, eller om livslängden är kortare än fem år, så att den överensstämmer med livslängden. Kommissionen har befogenhet att anta delegerade akter i fråga om fastställandet av längden på stödtiden, vilket beskrivs i avsnitt 2.1.9. Tillverkarna ska efter publiceringen hålla

dataskyddsuppdateringar tillgängliga under stödtiden eller åtminstone tio år, beroende på vilken av tidsperioderna som är längre. Tillverkarna ska iaktta tillbörlig aktsamhet när de integrerar komponenter som skaffats från tredje parter i sina produkter och anmäla konstaterade sårbarheter i den integrerade komponenten till dess tillverkare eller administratör och ingripa i sårbarheten och avhjälpa den.

Med stöd av artikel 13 i cyberresiliensförordningen ska tillverkarna innan en produkt släpps ut på marknaden sammanställa den tekniska dokumentation som avses i artikel 31 och genomföra de valda förfaranden för bedömning av överensstämmelse som avses i artikel 32. Dessutom ska tillverkarna upprätta en EU-försäkran om överensstämmelse i enlighet med artikel 28 och som en del av att de visar överensstämmelsen fästa eller foga en CE-märkning till produkten i enlighet med artikel 30. Tillverkarna ska kunna uppvisa den tekniska dokumentationen och EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna.

Med stöd av artikel 13 i cyberresiliensförordningen ska tillverkarna säkerställa att produkter med digitala element åtföljs av information och instruktioner till användaren enligt bilaga II. Varje medlemsstat bör tillsätta en gemensam kontaktpunkt som bland annat ska ansvara för att anmäla sårbarheter och sitt namn och sin kontaktinformation till användarna och marknadskontrollmyndigheterna.

En tillverkare kan genom skriftlig fullmakt utse en tillverkarens representant, som ska utföra de uppgifter som tillverkaren tilldelat den. Artikel 18 i cyberresiliensförordningen gäller utseende av tillverkarens representanter och den innehåller bestämmelser om de skyldigheter enligt artikel 13 vilka inte får omfattas av uppdraget för tillverkarens representant.

*Rapporteringsskyldigheter och samordnande av sårbarheter (artiklarna 14–17)*

Artikel 14 i cyberresiliensförordningen innehåller bestämmelser om skyldigheten för tillverkarna att rapportera:

- aktivt utnyttjade sårbarheter och allvarliga incidenter som ingår i produkter med digitala element, och
- allvarliga incidenter som påverkar säkerheten för produkten och som tillverkaren får kännedom om.

I enlighet med punkterna 1–5 i artikeln ska tillverkaren anmäla alla aktivt utnyttjade sårbarheter och allvarliga incidenter i fråga om en produkt samtidigt till CSIRT-enheten och Enisa. Anmälan görs via den nationella elektroniska anmälningstjänsten som inrättas i anslutning till Enisas centraliserade rapporteringsplattform. Den CSIRT-enhet som utsetts till samordnare kan vid behov begära att tillverkaren överlämnar en delrapport om situationen för en aktivt utnyttjad sårbarhet eller en incident.

Enligt skäl 65, som gäller rapportering, ska tillverkarna via den gemensamma rapporteringsplattformen, anmäla aktivt utnyttjade sårbarheter i produkter med digitala element samt allvarliga incidenter som påverkar dessa produkters säkerhet till både den enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) som utsetts till samordnare och till Enisa.

Med stöd av artikel 14.8 i cyberresiliensförordningen ska tillverkarna underrätta de drabbade användarna av produkter med digitala element om en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element. Tillverkaren ska informera alla användare om den sårbarheten eller incidenten och, vid behov, om riskreducering

och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident.

Artikel 15 i förordningen innehåller bestämmelser om det frivilliga anmälningsförfarandet. I enlighet med artikeln får tillverkarna och andra fysiska eller juridiska personer till en CSIRT-enhet som utsetts till samordnare eller till Enisa anmäla eventuella sårbarheter i en produkt med digitala element samt cyberhot som kan påverka riskprofilen för en produkt med digitala element. Det frivilliga anmälningsförfarandet omfattar även situationer som handlar om eventuella incidenter som påverkar en produkts dataskydd och tillbud som hade kunna leda till en incident.

Den CSIRT-enhet som utsett till samordnare tar emot de anmälningar som avses i artiklarna 14 och 15 i förordningen via den centrala rapporteringsplattform som Enisa inrättat. En CSIRT-enhet ska med stöd av artikel 16.2 efter att ha mottagit en anmälan sprida anmälan utan oskäligt dröjsmål via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits. På begäran av tillverkaren kan förmedlingen av en anmälan i exceptionella förhållanden skjutas upp på grund av cybersäkerhetsrelaterade orsakar till den absolut nödvändiga tiden, även då det samordnade förfarandet för offentliggörande av sårbarheter enligt artikel 12 i NIS 2-direktivet tillämpas på sårbarheten. Om CSIRT-enheten inte förmedlar anmälan, ska den ge information om den och motivera den till Enisa. I synnerligen exceptionella förhållanden som gäller en aktivt utnyttjad sårbarhet, är det möjligt att av säkerhetsskäl att lämna exakta uppgifter samtidigt till Enisa och CSIRT-enheten. CSIRT-enheten ska dessutom förmedla de uppgifter som behövs för att genomföra marknadskontrollen till den relevanta marknadskontrollmyndigheten i enlighet med artikel 16.3 i förordningen. I artikel 17.2 i förordningen föreskrivs att om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse, får den CSIRT-enhet som utsetts till samordnare för den berörda medlemsstaten, efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta.

Efter det att en säkerhetsuppdatering eller någon annan form av korrigerande eller riskreducerande åtgärd finns tillgänglig ska Enisa, i samförstånd med tillverkaren av den berörda produkten med digitala element, lägga till den allmänt kända sårbarhet som anmälts enligt artikel 14 eller 15 i den europeiska sårbarhetsdatabas som administreras av Enisa i enlighet med artikel 17.5 i cyberresiliensförordningen. Enisa får dessutom lämna anmäld information till Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), om informationen är relevant för den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och -kriser på operativ nivå (artikel 17.1). Utifrån de mottagna anmälningarna utarbetar Enisa även med 24 månaders mellanrum en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämnar den till NIS-samarbetsgruppen.

2.1.3.2 Importörer, distributörer, tillverkarens representanter och andra ekonomiska aktörer

Utöver tillverkarna hänför sig kraven på produkter med digitala element med stöd av artiklarna 18–22 i cyberresiliensförordningen till importörer, distributörer och representanter som bemyndigats av tillverkaren. Importörerna och distributörerna ansvarar i princip för att säkerställa att en produkt är försedd med behöriga märkningar och dokumentation då den släpps upp marknaden. Dessutom ställs krav på tillverkarens representanter då tillverkaren har tilldelat dem uppgifter som hör till tillverkarens ansvar (artikel 18). Med stöd av artiklarna 21–22 är det

möjligt att tillämpa skyldigheterna för tillverkare på importörer, distributörer eller andra aktörer då de gör en betydande ändring i en produkt och släpper ut eller tillhandahåller den på marknaden.

*Krav som tillämpas på importörer av produkter*

Artikel 19 i förordningen innehåller bestämmelser om skyldigheterna för importörer då de släpper ut produkter med digitala element på marknaden. Innan en produkt släpps ut på marknaden ska importören säkerställa att de tillämpliga förfarandena för bedömning av överensstämmelse har genomförts av tillverkaren, att tillverkaren har upprättat den tekniska dokumentationen, och att produkten med digitala element är försedd med CE-märkning och åtföljs av en EU-försäkran om överensstämmelse samt att produkten har ett serienummer eller en identifikationsuppgift, uppgifter om tillverkaren och information om när stödtiden tar slut. Om importören vet eller har skäl att misstänka att en produkt med digitala element eller de processer som tillverkaren infört inte uppfyller kraven i förordningen, ska den omedelbart vidta de behövliga korrigerande åtgärderna för att göra produkten förenlig med förordningen eller vid behov dra tillbaka produkten från marknaden. En import ska fästa sin kontaktinformation på produkten och informera tillverkaren och marknadskontrollmyndigheterna om produkten orsakar en betydande cybersäkerhetsrisk.

*Krav som tillämpas på distributörer*

Artikel 20 i förordningen innehåller bestämmelser om skyldigheter för distributörer då de släpper ut produkter med digitala element på marknaden. Innan distributörerna tillhandahåller en produkt på marknaden ska distributörerna kontrollera att produkten med digitala element är försedd med CE-märkning, tillverkaren och importören har fogat de krävda uppgifterna till produkten och har försett distributören med alla dokument som krävs. Om en distributör på grundval av information som distributören förfogar över har skäl att tro att produkten eller processerna inte överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I, får distributören inte tillhandahålla produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med denna förordning. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk, ska distributören dessutom utan onödigt dröjsmål underrätta tillverkaren och marknadskontrollmyndigheterna om detta. Om produkten redan har släppts ut på marknaden ska distributören se till att vidta alla de korrigerande åtgärder som behövs eller dra tillbaka eller återkalla produkten, om så är lämpligt. En distributör ska dessutom utan oskäligt dröjsmål informera tillverkaren om sårbarheter i en produkt med digitala element vilka den fått kännedom om.

*Tillämpning av ansvaren för tillverkare på importörer, distributörer och andra aktörer*

Med stöd av artikel 21 i förordningen betraktas en distributör eller importör som en tillverkare vid tillämpning cyberresiliensförordningen då importören eller distributören släpper ut en produkt med digitala element på marknaden i eget namn eller under eget varumärke eller utför en väsentlig ändring av en produkt med digitala element som redan har släppts ut på marknaden. I så fall tillämpas skyldigheterna för tillverkare enligt artiklarna 13 och 14 på importören och distributören.

En fysisk eller juridisk person, annan än tillverkaren, importören eller distributören, som utför en väsentlig ändring av en produkt och tillhandahåller den produkten på marknaden ska anses som tillverkare med stöd av artikel 22 i förordningen. Den person som avses i punkt 1 i denna artikel ska omfattas av de skyldigheter som fastställs i artiklarna 13 och 14 när det gäller den del av produkten med digitala element som påverkas av den väsentliga ändringen. Om den

väsentliga ändringen påverkar cybersäkerheten för produkten med digitala element som helhet, tillämpas skyldigheterna i fråga om hela produkten.

*Tillverkarens representanter*

I enlighet med artikel 18 får en tillverkare genom skriftlig fullmakt utse en tillverkarens representant. Tillverkarens representant ska utföra de uppgifter som anges i fullmakten från tillverkaren och på begäran lämna en kopia av fullmakten till marknadskontrollmyndigheterna. I punkt 2 i artikeln föreskrivs de skyldigheter för en tillverkare som inte får delegeras till tillverkarens representant. Artikelns 3 punkt innehåller bestämmelser om de uppgifter som tillverkarens representant åtminstone ska utföra utifrån en fullmakt.

2.1.3.3 Förvaltare av programvara med fri och öppen källkod

Artikel 24 i förordningen innehåller bestämmelser om skyldigheterna för förvaltare av programvara med fri och öppen källkod. Med förvaltare av programvara med fri och öppen källkod avses i enlighet med artikel 3.14 i förordningen en juridisk person, annan än en tillverkare, som har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av specifika produkter med digitala element, vilka klassificeras som programvara med fri och öppen källkod och är avsedda för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft.

På förvaltare av programvara med fri och öppen källkod tillämpas förenklade formulär på det sätt som konstaterats i skäl 19 i ingressen till förordningen och samma skyldigheter som för dem som verkar som tillverkare tillämpas inte på dem. Med stöd av artikel 24 ska en förvaltare av programvara med fri och öppen källkod på ett verifierbart sätt införa och dokumentera en cybersäkerhetspolicy så att det utvecklas en säker produkt med digitala element och så att utvecklarna av den produkten effektivt hanterar sårbarheter. Förvaltarna av programvara med fri och öppen källkod ska samarbeta med marknadskontrollmyndigheterna och på deras begäran förse dem med sin dokumenterade cybersäkerhetspolicy.

Skyldigheterna avseende aktivt utnyttjade sårbarheter som gäller produkter med digitala element ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån de deltar i utvecklingen av produkter med digitala element. Skyldigheterna att rapportera och informera användarna om allvarliga incidenter som påverkar en produkts dataskydd tillämpas dessutom på förvaltare av programvara med fri och öppen källkod i den mån allvarliga incidenter som påverkar säkerheten för produkter med digitala element påverkar de nätverks- och informationssystem som tillhandahålls av förvaltarna för programvara med fri och öppen källkod för utvecklingen av sådana produkter.

Kommissionen kan inrätta frivilliga program för säkerhetsintyg som kategoriseras som en programvara med fri och öppen källkod för att bedöma cybersäkerhetsegenskaperna hos produkter med digitala element. Kommissionens befogenhet att anta delegerade akter om detta beskrivs nedan i avsnitt 2.1.9.

2.1.4 Påvisande av överensstämmelse med kraven

*Överensstämmelse med kraven*

Artikel 27 i cyberresiliensförordningen innehåller bestämmelser om presumtionen om överensstämmelse. Med stöd av 1 punkten i artikeln ska produkter med digitala element och processer som införts av tillverkaren som överensstämmer med harmoniserade standarder, eller

delar av sådana, vilka har offentliggjorts i Europeiska unionens officiella tidning, förutsättas överensstämma med de väsentliga cybersäkerhetskrav i bilaga I som omfattas av dessa standarder eller delar av dem.

Med stöd av artikel 27.8 ska man dessutom anse att produkter är förenliga med de väsentliga cybersäkerhetskrav som fastställts i bilaga I även då de innehåller sådana produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkran om överensstämmelse eller ett certifikat enligt en europeiska ordning för cybersäkerhetscertifiering har utfärdats, om EU-försäkran om överensstämmelse eller det europeiska cybersäkerhetscertifikatet täcker dessa krav

Med stöd av artikel 27 har kommissionen befogenhet att anta delegerade akter om godkännande av gemensamma specifikationer, då ingen standard har publicerats, och om specificering av kompatibiliteten för europeiska ordningar för cybersäkerhetscertifiering. Befogenheten att anta delegerade akter beskrivs nedan i avsnitt 2.1.9.

*EU-försäkran om överensstämmelse, CE-märkning och teknisk dokumentation*

En tillverkare ska i enlighet med artikel 13.12 och artikel 28 upprätta en EU-försäkran om överensstämmelse, i vilken det konstateras att det har visats att de tillämpliga väsentliga cybersäkerhetskraven i bilaga I uppfylls. Genom att upprätta en EU-försäkran om överensstämmelse tar tillverkaren ansvaret för att en produkt med digitala element överensstämmer med krav med stöd av artikel 28.4 i förordningen. En EU-försäkran om överensstämmelse ska med stöd av artikel 28 i förordningen utformas i enlighet med mallen i bilaga V och innehålla de uppgifter som anges i de förfaranden för bedömning av överensstämmelse som fastställs i bilaga VIII. En EU-försäkran om överensstämmelse ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden. Om en produkt med digitala element omfattas av mer än en unionsrättsakt där det ställs krav på EU-försäkran om överensstämmelse, ska en enda EU-försäkran om överensstämmelse upprättas med avseende på alla dessa unionsrättsakter. Kommissionen ges befogenhet att anta delegerade akter om minimiinnehållet för EU-försäkran om överensstämmelse.

Bestämmelserna om CE-märkning ingår i artiklarna 29 och 30 i cyberresiliensförordningen. En CE-märkning ska fästas på en produkt med digitala element i enlighet med artikel 30 i cyberresiliensförordningen.

Det finns bestämmelser om den tekniska dokumentation som ska fästas på förpackningen i artikel 31 i förordningen. Teknisk dokumentation ska upprättas innan en produkt släpps ut på marknaden och vid behov uppdateras åtminstone under stödtiden för produkten. Den tekniska dokumentationen ska innehålla åtminstone de delar som fastställts i bilaga VII till förordningen och alla relevanta uppgifter eller detaljerade beskrivningar av de metoder med vilka tillverkaren fastställts att produkten och processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskrav som fastställts i bilaga I. Kommissionen har befogenhet att anta delegerade akter för att komplettera de delar som ska inkluderas i den tekniska dokumentationen.

*Bedömning av överensstämmelse med kraven*

Det finns bestämmelser om förfarandet för att bedöma överensstämmelsen med kraven för en produkt med digitala element i artikel 32 i förordningen. Överensstämmelse med kraven visas med något förfarande för bedömning av överensstämmelse enligt bilaga VIII, vilka baserar sig på de moduler som fastställts i Europaparlamentets och rådets beslut nr 768/2008/EG.

Förfarandena för bedömning har i bilagan delats in i fyra moduler (A, B, C och H) utifrån den risknivå för produktbedömningen som lämpar sig för förfarandet. Med stöd av punkt 1 i artikeln ska tillverkaren visa överensstämmelse med de väsentliga cybersäkerhetskraven genom att använda

- förfarandet för intern kontroll (baserat på modul A) enligt bilaga VIII,
- EU-typkontroll (baserat på modul B) enligt bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C),
- överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller
- en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9, om sådan finns och i tillämpliga fall.

I fråga om andra än viktiga produkter enligt bilaga III och kritiska produkter enligt bilaga IV kan överensstämmelse således visas bland annat utifrån en självbedömning av tillverkaren.

Punkterna 2 och 3 i artikeln gäller påvisande av överensstämmelse med kraven för viktiga produkter enligt bilaga III. Det tillämpliga förfarandet fastställs beroende på om produkten hör till kategori I eller II i bilaga III. Med stöd av artikel 32.2 krävs att viktiga produkter som hör till klass I antingen tillämpar en harmoniserad standard eller certifiering eller EU-typkontroll som baserar sig på bedömning av tredje part eller fullständig kvalitetssäkring. Med stöd av artikel 33.3 krävs att viktiga produkter som hör till klass II alltid är föremål för en bedömning av tredje part, även om produkten är förenlig med harmoniserade standarder eller en europeisk ordning för cybersäkerhetscertifiering.

I fråga om kritiska produkter enligt bilaga IV ska man med stöd av artikel 32.4 inhämta ett certifikat enligt EU:s cybersäkerhetsakt, vilket är av minst betydande assuransnivå. Om ett sådant inte är tillgängligt, ska produkten bedömas med något av de bedömningsförfaranden som baserar sig på bedömning av tredje part och som gäller vad som bestäms i klass II för produkter enligt bilaga III.

Med stöd av artiklarna 7 och 8 har kommissionen befogenhet att anta delegerade akter om produktkategorierna i bilaga III och bilaga IV enligt vad som beskrivs nedan i avsnitt 2.1.9.

Tillverkare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som omfattas av de kategorier som anges i bilaga III ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I genom att använda ett av de förfaranden som avses i artikel 35.1, förutsatt att den tekniska dokumentation som avses i artikel 31 görs tillgänglig för allmänheten när dessa produkter släpps ut på marknaden.

Artikel 33 i förordningen gäller medlemsstaternas stödåtgärder i synnerhet för mikroföretag och små företag. Med stöd av punkt 1 i artikeln ska medlemsstaterna, när så är lämpligt, vidta åtgärder som är anpassade till mikroföretags och små företags behov, såsom information, utbildning, kommunikation och stöd för testning. Med stöd av punkt 2 kan medlemsstaterna vid behov inrätta regulatoriska sandlådor för cyberresiliens. Enligt skäl 97 till förordningen bör syftet med regulatoriska sandlådor vara att främja innovation och konkurrenskraft för företag genom att inrätta kontrollerade testmiljöer innan produkter med digitala element släpps ut på marknaden. Regulatoriska sandlådor bör bidra till att förbättra rättssäkerheten för alla aktörer

som omfattas av denna förordning och underlätta och påskynda tillträdet till unionsmarknaden för produkter med digitala element, särskilt när de tillhandahålls av mikroföretag och små företag, inbegripet uppstartsföretag.

### 2.1.5 Anmälda organ

I kapitel IV i cyberresiliensförordningen (artiklarna 35–51) finns det bestämmelser om godkännande av organ för bedömning av överensstämmelse med kraven och anmälning av dem som anmälda organ, som utför bedömning av överensstämmelse som görs av tredje part i fråga om produkter med digitala element. Kapitlet innehåller även bestämmelser om bland annat utseendet av myndigheten med ansvar för anmälan, dess uppgifter, anmälningsförfarandet och de anmälda organens kompetens och skyldigheter.

Med stöd av artikel 35 ska medlemsstaterna till kommissionen och övriga medlemsstater anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning. Dessutom ska medlemsstaterna sträva efter att senast den 11 december 2026 säkerställa att det finns ett tillräckligt antal anmälda organ i unionen för att utföra bedömningar av överensstämmelse, i syfte att undvika flaskhalsar och hinder för marknadstillträde.

Med stöd av artikel 36 i förordningen ska medlemsstaterna utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll. Dessutom får medlemsstaterna besluta att bedömningen och övervakningen av anmälda organ ska utföras av ett nationellt ackrediteringsorgan. Den myndighet som ansvarar för anmälan ska uppfylla kraven enligt artikel 37. Medlemsstaterna ska underrätta kommissionen om förfaranden enligt artikel 38 i anknytning till bedömningen, anmälningen och övervakningen av organ för bedömning av överensstämmelse.

Det finns bestämmelser om kraven på anmälda organ i artikel 39 i cyberresiliensförordningen. För att ett organ för bedömning av överensstämmelse ska kunna anmälas, ska det uppfylla de krav som föreskrivs i artikel 39.2–39.12. Ett organ för bedömning av överensstämmelse ska bland annat kunna utföra alla förfaranden för bedömning av överensstämmelse enligt bilaga VII i fråga om de produkter eller produktkategorier för vilka det anmälts. När ett organ för bedömning av överensstämmelse kan visa att det är förenligt med de förutsättningar som fastställts i sådana väsentliga harmoniserade standarder eller i delar av dessa, vars anhängiggörande har publicerats i Europeiska unionens officiella tidning, förmodas det med stöd av artikel 40 i cyberresiliensförordningen uppfylla de krav som föreskrivs i artikel 39 till den del som de tillämpliga harmoniserade standarderna täcker dessa krav. Artikel 41 i cyberresiliensförordningen innehåller bestämmelser om villkoren för att utföra uppgifterna för ett anmält organ som underleverans eller via ett dotterbolag. Bland annat en underleverantör eller ett dotterbolag ska även uppfylla kraven i artikel 39. Dessutom ska ett anmält organ ta ansvar för en underleverantörs eller ett dotterbolags arbete, anmäla underleveransen till myndigheten med ansvar för anmälan och komma överens om detta med tillverkaren.

Det finns bestämmelser om ansökan om anmälning av ett organ för bedömning av överensstämmelse i artikel 42 i cyberresiliensförordningen, medan anmälningsförfarandet regleras i artikel 43. Ansökan om anmälning av ett organ för bedömning av överensstämmelse lämnas till myndigheten med ansvar för anmälan i den medlemsstat där organet för bedömning av överensstämmelse är etablerat. Med stöd av artikel 43.5 kan uppgifterna för ett anmält organ skötas endast om kommissionen eller de andra medlemsstaterna inte har rest några invändningar inom två veckor från anmälan, i de fall då ett ackrediteringsintyg används, eller inom två månader från anmälan, i de fall då ingen ackreditering används.

När den myndighet som ansvarar för anmälan konstaterar eller får veta att ett anmält organ inte uppfyller de krav som fastställts i artikel 39 eller inte iakttar sina skyldigheter, ska myndigheten med ansvar för anmälan med stöd av artikel 45 begränsa anmäla eller återkalla den tillsvidare eller helt och hållet, beroende på hur allvarligt det uteblivna iakttagandet av kraven eller skyldigheterna varit. Dessutom ska en avgränsning eller ett återkallande omedelbart anmälas till kommissionen och övriga medlemsstater. Artikel 46 i cyberresiliensförordningen innehåller bestämmelser om ifrågasättande av de anmälda organens kompetens. Om kommissionen konstaterar att ett anmält organ inte har uppfyllt eller inte längre uppfyller kraven för anmälan, ska den meddela detta till den anmälande medlemsstaten och anmoda medlemsstaten att vidta erforderliga korrigerande åtgärder och vid behov återta anmälan.

Det finns bestämmelser om de anmälda organens skyldigheter i artikel 47 i cyberresiliensförordningen. Anmälda organ ska utföra bedömningar av överensstämmelse i enlighet med förfarandena för bedömning av överensstämmelse i artikel 32 och bilaga VIII. Artikel 49 i cyberresiliensförordningen innehåller bestämmelser om de anmälda organens informationsskyldighet till den anmälande myndigheten och andra anmälda organ.

Medlemsstaten ska med stöd av artikel 48 i cyberresiliensförordningen säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut. Dessutom ska medlemsstaten säkerställa att dess anmälda organ deltar i det samarbete som kommissionen koordinerar i enlighet med artikel 51.

### 2.1.6 Marknadskontroll och genomförande

*Marknadskontrollmyndighet*

Det finns bestämmelser om marknadskontrollen av produkter som omfattas av cyberresiliensförordningens tillämpningsområde i kapitel V i förordningen (artiklarna 52–60). Enligt artikel 52 i förordningen tillämpas på marknadskontrollen av produkter vid sidan om de produkter som omfattas av förordningens tillämpningsområde även förordning (EU) 2019/1020 (den så kallade *marknadskontrollförordningen*).

Artikel 52.2 i förordningen förutsätter att medlemsstaterna utser en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av förordningen. Således tilldelas marknadskontrolluppgiften till en eller flera myndigheter enligt det nationella handlingsutrymmet. Vid sidan om marknadskontrollen ansvarar marknadskontrollmyndigheterna även för att övervaka de skyldigheter som föreskrivits i artikel 24 för en förvaltare av programvara med fri och öppen källkod.

Med stöd av artikel 52.8 i förordningen ska medlemsstaterna säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser, inbegripet vid behov verktyg för automatisk databehandling samt personalresurser med nödvändig cybersäkerhetskompetens för att kunna fullgöra sina uppgifter enligt denna förordning.

Artikel 52.14 i förordningen innehåller en specialbestämmelse om marknadskontrollen av AI-system med hög risk. Med stöd av punkten ska för produkter med digitala element som omfattas av tillämpningsområdet för cyberresiliensförordningen och som klassificeras som AI-system med hög risk enligt artikel 6 i förordningen om artificiell intelligens de marknadskontrollmyndigheter som utsetts enligt den förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i cyberresiliensförordningen. Till denna del är anordnandet av marknadskontrollen inte förknippat med nationellt handlingsutrymme. De marknadskontrollmyndigheter som utsetts enligt förordningen om artificiell intelligens ska vid

behov samarbeta med de marknadskontrollmyndigheter som utsetts i enlighet med den här förordningen och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheterna enligt cyberresiliensförordningen, med de CSIRT-enheter som utsetts till samordnare och Enisa.

I artikel 52 i förordningen finns det även bestämmelser om marknadskontrollmyndigheternas samarbete och informationsutbytet, marknadskontrollmyndigheternas skyldighet att ge konsumenterna information om kanalen för överklagan, marknadskontrollmyndighetens rapporteringsskyldighet, rådgivnings- och bedömningshjälpen av CSIRT-enheterna och Enisa samt marknadskontrollmyndighetens möjlighet att ge ekonomiska aktörer anvisningar och rådgivning i anknytning till genomförandet av förordningen. Vid behov ska marknadskontrollmyndigheterna samarbeta bland annat med de nationella myndigheterna som utfärdar cybersäkerhetscertifiering, CSIRT-enheten och Enisa, andra marknadskontrollmyndigheter, de myndigheter som övervakar dataskyddsregleringen och de relevanta berörda parterna (artikel 52.4–52.12). Dessutom innehåller artikeln bestämmelser om inrättandet av den administrativa samarbetsgrupp som består av företrädare för marknadskontrollmyndigheterna. Dessutom innehåller artikel 52.16 en specialbestämmelse om marknadskontrollmyndighetens skyldighet att följa fastställandet av stödtiden.

Artikel 53 i förordningen innehåller bestämmelser om skyldigheten att bevilja marknadskontrollmyndigheterna, på ett språk som lätt kan förstås av dem, tillgång till dokumentation eller data som behövs för att bedöma överensstämmelsen med kraven i cyberresiliensförordningen för produkter med digitala element och de processer som införts av tillverkarna.

*Reglering på nationell nivå*

Artikel 54 i förordningen innehåller bestämmelser om förfarandet på nationell nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk. Artikeln ställer en bedömningsskyldighet för marknadskontrollmyndigheten i situationer där den har en tillräcklig grund att anse att en produkt som omfattas av förordningens tillämpningsområde orsakar en betydande cybersäkerhetsrisk. Utvärderingen ska göras utan oskäligt dröjsmål och vid behov i samarbete med CSIRT-enheten. Om marknadskontrollmyndigheten konstaterar att en produkt inte överensstämmer med kraven, ska den kräva att den ekonomiska aktören vidtar de behövliga åtgärderna för att produkten ska överensstämma med kraven, dra tillbaka den från marknaden eller för att ordna återkallandet av den. Marknadskontrollmyndigheten har en skyldighet att anmäla utvärderingens resultat och åtgärder till det behöriga anmälda organet. Om överensstämmelsen med kraven inte begränsar sig till den relevanta medlemsstatens territorium, ska en anmälan göras även till kommissionen och de andra medlemsstaterna. Artikeln innehåller dessutom bestämmelser om marknadskontrollmyndighetens skyldighet att vidta provisoriska åtgärder, om en ekonomisk aktör inte vidtar de krävda åtgärderna. Marknadskontrollmyndigheten ska anmäla provisoriska åtgärder till kommissionen och andra medlemsstater.

I bedömningen av signifikansen för en produkts säkerhetsrisk ska marknadskontrollmyndigheten beakta även andra tekniska riskfaktorer, om de fastställts som ett resultat av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor i enlighet med artikel 22 i NIS 2-direktivet. Om marknadskontrollmyndigheten har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk på grund av andra än tekniska riskfaktorer, ska den med stöd av NIS 2-direktivet anmäla detta till de behöriga myndigheterna.

*Unionens skyddsförfarande*

Artikel 55 i förordningen innehåller bestämmelser om unionens förfarande i fråga om skyddsåtgärder. Unionens förfarande i fråga om skyddsåtgärder tillämpas på situationer där man har gjort invändningar mot en åtgärd som vidtagits av marknadskontrollmyndigheten i en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten. Om kommissionen anser att marknadskontrollmyndighetens åtgärd är berättigad, ska alla medlemsstater vidta de åtgärder som krävs för att säkerställa att den produkt med digitala element som inte uppfyller kraven dras tillbaka från deras marknader.

*Förfarandet på unionsnivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk*

Artikel 56 i förordningen innehåller bestämmelser om förfarandet på unionsnivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk. Om kommissionen har tillräckliga skäl att anse att en produkt med digitala element som utgör en betydande cybersäkerhetsrisk inte uppfyller kraven enligt förordningen, ska den informera de berörda marknadskontrollmyndigheterna. Förfarandena enligt artiklarna 54 och 55 tillämpas på bedömning av marknadskontrollmyndigheten som görs utifrån ett meddelande av kommissionen. I situationer som kräver omedelbara åtgärder kan kommissionen göra en bedömning av överensstämmelsen och besluta om korrigerande eller begränsande åtgärder på unionsnivå.

Utöver marknadskontrollmyndigheterna anmäler kommissionen en produkt som orsakar en betydande cybersäkerhetsrisk på grund av andra än tekniska riskfaktorer vid behov till de behöriga myndigheterna enligt NIS 2-direktivet och de ska vid behov samarbeta med dessa myndigheter. Kommissionen granskar även väsentligheten för identifierade risker i anknytning till den aktuella produkten med digitala element som en del av sina uppgifter som anknyter till den samordnade bedömningen av säkerhetsrisker på unionsnivå i kritiska leveranskedjor enligt artikel 22 i NIS 2-direktivet och hör vid behov NIS-samarbetsgruppen och Enisa.

Artikel 56.3–56.6 i förordningen innehåller bestämmelser om kommissionens åtgärder i vissa exceptionella situationer. Med stöd av punkt 5 i artikeln får kommissionen anta genomförandeakter för att föreskriva korrigerande eller begränsande åtgärder på unionsnivå, inbegripet krav på att de berörda produkterna med digitala element ska dras tillbaka från marknaden eller återkallas, inom en rimlig tid i förhållande till typen av risk.

*Överensstämmande produkter som orsakar en betydande cybersäkerhetsrisk*

Artikel 57 i förordningen innehåller bestämmelser om åtgärder avseende produkter som överensstämmer med kraven, men utgör en betydande cybersäkerhetsrisk. Enligt artikeln ska marknadskontrollmyndigheten i en medlemsstat kräva att en ekonomisk aktör vidtar alla lämpliga åtgärder om den, efter att ha gjort en utvärdering enligt artikel 54, konstaterar att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med denna förordning, men att de utgör en betydande cybersäkerhetsrisk och någon annan risk som nämns i punkt 1 a–d i artikeln. Medlemsstaten ska anmäla åtgärderna omedelbart till kommissionen och de andra medlemsstaterna för en bedömning av fortsatta åtgärder.

*Formell bristande överensstämmelse för produkter*

Artikel 58 i förordningen innehåller bestämmelser om formell bristande överensstämmelse. Om marknadskontrollmyndigheten i en medlemsstat konstaterar att en produkt inte uppfyller de

formella kraven, ska den ålägga den berörda tillverkaren att avhjälpa den bristande överensstämmelsen. De formella kraven på överensstämmelse utgörs av de omständigheter som räknas upp i artikel 58.1, såsom bristfälligt fästande av CE-märkningen, bristfälligt utarbetande av EU-försäkringar om överensstämmelse eller brister i den tekniska dokumentationen. Om tillverkaren inte avhjälper en bristande överensstämmelse, ska den berörda medlemsstaten vidta lämpliga åtgärder för att begränsa eller förbjuda tillhandahållandet av produkten med digitala element på marknaden eller säkerställa att den återkallas eller dras tillbaka från marknaden.

*Marknadskontrollmyndigheternas gemensamma aktiviteter och samtidiga samordnade kontrollåtgärder*

Artikel 59 i förordningen innehåller bestämmelser om marknadskontrollmyndigheternas gemensamma aktiviteter. Marknadskontrollmyndigheterna i medlemsstaterna får komma överens med andra berörda myndigheter om att genomföra gemensamma aktiviteter för att säkerställa cybersäkerheten och skyddet av konsumenter. Även kommissionen eller Enisa kan föreslå gemensamma aktiviteter, om det finns tecken på eller information om att produkter som omfattas av förordningens tillämpningsområde i flera medlemsstater inte uppfyller kraven i förordningen. Marknadskontrollmyndigheterna och kommissionen ska vid behov säkerställa att de gemensamma aktiviteterna inte leder till konkurrenssnedvridning mellan de ekonomiska aktörerna. Artikel 60 i förordningen innehåller bestämmelser om ”samtidiga samordnade kontrollåtgärder”, som i enlighet med huvudregeln samordnas av kommissionen.

### 2.1.7 Administrativa påföljder

I artikel 64 i cyberresiliensförordningen åläggs medlemsstaterna att utfärda bestämmelser om påföljder som tillämpas på överträdelse av förordningen, det vill säga en administrativ påföljdsavgift.

Det sanktionssystem som cyberresiliensförordningen förutsätter har tre steg på det sätt som artikel 64.2–64.4 förutsätter. Punkterna innehåller bestämmelser om grunderna för att påföra administrativa sanktionsavgifter och fastställer maximibeloppen av sanktionsavgifter för överträdelse av de olika skyldigheterna i förordningen.

Maximibeloppen av de administrativa sanktionsavgifterna har graderats i tre olika klasser. I den första klassen ska en administrativ sanktionsavgift påföras för uteblivet fullgörande av de väsentliga cybersäkerhetskrav som fastställts i bilaga I (punkt 2) och de skyldigheter som föreskrivits i artiklarna 13 och 14. Sanktionsavgiften uppgår högst till 15 miljoner euro eller om överträdelsen gjorts av företag, till högst 2,5 procent av dess globala omsättning för föregående räkenskapsperiod, beroende på vilket av dessa belopp som är högre. Skyldigheterna hänför sig i huvudsak till tillverkaren av en produkt med digitala element. Den andra klassen (punkt 3) handlar om överträdelse av de skyldigheter till vilka de hänvisas i punkten om ekonomiska aktörer och anmälda organ, för vilka en administrativ sanktionsavgift ska påföras till ett belopp som är högst 10 miljoner euro eller 2 procent av den globala omsättningen för föregående räkenskapsperiod. Den fjärde klassen (punkt 4) utgörs av tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och marknadskontrollmyndigheter som svar på en begäran, för vilket en administrativ sanktionsavgift på upp till 5 miljoner euro eller upp till 1 procent av den globala omsättningen för det föregående räkenskapsåret, beroende på vilket som är högst.

Punkt 5 innehåller bestämmelser om de omständigheter som ska beaktas utöver alla relevanta förhållande i den aktuella situationen då en påföljdsavgift påförs. Med stöd av punkt 6 i artikeln

ska marknadskontrollmyndigheter som påför administrativa sanktionsavgifter meddela marknadskontrollmyndigheterna i andra medlemsstater detta.

Artikel 64.10 i cyberresiliensförordningen innehåller bestämmelser om påförande av administrativa påföljdsavgifter. Med stöd av undantaget tillämpas bestämmelserna om den administrativa påföljdsavgiften inte på tillverkare som klassificeras som mikroföretag eller små företag när det gäller underlåtenhet att iaktta den tidsfrist på 24 timmar för att göra en anmälan enligt i artikel 14.2 a eller 14.4 a Med stöd av undantaget tillämpas bestämmelserna om den administrativa påföljdsavgiften inte heller på överträdelser av cyberresiliensförordningen som begås av förvaltare av programvara med fri och öppen källkod.

Med stöd av artikel 65 i cyberresiliensförordningen tillämpas direktivet om grupptalan (EU) 2020/1828 på grupptalan om ekonomiska aktörers överträdelser av bestämmelserna i denna förordning vilka skadar eller kan skada konsumenternas kollektiva intresse. Utifrån överträdelse av cyberresiliensförordningen ska det således vara möjligt att väcka en grupptalan enligt direktivet om grupptalan.

### 2.1.8 Ikraftträdande- och övergångsbestämmelser

I enlighet med artikel 71 tillämpas cyberresiliensförordningen från och med den 11 december 2027. Kapitel IV som gäller anmälda organ tillämpas från och med den 11 juni 2026 och artikel 14 som gäller rapporteringsskyldigheterna från och med den 11 september 2026.

Kraven i cyberresiliensförordningen tillämpas på produkter med digitala element som har släppts ut på marknaden före den 11 december 2027 endast om de, från och med den dagen, är föremål för en väsentlig ändring (artikel 69.2). Enligt artikel 3.30 i förordningen avses med väsentlig ändring en ändring av produkten med digitala element efter dess utsläppande på marknaden, vilken påverkar produktens överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I del I eller leder till en ändring av det avsedda ändamål för vilket produkten har bedömts.

De skyldigheter som fastställs i artikel 14 tillämpas med stöd av artikel 69.3 på alla produkter med digitala element som omfattas av denna förordnings tillämpningsområde och som har släppts ut på marknaden före den 11 december 2027.

Med stöd av artikel 69.1 i cyberresiliensförordningen ska EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av annan unionsharmoniseringslagstiftning än denna förordning fortsätta att gälla till och med den 11 juni 2028 eller enligt deras giltighet.

### 2.1.9 Kommissionens befogenheter att anta delegerade akter

Cyberresiliensförordningen innehåller flera bestämmelser om kommissionens befogenheter att anta delegerade akter.

*Delegerade akter*

Med stöd av andra stycket i artikel 2.5 ges kommissionen befogenhet att anta delegerade akter, som preciserar bestämmelsen om avgränsning av tillämpningsområdet för kraven i förordningen, till den del som den sektorsspecifika lagstiftningen innehåller en motsvarande eller högre nivå på cybersäkerhetsnivån vilken fastställts för produktkategorin.

Med stöd av artikel 7.3 kan kommissionen anta delegerade akter för att ändra bilaga III genom att införa en ny kategori inom varje klass i förteckningen över kategorier av produkter med digitala element och specificera dess definition, flytta en kategori av produkter från en klass till en annan eller stryka en befintlig kategori från förteckningen.

Med stöd av artikel 8.1 kan kommissionen anta delegerade akter, med vilka ett cybersäkerhetscertifikat enligt en europeisk ordning för cybersäkerhetscertifiering krävs av produkter enligt bilaga IV.

Med stöd av artikel 8.2 kan kommissionen anta delegerade akter med vilka bilaga IV ändras genom att lägga till eller avlägsna kategorier av kritiska produkter med digitala element.

Med stöd av artikel 13.8.4 kan kommissionen anta delegerade akter med vilka minimilängden för stödtiden fastställs för vissa produktkategorier.

Med stöd av artikel 14.9 ska kommissionen senast den 11 december anta delegerade akter med vilka villkoren fastställs för tillämpning av orsaker relaterade till cybersäkerheten då förmedlingen av anmälningar skjuts upp på det sätt som avses i artikel 16.2 i cyberresiliensförordningen.

Med stöd av artikel 25 kan kommissionen anta delegerade akter med vilka man inrättar frivilliga program för säkerhetsintyg som gör det möjligt för utvecklare eller användare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod samt andra tredje parter att bedöma sådana produkters överensstämmelse med cyberresiliensförordningen.

Med stöd av artikel 27.9 kan kommissionen anta delegerade akter med vilka man specificerar de europeiska ordningar för cybersäkerhetscertifiering som kan användas för att visa att produkter med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I, eller delar av dessa.

Med stöd av artikel 28.5 kan kommissionen anta delegerade akter med vilka man lägger till uppgifter till det minimiinnehåll för EU-försäkran om överensstämmelse som fastställs i bilaga V, för att ta hänsyn till den tekniska utvecklingen.

Med stöd av artikel 31.5 kan kommissionen anta delegerade akter med vilka man lägger till aspekter som ska ingå i den tekniska dokumentationen enligt bilaga VII för att ta hänsyn till den tekniska utvecklingen, samt utveckling som skett under denna förordnings genomförandeprocess.

*Genomförandeakter*

Med stöd av artikel 7.4 ska kommissionen senast den 11 december 2025 anta en genomförandeakt som specificerar den tekniska beskrivningen av kategorierna av produkter med digitala element vilka fastställts i bilagorna III och IV.

Med stöd av artikel 13.24 kan kommissionen anta en genomförandeakt som preciserar formen på programvaruförteckningen för material och dess delfaktorer.

Med stöd av artikel 14.10 kan kommissionen anta genomförandeakter som preciserar formen på anmälningar enligt artiklarna 14–16 och de anknutna förfarandena.

Med stöd av artikel 27.2 kan kommissionen anta genomförandeakter med vilka man fastställer gemensamma specifikationer som omfattar tekniska krav, om de behövliga standarderna inte är tillgängliga.

Med stöd av artikel 30.6 kan kommissionen anta genomförandeakter med vilka man fastställer tekniska specifikationer för etiketter, piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, deras stödperioder och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten hos produkter med digitala element.

Med stöd av artikel 33.5 kan kommissionen genom en genomförandeakt precisera det förenklade formuläret för teknisk dokumentation med hänsyn till mikroföretagens och småföretagens behov.

Med stöd av artiklarna 56.5 och 58.9 kan kommissionen anta genomförandeakter om korrigerande eller begränsande åtgärder på unionsnivå som gäller överensstämmelsen för produkter med digitala element.

*Anvisningar och förteckning*

Kommissionen kan dessutom i enlighet med artikel 26.1 offentliggöra andra anvisningar som hjälper de ekonomiska aktörerna att tillämpa förordningen.

Kommissionen ska i enlighet med artikel 26.2 föra en förteckning över delegerade akter och genomförandeakter som antagits med stöd av cyberresiliensförordningen.

2.1.10 Det nationella handlingsutrymmet och behovet av kompletterande reglering

Cyberresiliensförordningen är en direkt tillämplig förordning och den innehåller i princip inte nationellt handlingsutrymme.

Med stöd av artikel 4.1 i cyberresiliensförordningen får medlemsstaterna inte, med hänvisning till aspekter som omfattas av cyberresiliensförordningen, hindra att produkter med digitala element som uppfyller kraven i cyberresiliensförordningen tillhandahålls på marknaden. Således kan produkter med digitala element som hör till cyberresiliensförordningens tillämpningsområde framöver regleras nationellt endast till den del som det inte handlar om en omständighet som inte omfattas av cyberresiliensförordningens tillämpningsområde. Dessutom hindrar förordningen inte medlemsstaterna från att ställa högre cybersäkerhetskrav på en produkt med digitala element då den skaffas eller används för ett ändamål som avses i artikel 5.1 i cyberresiliensförordningen.

Cyberresiliensförordningen innehåller nationellt handlingsutrymme om ordnandet av myndighetsuppgifterna i anknytning till anmälning av organ för bedömning av överensstämmelse och ordnande av marknadskontrollen.

Med stöd av artikel 36 ska medlemsstaterna utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll. Medlemsstaterna får besluta att bedömningen och övervakningen av organ för bedömning av överensstämmelse ska utföras av ett nationellt ackrediteringsorgan (artikel 36.2). Medlemsstaterna ska till kommissionen och de andra medlemsstaterna anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning och sträva efter att senast den 11 december

2026 säkerställa att det finns ett tillräckligt antal anmälda organ i unionen för att utföra bedömningar av överensstämmelse (artikel 35). Medlemsstaterna ska dessutom säkerställa att det på nationell nivå finns ett förfarande för överklagande av de anmälda organens beslut (artikel 48).

Varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av marknadskontrollförordningen och för att genomföra marknadskontrollåtgärderna (artikel 55.2). Medlemsstaterna ska säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser, inbegripet vid behov verktyg för automatisk databehandling samt personalresurser med nödvändig cybersäkerhetskompetens för att kunna fullgöra sina uppgifter enligt denna förordning (artikel 52.8). Marknadskontrollmyndighetens uppgifter anvisas i cyberresiliensförordningen och marknadskontrollförordningen.

Med stöd av artikel 64 i cyberresiliensförordningen ska medlemsstaterna utfärda bestämmelser om påföljder som tillämpas på överträdelse av cyberresiliensförordningen och vidta alla behövliga åtgärder för att säkerställa att de genomförs. Påföljderna ska vara effektiva, proportionella och avskräckande. Artikel 64.2–64.4 i förordningen innehåller bestämmelser om de överträdelser som en medlemsstat ska sanktionera och om maximibeloppen av de administrativa böter som påförs för sådana. Enligt artikel 64.7 ska en medlemsstat dessutom fastställa regler om huruvida en myndighet eller ett offentligt organ kan påföras administrativa sanktionsavgifter.

Med stöd av artikel 5.2 i cyberresiliensförordningen ska medlemsstaterna, när produkter med digitala element som omfattas av denna förordnings tillämpningsområde upphandlas, säkerställa att överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till denna förordning, inbegripet tillverkarnas förmåga att ändamålsenligt hantera sårbarheter, beaktas i upphandlingsprocessen, dock utan att begränsa tillämpningen av direktiven om offentliga upphandlingar.

Med stöd av artikel 10 i cyberresiliensförordningen ska en medlemsstat vid behov med stöd av Europeiska kompetenscentrumet för cybersäkerhet och Enisa främja åtgärder och strategier som syftar till att:

a) utveckla cybersäkerhetskompetensen och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse,

b) förbättra samarbetet mellan den privata sektorn, ekonomiska aktörer, bland annat genom omskolning eller kompetenshöjning för tillverkares anställda, konsumenter, utbildningsanordnare och även offentliga förvaltningar, och därmed utöka möjligheterna för unga att få jobb inom cybersäkerhetssektorn.

Artikel 33 i cyberresiliensförordningen innehåller bestämmelser om medlemsstaternas stödåtgärder till mikroföretag och små och medelstora företag. Med stöd av punkt 1 i artikeln ska medlemsstaterna, när så är lämpligt, vidta följande åtgärder som är anpassade till mikroföretags och små företags behov:

a) anordna särskild informations- och utbildningsverksamhet om tillämpningen av denna förordning,

b) inrätta en särskild kanal för kommunikation med mikroföretag och små företag och, när så är lämpligt, lokala myndigheter för att ge råd och besvara frågor om genomförandet av denna förordning,

c) stödja provning och bedömning av överensstämmelse, när så är lämpligt även med stöd av Europeiska kompetenscentrumet för cybersäkerhet.

Med stöd av artikel 33.2 i cyberresiliensförordningen kan medlemsstaterna vid behov inrätta regulatoriska sandlådor för cyberresiliens. En sådan regulatorisk sandlåda ska innehålla övervakade sandlådor för innovativa produkter med digitala element, vilka underlättar utvecklingen, planeringen, valideringen och testningen av dessa för att iaktta förordningen, innan produkterna släpps ut på marknaden. Kommissionen och vid behov Enisa kan erbjuda tekniskt stöd, rådgivning och instrument för att inrätta regulatoriska sandlådor och för verksamheten i dessa. Regulatoriska sandlådor ska inrättas under direkt tillsyn och handledning av marknadskontrollmyndigheterna och med deras stöd. Medlemsstaterna ska underrätta kommissionen och övriga marknadskontrollmyndigheter om inrättande av en regulatorisk sandlåda via den administrativa samarbetsgruppen. De regulatoriska sandlådorna ska inte påverka de behöriga myndigheternas tillsynsbefogenheter och korrigerande befogenheter. Medlemsstaterna ska säkerställa öppen, rättvis och transparent tillgång till regulatoriska sandlådor, och i synnerhet underlätta tillgång för mikroföretag och små företag, inbegripet uppstartsföretag.

Med stöd av artiklarna 65 och 67 i cyberresiliensförordningen ska direktivet om grupptalan tillämpas även på grupptalan som väcks mot ekonomiska aktörer för överträdelser av cyberresiliensförordningen, vilka skadar eller kan skada konsumenters kollektiva intresse.

## 2.2 Cybersäkerhetsakten

### 2.2.1 En europeisk ordning för cybersäkerhetscertifiering

Målet med cybersäkerhetsakten är att trygga den inre marknadens funktion genom att stärka cybersäkerheten, toleransförmågan och förtroendet i EU. Förordningen innehåller bestämmelser om cybersäkerhetsverket Enisa och EU:s certifieringsregelverk för cybersäkerhet, vilket möjliggör certifiering av IKT-produkter, IKT-tjänster och IKT-processer och i och med ändringsförordningen (EU) 2025/37 även dataskyddstjänster utifrån europeiska ordningar för cybersäkerhetscertifiering som inrättas separat.

Innehållet i cybersäkerhetsakten har tidigare beskrivits i regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den, RP 98/2020 rd, s. 39–40. Detta avsnitt innehåller en koncis beskrivning av innehållet i förordningen till den del som det är betydelsefullt med tanke på förslagen i anknytning till cybersäkerhetscertifieringen. Avdelning III i cybersäkerhetsakten gäller inrättande av det europeiska ramverket för cybersäkerhetscertifiering.

I cybersäkerhetscertifieringen får en viss produkt, process eller tjänst ett certifikat som visar att den på en viss assuransnivå har bedömts uppfylla vissa fastställda cybersäkerhetskrav. Cybersäkerhetsakten i sig leder inte till att ett certifikat existerar och den innehåller inte skyldigheter som gäller inhämtande av certifikat. Genom förordningen fastställs en mekanism med vilken en europeisk ordning för cybersäkerhetscertifiering utarbetas. Genom förordningen fastställs uppgifter som gäller utarbetande av certifieringssystem, innehållet i dessa och tillsynen av dessa till Europeiska kommissionen, Enisa och medlemsstaternas myndigheter.

Med stöd av artikel 48 i cybersäkerhetsakten publicerar kommissionen ett löpande arbetsprogram för unionen, i vilket man ska inkludera en förteckning över sådana produkter, tjänster eller processer som kan gagnas av att omfattas av en europeisk ordning för cybersäkerhetscertifiering. Utifrån det löpande arbetsprogrammet kan kommissionen begära att Enisa bereder en föreslagen certifieringsordning eller granskar en giltig certifieringsordning. Enisa har på begäran av kommissionen skyldighet att bereda en certifieringsordning under de förutsättningar som föreskrivs i cybersäkerhetsakten. Beredningen av certifieringsordningarna har framskridit långsamt. Den första certifieringsordningen (EUCC) har godkänts i början av år 2024 genom kommissionens genomförandeförordningen (EU) 2024/482 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska ordningen för cybersäkerhetscertifiering (EUCC) som baserar sig på gemensamma kriterier. EUCC är en certifieringsordning som gäller informations- och kommunikationstekniska produkter och som baserar sig på gemensamma kriterier för säkerhetsbedömning av informationsteknologi (Common Criteria for Information Technology Security Evaluation, CC) och gemensamma bedömningsmetoder för informationstekniksäkerhet (Common Methodology for Information Technology Security Evaluation, CEM), vilka har publicerats till exempel i form av standarderna ISO/IEC 15408 och ISO/IEC 18405. Dessutom bereds certifieringsordningar som gäller molntjänster, 5G och den europeiska digitala identitetsplånboken.

I enlighet med artikel 52 i cybersäkerhetsakten är det möjligt att i en europeisk ordning för cybersäkerhetscertifiering fastställa certifikat av tre assuransnivåer: certifikat av grundläggande, betydande eller hög nivå. Certifikat av grundläggande och betydande nivå utfärdas i regel av organ för bedömning av överensstämmelse som är ackrediterade och som anmälts och vid behov bemyndigats av en myndighet. Tillverkarna och tjänsteleverantörerna kan ansöka om certifiering från organen för bedömning av överensstämmelse eller beroende på fallet från den myndighet som utfärdar cybersäkerhetscertifiering. Ett bedömningsorgan ska uppfylla de krav som fastställs i förordningen och dess bilaga. Med stöd av artikel 53 i cybersäkerhetsakten kan en ordning för cybersäkerhetscertifiering även tillåta att självbedömningen av överensstämmelsen uteslutande omfattas av ansvaret för tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer. Självbedömning kan dock tillämpas endast på den grundläggande assuransnivån. Artikel 55 i cybersäkerhetsakten innehåller bestämmelser om skyldigheten för en tillverkare eller leverantör att offentligt tillgängliggöra vissa uppgifter som främjar en produkts eller tjänsts cybersäkerhet.

### 2.2.2 Certifieringsskyldigheter

Enligt cybersäkerhetsakten är cybersäkerhetscertifiering frivilligt, om inte annat anges i unionslagstiftningen eller medlemsstaternas lagstiftning. Cybersäkerhetsakten innehåller inte krav på användning av certifieringsordningar. På det sätt som konstaterats ovan har den första ordningen för certifiering (EUCC) godkänts i början av år 2024.

Artikel 32 i cyberresiliensförordningen innehåller bestämmelser om förfarandet för att bedöma överensstämmelsen för produkter med digitala element. När en europeisk ordning för cybersäkerhetscertifiering är tillgänglig och tillämplig för en produkt med digitala element, är det möjligt att med stöd av artikel 32 i cyberresiliensförordningen visa att en produkt med digitala element överensstämmer med kraven i cyberresiliensförordningen bland annat genom att använda en europeisk ordning för cybersäkerhetscertifiering. I fråga om viktiga produkter enligt bilaga III till cybersäkerhetsakten är en förutsättning för att visa överensstämmelse i så fall att cybersäkerhetscertifikat av assuransnivå ”betydande” används. Med stöd av artikel 8.1 och artikel 32.4 i cyberresiliensförordningen förutsätts att produkter enligt bilaga IV till förordningen i regel har assuransnivån ”betydande” av de assuransnivåer som används i en

europeisk ordning för cybersäkerhetscertifiering. På det sätt som beskrivs i avsnitt 2.1.9 har kommissionen befogenhet att anta delegerade akter om ändring av produktlistorna med vissa randvillkor och att närmare definiera de produkter som omfattas av förutsättningen. Användningen av europeiska ordningar för cybersäkerhetscertifiering kan förmodas öka i och med cyberresiliensförordningen.

Cybersäkerhetscertifieringen har kopplingar även till EU:s cybersäkerhetsdirektiv, det vill säga NIS 2-direktivet EU (2022/2555). Med stöd av artikel 24.1 i NIS 2-direktivet får en medlemsstat för att visa att vissa de krav som gäller riskhanteringsskyldigheten är uppfyllda ålägga väsentliga och viktiga entiteter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller upphandlats från tredje parter, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering. I det nationella genomförandet av direktivet infördes inte sådana bestämmelser i cybersäkerhetslagen (124/2025; RP 57/2024 rd), men framöver är det möjligt att ställa tilläggskrav i speciallagstiftning. Dessutom är det inom ramen för det nationella handlingsutrymme som unionsrätten tillåter möjligt att ställa andra nationella krav på användning av cybersäkerhetscertifieringar.

I artikel 24.2 i NIS 2-direktivet föreskrivs vidare att kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 i direktivet för att komplettera detta direktiv genom att ange vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt artikel 49 i cybersäkerhetsakten. Kommissionen har tills vidare inte antagit fler sådana delegerade akter.

### 2.2.3 Nationell myndighet för cybersäkerhetscertifiering

Artikel 58 i cybersäkerhetsakten ålägger medlemsstaterna att utse en eller flera nationella myndigheter som utfärdar cybersäkerhetscertifiering. En medlemsstat kan även genom ett avtal med en annan medlemsstat utse en eller flera nationella myndigheter som utfärdar cybersäkerhetscertifiering och som är etablerade i denna andra medlemsstat för att ansvara för tillsynsuppgifterna inom denna utseende medlemsstats territorium. De nationella myndigheterna som utfärdar cybersäkerhetscertifiering ska ansvara för genomförandet av de europeiska ordningarna för cybersäkerhetscertifiering och för övervakningen av dessa samt för att certifikat som utfärdats enligt dessa ordningar är i kraft och erkänns i hela unionen. Medlemsstaterna ska visa att de nationella myndigheterna har tillräckliga resurser att utöva sina befogenheter och framgångsrikt och effektivt sköta de uppgifter som tilldelats dem.

Trots begreppet ”kyberturvallisuussertifioinnin myöntävä viranomainen” (myndighet som utfärdar cybersäkerhetscertifiering) i den finska versionen av cybersäkerhetsakten handlar myndighetens uppgifter de facto även om övervakning av efterlevnaden av certifieringsordningarna och inte endast om en uppgift som gäller utfärdande av certifikat.

Med stöd av artikel 58.3 i förordningen ska en myndighet i fråga om organisation, finansieringsbeslut, juridisk struktur och beslutsfattande vara oberoende av de enheter som den övervakar. Med stöd av 4 punkten i artikeln ska verksamheten i anknytning till utfärdande av cybersäkerhetscertifikat hos den myndighet som utfärdar cybersäkerhetscertifiering vara strikt avskild från myndighetens tillsynsverksamhet enligt artikel 58. Befogenheterna för den nationella myndighet som utfärdar cybersäkerhetscertifiering omfattar med stöd av artikel 56.6 i förordningen utfärdande av cybersäkerhetscertifikat av hög assuransnivå. På vissa villkor kan uppgiften delegeras till ett organ för bedömning av överensstämmelse.

De nationella myndigheterna för cybersäkerhetscertifiering deltar i den europeiska gruppen för cybersäkerhetscertifiering. Myndigheterna ska 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.

Artikel 58.7 i cybersäkerhetsakten innehåller bestämmelser om tillsynsuppgifterna för den nationella myndighet som utfärdar cybersäkerhetscertifiering. Uppgifterna för den nationella myndigheten omfattar för det första att övervaka försäkringar om överensstämmelse som baserar sig på självbedömning och att kraven på europeiska cybersäkerhetscertifikat och reglerna för certifieringsordningarna iakttas inom dess område. För det andra omfattar myndighetens uppgifter att stödja ackrediteringsorganen då de övervakar organ för bedömning av överensstämmelse och bemyndiga organ för bedömning av överensstämmelse om certifieringsordningarna så förutsätter samt att avbryta eller återkalla bemyndiganden, om kraven i förordningen inte iakttas. För det tredje har myndigheten med stöd av artikel 56.5 i förordningen till uppgift att övervaka offentliga organ som exceptionellt utfärdar europeiska cybersäkerhetscertifikat av grundläggande eller betydande assuransnivå. För det fjärde har myndigheten till uppgift att behandla klagomål som lämnas in av fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av de nationella myndigheterna för cybersäkerhetscertifiering eller organ för bedömning av överensstämmelsen i enlighet med artikel 56.6 eller avseende EU-försäkringar om överensstämmelse. Dessutom ska myndigheten årligen upprätta en sammanfattande rapport om sina åtgärder till Enisa och europeiska gruppen för cybersäkerhetscertifiering, samarbeta med övriga nationella myndigheter som utfärdar cybersäkerhetscertifiering, till exempel genom att dela information om eventuella fall där IKT-produkter, IKT-tjänster och IKT-processer eller dataskyddstjänsten inte motsvarar kraven i förordningen eller enskilda europeiska ordningar för cybersäkerhetscertifiering, samt följa utvecklingen inom cybersäkerhetscertifieringens område.

De myndighetsbefogenheter som artikel 58.8 i cybersäkerhetsakten förutsätter omfattar bland annat rätten att få uppgifter från organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare en EU-försäkran om överensstämmelse, göra inspektioner i fråga om dessa och få tillgång till deras lokaler samt vidta andra åtgärder i enlighet med den nationella lagstiftningen i syfte att säkerställa att de iakttar kraven i förordningen eller en europeisk ordning för cybersäkerhetscertifiering. Tillsynsmyndigheterna har även rätt att återkalla europeiska cybersäkerhetscertifikat som utfärdats av den nationella myndighet som utfärdar cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat av hög assuransnivå som utfärdats av organ för bedömning av överensstämmelse utifrån delegering, om de inte uppfyller kraven i förordningen eller i en europeisk ordning för cybersäkerhetscertifiering. Myndigheterna har dessutom rätt att påföra påföljder i enlighet med den nationella lagstiftningen för överträdelse av förordningen och kräva att överträdelserna av förordningen ska upphöra.

### 2.2.4 Organ för bedömning av överensstämmelse

Artiklarna 60 och 61 i cybersäkerhetsakten innehåller bestämmelser om ackreditering, bemyndigande och anmälning av organ för bedömning av överensstämmelse till kommissionen. Bilagan till förordningen innehåller förutsättningarna för ackreditering av det nationella ackrediteringsorganet. En certifieringsordning kan innehålla särskilda krav eller tilläggskrav, varvid den nationella myndigheten för cybersäkerhetscertifiering bemyndigar endast de organ för bedömning av överensstämmelse som uppfyller dessa krav. Ackreditering beviljas för högst fem år och kan förnyas. Om förutsättningarna för ackreditering inte längre är uppfyllda eller om verksamheten vid ett organ för bedömning av överensstämmelse bryter mot bestämmelserna i

förordningen, ska de nationella ackrediteringsorganen begränsa ackrediteringen eller avbryta eller återkalla den.

Den nationella myndigheten för cybersäkerhetscertifiering underrättar kommissionen om organ för bedömning av överensstämmelse som ackrediterats och bemyndigats att utfärda europeiska cybersäkerhetscertifikat på de fastställda assuransnivåerna och om anknutna ändringar. Kommissionen ger ut en förteckning över anmälda organ för bedömning av överensstämmelse. Den nationella myndigheten för cybersäkerhetscertifiering kan till kommissionen framföra en begäran om att från förteckningen avföra ett organ för bedömning av överensstämmelse som det anmält.

### 2.2.5 Kommissionens befogenheter att anta delegerade akter

Cybersäkerhetsakten innehåller befogenheter att anta delegerade akter för kommissionen. Kommissionen meddelar en europeisk ordning för cybersäkerhetscertifiering genom en genomförandeakt med stöd av artikel 49 i förordningen. På det sätt som konstaterats ovan har den första ordningen för certifiering (EUCC) godkänts i början av år 2024 genom kommissionens genomförandet akt (EU) 2024/482.

Med stöd av artikel 61.5 kan kommissionen även anta genomförandeakter för att fastställa förutsättningar, format och förfaranden för de anmälningar som den nationella myndigheten för cybersäkerhetscertifiering ger om organ för bedömning av överensstämmelse. Med stöd av detta har kommissionen gett genomförandeförordningen (EU) 2024/3143 om fastställande av förutsättningar, format och förfaranden för anmälningar enligt artikel 61.5 i Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik.

Dessutom kan kommissionen med stöd av artikel 59.5 i förordningen anta genomförandeakter om planerna för inbördes granskningar av de nationella myndigheter som utfärdar cybersäkerhetscertifiering.

### 2.2.6 Det nationella handlingsutrymmet och behovet av kompletterande reglering

Cybersäkerhetsakten innehåller i princip inte något nationellt handlingsutrymme, utan den är en direkt tillämplig förordning. Nationellt är det dock möjligt att ställa krav på användning av europeiska ordningar för cybersäkerhetscertifiering inom ramen för det nationella handlingsutrymme som EU-rätten tillåter (se avsnitt 2.2.2). Det finns också nationellt handlingsutrymme i förhållande till hur uppgifterna för den nationella myndigheten för cybersäkerhetscertifiering ordnas. För närvarande har uppgiften tilldelats Transport- och kommunikationsverket i lagen om tjänster inom elektronisk kommunikation. Nationella bestämmelser ska utfärdas om myndighetens befogenheter. I fråga om inspektionsrätten ger cybersäkerhetsakten till följd av hänvisningen till den nationella processrätten mer nationellt handlingsutrymme än marknadskontrollförordningen, som blir tillämplig på övervakning enligt cyberresiliensförordningen, i fråga om möjligheten att utsträcka inspektionsrätten till hemfridsskyddet. Dessutom förutsätter förordningen nationell kompletterande reglering om ställningen för organen för bedömning av överensstämmelse då de sköter en offentlig förvaltningsuppgift.

Det finns nationellt handlingsutrymme även i anknytning till påförandet av påföljder. Enligt artikel 65 i cybersäkerhetsakten ska medlemsstaterna fastställa regler om sanktioner vid överträdelse av denna avdelning och överträdelser av europeiska ordningar för

cybersäkerhetscertifiering, och de ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

### 2.3 Registrarer

Europeiska unionens cybersäkerhetsdirektiv, det vill säga Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, nedan NIS 2-direktivet, har som mål att stärka nivån på EU:s gemensamma och medlemsstaternas nationella cybersäkerhet i fråga om sektorer och typer av entiteter som är centrala för samhällets funktion. Medlemsstaterna åläggs att fastställa skyldigheter för de aktörer som omfattas av direktivets tillämpningsområde i fråga om riskhantering som gäller cybersäkerhet och om anmälning av betydande cybersäkerhetsincidenter. Dessutom innehåller direktivet bestämmelser om medlemsstaternas skyldighet att anta nationella strategier för cybersäkerhet och att inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser, gemensamma kontaktpunkter för cybersäkerhet och enheter för hantering av it-säkerhetsincidenter (Computer security incident response team, nedan *CSIRT-enhet*). Dessutom innehåller direktivet bestämmelser om databasen för registreringsuppgifter om domännamn.

NIS 2-direktivets centrala innehåll beskrivs mer ingående i avsnitt 2 i regeringens proposition RP 57/2024 rd. I detta sammanhang behandlas de centrala bestämmelserna om registrarer i NIS 2-direktivet.

I artikel 6.22 i NIS 2-direktivet föreskrivs att en ”entitet som tillhandahåller domännamnsregistreringstjänster” avser en registrar eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster. Entiteter som tillhandahåller domännamnsregistreringstjänster är inte väsentliga entiteter enligt artikel 3 i direktivet, på vilka de skyldigheter som gäller riskhantering avseende cybersäkerhet eller anmälning av betydande incidenter enligt artiklarna 21 och 23 i direktivet inte ska tillämpas. Reglering kring entiteter som tillhandahåller domännamnsregistreringstjänster ingår i artikel 3.3 och 3.4, artikel 27 och artikel 28 i direktivet.

Enligt artikel 3.3 i NIS 2-direktivet ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Enligt samma punkt ska medlemsstaterna regelbundet och minst vartannat år därefter se över förteckningen och när det är lämpligt uppdatera den. Enligt artikel 3.4 i NIS 2-direktivet ska medlemsstaterna vid upprättandet av den förteckning som avses i punkt 3 ålägga de entiteter som avses i den punkten att lämna viss information till de behöriga myndigheterna. Dessutom ska entiteterna anmäla alla ändringar i sådana uppgifter utan dröjsmål och i varje fall inom två veckor från ändringsdagen.

Med stöd av artikel 27.2 och artikel 27.3 i NIS 2-direktivet ska en medlemsstat förutsätta att vissa aktörer, inbegripet entiteter som tillhandahåller domännamnsregistreringstjänster, ska överlämna de uppgifter som avses i punkten till den behöriga myndigheten i medlemsstaten. Medlemsstaterna ska säkerställa att entiteterna till den behöriga myndigheten anmäler alla ändringar i uppgifter som de ska lämna i enlighet med 2 punkten utan dröjsmål och i varje fall inom tre månader från ändringsdagen.

Artikel 28 i NIS 2-direktivet innehåller bestämmelser om databasen med registreringsuppgifter för domännamn. Med stöd av artikel 1 ska medlemsstaterna för att bidra till domännamnssystemets säkerhet, stabilitet och motståndskraft ålägga registreringsenheter för

toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.

Med stöd av artikel 28.2 i NIS 2-direktivet ska en medlemsstat för tillämpningen av artikel 28.1 föreskriva att databasen med registreringsuppgifter för domännamn innehåller nödvändig information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna. Denna information ska omfatta följande: domännamn, registreringsdatum, registrantens namn, e-postadress och telefonnummer och e-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet, om dessa inte är desamma som för registranten.

Med stöd av artikel 28.3 i NIS 2-direktivet ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ha strategier och förfaranden, inbegripet kontrollförfaranden, för att säkerställa att databaserna innehåller korrekt och fullständig information. Medlemsstaterna ska föreskriva att sådana strategier och förfaranden offentliggörs.

Med stöd av artikel 28.4 och artikel 28.5 i NIS 2-direktivet ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål efter registreringen av ett domännamn offentliggöra registreringsuppgifter för domännamn som inte är personuppgifter. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ge åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål och under alla omständigheter inom 72 timmar från mottagandet besvarar en begäran om åtkomst. Medlemsstaterna ska föreskriva att strategier och förfaranden för utlämning av sådana uppgifter offentliggörs.

Med stöd av artikel 28.6 i NIS 2-direktivet får efterlevnad av de skyldigheter som föreskrivits i 1–5 punkten inte leda till överlappningar i insamlingen av registreringsuppgifter om domännamn. För detta ska medlemsstaterna förutsätta att toppdomänregister och de entiteter som tillhandahåller domännamnsregistreringstjänster ska samarbeta med varandra.

Artikel 26 i NIS 2-direktivet innehåller bestämmelser om medlemsstaternas jurisdiktion i fråga om entiteter som tillhandahåller domännamnsregistreringstjänster. Med stöd av artikel 26.1 omfattas entiteter som tillhandahåller domännamnsregistreringstjänster av den jurisdiktion där dess huvudsakliga etableringsställe finns. Det finns bestämmelser om det huvudsakliga etableringsstället och utseendet av en företrädare i unionen i punkterna 2–5 i artikel 26.

# 3 Nuläge och bedömning av nuläget

## 3.1 Cyberresiliensförordningen

### 3.1.1 Produktreglering

I Finland finns det inte någon gällande nationell produktreglering som fastställer horisontella cybersäkerhetskrav av samma karaktär som i cyberresiliensförordningen på produkter med digitala element eller på tillverkarna, importörerna eller återförsäljarna av sådana. För

närvarande ställs inte horisontella cybersäkerhetskrav på enheter och programvaror i lagen. Kraven är således nya för ekonomiska aktörer. Kraven gäller bland annat enhetens eller programvarans egenskaper, dokumentation av omständigheter som påverkar cybersäkerheten och hanteringen av sårbarheter.

De produktspecifika specialakterna kan innehålla krav på produkternas dataskydd. Den produktspecifika regleringen kring cybersäkerhet eller hantering av sårbarheter är dock överlag begränsad och den fokuserar på produkter med hög säkerhetsrisk. I beredningen av propositionen identifierades inte sådan nationell lagstiftning som strider mot cyberresiliensförordningen på så sätt att förslag om att upphäva nationell lagstiftning ska läggas fram eller i övrigt inte ska tillämpas framöver på grund av att den strider mot cyberresiliensförordningen.

Dataskyddskrav som förbättrar cybersäkerheten har föreskrivits i artikel 3.3 d, 3.3 e och 3.3 f i EU:s direktiv om radioutrustning (2014/53/EU), vilka tillämpas på radioutrustning som regleras i kommissionens delegerade förordning 2022/30. Kraven i direktivet om radioutrustning har genomförts genom lagen om tjänster inom elektronisk kommunikation (2014/917) och statsrådets förordning om radioutrustnings överensstämmelse med kraven (152/2024). Cyberresiliensförordningen täcker alla krav på dataskydd i direktivet om radioutrustning och den tillämpas på överlappande sätt på produkter enligt kommissionens delegerade förordning fram till dess att kommissionen upphäver den delegerade förordningen eller ändrar dess tillämpningsområde.

I nuläget finns det, utöver i lagstiftningen, cybersäkerhetskrav i de standarder som gäller cybersäkerheten inom olika produktsektorer. Genom att iaktta dessa är det under vissa förutsättningar möjligt att visa överensstämmelse med kraven för en produkt. Utnyttjandet av standarderna är i princip frivilligt för tillverkarna och det baserar sig på affärsverksamhetsintressena. Villkor som gäller cybersäkerheten och hantering av sårbarheter kan ingå i upphandlingsavtalen för produkter som omfattas av tillämpningsområdet eller en frivillig garanti som erbjuds för en produkt.

För närvarande ställer lagstiftningen inte cybersäkerhetskrav som gäller för programvaror med fri och öppen källkod eller förvaltare av programvaror med fri och öppen källkod.

Eftersom cyberresiliensförordningen är direkt tillämplig, bedöms nuläget närmare endast i fråga om de helheter för vilka det finns ett behov av att föreslå nationell reglering som kompletterar förordningen. Sådana helheter är anmälda organ, myndighetsuppgifterna i fråga om marknadskontroll samt administrativa påföljder enligt cyberresiliensförordningen. I fråga om cybersäkerhetsakten bedöms på motsvarande sätt regleringen kring organ för bedömning av överensstämmelse och myndighetsbefogenheterna samt sanktionerna.

### 3.1.2 Marknadskontroll

Med marknadskontroll avses kontroll i efterskott utifrån en riskbedömning på marknaden. Syftet med marknadskontrollen är att säkerställa att bestämmelserna och föreskrifterna om produkter iakttas och att produkter som är farliga eller har bristfällig säkerhet inte finns på EU:s inre marknad. Ansvaret för produkternas överensstämmelse innehas av tillverkarna, importörerna och återförsäljarna, som ska visa produktens överensstämmelse innan den släpps ut på marknaden.

I Finland har marknadskontrolluppgifterna fördelats enligt produktkategori till olika myndigheter inom olika ministeriers förvaltningsområden. Marknadskontrollmyndigheterna

enligt situationen per februari 2020 presenteras enligt produktkategori i arbets- och näringsministeriets promemoria (länk). Bland myndigheterna innehas det största uppgiftsområdet i anknytning till marknadskontrollen av Säkerhets- och kemikalieverket (Tukes). Verket sköter marknadskontrolluppgifter inom arbets- och näringsministeriets förvaltningsområde inom flera olika produktsektorer och ackrediteringsenheten, det vill säga ackrediteringstjänsten FINAS, som verkar i anslutning till det, sköter uppgifterna för det nationella ackrediteringsorganet. Transport- och kommunikationsverket Traficom har för närvarande tilldelats marknadskontrolluppgifter i den produktspecifika regleringen i fråga om radioutrustning, fritidsbåtar, fartygsutrustning, obemannade luftfarkoster och fordon. Andra produktspecifika marknadskontrollmyndigheter utgörs av bland annat Polisstyrelsen, Tullen, Finlands miljöcentral, NTM-centralerna, de kommunala miljöskyddsmyndigheterna, ansvarsområdena för arbetarskyddet vid regionförvaltningsverken och Livsmedelsverket.

Cyberresiliensförordningen förutsätter att medlemsstaterna ordnar marknadskontrollen av överensstämmelsen av produkter som omfattas av dess tillämpningsområde. Den föreslagna uppgiften är ny och den ska ordnas hos en myndighet för första gången, eftersom förordningen med kraven i den på motsvarande sätt är ny. Inga nationella bestämmelser har utfärdats om myndighetsuppgifterna i fråga om motsvarande krav eller tillsyn.

Transport- och kommunikationsverkets Cybersäkerhetscenter har från och med år 2019 beviljat och även övervakat användningen av Cybersäkerhetsmärken, som visar att en produkt eller tjänst som försetts med märket har planerats för att vara datasäker och att den uppfyller Transport- och kommunikationsverkets dataskyddskrav. Det har varit frivilligt för tillverkare och säljare att skaffa Cybersäkerhetsmärket och det har inte varit en förutsättning för att komma in på marknaden.

*Lagen om marknadskontrollen av vissa produkter*

Lagen om om marknadskontrollen av vissa produkter (2016/1137, nedan *marknadskontrollagen*) innehåller grundläggande bestämmelser om marknadskontrollen om de produktgrupper som omfattas av dess tillämpningsområde. Marknadskontrollagen är en horisontell allmän lag som reglerar marknadskontrollen och som tillämpas på marknadskontroll av de produktakter som omfattas av dess tillämpningsområde.

Genom marknadskontrollagen genomfördes Europaparlamentets och rådets förordning (EU) 2019/1020 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (*marknadskontrollförordningen*), som ställer enhetliga regler för marknadskontrollen av vissa produktkategorier och minimikrav för marknadskontrollmyndigheternas befogenheter. I samband med genomförandet av marknadskontrollförordningen fogades till tillämpningsområdet för marknadskontrollagen flera produktgrupper och bestämmelser om marknadskontrollmyndigheternas befogenheter och kontrollmetoder.

Marknadskontrollagens innehåller bestämmelser om marknadskontrollen av de produkter som avses i 1 §. Det finns bestämmelser om marknadskontrollen av andra produkter än de som omfattas av marknadskontrollagen i de produktspecifika lagarna. Marknadskontrollagen har en karaktär av en allmän lag, som tillämpas med stöd av dess 1 §, då annat inte bestäms i de produktspecifika akterna.

Marknadskontrollagens 4 § innehåller bestämmelser om marknadskontrollmyndigheterna enligt lagen. Marknadskontrollmyndigheterna utgörs av Säkerhets- och kemikalieverket, Tullen, Strålsäkerhetscentralen, Transport- och kommunikationsverket, Finlands miljöcentral,

Säkerhets- och utvecklingscentret för läkemedelsområdet, Tillstånds- och tillsynsverket för social- och hälsovården (från och med den 1 januari 2026 Tillstånds- och tillsynsverket), kommunerna samt Livsmedelsverket. En beskrivning av marknadskontrollmyndigheternas centrala uppgifter finns i regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s förordning om artificiell intelligens RP 46/2025 rd.

Med stöd av 4 a § i marknadskontrollagen är Säkerhets- och kemikalieverket det samordningskontor för marknadskontroll som avses i artikel 10.3 i marknadskontrollförordningen. Samarbetsgruppen för marknadskontroll verkar i anslutning till samordningskontoret för marknadskontroll.

Med stöd av 4 § 4 mom. i marknadskontrollagen fungerar Transport- och kommunikationsverket som marknadskontrollmyndighet när det gäller de produkter som avses i luftfartslagen, fordonslagen, 24 a § 3 mom. i miljöskyddslagen, lagen om säkerhet och utsläppskrav för fritidsbåtar, lagen om tjänster inom elektronisk kommunikation, lagen om marin utrustning och lagen om tillgänglighetskrav för vissa produkter.

Regeringens proposition RP 46/2025 rd innehåller ett förslag om att marknadskontrollagen genom en hänvisningsbestämmelse innehåller föreskrifter även om marknadskontrollmyndigheterna för AI-system. Enligt förslaget innehåller 3 § i lagen om tillsyn över vissa system för artificiell intelligens bestämmelser om marknadskontrollmyndigheterna för system för artificiell intelligens med hög risk, vilka från fall till fall är Säkerhets- och kemikalieverket, Tullen, Transport- och kommunikationsverket, arbetarskyddsmyndigheten, Säkerhets- och utvecklingscentret för läkemedelsområdet, Energimyndigheten, dataombudsmannen, Tillstånds- och tillsynsverket, Finansinspektionen och regionförvaltningsverket i Sydvästra Finland.

Enligt artikel 52 i cyberresiliensförordningen tillämpas marknadskontrollförordningen på marknadskontrollen av produkter som omfattas av förordningens tillämpningsområde. Den nationella regleringen för att genomföra marknadskontrollförordningen ingår i marknadskontrollagen. Dessutom omfattar cyberresiliensförordningen produkter som är föremål för redan gällande produktreglering samt den marknadskontroll som den förutsätter.

De marknadskontrolluppgifter som gäller produkters cybersäkerhet handlar om nya myndighetsuppgifter, som inte ingår i någon myndighets lagstadgade uppgifter.

Eftersom marknadskontrollförordningen, som nationellt kompletterats genom marknadskontrollagen, tillämpas på övervakningen av cyberresiliensförordningen, finns det ett behov av att utvidga tillämpningsområdet för 1 § i marknadskontrollagen till att täcka även övervakningen av produkter som omfattas av tillämpningsområdet för cyberresiliensförordningen. Marknadskontrollagens 4 § innehåller bestämmelser om de behöriga tillsynsmyndigheterna enligt lagen, varför det är behövligt att till den foga en hänvisning till de myndigheter som blir behöriga myndigheter i och med den föreslagna lagen. På grund av lagtekniska skäl är det behövligt att göra ändringen delvis genom hänvisningar, eftersom antalet myndigheter är många, då befogenheten i vissa fall hör till de myndigheter som övervakar förordningen om artificiell intelligens. Syftet med den föreslagna lagändringen är att säkerställa att de myndigheter som blir behöriga med stöd av den föreslagna lagen har alla de befogenheter som föreskrivits i marknadskontrollagen på grundval av marknadskontrollförordningen så att de kan fullgöra sina uppgifter som gäller kontrollen av produkter med digitala element. Till övriga delar anses det inte finnas något behov av att göra ändringar i marknadskontrollagen, eftersom marknadskontrollförordningen är fullt tillämplig på cyberresiliensförordningen och således är även marknadskontrollagen fullt tillämplig, då

cyberresiliensförordningen och den lag som föreslagits för att genomföra den tillämpas. På det sätt som anges nedan är det dock behövligt att till vissa delar avvika från och komplettera regleringen i marknadskontrollagen.

I 4 a § i marknadskontrollagen finns det bestämmelser om att Säkerhets- och kemikalieverket är det centrala samordningskontor för marknadskontroll som avses i artikel 10.3 i marknadskontrollförordningen. Säkerhets- och kemikalieverket fungerar som samordningskontor för marknadskontrollen även i fråga om cyberresiliensförordningen, eftersom endast ett samordningskontor kan utses. Vid Säkerhets- och kemikalieverket har samordningskontoret förlagts till produktenhetens Fipoint-grupp. I skötseln av samordningskontorets uppgifter fungerar Fipoint opartiskt i förhållande till alla marknadskontrollmyndigheter och Tullen. I enlighet med artikel 10 i marknadskontrollförordningen ansvarar samordningskontoret för att lägga fram marknadskontrollmyndigheternas och Tullens samordnade ståndpunkt samt anmälningen av den nationella marknadskontrollstrategin i ICSMS-systemet. Utöver de uppgifter som föreskrivits i marknadskontrollförordningen har samordningskontoret tilldelats uppgifter i 4 a § i marknadskontrollagen. Enligt marknadskontrollagen samordnar samordningskontoret i Finland myndighetssamarbetet inom marknadskontrollen och bistår marknadskontrollmyndigheterna vid det nationella och internationella samarbetet. Dessutom har samordningskontoret till uppgift att utarbeta en nationell strategi för marknadskontroll tillsammans med samarbetsgruppen för marknadskontroll.

I beredningen av propositionen har man inte identifierat existerande myndigheter till vars befintliga uppgifter det vore särskilt naturligt att föreslå marknadskontroll enligt cyberresiliensförordningen. De myndigheter som lämpar sig för marknadskontrolluppgiften utgörs av Säkerhets- och kemikalieverket, som för närvarande har flera uppgifter i anknytning till marknadskontrollen, och Transport- och kommunikationsverket, som redan från tidigare ansvarar för flera myndighetsuppgifter som hänför sig till cybersäkerhet. Transport- och kommunikationsverket ansvarar dessutom för marknadskontrolluppgifter som gäller flera produktkategorier, vilka regleras bland annat i luftfartslagen (864/2014), fordonslagen (82/2021), lagen om säkerhet och utsläppskrav för fritidsbåtar (1712/2015) och lagen om tjänster inom ekonomisk kommunikation (917/2014). Nedan i avsnitt 5.1.1 bedöms alternativen till ordnandet av marknadskontrollen.

Det har föreslagits att bestämmelser om tillsynen över system för artificiell intelligens med hög risk utfärdas i lagen om tillsyn över vissa system för artificiell intelligens (RP 46/2025 rd). De myndigheter som övervakar den nämnda lagen fungerar enligt förslaget i fråga om AI-system med hög risk även som övervakare av kraven i cyberresiliensförordningen på grund av sambandet mellan EU:s förordning om artificiell intelligens och cyberresiliensförordningen, så som beskrivs i avsnitt 2.1.6. Således fungerar i varje fall flera myndigheter som marknadskontrollmyndigheter enligt cyberresiliensförordningen på grund av att kontrollen delvis är utspridd till de behöriga myndigheterna för kontrollen enligt förordningen om artificiell intelligens. Av den nuvarande regleringen blir artikel 22.1 i marknadskontrollförordningen, 4 a § och 4 b § i marknadskontrollagen samt 10 § i förvaltningslagen tillämpliga på marknadskontrollmyndigheternas skyldighet att föra samarbete även i övervakningen enligt cyberresiliensförordningen. Marknadskontrollagen innehåller bestämmelser bland annat om utarbetandet av den nationella marknadskontrollstrategin. Strategin ska vid behov uppdateras så att den beaktar de nya typerna av krav i cyberresiliensförordningen. Marknadskontrollagens 7 § innehåller bestämmelser om marknadskontrollmyndighetens skyldighet att göra upp en kontrollplan.

I kontrollen enligt cyberresiliensförordningen är det motiverat att sträva efter att kontrollen av kraven i cyberresiliensförordningen är maximalt harmoniserad oberoende av marknadskontrollmyndigheten. I kontrollen ska man således rikta uppmärksamhet på marknadskontrollmyndigheternas samarbete. Med hänsyn till Transport- och kommunikationsverkets centrala roll och expertis kan det finnas ett behov av att utfärda bestämmelser om att det har möjlighet att ge expertstöd till marknadskontrollmyndigheterna enligt cyberresiliensförordningen i synnerhet om deras marknadskontrolluppgift är av begränsad omfattning.

*Befogenheterna för marknadskontroll*

Det finns bestämmelser om marknadskontrollmyndigheternas befogenheter för marknadskontroll och rätt att få information i 3 kap. i marknadskontrollagen. Befogenheterna omfattar till exempel rätt att få information, rätt att ta produkter för undersökning och rätt att förelägga förbud och vid behov rätt att förordna att en produkt ska förstöras.

Lagens 8 § innehåller bestämmelser om en myndighets rätt att få information från en ekonomisk aktör. Enligt paragrafen har marknadskontrollmyndigheten och Tullen rätt att få information som är nödvändig för kontrollen, vilken kan omfatta även de uppgifter som avses i artikel 14.4 led a och b i marknadskontrollförordningen Rätten att få information gäller även sådana upplysningar som är nödvändiga för tillsynen och som är sekretessbelagda på grund av att de gäller enskild affärsverksamhet eller yrkesutövning eller en enskild persons ekonomiska ställning eller hälsotillstånd eller annars är sekretessbelagda med stöd av lagen om offentlighet i myndigheternas verksamhet (621/1999) när de innehas av en myndighet. Enligt paragrafens 2 mom. gäller rätten att få information även sådana upplysningar som är nödvändiga för att verifiera ägare av onlinegränssnitt.

Marknadskontrollagens 9 § innehåller bestämmelser om myndighetens rätt att företa inspektioner. Marknadskontrollmyndigheten har med tanke på kontrollen rätt att få tillträde till alla lokaler där det bedrivs sådan verksamhet som avses i de lagar som nämns i 1 § 1 mom. eller där det förvaras uppgifter som är betydelsefulla för kontrollen, och utföra sådana inspektioner som behövs för kontrollen. I regel är det dock inte tillåtet att utsträcka inspektioner till utrymmen som används för boende av permanent natur. Vid inspektionerna följs bestämmelserna i 39 § i förvaltningslagen (434/2003).

Det är behövligt att avvika från bestämmelserna i marknadskontrollagen till vissa delar. Marknadskontrollagen har en karaktär av allmän lag, från vilken det är möjligt att avvika i de produktspecifika lagarna i enlighet med dess 1 §.

Med avvikelse från marknadskontrollagen är det behövligt att utfärda bestämmelser om att inspektioner kan utsträckas till utrymmen som används för boende av permanent natur. Marknadskontrollagen möjliggör inte att inspektioner utsträcks till utrymmen som används för boende av permanent natur, eftersom det i 9 § 2 mom. i den lagen föreskrivs att marknadskontrollmyndighetens rätt att utsträcka inspektioner till utrymmen som används för boende av permanent natur vid behov föreskrivs särskilt. Befogenheten behövs för att genomföra kontrollen, eftersom näringsverksamhet som omfattas av cyberresiliensförordningen vanligen kan utövas även i hemfridsskyddade utrymmen, i synnerhet inom programvarubranschen. I enlighet med marknadskontrollförordningen ska det vara möjligt att göra inspektioner i lokaler.

Dessutom innehåller 10 § i marknadskontrollmyndigheten bestämmelser om marknadskontrollmyndighetens rätt att ta produkter för undersökning, om det behövs för

kontrollen av att produkterna överensstämmer med kraven. En ersättning ska betalas för att en produkt tas för undersökning, vilket baserar sig på skadan av förlusten av föremålet för den ekonomiska aktören. Bestämmelsen kan även tillämpas på de programvaruprodukter som omfattas av cyberresiliensförordningen, vilka vanligtvis är immateriella och inte orsakar någon motsvarande skada för den ekonomiska aktören.

Det finns även ett behov av att komplettera bestämmelserna om utbyte av uppgifter i marknadskontrollagen i synnerhet för att behandla sådana uppgifter som omfattas av de anmälningsskyldigheter som ingår i cyberresiliensförordningen. Dessutom innehåller artiklarna 52 och 54 i cyberresiliensförordningen bestämmelser om det samarbete som krävs mellan marknadskontrollmyndigheterna och de nationella certifieringsmyndigheterna för cybersäkerhetscertifiering, CSIRT-enheterna och Enisa, dataskyddsmyndigheterna, kommissionen och de behöriga myndigheter som övervakar NIS 2-direktivet samt med de andra medlemsstaterna och de andra marknadskontrollmyndigheterna i fråga om informationsutbyte och annat utlämnande av information som eventuellt är sekretessbelagd.

Enligt 11 § i marknadskontrollagen har marknadskontrollmyndigheten och Tullen, oberoende av sekretessbestämmelserna och andra begränsningar som gäller erhållande av information, rätt att lämna ut information som är nödvändig för kontrollen till varandra och att av andra tillsynsmyndigheter få sådan information. Dessutom innehåller 13 § i marknadskontrollagen bestämmelser om marknadskontrollmyndighetens rätt att lämna ut sekretessbelagda uppgifter som gäller en enskild persons eller en sammanslutnings ekonomiska ställning eller företagshemlighet eller en enskilds personliga förhållanden till vissa behöriga myndigheter i utlandet och till internationella organ, för fullgörande av förpliktelser som grundar sig på Europeiska unionens rättsakter eller internationella överenskommelser som är bindande för Finland. Det finns ett behov av att komplettera dessa bestämmelser genom att utfärda bestämmelser om rätten att lämna ut uppgifter även till sådana myndigheter som inte nämns i marknadskontrollagen, men med vilka marknadskontrollmyndigheten ska samarbeta. Dessutom ska kretsen av uppgifter som lämnas ut anses vara för snäv med beaktande av cyberresiliensförordningens mål. Således ska omfattningen av rätten att lämna ut uppgifter enligt marknadskontrollagen utvidgas till dessa uppgifter.

I 318 § 2 mom. i lagen om tjänster inom elektronisk kommunikation (i lag 703/2025, träder i kraft den 1 januari 2026) finns det bestämmelser om Transport- och kommunikationsverkets rätt att lämna ut sekretessbelagd information till Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården samt livskraftscentralen, om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerheten. Bestämmelsen tillämpas även på sådana uppgifter för Transport- och kommunikationsverket som regleras i en annan lag än lagen om tjänster inom elektronisk kommunikation. Marknadskontrollmyndigheten ska vid behov samarbeta med dessa myndigheter med anledning av sådana uppgifter som hör till en behörig myndighet enligt NIS 2-direktivet. Eftersom bestämmelsen gäller endast för Transport- och kommunikationsverkets rätt att lämna ut information, finns det ett behov att komplettera den existerande regleringen så att man beaktar även situationer där den myndighet som övervakar förordningen om artificiell intelligens undantagsvis fungerar som marknadskontrollmyndighet.

Enligt artikel 52.2.7 i cyberresiliensförordningen ska myndigheter som utövar tillsyn över unionens dataskyddsrätt ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning när de behöver åtkomst till sådan dokumentation för att utföra sina uppgifter. De ska på begäran underrätta de utsedda marknadskontrollmyndigheterna i den relevanta medlemsstaten om en sådan begäran, vilket gäller i synnerhet situationer där uppgifter begärs direkt från tillverkaren eller det anmälda

organet. Ett dokument, såsom en sårbarhets- eller incidentsanmälan, kan dock innehas även av marknadskontrollmyndigheten. I Finland finns det bestämmelser om dataombudsmannens rätt att få information i 18 § i dataskyddslagen. Enligt den har dataombudsmannen utan hinder av sekretessbestämmelserna rätt att avgiftsfritt få de uppgifter som den behöver för att sköta sina uppgifter. Således förutsätter cyberresiliensförordningen inte till denna del ny nationell lagstiftning, eftersom dataombudsmannen med stöd av dataskyddslagen har rätt att få information om ett sekretessbelagt dokument om en enskild person eller myndighet även inom cyberresiliensförordningens tillämpningsområde.

Enligt artikel 52.13 i cyberresiliensförordningen ska marknadskontrollmyndigheterna årligen rapportera resultaten av relevant marknadskontroll till kommissionen. Artikel 54.3 och artikel 54.5–8 i cyberresiliensförordningen innehåller å sin sida bestämmelser om anmälningar av marknadskontrollmyndigheten till kommissionen och till de andra medlemsstaterna i vissa fall där en produkt med digitala element på befogade grunder kan bedömas orsaka en betydande cybersäkerhetsrisk utifrån andra än tekniska riskfaktorer och där den bristande överensstämmelsen inte begränsar sig till det nationella territoriet. Anmälningarna kan innehålla sekretessbelagda uppgifter. Marknadskontrollagens 13 § 3 punkt möjliggör utbyte av uppgifter i anknytning till detta, eftersom 3 punkten innehåller bestämmelser om utlämnande av uppgifter bland annat till en behörig myndighet i utlandet och till ett internationellt organ för att fullgöra en skyldighet som baserar sig på en EU-rättsakt.

Marknadskontrollagens 17 § möjliggör att ett åtgärdsföreläggande ges till en ekonomisk aktör, om produkten eller förfarandena avseende produkten inte är förenliga med kraven eller om produkten orsakar en sådan risk som fastställts i den. Ett åtgärdsföreläggande kan ges även i situationer där tillverkaren inte fullgör rapporteringsskyldigheterna enligt artikel 14 i cyberresiliensförordningen.

Marknadskontrollmyndigheten ansvarar även för övervakningen av skyldigheterna för förvaltare av programvara med fri och öppen källkod med stöd av artikel 52.3 i cyberresiliensförordningen. Om marknadskontrollmyndigheten konstaterar att en förvaltare av programvara med fri och öppen källkod inte iakttar de skyldigheter som föreskrivits i den nämnda artikeln, ska den kräva att förvaltaren av programvara med fri och öppen källkod vidtar alla lämpliga korrigerande åtgärder. En förvaltare av programvara med fri och öppen källkod ska säkerställa att alla lämpliga korrigerande åtgärder vidtas för att fullgöra skyldigheterna enligt denna förordning.

I enlighet med cyberresiliensförordningen tillämpas på förvaltare av programvara med fri och öppen källkod lindrigare krav än för tillverkare. Dessa omfattar en samarbetsskyldighet och en skyldighet att införa en cybersäkerhetspolicy samt att rapportera sårbarheter och incidenter (se avsnitt 2.1.3.3). En förvaltare av programvara med fri och öppen källkod anses dock inte tillhandahålla en programvaruprodukt på marknaden (skäl 19 i cyberresiliensförordningen). Då möjligheten att utfärda ett åtgärdsföreläggande med stöd av 17 § i marknadskontrollagen i en sådan situation inte är entydig och då avsikten är att tillämpa ett regleringssystem som är separat i förhållande till den övriga övervakningen av cyberresiliensen, är det motiverat att i förslaget inkludera förtydligande bestämmelser om möjligheten att ge ett förpliktande föreläggande för att genomföra åtgärderna, vilket kan förenas med vite.

Marknadskontrolllagens 28 § möjliggör att marknadskontrollmyndigheten får förena ett förbud eller föreläggande med vite. Enligt skäl 120 i ingressen till cyberresiliensförordningen får medlemsstaterna inte påföra heller andra typer av sanktioner av ekonomisk karaktär för mikroföretag eller små företag och inte heller för förvaltare av programvara med fri och öppen källkod, då administrativa sanktioner inte påförs för dem enligt förordningen. Vid beredningen

har det bedömts att detta dock inte avser vite, som inte är en påföljd av straffkaraktär, utan ett medel inom förvaltningstvång, och som säkerställer att den egentliga huvudförpliktelsen iakttas.

En beskrivning av de övriga befogenheter som ingår i marknadskontrollagen finns till exempel i regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s förordning om artificiell intelligens, RP 46/2025 rd, avsnitt 3.2.

### 3.1.3 Godkännande, utseende och övervakningen av anmälda organ

*Lagen om anmälda organ för vissa produktgrupper*

Med anmälda organ avses allmänt organ för bedömning av överensstämmelse, som godkänts och utsetts att sköta bedömningsuppgifter som gäller överensstämmelse och som baserar sig på i EU:s produktakter. Ett anmält organ är en aktör som en medlemsstat anmält till kommissionen och som har tillstånd att utföra uppgifter för att bedöma överensstämmelsen. I detta avsnitt behandlas nuläget för de anmälda organen med tanke på cyberresiliensförordningen. De organ för bedömning av överensstämmelse som sköter de uppgifter som avses i cybersäkerhetsakten behandlas nedan i avsnitt 3.2.4.

Det finns bestämmelser om godkännande, utseende och övervakningen av anmälda organ i den lag som gäller respektive produktgrupp. Produktreglering finns inom flera olika ministeriers förvaltningsområden.

I fråga om nya produktgrupper finns det bestämmelser om anmälda organ i lagen om anmälda organ för vissa produktgrupper (278/2016), som trädde i kraft den 27 april 2016. Genom lagen genomfördes nio produktspecifika direktiv som godkänts av Europaparlamentet och råd (så kallat *Alignment Package*), vilka fastställer enhetliga regler för godkännande av organ för bedömning av produkters överensstämmelse som så kallade anmälda organ. Lagen är horisontell och den innehåller bestämmelser om en ansökan om godkännande som anmält organ, den behöriga myndigheten och det nationella godkännande- och anmälningsförfarandet. Dessutom innehåller lagen bland annat bestämmelser om de allmänna kraven på anmälda organ, organens verksamhet och kraven på dess personal samt skyldigheten för ett anmält organ att delta i standardiserings- och samordningsarbetet.

Lagen om anmälda organ för vissa produktgrupper tillämpades då den trädde i kraft till en början på följande produktlagar: hissäkerhetslagen (1134/2016), lagen om mätinstrument (707/2011), lagen om tryckbärande anordningar (1144/2016), lagen om pyrotekniska artiklars överensstämmelse med kraven (180/2015), lagen om överensstämmelse med kraven för utrustning och säkerhetssystem som är avsedda för användning i explosionsfarliga omgivningar (1139/2015), lagen om explosiva varors överensstämmelse med kraven (1140/2016) och elsäkerhetslagen (1135/2016). Senare har lagens tillämpningsområde utvidgats även till andra produktlagar, såsom gasanordningslagen (502/2018), luftfartslagen (864/2014) och 30 kap. i lagen om tjänster inom elektronisk kommunikation (917/2014). I fråga om andra produktgrupper än de som omfattas av lagens tillämpningsområde baserar sig regleringen kring anmälda organ fortfarande på den produktlag som gäller denna produktgrupp.

I regel fogas ett ackrediteringsintyg som utfärdats av det nationella ackrediteringsorganet till en ansökan om godkännande och utseende av ett anmält organ. Med stöd av 2 a § i lagen om Säkerhets- och kemikalieverket (1261/2010) verkar Säkerhets- och kemikalieverkets ackrediteringsenhet (ackrediteringstjänsten FINAS) som nationellt ackrediteringsorgan i Finland. På ackreditering av en ackrediteringsenhet och jämställbar behörighet till bedömning tillämpas lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av

överensstämmelse med kraven (920/2005) oberoende av om lagen om om anmälda organ för vissa produktgrupper eller någon annan produktspecifik författning tillämpas på produktgruppen.

Cyberresiliensförordningen är en ny rättsakt. Det finns inga gällande bestämmelser om anmälda organ med ett överlappande tillämpningsområde. I artikel 36 i cyberresiliensförordningen förutsätts att medlemsstaterna ska utse en myndighet med ansvar för anmälan av bedömningsorgan. Den har till uppgift att utarbeta och genomföra behövliga förfaranden som gäller godkännande, utseende och anmälning av bedömningsorganen och övervakning av de anmälda organen.

Det finns skäl att avhålla sig från nationell överlappande reglering, eftersom kapitel IV i cyberresiliensförordningen innehåller detaljerade och direkt tillämpliga bestämmelser om anmälan om organ för bedömning av överensstämmelse. På grund av detta är det inte behövligt att utfärda bestämmelser om att anmälda organ som omfattas av cyberresiliensförordningens tillämpningsområde omfattas av tillämpningsområdet för lagen om anmälda organ för vissa produktgrupper. Till den del som tillämpningen av cyberresiliensförordningen så kräver, kan bestämmelser om anmälda organ inkluderas i en annan lag.

*Lagarna om bedömning och bedömningsorgan*

Bedömning av datasäkerhetsnivån omfattas nationellt även av lagen om bedömningsorgan för informationssäkerhet (1405/2011, lagen om bedömningsorgan) och lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011, bedömningslagen). Lagen om bedömningsorgan tillämpas på organisationer som tillhandahåller tjänster för bedömning av informationssäkerhet till den offentliga förvaltningen, vilka på uppdrag bedömer nivån på informationssäkerheten och ansöker om godkännande för denna verksamhet från Transport- och kommunikationsverket. Med stöd av lagen har tolv beslut för fyra olika företag getts om godkännande som organ för bedömning av överensstämmelse för olika kompetensområden.[1] Arbetsgruppen för uppdatering och förbättring av överensstämmelsebedömningen av informationssystem för offentlig förvaltning (VN/36127/2023) har utarbetat en bedömning av nuläget för bedömningen av överensstämmelsen för informationssystemens datasäkerhet och beredskap. I linje med detta har man i beredningen av regeringens proposition bedömt att det finns överlappningar i fråga om cyberresiliensförordningen och cybersäkerhetsakten i dessa nationella rättsakter. Eftersom rättsakternas mål och syfte avviker från varandra, förutsätts avsevärda ändringar i lagarna om bedömning och bedömningsorgan för att kunna utnyttja dessa i bedömning av överensstämmelse enligt cyberresiliensförordningen och i den bedömningsverksamhet som görs i nuläget med stöd av dessa.

Den nationella regleringen kring bedömning av datasäkerheten och beredskapen i myndigheternas informationssystem hänför sig till informationssystem som omfattas av myndigheternas beslutanderätt eller som planerats att upphandlas av den samt till en fallspecifik bedömning av beredskapen, det vill säga inte till kraven på produkter, tjänster eller processer som tillhandahålls allmänt på marknaden. Målområdena för bedömningen och syftet med bedömningens resultat enligt lagen om bedömningsorgan avviker från EU:s

[1] Källa: Transport- och kommunikationsverket Traficom, Cybersäkerhetscentret Läst den 31 juli 2023. (https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset)

certifieringsreglering. En fråga som är separat från detta är att ackreditering som utfärdats av ackrediteringstjänsten FINAS kan vara en förutsättning för bedömningsverksamhet enligt såväl EU:s reglering som den nationella regleringen. Verksamhet enligt lagarna om bedömning och bedömningsorgan kan med stöd av artikel 2.7 i cyberresiliensförordningen tolkas som verksamhet utanför dess tillämpningsområde.

### 3.1.4 Sårbarhetssamordning

Transport- och kommunikationsverkets Cybersäkerhetscenter genomför för närvarande sårbarhetssamordningen som en del av de uppgifter som föreskrivits för den. Med sårbarhetssamordning avses verksamhet för att säkerställa att information om en observerad sårbarhet eller ett annat allvarligt programvarufel når tillverkaren av programvaran. Genomförandet av sårbarhetssamordningen baserar sig på frivilliga anmälningar om sårbarheter i programvarorna och Cybersäkerhetscentrets uppgifter att utreda hot mot webbtjänster och informationssystem.

Den nuvarande sårbarhetssamordningen vid CSIRT-enheten vid Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter är att biträda den som hittat en sårbarhet att samarbeta med programvarutillverkarna för att avhjälpa sårbarheten. Målet är med andra ord att säkerställa att information om sårbarheten och ändamålsenligt avhjälpande av den når alla relevanta parter, det vill säga även slutanvändarna av produkten.

Samordningsprocessen börjar i allmänhet då en sårbarhet rapporteras till Cybersäkerhetscentret. En anmälan kan göras till exempel i en organisations namn, personligen eller anonymt. Efter anmälan analyserar Cybersäkerhetscentret den anmälda sårbarheten och säkerställer behövliga tekniska detaljer tillsammans med anmälaren. Därefter kontaktar Cybersäkerhetscentret enhetstillverkaren eller tjänsteleverantören och kommer överens om en tidsplan för att avhjälpa sårbarheten och om informationen om sårbarheten. I samordningen är det synnerligen viktigt att mellan alla parter säkerställa att information behandlas ansvarsfullt. När korrigeringen är färdig överenskoms publiceringssättet och tidsplanerna i fråga om sårbarheten med alla parter.

År 2024 anmäldes 489 sårbarheter till Cybersäkerhetscentret. Därtill tog Cybersäkerhetscentret under år 2024 på föregripande sätt kontakt med över tusen organisationer som äger en sårbar VPN-enhet och publicerade sammanlagt 26 sårbarhetsmeddelanden.

I Finland finns det för närvarande inte någon gällande horisontell reglering som ålägger att anmäla sårbarheter i programvaror till någon myndighet. De sårbarhetsanmälningar som Cybersäkerhetscentret tar emot baserar sig på frivillighet och samarbete med intressentgrupperna.

Genom cyberresiliensförordningen ställs en skyldighet för CSIRT-enheten att behandla obligatoriska och frivilliga sårbarhetsobservationer som gjorts med stöd av cyberresiliensförordningen och anmäla dessa till övriga länders CSIRT-enheter. Detta kommer att påverka CSIRT-enhetens nuvarande sårbarhetssamordning med tanke på dess praktiska arrangemang. Cyberresiliensförordningen förutsätter dock inte ändringar i den gällande lagstiftningen i fråga om den i nuläget genomförda sårbarhetssamordningen. Cyberresiliensförordningen förutsätter kompletterande reglering för att genomföra sårbarhetssamordning enligt den nämnda förordningen.

För klarhetens skull konstateras att CSIRT-enheten, det vill säga Cybersäkerhetscentret, även framöver ska kunna ta emot sårbarhetsanmälningar som baserar sig på frivillighet och samarbete med intressentgrupperna. Framöver tar CSIRT-enheten emot anmälningar enligt

cyberresiliensförordningen och även andra än frivilliga rapporter om sårbarheter enligt cyberresiliensförordningen som en del av skötseln av dess befintliga uppgifter enligt cybersäkerhetslagen. CSIRT-enhetens uppgift som gäller sårbarhetssamordning enligt 22 § i cybersäkerhetslagen täcker sårbarhetsanmälningar om produkter och tjänster som lämnar utanför tillämpningsområdet för cyberresiliensförordningen och sårbarhetsanmälningar som gäller verksamheten vid olika organisationer. Efter att bestämmelserna om sårbarhetsmeddelanden i cyberresiliensförordningen tillämpas, mottar CSIRT-enheten således sårbarhetsanmälningar som kan delas in i tre klasser enligt följande:

1) obligatoriska rapporter om sårbarheter enligt artikel 14 i cyberresiliensförordningen,

2) frivilliga rapporter om sårbarheter enligt artikel 15 i cyberresiliensförordningen, och

3) andra frivilliga rapporter om sårbarheter.

Artiklarna 16 och 17 i cyberresiliensförordningen innehåller bestämmelser om vissa skyldigheter för CSIRT-enheten som kan förutsätta utlämnande av uppgifter som sekretessbelagts i offentlighetslagen. Det finns ett behov av att utfärda separata bestämmelser om dessa situationer.

Artikel 15.4 i cyberresiliensförordningen innehåller bestämmelser om en situation där en annan aktör än en tillverkare anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar dataskyddet för en produkt med digitala element. Den CSIRT-enhet som utsetts till samordnare ska i så fall utan oskäligt dröjsmål anmäla ärendet till tillverkaren. På tillverkaren tillämpas i så fall bestämmelserna om rätten att få information för en part i offentlighetslagen. En part har med vissa begränsningar rätt att få information av den myndighet som behandlar eller behandlat ärendet i fråga om innehållet även i en annan än en offentlig handling, vilket har eller kunnat påverka behandlingen av partens ärende. På grund av detta behövs till denna del inte ny reglering för att lämna ut uppgifter.

Enligt artikel 15.5 i cyberresiliensförordningen ska den CSIRT-enhet som utsetts till samordnare och Enisa säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls av den anmälande fysiska eller juridiska personen. I fråga om en CSIRT-enhet kan det anses att bestämmelserna i offentlighetslagen säkerställer sekretessen för dessa uppgifter till den del som det är befogat. Sekretessen kan baseras på 24 § 7 punkten i offentlighetslagen, enligt vilken handlingar som gäller skyddsarrangemang för data- och kommunikationssystem och genomförandet av arrangemangen ska sekretessbeläggas, på övervakningshemligheten enligt 15 punkten eller på sekretessen för affärshemligheter och andra näringshemligheter enligt 20 punkten.

### 3.1.5 Cybersäkerhetsmärket

Transport- och kommunikationsverkets Cybersäkerhetscenter lanserade Cybersäkerhetsmärket för smarta konsumentenheter, det vill säga IoT-enheter, år 2019. Cybersäkerhetsmärket var ett bevis som beviljats av Cybersäkerhetscentret vid Transport- och kommunikationsverket om att en produkt som är försedd med märket redan från början planerats att vara datasäkert och och att det uppfyller Transport- och kommunikationsverkets dataskyddskrav.

Det var frivilligt för produkttillverkarna att ansöka om Cybersäkerhetsmärket. Cybersäkerhetsmärket var inte en förutsättning för att släppa ut en produkt på marknaden.

Kraven på Cybersäkerhetsmärket baserade sig på ETSI:s standard EN 303 645, som är en sammanställning av dataskyddskrav på grundnivå för IoT-enheter riktade till konsumenterna. I valet av kraven på Cybersäkerhetsmärket riktades särskild uppmärksamhet på skyddet av användaren. Av produkten förutsattes bland annat information om stödperioden, handledning om datasäker användning och säkra förvalda installationer. På produkten ställdes krav som gäller lösenordspraxis, kryptering, hantering av sårbarheter och programvaruuppdateringar samt minskning av attackytan.

Transport- och kommunikationsverket beviljade Cybersäkerhetsmärket till produkter och tjänster, för vilka märket ansöktes frivilligt och vilka uppfyllde dataskyddskragen samt kom igenom en kontroll som gjordes av en tredje part. Intressentgrupperna ansåg att kontrollen av en tredje part var en viktig åtgärd jämfört med att visshet om produktens cybersäkerhetsegenskaper inhämtas utifrån självbedömning. Med regelbundna årliga granskningar säkerställdes att en produkts cybersäkerhetsegenskaper är uppdaterade i den föränderliga hotmiljön.

Sammanlagt 27 konsumentenheter beviljades Cybersäkerhetsmärket. Cybersäkerhetsmärket ansöktes för flera produkter, men omkring 40 % av ansökningarna ledde inte till någon slutlig märkning på grund av att brister framkom i produkten. Resultaten visade att tillverkarens mognad i genomförandet av cybersäkerheten för produkter varierar. Utmaningar orsakades av långa leveranskedjor, det stora antalet intressentgrupper samt den ökade integreringen av komponenter och ekosystem.

Transport- och kommunikationsverket har slutat att bevilja nya Cybersäkerhetsmärken. Bakgrunden till beslutet utgörs bland annat av att cyberresiliensförordningen och direktivet om radioutrustning trätt i kraft, eftersom den nya EU-regleringen för med sig motsvarande dataskyddskrav som framöver är förpliktande för alla nätanslutna enheter. Transport- och kommunikationsverket har inte för avsikt att förlänga giltigheten för de nuvarande Cybersäkerhetsmärkena efter att direktivet om radioutrustning trätt i kraft den 1 augusti 2025.

### 3.1.6 Regulatorisk sandlåda

I Finland har man inte genomfört regulatoriska sandlådor enligt cyberresiliensförordningen. I de andra EU-medlemsstaterna har de viktigaste tillämpningsområdena för regulatoriska sandlådor utgjorts av finansiella tjänster (*fintech*), energi och trafik.

Även EU:s förordning om artificiell intelligens innehåller reglering om regulatoriska sandlådor som liknar regleringen i cyberresiliensförordningen. I jämförelse med cyberresiliensförordningen innehåller förordningen om artificiell intelligens mer detaljerad reglering om användning av regulatoriska sandlådor för produkter som omfattas av tillämpningsområdet för förordningen om artificiell intelligens.

Dessutom innehåller vissa EU-rättsakter som utfärdats under den senaste tiden bestämmelser om inrättande av regulatoriska sandlådor. Inrättandet av regulatoriska sandlådor enligt dessa rättsakter och detaljerna i verksamheten avviker i viss mån från varandra. Till exempel Europaparlamentets och rådets förordning EU 2024/1735 om inrättande av en åtgärdsram för att stärka Europas ekosystem för tillverkning av nettonollteknik och om ändring av förordning (EU) 2018/1724 (den så kallade nettonollförordningen) möjliggör att medlemsstaterna frivilligt kan inrätta regulatoriska sandlådor som gäller nettonollteknik. I det nationella genomförandet av nettonollförordningen har man inte tills vidare bestämt sig för att inrätta någon regulatorisk sandlåda i Finland.

### 3.1.7 Grupptalan

Med stöd av artikel 65 i cyberresiliensförordningen tillämpas direktivet om grupptalan (EU) 2020/1828 på grupptalan om ekonomiska aktörers överträdelser av bestämmelserna i denna förordning vilka skadar eller kan skada konsumenternas kollektiva intresse.

Det finns bestämmelser om grupptalan enligt direktivet om grupptalan i lagen om grupptalan om åtgärder för förbudsföreläggande (1101/2022) och lagen om grupptalan (1103/2022). En grupptalan gör det möjligt att kräva att en näringsidkares förfarande ska förbjudas. Dessutom är det möjligt att kräva gottgörelse för skada som åsamkats konsumenter. Grupptalan utgörs av grupptalan som gäller yrkande på gottgörelse och grupptalan som gäller förbudsföreläggande.

Det förutsätts inte nationell kompletterande reglering för att tillämpa de bestämmelser som genomför direktivet om grupptalan även på överträdelse av cyberresiliensförordningen. Genom artikel 67 i cyberresiliensförordningen fogas cyberresiliensförordningen till listan över de rättsakter som avses i bilaga I till direktivet om grupptalan. Tillägget möjliggör att nationella bestämmelser om grupptalan tillämpas i oförändrad form även på grupptalan som gäller överträdelse av cyberresiliensförordningen. Med stöd av 4 § 1 mom. i lagen om grupptalan om åtgärder för förbudsföreläggande kan grupptalan väckas mot en näringsidkare som har handlat i strid med bestämmelserna om skydd för konsumenters kollektiva intressen i de rättsakter som nämns i bilaga I till direktivet om grupptalan. Regleringen är till denna del tillräcklig i fråga om grupptalan.

## 3.2 Cybersäkerhetsakten

### 3.2.1 Uppgifterna för myndigheten för cybersäkerhetscertifiering

Europeiska cybersäkerhetscertifikat och försäkringar om överensstämmelse enligt cyberresiliensförordningen kommer enligt bedömningen att vara viktiga för att uppfylla kraven i cyberresiliensförordningen. I princip ändras karaktären på cybersäkerhetscertifieringen då cyberresiliensförordningen träder i kraft. I de fall som avses i artikel 27.8 i cyberresiliensförordningen är det möjligt att med EU-försäkringar om överensstämmelse eller ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering, vid sidan om andra tillämpliga förfaranden, visa att en produkt är förenlig med de informationssäkerhetskrav som ställs i cyberresiliensförordningen. Efterfrågan på cybersäkerhetscertifieringar bedöms öka innan de enhetliga standarder som ska utarbetas med anledning av cyberresiliensförordningen är tillgängliga. I artiklarna 8 och 32 i cyberresiliensförordningen fastställs därtill situationer där ett cybersäkerhetscertifikat av betydande eller hög assuransnivå krävs av en kritisk produkt.

Det finns bestämmelser om uppgifterna för den myndighet som utfärdar cybersäkerhetscertifiering i artikel 58 i cybersäkerhetsakten. Trots det begrepp som används i den finskspråkiga versionen av förordningen täcker uppgiften även tillsynsverksamhet (se närmare i detaljmotiveringen till 21 § i lagförslag 1). Genom lag 1210/2020 utfärdades bestämmelser om tilldelningen av uppgifterna för den nationella myndigheten för cybersäkerhetscertifiering enligt cybersäkerhetsakten (regeringen proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den RP 98/2020 rd). Vid den tidpunkten infördes i 304 § i lagen om tjänster inom elektronisk kommunikation en bestämmelse om att Transport- och kommunikationsverket har till uppgift att fungera som nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten. Den uppgift som föreskrivits i denna lag täcker såväl utfärdande av cybersäkerhetscertifikat som kontrolluppgifter enligt förordningen, vilka enligt artikel 58.4 i förordningen ska avskiljas från varandra.

När bestämmelserna om uppgiften utfärdades infördes dock inte nya bestämmelser om befogenheterna för den nationella myndigheten för cybersäkerhetscertifiering i lagen. I praktiken har man sedermera observerat att myndighetsbefogenheterna i lagen om tjänster inom elektronisk kommunikation, såsom för inspektioner och påföljder, i detta hänseende förutsätter komplettering, eftersom de inte ger möjlighet att på omfattande sätt tillämpas på de fall som cybersäkerhetsakten förutsätter. Den centrala orsaken till detta är att myndigheternas befogenheter i lagen om tjänster inom elektronisk kommunikation har kopplats till situationer som handlar om tillämpning eller överträdelse av rättigheterna eller skyldigheterna enligt den lagen, vilket det inte handlar om i ett fall enligt den direkt tillämpliga förordningen. Inga bestämmelser om ställningen för organ för bedömning av överensstämmelse inkluderades heller i lagen om tjänster inom ekonomisk kommunikation. På grund av detta finns det ett behov av att komplettera den nationella reglering som cyberresiliensförordningen förutsätter.

### 3.2.2 Befogenheterna för certifieringsmyndigheten för cybersäkerhet i anknytning till kontrollen

Artikel 58.8 i cybersäkerhetsakten innehåller bestämmelser om befogenheterna för den nationella myndighet som utfärdar cybersäkerhetscertifiering.

Enligt artikel 58.8 a i förordningen ska myndigheten ha befogenhet att 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. Lagen om tjänster inom ekonomisk kommunikation, som för närvarande innehåller bestämmelser om Transport- och kommunikationsverkets uppgift att fungera som en sådan myndighet, är dock för tillfället inte en tillräckligt kompletterande nationell reglering. Rätten att få uppgifter enligt 315 § i lagen gäller nämligen endast aktörer vars rättigheter eller skyldigheter föreskrivs i lagen om tjänster inom elektronisk kommunikation, varför den inte är tillämplig på övervakning av förordningen.

Enligt underpunkt b ska myndigheten ha befogenhet att 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. Enligt underpunkt d ska myndigheten 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. medlemsstaternas processrätt Bestämmelserna om inspektioner i 325 § i lagen om tjänster inom elektronisk kommunikation är dock tillämpliga främst på inspektioner av teleföretag. För att genomföra inspektioner finns det ett behov av en möjlighet att få handräckning även av polisen.

Underpunkterna c och f gäller myndighetens verkställighetsbefogenheter. Enligt underpunkt c ska myndigheten 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. Enligt underpunkt f ska myndigheten dessutom ha befogenheter att utdöma sanktioner i enlighet med nationell rätt, enligt artikel 65, och kräva att överträdelser av skyldigheterna i denna förordning omedelbart upphör. I artikel 65 i förordningen föreskrivs ännu att medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av denna avdelning och överträdelser av europeiska ordningar för cybersäkerhetscertifiering, och att de ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I 330–332 § i lagen om tjänster inom elektronisk kommunikation finns det för närvarande bestämmelser om ett

tillsynsbeslut och tillfälligt beslut och om hot om vite, hot om avbrytande och hot om tvångsutförande. Dessutom innehåller 309 § i lagen bestämmelser om Transport- och kommunikationsverkets rätt att få handräckning. Dessa bestämmelser gäller dock främst överträdelse av den nämnda lagen. Bestämmelserna om påföljdsavgifter eller straffrättsliga straff i lagen är inte heller tillämpliga på genomförandet av förordningen. Således är det behövligt att komplettera regleringen.

Enligt underpunkt e ska myndigheten ha befogenheter att 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. Lagen om tjänster inom elektronisk kommunikation innehåller inte sådana nationella bestämmelser, även om sådan befogenhet ska anses vara behövlig.

Dessutom innehåller artikel 58.7 e i cybersäkerhetsakten bestämmelser som förutsätter nationell reglering om att myndigheterna i tillämpliga fall ska 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. För sådana situationer är det dessutom behövligt att utfärda bestämmelser om förvaring av handlingar då verksamheten enligt cybersäkerhetsakten upphör vid ett organ för bedömning av överensstämmelse.

### 3.2.3 Regleringen kring informationsutbyte

Uppgifterna för den myndighet som utfärdar cybersäkerhetscertifiering omfattar samarbete och utbyte av uppgifter med flera aktörer. Artikel 58.7 a i cybersäkerhetsakten förutsätter tillsynssamarbete med de relevanta marknadskontrollmyndigheterna. Underpunkt c förutsätter å sin sida att den myndighet som utfärdar cybersäkerhetscertifiering aktivt bistår och stödjer de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning. I enlighet med underpunkt g ska den myndighet som utfärdar cybersäkerhetscertifiering 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, vilket hänvisar till de kontrollåtgärder som hänför sig till olika instanser. Utifrån underpunkt h ska den myndighet som utfärdar 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 denna förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering. I punkt 102 i ingressen till förordningen konstateras att kommissionen ska underlätta sådant utbyte av information genom att erbjuda tillgång till ett allmänt stödsystem för elektronisk information. I artikel 58.9 i cybersäkerhetsakten föreskrivs dessutom att de myndigheter som utfärdar 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.

Genom artikel 62 i cybersäkerhetsakten har Europeiska gruppen för cybersäkerhetscertifiering inrättats, vilken utgörs av företrädare för de nationella myndigheter som utfärdar cybersäkerhetscertifiering eller andra relevanta nationella myndigheter. Gruppen har bland annat till uppgift att granska betydelsefull utveckling inom cybersäkerhetscertifiering och utbyta information och god praxis kring ordningar för cybersäkerhetscertifiering (artikel 62.4 f) och

underlätta samarbetet enligt denna avdelning mellan de nationella myndigheter som utfärdar cybersäkerhetscertifiering genom utveckling av färdigheterna och informationsutbyte i synnerhet genom att införa metoder för att utbyta information effektivt om alla frågor som rör cybersäkerhetscertifiering (artikel 62.4 g).

Den myndighet som utfärdar cybersäkerhetscertifiering ska således vid behov kunna dela även sekretessbelagd information med ovan nämnda aktörer. Sekretessbeläggningen av uppgifter kan i typfallet basera sig till exempel på en privat affärshemlighet eller en annan affärshemlighet enligt 24 § 1 mom. 20 punkten i offentlighetslagen eller en uppgift som gäller skyddsarrangemangen i informations- och kommunikationssystem enligt 7 punkten.

För samarbetet på EU-nivå kan det finnas ett behov av att lämna ut uppgifter till de nationella myndigheter som utfärdar cybersäkerhetscertifiering i de olika medlemsstaterna och till andra medlemmar av Europeiska gruppen för cybersäkerhetscertifiering samt till kommissionen. Därtill är det behövligt att överlåta uppgifter till finländska och europeiska marknadskontrollmyndigheter och ackrediteringsenheter.

Med stöd av artikel 56.8 i cybersäkerhetsakten får en myndighet som utfärdar cybersäkerhetscertifiering från certifikatinnehavarna anmälningar om sårbarheter eller oriktigheter som kan påverka överensstämmelsen med de krav som sammanhänger med certifieringen. Det är nödvändigt att dela dessa uppgifter med CSIRT-enheten, så att bland annat användare av certifierade produkter kan nås effektivt och så att de behövliga åtgärderna kan vidtas för att minimera skador.

I 318 § 2 mom. i lagen om tjänster inom elektronisk kommunikation (i lag 703/2025) finns det bestämmelser om att Transport- och kommunikationsverket har rätt att lämna ut sekretessbelagd information till Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket samt livskraftscentralen, om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerhet. Bestämmelsen kan i princip tillämpas även på uppgifter enligt cybersäkerhetsakten, men förteckningen täcker inte alla finländska myndigheter, med vilka samarbete kan anses vara behövligt. Således ska bestämmelser om informationsutbytet utfärdas på ett mer omfattande sätt med tanke på samarbetet såväl inom Finland som på EU-nivå.

### 3.2.4 Organen för bedömning av överensstämmelse och den offentliga förvaltningsuppgiften

Artikel 56.4–56.6 i cybersäkerhetsakten innehåller bestämmelser om utfärdaren av cybersäkerhetscertifikat. Organ för bedömning av överensstämmelse enligt artikel 60 utfärdar europeiska cybersäkerhetscertifikat av assuransnivå ”grundläggande” eller ”betydande” utifrån kriterier som ingår i en europeisk ordning för cybersäkerhetscertifiering som godkänts av kommissionen i enlighet med artikel 49. I en certifieringsordning är det dock möjligt att förordna att det europeiska cybersäkerhetscertifikat som fås ur ordningen utfärdas endast av ett offentligt organ, som kan vara antingen den nationella myndighet som utfärdar cybersäkerhetscertifiering eller ett offentligt organ som ackrediterats som ett organ för bedömning av överensstämmelse. Utfärdaren av ett cybersäkerhetscertifikat av hög assuransnivå är å sin sida i princip den nationella myndighet som utfärdar cybersäkerhetscertifiering. Ett organ för bedömning av överensstämmelse kan dock utfärda ett certifikat av hög assuransnivå a) efter förhandsgodkännande av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse eller 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.

Artiklarna 60–61 i förordningen innehåller bestämmelser om organ för bedömning av överensstämmelse och anmälning av sådana. Nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008 ska ackreditera ett organ för bedömning av överensstämmelse. 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.

Den certifiering som görs av ett organ för bedömning av överensstämmelse ska ses som en offentlig förvaltningsuppgift enligt 124 § i grundlagen. Den nationella lagen innehåller dock för närvarande inte sådana bestämmelser som grundlagen förutsätter om att man på ett organ för bedömning av överensstämmelse som sköter cybersäkerhetscertifiering tillämpar samma bestämmelser som tillämpas på den som sköter en motsvarande uppgift med myndighetsansvar. Så som konstateras i avsnitt 3.1.3 blir lagen om bedömningsorgan och bedömningslagen tillämplig på certifieringsverksamhet enligt cybersäkerhetsakten. Verksamheten omfattas inte heller av tillämpningsområdet för lagen om anmälda organ för vissa produktgrupper. På grund av detta är det behövligt att i lagen inkludera de kompletterande bestämmelser som cybersäkerhetsakten förutsätter om anmälning och bemyndigande av organ för bedömning av överensstämmelse och om deras skyldigheter och ansvar till den del som de inte anses följa direkt av förordningen. Likaså är det behövligt att utfärda bestämmelser om möjligheten att delegera utfärdandet av certifikat av hög assuransnivå till organ för bedömning av överensstämmelse.

### 3.2.5 Rättsskyddsmedel

Artikel 63 i cybersäkerhetsakten innehåller bestämmelser om rätten att lämna in klagomål. Enligt punkt 1 i artikeln ska fysiska och juridiska personer 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. Det sist nämnda fallet handlar om en situation där ett organ för bedömning av överensstämmelse har utfärdat ett cybersäkerhetscertifikat av hög assuransnivå med ett godkännande för ett enskilt fall av myndigheten för cybersäkerhetscertifiering eller utifrån en allmän delegering. Enligt skäl 102 till akten bör de nationella myndigheterna för cybersäkerhetscertifiering 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”, i lämplig utsträckning undersöka det ärende som klagomålet gäller och bör underrätta den klagande om utvecklingen och resultatet av utredningen inom rimlig tid. Artikeln handlar således om situationer där en utomstående riktar en myndighets eller bedömningsorganets uppmärksamhet till exempel på en observerad brist i efterlevnaden av kraven i certifieringsordningen eller tillverkarens skyldigheter att ge information.

Även om begreppet klagomål används i artikel 63 i förordningen, handlar det nationellt i detta sammanhang om en tillsynsanmälan (begäran om åtgärd), det vill säga en begäran till en myndighet att undersöka ett lagstridigt förfarande. Det handlar om ett förvaltningsärende. För närvarande finns det specialreglering om behandling av tillsynsärenden vid Transport- och kommunikationsverket i 313 § i lagen om tjänster inom elektronisk kommunikation. Enligt den kan Transport- och kommunikationsverket på begäran av en part och på eget initiativ ta ett ärende för undersökning, och därtill prioritera sina tillsynsuppgifter och avvisa ärendet.

Bestämmelserna i lagen om tjänster inom elektronisk kommunikation uppfyller för närvarande kraven i cybersäkerhetsakten till denna del. Artikeln bedöms dock inte nödvändigtvis förutsätta nationell kompletterande reglering då den reglering som kompletterar förordningen överförs till den föreslagna speciallagen, utan förvaltningslagen kan i detta hänseende anses vara tillräcklig. Enligt 19 § i förvaltningslagen inleds ett ärende genom att yrkandena med grunderna för dem anges.

Ett sådant krav kan framföras även till det organ för bedömning av överensstämmelse som utfärdat certifikatet i de fall där uppgiften hör till bedömningsorganet. Artikel 63 i cybersäkerhetsakten gäller sådana certifikatutfärdare som inte är myndigheter. Det handlar om organ för bedömning av överensstämmelse som kan utfärda certifikat i vissa fall. Detta betraktas som skötsel av en offentlig förvaltningsuppgift, varvid de allmänna förvaltningslagarna är tillämpliga på verksamheten. Organet ska således behandla en begäran om en åtgärd i enlighet med förvaltningslagen. Den nationella lagen innehåller dock inte bestämmelser om att man på den som sköter uppgiften tillämpar samma bestämmelser som på den som sköter uppgiften med myndighetsansvar, varför den nationella lagstiftningen ska kompletteras i detta hänseende.

Enligt artikel 63.2 i cyberresiliensförordningen ska myndigheten eller organet till vilket klagomålet har lämnats in underrätta den klagande om hur förfarandet fortskrider och vilket beslut som fattats, och informera den klagande om rätten till effektiva rättsmedel enligt artikel 64. Kravet förutsätter inte kompletterande nationell reglering. De allmänna förvaltningslagarna är tillämpliga såväl på den som sköter en offentlig förvaltningsuppgift som på organet för bedömning av överensstämmelse. Med stöd av principerna om god förvaltning (7 och 8 § i förvaltningslagen) ska sakliga förfrågningar till exempel om handläggningssituationen besvaras. Förvaltningslagen innehåller även bestämmelser om tilldelningen av besvärsrätt.

I artikel 64 finns det bestämmelser om rätten till effektiva rättsmedel. I punkt 1 i artikeln föreskrivs att utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol ska fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende beslut fattade av den myndighet eller det organ som avses i artikel 63.1. Detta inbegriper åtminstone felaktiga beslut om utfärdande av cybersäkerhetscertifikat, beslut om att inte utfärda ett europeisk cybersäkerhetscertifikat eller beslut om att erkänna ett europeiskt cybersäkerhetscertifikat som innehas av dessa fysiska personer och juridiska personer. För det andra täcker rätten en situation med underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till den myndighet eller det organ som avses i artikel 63.1. Enligt punkt 2 i artikeln ska förfaranden enligt denna artikel inledas vid domstolarna i den medlemsstat där myndigheten eller organet som det rättsmedlen avser är beläget.

Vid överklagande av myndigheters beslut handlar det i Finland om en förvaltningsprocess. Besvärsrätt har parterna eller den om vars besvärsrätt det föreskrivs särskilt i lag. Även om begreppet talan används i punkten, anhängiggörs ärendet genom att överklaga till en domstol i Finland. Lagen om rättegång i förvaltningsärenden (808/2019) innehåller grundläggande bestämmelser om ändringssökande. Bestämmelserna i den allmänna lagen om att överklaga ett förvaltningsbeslut av en myndighet till förvaltningsdomstolen täcker även förvaltningsbeslut som fattats av enskilda personer som utför en offentlig förvaltningsuppgift. För närvarande innehåller 344 § i lagen om tjänster inom elektronisk kommunikation en informativ hänvisning till ovan nämnda lag. Paragrafen innehåller även bestämmelser om möjligheten för den myndighet eller det anmälda organ som fattat beslutet att förordna att ett beslut ska iakttas trots ändringssökande, om besvärsmyndigheten inte bestämmer annat. Det finns skäl att inkludera motsvarande reglering i lagen, dock på så sätt att även ett organ för bedömning av överensstämmelse kan förordna att ett beslut ska iakttas trots ändringssökande.

Om man nationellt först vill använda en begäran om omprövning som rättsmedel i enlighet med 7 a kap. i förvaltningslagen, ska separata bestämmelser utfärdas om detta. Även om syftet är att en begäran om omprövning ska användas på ett så omfattande sätt som möjligt som den första fasen av ändringssökandet, lämpar sig förfarandet för begäran om omprövning inte på en myndighets tillsynsförfarande, som baserar sig på detaljerad utredning av ett ärende. I fråga om beslut som fattats av organen för bedömning av överensstämmelse kan det dock anses att förfarandet med begäran om omprövning är motiverat på samma sätt som för ett beslut om betalningsskyldighet av en myndighet.

Enligt cybersäkerhetsakten ska rättsskyddsmedlen täcka även en situation där en begäran om åtgärd inte behandlas. Så kallade passivitetsbesvär ingår inte i lagen om tjänster inom elektronisk kommunikation. Så som förs fram mer ingående nedan i bedömningen av alternativen, kan det i situationer med dröjsmål anses att ett tillräckligt rättsskyddsmedel utgörs av möjligheten att klaga över verksamheten vid en myndighet eller den som sköter en offentlig förvaltningsuppgift till de högsta laglighetsövervakarna.

Som sammandrag kan det konstateras att cybersäkerhetsakten förutsätter kompletterande nationell reglering om skötseln av en offentlig förvaltningsuppgift och befogenheterna för certifieringsmyndigheten, liksom även om påföljder och ändringssökande. Dessutom finns det ett behov av att utfärda bestämmelser även om rätten att få handräckning, liksom även om myndighetssamarbetet och det anknutna utbytet av uppgifter.

### 3.3 Myndighetsverksamhetens avgiftsbelagdhet

Lagen om grunderna för avgifter till staten (150/1992) innehåller bestämmelser om de allmänna grunderna för när statliga myndigheters prestationer ska vara avgiftsbelagda och för storleken av de avgifter som uppbärs för prestationerna samt om övriga grunder för avgifterna. Det handlar om en allmän lag och det är möjligt att separat utfärda bestämmelser om avgifter vid sidan om den. Lagen innehåller bestämmelser om de allmänna grunderna för när prestationer ska vara avgiftsbelagda (2 kap.), inbegripet bestämmelser om vissa prestationer som är antingen avgiftsbelagda eller avgiftsfria. Enligt lagen om grunderna för avgifter till staten avses med ”offentligrättslig prestation” en sådan prestation av en statlig myndighet vars efterfrågan grundar sig på lag eller förordning och som myndigheten har faktisk ensamrätt att utföra. Enligt 6 § i lagen om grunderna för avgifter till staten ska beloppet av den avgift som tas ut för en offentligrättslig prestation till staten motsvara beloppet av statens totalkostnader för prestationen. I 8 § i lagen om grunderna för avgifter till staten finns bestämmelser om de ärenden som kan föreskrivas genom förordning och om bemyndigande av ett ministerium. Enligt 12 i § i lagen om grunderna för avgifter till staten är det möjligt att genom förordning utfärda närmare bestämmelser om de kostnader som omfattas av självkostnadsvärdet.

Regleringen om avgiftsbelagdheten för myndigheternas prestationer och grunderna för avgifterna för prestationerna i lagen om grunderna för avgifter till staten bedöms vara tillräcklig. Myndigheters utfärdande av certifikat av hög assuransnivå ska inom ramen för lagen om grunderna för avgifter till staten anses vara en offentligrättslig prestation. Likaså ska bland annat utseende av organ för bedömning av överensstämmelse som anmälda organ inom ramen för cyberresiliensförordningen, anmälning av sådana för cybersäkerhetscertifiering samt tillsyn över dessa betraktas som en offentligrättslig prestation. När dessa prestationer gäller den ekonomiska verksamheten vid en aktör som ansöker om certifiering eller ett organ för bedömning av överensstämmelse, finns det inte något i lagen om grunderna för avgifter till staten avsett särskilt skäl att avvika från avgiftsbelagdheten för dessa. Även användning av en regulatorisk sandlåda för cyberresiliens ska utifrån utgångspunkten i lagen om grunderna för avgifter till staten som förval vara avgiftsbelagd, eftersom avgifterna täcker kostnader för

myndigheten för att administrera och använda den regulatoriska sandlådan. Lagen om grunderna för avgifter till staten möjliggör dock att en avgift utifrån särskilda skäl kan förordnas att tas ut av en viss grupp till ett värde som är lägre än självkostnadsvärdet eller att den inte alls tas ut. Detta möjliggör vid behov lättnader av avgiftsbelagdheten i synnerhet då en regulatorisk sandlåda inrättas i en testmiljö enligt förordningen om artificiell intelligens, eftersom tillgång till en testmiljö enligt förordningen om artificiell intelligens ska ges avgiftsfritt till små och medelstora företag.

I 3 § i förordningen om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation (1190/2023, ändrad genom förordningen 905/2024) finns det bestämmelser bland annat om avgiftsbelagdheten för prestationer i anknytning till bedömningen av säkerhetsnivån hos dataskyddsprodukter och produkter som utnyttjar datakommunikationsförbindelser. En avgift enligt självkostnadsvärdet tas ut för prestationen. Enligt 4 punkten i samma paragraf tas en avgift ut också för åtgärder i anknytning till godkännande av organ för bedömning av informationssäkerheten. I samband med uppdateringen av förordningen finns det ett behov av att bedöma behovet av att precisera förordningen, så att den täcker prestationer som även anknyter till cyberresiliensförordningen och cybersäkerhetsakten.

### 3.4 Registrarer

Bestämmelserna om entiteter som tillhandahåller domännamnsregistreringstjänster i artikel 3 och artiklarna 26–28 i NIS 2-direktivet har genomförts genom lagen om ändring av lagen om tjänster inom elektronisk kommunikation (L 126/2025; RP 57/2024 rd).

I 21 kap. i lagen om tjänster inom elektronisk kommunikation finns det bestämmelser om domännamn under den nationella toppdomänen för Finland (*toppdomänen fi*) och under toppdomänen för landskapet Åland (*toppdomänen ax*) samt på domännamnsverksamhet och registreringstjänster för domännamn i samband därmed. Det finns bestämmelser om anmälningsskyldigheten för registrarer enligt artikel 27 i NIS 2-direktivet i 165 § i lagen om tjänster inom elektronisk kommunikation. Det finns bestämmelser som genomför artikel 28 i NIS 2-direktivet i 167 § och 170 § i lagen om tjänster inom elektronisk kommunikation.

Bestämmelserna om andra entiteter än entiteter som tillhandahåller domännamnsregisteringstjänster i NIS 2-direktivet har genomförts genom cybersäkerhetslagen (142/2025) och lagen om ändring av lagen om informationshantering inom den offentliga förvaltningen (L 125/2025). De nämnda lagarna innehåller inte bestämmelser om registrarer.

Bestämmelserna i 21 kap. i lagen om tjänster inom elektronisk kommunikation är tillämpliga endast på domännamn som slutar med den nationella toppdomänen fi och toppdomänen för landskap ax och anknuten förmedling av domännamn av registrarer. Artiklarna 26–28 i NIS 2-direktivet kräver att medlemsstaterna förutsätter åtgärder enligt artiklarna 27–28 även av registrarer som förmedlar andra domäner, då registraren med stöd av artikel 26 i NIS 2-direktivet omfattas av Finlands jurisdiktion. Således finns det ett behov av att komplettera genomförandet av NIS 2-direktivet i fråga om entiteter som tillhandahåller domännamnsregistrering då det handlar om annan domännamnsregistrering än verksamhet som anknyter till domännamn med den nationella toppdomänen fi eller toppdomänen för landskap ax. Dessutom ska tillämpningen av 21 kap. för att säkerställa ett heltäckande genomförande av direktivet till vissa delar utvidgas till aktörer som verkar för registrarers räkning. Kompletteringarna förutsätter ändringar i lagen om tjänster inom elektronisk kommunikation och i cybersäkerhetslagen.

I Finland finns det för närvarande inte någon gällande reglering kring registrering av andra domännamn än domännamn med den nationella toppdomänen fi eller toppdomänen för landskap ax. Med stöd av 21 kap. i lagen om tjänster inom elektronisk kommunikation har Transport- och kommunikationsverket gett en föreskrift om domännamn, som gäller registrering av domännamn med den nationella toppdomänen fi eller toppdomänen för landskap ax.

Flera frivilliga standarder på Internet har i internationellt samarbete utarbetats om insamling av, offentliggörande av och tillträde till registreringsuppgifter om domännamn och om praxis inom branschen. Utifrån dessa har det uppkommit en praxis, enligt vilken varje toppdomänregister själv administrerar en så kallad WHOIS-tjänst, där de registreringsuppgifter om domännamn som registret innehar publiceras. ICANN (Internet Corporation for Assigned Names and Numbers) som administrerar generiska toppdomäner på Internet har infört denna princip i sina egna avtal om register över generiska toppdomäner (gTLD) på så sätt att ansvaret för att publicera registreringsuppgifter numera ligger på den aktuella förvaltaren av ett toppdomänregister och därtill på de registrarer som den bemyndigat, var och en för egen del på så sätt att bägge aktörers ansvar för offentliggörandet av de olika datatyperna avviker en aning från varandra. I avtalet regleras även överföringen av registeruppgifter från registraren till en förvaltare av toppdomänregister under de förutsättningar som följer av lagstiftningen kring behandling av personuppgifter. I fråga om nationella toppdomäner (ccTLD) finns det däremot inte någon enhetlig praxis. De lagändringar som gäller kompletteringen av genomförandet av NIS 2-direktivet i fråga om dess artikel 28, vilka gäller offentligheten för registreringsuppgifter om domännamn, ska beredas på så sätt att de i mån av möjlighet ligger i linje med de internationella standarderna och praxis som uppkommit utifrån dessa. Direktivet kan anses möjliggöra olika tekniska genomförandemodeller, så länge som de uppgifter som förutsätts i artikel 28 i direktivet är offentligt tillgängliga och så länge som de som förvaltar toppdomänregister och registrarerna förmår ge tillträde till uppgifter som ingår i personuppgifter i enlighet med kraven i direktivet.

Befogenheterna för Transport- och kommunikationsverket enligt lagen om tjänster inom elektronisk kommunikation, såsom rätten få information och möjligheten att förelägga vite, kan riktas även på annan domännamnsverksamhet än på de registrarer som för närvarande föreskrivs i 21 kap., om kompletterande skyldigheter föreskrivs i den aktuella lagen. Den särskilda bestämmelsen om rätten till information i fråga om handlingar som gäller domännamn i 312 § 2 mom. i lagen om tjänster inom elektronisk kommunikation är även tillämplig på andra ärenden som gäller domännamn än de som för närvarande föreskrivits i 21 kap.

# 4 Förslagen och deras konsekvenser

## 4.1 De viktigaste förslagen

Med propositionen föreslås att en ny lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering utfärdas.

Det föreslås att lagen innehåller bestämmelser om marknadskontrollen enligt cyberresiliensförordningen, anmälan av organ för bedömning av överensstämmelse för bedömningsuppgifter enligt cyberresiliensförordningen samt om de administrativa påföljder som anknyter till överträdelse av cyberresiliensförordningen. Dessutom innehåller lagen bestämmelser om inrättande av en regulatorisk sandlåda för cyberresiliens, användning av ej färdigställda produkter i vissa förhållanden och om beaktande av kraven i cyberresiliensförordningen i offentliga upphandlingar.

Transport- och kommunikationsverket ansvarar på centraliserat sätt för uppgifterna för marknadskontrollmyndigheten enligt cyberresiliensförordningen. Dessutom fungerar den behöriga tillsynsmyndigheten enligt lagen om tillsyn över vissa system för artificiell intelligens som marknadskontrollmyndighet för AI-system med hög risk. På marknadskontrollen enligt cyberresiliensförordningen tillämpas lagen om marknadskontroll av vissa produkter samt marknadskontrollförordningen.

Transport- och kommunikationsverket ansvarar även för uppgifterna för den anmälande myndigheten enligt cyberresiliensförordningen. Ett organ för bedömning av överensstämmelse som är etablerat i Finland ansöker enligt förslaget om att bli ett anmält organ enligt cyberresiliensförordningen hos Transport- och kommunikationsverket. Ett ackrediteringsintyg av ackrediteringstjänsten FINAS om att ett bedömningsorgan uppfyller kraven i cyberresiliensförordningen ska i princip fogas till ansökan.

Genom propositionen utfärdas även bestämmelser som kompletterar EU:s cybersäkerhetsakt om uppgifterna för den nationella myndigheten för cybersäkerhetscertifiering och dess befogenheter. För närvarande har uppgiften tilldelats Transport- och kommunikationsverket med stöd av lagen om tjänster inom elektronisk kommunikation. Det föreslås att Transport- och kommunikationsverket fortsätter att sköta uppgiften. De nationella bestämmelserna om uppgiften och befogenheterna ingår dock i den nya lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering. Genom förslaget kompletteras och preciseras befogenheterna för myndighetsuppgifterna i anknytning till cybersäkerhetscertifiering, anmälan av organ för bedömning av överensstämmelse och påförande av påföljdsavgifter för missbruk i anknytning till cybersäkerhetscertifieringen.

Det föreslås att nya 21 kap. fogas till lagen om tjänster inom elektronisk kommunikation. Det innehåller bestämmelser om insamling och utlämnande av registreringsuppgifter om domännamn i fråga om andra domännamn än de som slutar med den nationella toppdomänen fi och toppdomänen för landskap ax. Kapitlet innehåller även bestämmelser om en registrars anmälningsskyldighet till Transport- och kommunikationsverket. Genom förslagen kompletteras genomförandet av EU:s cybersäkerhetsakt i fråga om registreringsuppgifterna om domännamn.

### 4.2 De huvudsakliga konsekvenserna

#### 4.2.1 Konsekvenser för företagen

*Cyberresiliensförordningen och den nationella reglering som kompletterar den*

Cyberresiliensförordningens tillämpningsområde omfattar en avsevärd grupp olika enheter och programvaror. Författningen tillämpas horisontellt på alla enheter och programvaror som innehåller i förordningen avsedda ”digitala element”, det vill säga sådana som kan kopplas antingen direkt eller indirekt till nätet eller en annan enhet. I princip omfattas alla enheter och programvaror som kan kopplas direkt eller indirekt till Internet av tillämpningsområdet. Vissa produkter (fordon, luftfartyg och viss medicinsk utrustning) har avgränsats utanför tillämpningsområdet, eftersom deras produktspecifika reglering på ett detaljerat sätt täcker även kraven på cybersäkerhet.

Det antal produkter som omfattas av tillämpningsområdet är avsevärt stort. Det föreslås att enheter och programvaror som kan koppas till nätet eller en annan enhet och som används såväl av konsumenter som företag omfattas av tillämpningsområdet. De krav som ställts på produkterna berör direkt eller indirekt så gott som alla nuvarande produkter med digitala

element som omfattas av marknadskontrollmyndigheternas kontroll. Kraven berör även en avsevärd mängd produkter som för närvarande inte är föremål för marknadskontroll eller säkerhetskrav som baserar sig på produktregleringen. Enligt konsekvensbedömningen av Europeiska kommissionen har marknadsvärdet för de produkter som omfattas av tillämpningsområdet för cyberresiliensförordningen grovt uppskattat varit 1 485 miljarder euro på EU-nivå (år 2019).[2]

Cyberresiliensförordningen och den nationella reglering som kompletterar den har konsekvenser för ekonomiska aktörer som tillverkar, importerar och distribuerar produkter som omfattas av cyberresiliensförordningens tillämpningsområde. Propositionen har med andra ord konsekvenser för tillverkare, importörer och företag som säljer produkter med digitala element. Största delen av konsekvenserna orsakas direkt av förordningen utan att vara föremål för något nationellt handlingsutrymme.

De konsekvenser som hänför sig till företagen utgörs av att de väsentliga cybersäkerhetskrav som ingår i cyberresiliensförordningen ska uppfyllas. Egenskaperna hos produkter med digitala element ska uppfylla de krav som ställs i del I i bilaga I till förordningen och de processer som tillverkaren infört och tillverkarens behandling av sårbarheter ska uppfylla de krav som fastställts i del II i bilaga I till förordningen, vilka i enlighet med artikel 27 i förordningen granskas i förhållande till harmoniserade standarder eller kommissionens genomförandeakter. Tillverkaren ska dessutom bedöma och visa överensstämmelsen i enlighet med cyberresiliensförordningen. Tillverkarna orsakas dessutom kostnader av behandlingen av sårbarheter under stödtiden för produkten och av de sårbarhets- och incidentsanmälningar som cyberresiliensförordningen förutsätter. Marknadskontrollen i anknytning till cyberresiliensförordningen orsakar administrativa kostnader för de ekonomiska aktörerna.

Cyberresiliensförordningens tillämpningsområde omfattar produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät. De produkter med digitala element som omfattas av tillämpningsområdet är till exempel enheter med en direkt eller indirekt nätanslutning (IoT-enheter, smarta enheter, industriella komponenter), anknutna programvaror, andra programvaruprodukter och spel. Tillämpningsområdet omfattar till exempel datorer, telefoner, fjärravlästa sensorer, bärbara smarta enheter, nätanslutna IoT-enheter och nätansluten hemelektronik samt nätanslutna system

[2] Commission Staff Working Document Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, SWD/2022/282 final. Då storleken på Europeiska unionens inre marknad uppgått till 13 900 miljarder euro år 2019, kan kraven i cyberresiliensförordningen således utifrån kommissionens konsekvensbedömning beröra hela 10,6 procent av den inre marknaden. År 2021 var värdet på EU:s inre marknad 6 786 miljarder euro, varför det är möjligt att göra en grov beräkning om att 21,8 procent av den inre marknadens omsättning omfattas av ett digitalt element. När det gäller den finländska marknaden har det uppskattats att värdet på IoT-marknaden är 1 903 miljoner dollar (omkring 1 742 miljoner euro) år 2024 och att marknaden växer med 9,3 % årligen. De ovan beskrivna värdena är förknippade med avsevärda osäkerhetsfaktorer, men de ger en fingervisning om tillämpningsområdets omfattning. Det kan bedömas att IoT-enheter i regel omfattas av cyberresiliensförordningens tillämpningsområde, men förordningen täcker även många andra produkter, såsom sedvanliga terminalutrustningar och programvaror.

för industriell automation. Tillämpningsområdet omfattar även till exempel driftsystem, dator- och mobilprogram och spel. Med andra ord omfattar cyberresiliensförordningens tillämpningsområde således en avsevärd grupp olika enheter och programvaror. I princip omfattas alla enheter och programvaror som kan kopplas direkt eller indirekt till Internet av tillämpningsområdet. Vissa produkter (fordon, luftfartyg och viss medicinsk utrustning) har avgränsats utanför tillämpningsområdet, eftersom deras produktspecifika reglering på ett detaljerat sätt täcker även kraven på cybersäkerhet. Ingen samlad statistisk information är tillgänglig över antalet produkter som omfattas av tillämpningsområdet eller storleken av den finländska marknaden. Det är väldigt besvärligt att uppskatta antalet produkter på marknaden, eftersom de statistiska uppgifterna om olika produktkategorier inte specificerar om produkterna innehåller ett digitalt element. Det är dock väldigt vanligt att produkter som omfattas av tillämpningsområdet används. Antalet enheter och programvaror som omfattas av tillämpningsområdet uppskattas vara avsevärt såväl i de privata hushållen som i företagen.

På det sätt som konstaterats ovan är antalet produkter som omfattas av tillämpningsområdet avsevärt stort. Det föreslås att enheter och programvaror som kan koppas till nätet eller en annan enhet och som används såväl av konsumenter som företag omfattas av tillämpningsområdet. De krav som ställts på produkterna berör direkt eller indirekt så gott som alla nuvarande produkter med digitala element som omfattas av marknadskontrollmyndigheternas kontroll. Kraven berör även en avsevärd mängd produkter som för närvarande inte är föremål för marknadskontroll eller säkerhetskrav som baserar sig på produktregleringen.

Enligt Europeiska kommissionens konsekvensbedömning har den globala omsättningen för produkter med digitala element varit 550–1 485 miljarder euro år 2019 beroende på de produktklassificeringar som inkluderas i bedömningen.[3] Enligt Europeiska kommissionens konsekvensbedömning kan kostnaderna för att utveckla produkter med digitala element utifrån de krav på säkerhetsnivån som cyberresiliensförordningen förutsätter ha en inverkan som höjer produktutvecklingskostnaderna med i snitt 30,5 % (variationsintervall på 19–42 %) .[4] Den konsekvensbedömning som offentliggjorts av Europeiska kommissionen den 15 september 2022 är tillgänglig på kommissionens webbplats: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

Enligt Statistikcentralens statistik Befolkningens användning av informations- och kommunikationsteknik har 94 % av finländarna år 2024 använt Internet under de tre senaste månaderna och 83 % använder Internet flera gånger per dag. Under de senaste tre månaderna har Internet använts av 100 % i åldersgruppen 16–54-åringar. Således har var och en i denna åldersgrupp använt en eller flera produkter med digitala element som hör till cyberresiliensförordningens tillämpningsområde. På en nivå som omspänner hela befolkningen används produkter av 94 % av befolkningen. Enligt den senaste statistiken har en smarttelefon med pekskärm varit i användning hos 90 % av befolkningen. Enligt statistiken har 14 % av finländarna under de tre senaste månaderna använt ett nätanslutet uppvärmnings-, belysnings- eller annat motsvarande system i hemmet, medan 13 % av finländarna under de tre senaste månaderna har använt ett nätanslutet larmsystem i hemmet, till exempel lås, brandvarnare eller säkerhetskameror. I fråga om användning av nätanslutna vitvaror eller enheter är den motsvarande siffran för de tre senaste månaderna 11 %. Under de tre senaste månaderna har 13 % av finländarna använt en virtuell assistent via en smart högtalare, dator eller telefonapp.

[3] Commission staff working document. Impact assessment report. SWD(2022) 282 final. Part 2/3, s. 48.
[4] Commission staff working document. Impact assessment report. SWD(2022) 282 final. Part 2/3, s. 55–56.

Under de tre senaste åren har 55 % av finländarna använt Internet via en smart-tv eller en digibox som är direkt ansluten till Internet. Dessutom har 40 % av finländarna spelat eller laddat ner spel; i åldersgruppen med 16–44-åringar fler än varannan och i åldersgruppen med 44–89-åringar färre än varannan.[5]

Utöver konsumentanvändningen är användning av produkter med digitala element vanlig även i företagen. Utbredningen av användningen illustreras av att en internetuppkoppling på över 100 Mbit/s användes av 80 % av företagen år 2024. Utifrån detta är det möjligt att dra en slutsats om att företagen använder åtminstone en eller flera produkter med ett digitalt element. Smart teknik har använts av 24 % av alla företag.[6]

Ingen samlad statistisk information är tillgänglig om tillverkarna, importörerna eller distributörerna av produkter med digitala element. Företagsverksamheten i anknytning till produkterna är fördelad över olika näringsgrenar. I Finland har sammanlagt 14 095 företag verkat inom näringsgrenen IT-tjänster år 2023 och den sammanräknade omsättningen för företagen i näringsgrenen har varit omkring 12,8 miljarder euro och personalvolymen har varit omkring 65 000 årsverken.[7]

Så som konstateras ovan har de centrala konsekvenserna för företagen sitt ursprung direkt i bestämmelserna i förordningen. Utöver produktutvecklingen och behandlingen av sårbarheter orsakas administrativa kostnader för företagen. Företagen ska framöver utarbeta och administrera teknisk dokumentation som visar att en produkt eller en programvara uppfyller cybersäkerhetskraven i förordningen. Denna dokumentation är en central del av CE-märkningsprocessen och villkoren för att få tillträde till marknaden. Den tekniska dokumentationen ska innehålla en produktbeskrivning, en bedömning av cybersäkerhetsriskerna och en beskrivning av säkerhetsåtgärderna och hanteringen av sårbarhetsrisker. Dessutom ska företagen göra en bedömning av deras produkters överensstämmelse antingen som en självbedömning eller som en bedömning som görs av en tredje part, beroende på produktens riskklass. För produkter med hög risk krävs en bedömning av tre parter, vilket för med sig extra kostnader bland annat i fråga om beredningen av auditering, de avgifter som organen för bedömning av överensstämmelse tar ut och eventuella kontroller som utförs på nytt.

Överensstämmelse med cyberresiliensförordningen visas genom att fästa en CE-märkning på enheten. Framöver kan produkter med digitala element inte komma in på EU:s inre marknad utan att en tillräcklig cybersäkerhetsnivå visas i enlighet med cyberresiliensförordningen. Förordningen eller den nationella reglering som kompletterar den identifieras inte ha någon konkurrenssnedvridande konsekvens, eftersom kraven ställs på alla företag, oberoende av storlek och näringsgren. Eftersom kraven i cyberresiliensförordningen berör alla företag

[5] Källa: Statistikcentralen. Statstiken Befolkningens användning av informations- och kommunikationsteknik. Uppgifterna gäller år 2024. Statistikens population består av hela befolkningen i åldern 16–89 år som bor stadigvarande i Finland och privata hushåll med åtminstone en person i åldern 16–89 år. Uppgifterna har hämtats den 1 april 2025.

[6] Källa: Statistikcentralen. Statistiken Användning av datateknik i företag. Uppgifterna gäller år 2024. Statistikens population täcker företag som sysselsätter minst tio personer i de näringsgrenar som beskrivs i de grundläggande uppgifterna om statistiken. Uppgifterna har hämtats den 1 april 2025.

[7] Källa: Statistikcentralen. Struktur- och bokslutsstatistik över företag. Uppgifterna gäller år 2023. Statistikens population täcker alla företag som bedriver affärsverksamhet i Finland. Uppgifterna har hämtats den 1 april 2025.

jämbördigt, harmoniserar regleringen marknaden. Kostnader uppkommer inte för sådana produkttillverkare och importörer som har enheter vars cybersäkerhet redan har ombesörjts på tillräcklig nivå. Däremot är det möjligt att ett stort antal aktörer måste investera och utföra produktutveckling för att förbättra cybersäkerheten. Å andra sidan är de kostnader som orsakas av cyberresiliensförordningen i proportion till omsättningen högre för mikroföretag, små och medelstora företag än för stora företag, varför det i genomförandet är nödvändigt att fokusera i synnerhet på rådgivning och myndighetsstöd som riktas på dessa företag.

Även om det inte är möjligt att genom den nationella lagstiftningen påverka nivån på kraven på grund av cyberresiliensförordningen eller de kostnader som de orsakar, möjliggörs genom lagförslag 1 i regeringens proposition dock att en regulatorisk sandlåda för cyberresiliens enligt cyberresiliensförordningen inrättas på beslut av marknadskontrollmyndigheten. Utnyttjande av en regulatorisk sandlåda för cyberresiliens i produktutvecklingen kan ha en sänkande inverkan på produktutvecklingskostnaderna i synnerhet för små och medelstora företag. Dessutom är det möjligt att i samband med en regulatorisk sandlåda för cyberresiliens erbjuda rådgivning och stöd kring kraven i regleringen för små och medelstora företag.

Med stöd av regeringens proposition är det möjligt att på det sätt som cyberresiliensförordningen förutsätter påföra en administrativ påföljdsavgift för ett företag, om det underlåter att fullgöra kraven i cyberresiliensförordningen. Det är möjligt att en administrativ påföljdsavgift påförs för ett företag, vilken är högst 15 miljoner euro eller 2,5 % av företagets globala årliga omsättning. Det är även möjligt att förordna att en produkt ska återkallas från marknaden till exempel då en allvarlig sårbarhet konstateras hos produkten och tillverkaren inte vidtar korrigerande åtgärder. Marknadskontrollen kan orsaka administrativa kostnader för ett företag.

Cyberresiliensförordningen har en konsekvens för marknaden i fråga om tillträdet till marknaden för sådana produkter som inte uppfyller kraven. Det är möjligt att myndigheterna hindrar att en produkt släpps ut på marknaden eller att försäljningen fortsätter, om överensstämmelse inte har visats. I fråga om de produkter som inte redan uppfyller kraven i cyberresiliensförordningen är det möjligt att företagen måste utföra produktutveckling. För att det ska vara möjligt att inleda företagsverksamhet och komma in på marknaden kan det framöver krävas initiala investeringar för sådana företag som utvecklar, tillverkar eller importerar nätanslutna produkter och programvaror till EU-marknaden. Nya företag som utvecklar digitala produkter ska beakta kraven i cyberresiliensförordningen redan i det initiala skedet av produktutvecklingen. Detta kan öka de initiala investeringarna eftersom det är möjligt att bredare cybersäkerhetskompetens, dokumentation och eventuellt utvärderingar av tredje parter kommer att behövas. I synnerhet för små och medelstora företag kan detta skapa ett större behov av extern expertis.

I och med kraven i cyberresiliensförordningen ska cybersäkerheten beaktas i produktutvecklingen, varvid tryggare enheter släpps ut på marknaden. Enligt bedömning är konsekvensen av detta att dataskyddsincidenterna och kostnaderna på grund av dem samt skador på anseendet minskar på lång sikt.

*Registrarer och de som förvaltar ett toppdomänregister*

Nya föreslagna 21 a kap. i lagen om tjänster inom elektronisk kommunikation har konsekvenser för dem som förvaltar ett toppdomänregister och registrarer vilka är etablerade i Finland och även för andra sådana som omfattas av Finlands jurisdiktion. Konsekvenserna orsakas i synnerhet av behandlingen av registreringsuppgifter om domännamn och svarandet på begäranden om att få tillgång till sådana. Dessutom orsakas kostnader av skyldigheten att

anmäla uppgifter till Transport- och kommunikationsverket för registrarerna. Med de föreslagna ändringarna förbättras tillträdet till registreringsuppgifterna om domännamn, vilket kan ha positiva konsekvenser för samhället i situationer där myndigheternas och övriga instansers möjligheter att ingripa i lagstridig verksamhet förbättras. Det råder osäkerhet kring prognosen över de aktörer som kommer att omfattas av tillämpningsområdet för kapitlet, men det kan uppskattas vara sammanlagt några hundra, inbegripet såväl egentliga registrarer som de aktörer som verkar för deras räkning, såsom återförsäljare som tillhandahåller registreringstjänster för domännamn. Det uppskattas finnas ett väldigt litet antal sådana förvaltare av ett toppdomänregister som är etablerade i Finland och inte använder ett domännamn endast för egna ändamål.

4.2.2 Konsekvenser för myndigheterna

4.2.2.1 Transport- och kommunikationsverket

*Kostnader*

Propositionen har direkta och avsevärda konsekvenser för Transport- och kommunikationsverket i dess olika verksamheter. Propositionen ökar antalet uppgifter för Transport- och kommunikationsverket. I fråga om genomförandet av cyberresiliensförordningen och uppgifterna i anknytning till cybersäkerhetscertifieringen uppskattas uppgången i volymen på Transport- och kommunikationsverkets uppgifter vara sammanlagt tio årsverken. Därtill uppskattas uppgiftsmängden för Transport- och kommunikationsverket i anknytning till domännamn öka med 0,5 årsverken.

Dessutom orsakar propositionen kostnader relaterade till cyberresiliensförordningen på grund av utvecklingen av informationssystemen och tjänsterna och laboratoriegranskningarna i anknytning till marknadskontrollen enligt följande:

| Engångskostnader | | Kostnader av permanent karaktär | |
|---|---|---|---|
| Förklaring | Kostnad | Förklaring | Kostnad |
| Informationssystem i anknytning till rapporteringen av sårbarheter | 150 000 euro | Laboratoriegranskningar i anknytning till marknadskontrollen | 150 000 euro årligen |
| Informationssystem i anknytning till marknadskontrollen | 150 000 euro | Administrering och utveckling av informationssystem och tjänster | 150 000 euro årligen |
| Ackreditering som testlaboratorium | 200 000 euro | Omfattningen av det uppskattade tillägget i uppgiftsmängden | 10 årsverken |

Uppgifterna i anknytning till domännamn uppskattas dessutom orsaka en kostnad av engångsnatur på 150 000 euro på grund av utvecklingen av informationssystemen.

Propositionen orsakar således, utöver det utökade antalet uppgifter som enligt uppskattning är av en volym på 10,5 årsverken, en engångskostnad på sammanlagt 650 000 euro, som realiseras under åren 2026–2027, och en kostnad av permanent karaktär på 200 000 euro, som realiseras till fullt belopp årligen från och med år 2028.

Uppgången i uppgiftsmängden, engångskostnaderna och de löpande kostnaderna på grund av propositionen täcks ur Transport- och kommunikationsverkets nuvarande ramanslag. Således har propositionen inte konsekvenser för statsbudgeten.

Enligt Transport- och kommunikationsverkets bedömning är det mycket utmanande att genomföra de nya uppgifterna inom ramen för de nuvarande anslagen. Det är mycket utmanande att sköta uppgifterna på miniminivå, även med beaktande av möjligheten att fullt ut dra nytta av omorganisering av de nuvarande uppgifterna.

*Nya uppgifter*

Enligt propositionen ansvarar Transport- och kommunikationsverket för marknadskontrollen enligt cyberresiliensförordningen. Uppgiften är ny för verket.

Transport- och kommunikationsverket har som en ny uppgift till ansvar att anmäla och övervaka organ för bedömning av överensstämmelse som sköter uppgifterna för ett anmält organ enligt cyberresiliensförordningen. Dessutom ökar ikraftträdandet av cyberresiliensförordningen uppgiftsmängden vid CSIRT-enheten vid Transport- och kommunikationsverkets Cybersäkerhetscenter på grund av behandlingen och samordningen av incidents- och sårbarhetsanmälningar. Transport- och kommunikationsverket fortsätter med uppgiften som nationell myndighet för cybersäkerhetscertifiering och i anknytning till detta förutspås volymen på uppgifterna öka i och med att cyberresiliensförordningen träder i kraft.

Marknadskontroll är en central del för att säkerställa fungerande marknader. Genom den säkerställs att produkterna överensstämmer med kraven. I uppgiften riktar Transport- och kommunikationsverket marknadskontrollen av produkter med digitala element på samma sätt som i övrigt på den nuvarande verksamheten utifrån produktakterna. Utöver kontrolluppgifterna ger marknadskontrollmyndigheten handledning och rådgivning till de ekonomiska aktörerna i frågor som gäller tillämpningen. Utifrån erfarenheterna från Cybersäkerhetsmärket som har genomförts under tidigare år och pilotprojektet kring bedömning av informationssäkerheten för produkter enligt direktivet om radioutrustning åren 2023–2024 finns det problem i överensstämmelsen med kraven på informationssäkerhet bland alla typer av produkter som togs för bedömning. Det finns brister och fel såväl i genomförandet av det tekniska dataskyddet för produkterna som till exempel i användningsvillkoren. Tillsynsuppgifter utförs i tätt samarbete med övriga behöriga myndigheter. Kontrollen hänför sig till en exceptionellt stor grupp av produkter, vars kontroll kräver särskilt tekniskt kunnande. Uppgifterna enligt cyberresiliensförordningen kräver extra resurser för krypterings- och produktsäkerhetskontroller. Särskild expertis och fördjupat teknisk förståelse behövs då man tolkar produkternas tekniska lösningar och bedömer de anmälda organens förmåga. Marknadskontrollmyndigheten orsakas kostnader även av myndighetshandledningen och -rådgivningen. På grund av det breda horisontella tillämpningsområdet förutspås det att handlednings- och rådgivningsbehovet är stort i synnerhet under cyberresiliensförordningens övergångstid och i början av tillämpningen.

Uppgifterna i anknytning till sårbarhetssamordningen vid Cybersäkerhetscentrets CSIRT-enhet kommer att öka avsevärt i och med tillämpningen av cyberresiliensförordningen. Enligt cyberresiliensförordningen har en tillverkare en skyldighet att anmäla aktivt utnyttjade

sårbarheter och allvarliga incidenter till myndigheterna. Dessutom kan tillverkarna frivilligt anmäla sårbarheter som de upptäckt till CSIRT-enheten. De obligatoriska sårbarhetsanmälningarna omfattas av snäva tidsfrister, varför CSIRT-enheten ska förbereda sig på snabb handläggning av anmälningar. I nuläget inkommer i snitt omkring 100–400 anmälningar på årsnivå till sårbarhetssamordningen. I och med cyberresiliensförordningen kommer skyldigheten att anmäla aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar en produkts informationssäkerhet att öka mängden avsevärt. Det finns inte någon exakt uppskattning av hur många sårbarheter som inte rapporteras. Experterna har bedömt att omkring 50 till 90 % av sårbarheterna inte anmäls i nuläget. Därtill anmäls sårbarheter inte nödvändigtvis till CSIRT-enheterna, utan direkt till andra instanser. Enligt en försiktig uppskattning inkommer över 50 sårbarhetsanmälningar per vecka till sårbarhetssamordningen på grund av förslaget. Dessa anmälningar inkommer även för behandling till marknadskontrollmyndigheterna.

Cyberresiliensförordningen innehåller även en skyldighet att tillhandahålla stöd till mindre organisationer för att utreda sårbarheter och incidenter. Med CSIRT-enhetens nuvarande resurser är det möjligt att undersöka endast de allvarligaste fallen, varvid det inte finns tillräckligt med resurser för att undersöka fall med mindre genomslag eller så är det alternativt nödvändigt att låta bli att undersöka andra allvarliga fall. Längden på undersökningen varierar stort och i och med kraven i cyberresiliensförordningen är det möjligt att uppskattningsvis 1–3 fall inkommer för undersökning utöver de nuvarande arbetsuppgifterna. Enligt förslaget anmäls sårbarheter till Enisas sårbarhetsdatabas. Behandlingen av uppgifterna om sårbarheter kommer att kräva ett tätt samarbete mellan myndigheterna såväl nationellt som internationellt. Med avvikelse från nuläget ökar i synnerhet behovet av internationell koordinering.

Transport- och kommunikationsverket ansvarar även för uppgiften som anmälande myndighet. I denna uppgift godkänner myndigheten organ och den ansvarar för att övervaka dessa. Uppgiften omfattar utöver godkännandeförfarandet anmälningsskyldigheter gentemot kommissionen. Cyberresiliensförordningen omfattar påvisande av överensstämmelse som avviker från övriga produktsäkerhetskrav. Av en del av produkterna krävs särskilt påvisande av överensstämmelse, såsom ett typgodkännandeförfarande som utförs av ett anmält organ. Cyberresiliensförordningens breda tillämpningsområde medför egna särdrag även för den myndighet som ansvarar för att godkänna och övervaka anmälda organ. Myndigheten ska säkerställa att ett anmält organ har förmåga att göra bedömningen i förhållande till varje harmoniserad standard som den utfärdat. Det stora antalet standarder orsakar en börda i fråga om introduktionen och särskilda behov i anknytning till den tekniska prestandan för den behöriga myndigheten. Genom tillräcklig resursallokering till den myndighet som ansvarar för att godkänna anmälda organ säkerställs att processen är smidig och att det finns ett tillräckligt antal anmälda organ och därtill förebyggs flaskhalsar i inträdet på marknaden.

Transport- och kommunikationsverket ansvarar även framöver för uppgiften som nationell myndighet för cybersäkerhetscertifieringen enligt cyberresiliensförordningen. Transport- och kommunikationsverket sköter redan för närvarande uppgiften med stöd av lagen om tjänster inom elektronisk kommunikation. Propositionen bedöms i anknytning till denna uppgift således inte ha någon direkt konsekvens som ökar Transport- och kommunikationsverkets arbetsmängd. Det förutspås dock att arbetsmängden i anknytning till uppgifterna som nationell myndighet för cybersäkerhetscertifiering ökar efter att tillämpningen av cyberresiliensförordningen börjat, om antalet cybersäkerhetscertifieringar och efterfrågan ökar på förutspått sätt. Efterfrågan på cybersäkerhetscertifikat och ansökningarna av organen för bedömning av överensstämmelse för att sköta cybersäkerhetscertifieringsuppgifter beror till exempel på hur utvecklingsarbetet för certifieringsordningarna framskrider och möjligheten att utnyttja certifikat för att visa en nivå på överensstämmelse som är förenlig med cyberresiliensförordningen eller andra krav på överensstämmelse. I fall europeiska ordningar för cybersäkerhetscertifiering utvecklas i

framtiden och de utnyttjas för att visa överensstämmelse med kraven i cyberresiliensförordningen, förutspås Transport- och kommunikationsverkets arbetsmängd öka väsentligt i anknytning till denna verksamhet. Propositionen förbättrar dock Transport- och kommunikationsverkets möjligheter att utföra en slagkraftig övervakning. Dessutom främjar förslaget att myndigheternas uppgifter sköts på en maximalt hög nivå genom att möjliggöra att utfärdande av cybersäkerhetscertifikat delegeras till organ för bedömning av överensstämmelse. Till denna del förtydligar och förbättrar förslaget myndighetens verksamhetsförutsättningar i uppgiften.

Nya föreslagna 21 a kap. i lagen om tjänster inom elektronisk kommunikation har konsekvenser för Transport- och kommunikationsverkets uppgifter. Verket ska föra en förteckning över aktörerna i fråga om de nya registrarer som omfattas av kapitlets tillämpningsområde och vid behov övervaka att de nya skyldigheterna fullgörs enligt deras befogenheter. Även utvidgningen av tillämpningsområdet för 21 kap. till aktörer som verkar för registrarers räkning, såsom återförsäljare, ökar i liten mån verkets uppgifter, även om information om återförsäljare ska ha lämnats till verket redan med stöd av verkets nya domännamnsföreskrift som trädde i kraft år 2025.

#### 4.2.2.2 Övriga konsekvenser för myndigheterna

Propositionen har konsekvenser för de myndigheter som övervakar AI-system med hög risk. Myndigheternas arbetsmängd ökar, eftersom de fungerar som marknadskontrollmyndigheter för AI-system med hög risk i fråga om cyberresiliensförordningen. På grund av detta ska de myndigheter som övervakar AI-system med hög risk inhämta och utveckla förmåga att uppfylla kraven i cyberresiliensförordningen och sköta övervakningen i fråga om AI-system med hög risk. Konsekvenserna för marknadskontrollmyndigheternas uppgifter realiseras fullt ut då cyberresiliensförordningen blir tillämplig i sin helhet den 11 december 2027.

Det är besvärligt att bedöma myndighetskonsekvenserna på grund av det breda horisontella tillämpningsområdet för cyberresiliensförordningen och därtill på grund av att det är väldigt svårt att göra en sektorsvis bedömning av det framtida antalet produkter med digitala element vilka anses utgöra AI-system med hög risk. Detta påverkar vilken andel av marknadskontrolluppgifterna som kommer att höra till de myndigheter som övervakar AI-system. Det finns skäl att följa resursbehoven och se över dem på nytt efter att kontrolluppgifterna börjat.

Behoven av resurser för marknadskontrollen av förordningen om artificiell intelligens har bedömts i regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s förordning om artificiell intelligens (RP 46/2025 rd, s. 106–110). Dataombudsmannens byrå har bedömt att marknadskontrollen av AI-system förutsätter en resurs på 3,5 årsverken. Den mer detaljerade regleringen kring cybersäkerhet i cyberresiliensförordningen kan bedömas öka denna uppskattade arbetsmängd i viss mån. Energimyndigheten har å sin sida uppskattat att skötseln av uppgifterna i anknytning till AI-system med hög risk enligt cyberresiliensförordningen förutsätter en tilläggsresurs på åtminstone ett årsverke utöver det behov av tilläggsresurser för Energimyndigheten vilket uppskattats vid den nationella beredningen av förordningen om artificiell intelligens. Finansinspektionen har å sin sida ansett att 0,5 årsverken till denna del är en riktgivande uppskattning av resurskonsekvenserna. Enligt Tullens uppskattning är behovet av tilläggsresurser för marknadskontrollen av cybersäkerheten inklusive AI-egenskaper som helhet tre årsverken (jämför med RP 46/2025 rd, s. 111). Tullen fungerar vid sidan om Säkerhets- och kemikalieverket Tukes som marknadskontrollmyndighet, eftersom det handlar om ett AI-system med hög risk, på vilket leksaksdirektivet tillämpas. Dessutom verkar Tullen som myndighet med ansvar för kontrollerna vid den yttre gränsen.

Säkerhets- och kemikalieverket Tukes uppskattar att behovet av extra resurser på grund av övervakningen enligt cyberresiliensförordningen är 1–2 årsverken, och därtill förutsätter övervakningen en post av engångsnatur på 50 000 euro för vissa åtgärder, såsom uppdateringen av informationssystemen. Den utökade uppgiftsmängden hos Tillstånds- och tillsynsverket för social- och hälsovården (Tillstånds- och tillsynsverket från och med den 1 januari 2026) kan bedömas kräva ett behov av resurser på tre årsverken, vilket ligger i linje med föregående jämförbara uppskattning, som gjordes för verket i fråga om förordningen om artificiell intelligens. Regeringen föreslår inte något anslag för att genomföra cyberresiliensförordningen i statsbudgeten för 2026. Därför finansieras genomförandet av förordningen med myndigheternas befintliga resurser genom att allokera dem på nytt.

Propositionen har konsekvenser för Säkerhets- och kemikalieverkets FINAS-ackrediteringsenhet. Det antal ackrediteringar som det utför ökar, om organen för bedömning av överensstämmelse ansöker om ackreditering för att anmäla sig som anmälda organ i Finland i enlighet med cyberresiliensförordningen. Dessutom har propositionen och början av tillämpningen av cyberresiliensförordningen konsekvenser som ökar arbetsmängden för verksamheten vid det samordningskontor och den samarbetsgrupp för marknadskontroll som verkar i anslutning till Säkerhets- och kemikalieverket.

Propositionen orsakar därtill i viss mån ett behov av extra personal för Rättsregistercentralen, som ansvarar för att verkställa administrativa påföljdsavgifter. Omfattningen av konsekvenserna beror på antalet administrativa påföljdsavgifter som påförs med stöd av lagen och antalet viten som döms att betalas. Avsikten är att anmälningar om verkställighet av administrativa påföljder görs via en eventuell myndighetsportal då förslaget har trätt i kraft. Den ökning av arbetsmängden som denna proposition medför måste täckas med befintliga anslag enligt rambesluten för statsfinanserna och enligt statsbudgeten. Rättsregistercentralens behov av anslag för att verkställa alla påföljdsavgifter bedöms i samband med ramförhandlings- och budgetberedningen.

Det uppskattas att administrativa påföljdsavgifter påförs regelbundet från och med år 2028. Beloppet av påföljdsavgifterna är lägre under de första åren av tillämpningen och det ökar årligen fram till dess att beloppet stabiliseras efter omkring 2–3 års tillämpning. Beloppet av de administrativa påföljdsavgifterna påverkas av resursallokeringen för övervakningen enligt cyberresiliensförordningen och aktiviteten och å andra sidan av omfattningen av den ekonomiska verksamhet som omfattas av tillämpningsområdet i Finland. I början av tillämpningen av regleringen bedöms antalet administrativa påföljdsavgifter etablera sig på ett intervall mellan 5 och 50 fall per år. Antalet viten som döms att betalas bedöms underskrida detta med bred marginal.

### 4.2.3 Övriga konsekvenser

Genom cyberresiliensförordningen förbättras nivån på dataskyddet för produkter, enheter och programvaror som kan anslutas till nätet eller en annan enhet. Cyberresiliensförordningen ställer minimikrav på egenskaper som påverkar produkternas cybersäkerhet, sårbarheter som påverkar produkternas säkerhet, hanteringen av incidenter samt anmälningen av en produkt efter att den släppts ut på marknaden. Propositionen bedöms ha positiva konsekvenser för nivån på produkternas dataskydd. Eftersom propositionens tillämpningsområde är brett, har propositionen indirekt omfattande positiva konsekvenser för nivån på dataskyddet i Finland för enheter och programvaror med digitala element vilka används i samhället.

Konsekvensbedömningen av cybersäkerhetsakten ingår i regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av

vissa lagar som har samband med den (RP 98/2020 rd, s. 151–152). I fråga om cybersäkerhetscertifieringen bedöms propositionen inte ha andra ekonomiska konsekvenser eller konsekvenser för informationssamhället vilka avviker från den tidigare bedömningen av myndighetskonsekvenserna. Tydliggörandet av myndighetens befogenheter bidrar till att förbättra företagens förutsättningar att dra nytta av de europeiska ordningarna för cybersäkerhetscertifiering och myndigheternas möjligheter att uppfylla kraven i certifieringsordningarna, vilket har indirekta positiva konsekvenser för informationssamhället.

# 5 Alternativa handlingsvägar

## 5.1 Handlingsalternativen och deras konsekvenser

### 5.1.1 Marknadskontroll

I beredningen av propositionen bedömdes alternativ där myndighetsuppgifterna i anknytning till marknadskontroll samlas till en myndighet eller delvis fördelas över flera myndigheter, som för närvarande utför marknadskontroll utifrån de andra produktakterna. I beredningen har man i fråga om centraliseringen av myndighetsuppgifterna i anknytning till marknadskontroll bedömt ett alternativ där uppgifterna tilldelas Säkerhets- och kemikalieverket Tukes och Transport- och kommunikationsverket, i praktiken till dess Cybersäkerhetscenter.

Den marknadskontroll som cyberresiliensförordningen förutsätter handlar om en helt ny myndighetsuppgift, vars tillämpningsområde är brett och horisontellt. Den nya horisontella kontrollen som gäller en EU-förordning är inte direkt tillämplig på de nuvarande uppgifterna för de nationella myndigheterna eller på de befintliga administrativa strukturerna. På grund av den utmanande situationen i den offentliga ekonomin är myndigheternas förmåga att ta emot nya uppgifter nedsatt, och i bedömningen av alternativen har man betonat anpassning av nya uppgifter med kostnadseffektiviteten som en del av myndigheternas nuvarande verksamhet. I beredningen har man konstaterat att det inte är möjligt att identifiera något alternativ där den marknadskontroll som cyberresiliensförordningen förutsätter kan genomföras helt utan nya kostnads- och resurskonsekvenser för myndigheten.

Fördelen med en samlad kontroll är att kunnandet och expertisen om cyberresiliensförordningen samlas till en myndighet. Bedömningen av cybersäkerhetsegenskaperna är i sig i princip likadan oberoende av användningsändamålet för produkten, i synnerhet då bedömningen hänför sig till egenskaperna i en produkts programvara. En samlad expertis förutspås även leda till en mer harmoniserad tillämpningspraxis i fråga om cyberresiliensförordningen. Utmaningarna i den samlade kontrollen är det stora antalet produkter som omfattas av cyberresiliensförordningens tillämpningsområde och således kontrolluppgiftens omfattning. Dessutom har marknadskontrollmyndigheten inte något särskilt produktspecifikt specialkunnande till exempel i fråga om riskbedömning. Ur tillverkarnas synvinkel kan en samlad kontroll leda till överlappningar, då det är möjligt att samma produkter är föremål för marknadskontroll utifrån olika produktakter av fler än en marknadskontrollmyndighet. Även om den beskrivna situationen kan vara typisk på grund av cyberresiliensförordningens omfattande horisontella tillämpningsområde, uppskattas tillverkarnas kostnader på grund av överlappningen vara små utifrån erfarenheterna från marknadskontrollen utifrån övriga produktakter på samma produkter. En samlad kontroll kan bedömt som helhet vara den kostnadseffektivaste lösningen för att ordna marknadskontrollen.

Fördelen med en utspridd kontroll är möjligheten att kombinera marknadskontrollen enligt cyberresiliensförordningen även med marknadskontrollen av andra produktföreskrifter som hänför sig till samma produkt. Dessutom är det möjligt att en utspridd kontroll ger bättre

möjligheter att dra fördel av den nuvarande produkt- och branschspecifika expertisen hos myndigheten även i kontrollen enligt cyberresiliensförordningen. En utspridd kontroll utvidgar och utvecklar kunnandet om cybersäkerhet hos de nuvarande marknadskontrollmyndigheterna. Utmaningen med en utspridd kontroll är dock att cybersäkerhetsexpertis ska inhämtas till flera myndigheter. Utspridd kontroll är förmodligen ett sätt att ordna kontroll som skapar större kostnader än samlad kontroll. Cyberresiliensförordningens tillämpningsområde omfattar en avsevärd mängd produkter och programvaror som tidigare inte varit föremål för produktsäkerhetsföreskrifter eller kontroll, vars kontroll blir en ny uppgift även i den utspridda modellen. Dessutom skapar utspridning av kontrollen en risk för att tillämpningen och tolkningen av cyberresiliensförordningen sprids ut.

På grund av utmaningarna i anknytning till den utspridda kontrollen och den ringa betydelsen för tillverkarna av överlappningarna på grund av den samlade kontrollen har man i propositionen beslutat sig för att föreslå att marknadskontrollen ordnas maximalt samlat.

I fråga om en samlad kontroll har man bedömt ett alternativ där marknadskontrollen tilldelas antingen Transport- och kommunikationsverket Traficom eller Säkerhets- och kemikalieverket Tukes.

Transport- och kommunikationsverkets Cybersäkerhetscenter innehar befintligt kunnande om enheternas cybersäkerhetsegenskaper och bedömning av dessa. Transport- och kommunikationsverket har från och med år 2019 beviljat det frivilliga Cybersäkerhetsmärket till tillverkarna och bedömt enheternas cybersäkerhetsegenskaper i fråga om dess krav för Cybersäkerhetsmärket. Dessutom övervakar Transport- och kommunikationsverket dataskyddskraven enligt produktakten för radioutrustning från och med den 1 augusti 2025. Transport- och kommunikationsverket har även andra myndighetsuppgifter som gäller marknadskontrollen. Med stöd av lagen om marknadskontroll av vissa produkter (1137/2016) utför Transport- och kommunikationsverket marknadskontroll som hänför sig till luftfartyg, fordon, fritidsbåtar, fartygsutrustning, radioutrustning och vissa produkter tillgänglighetskrav. Å andra sidan har Transport- och kommunikationsverkets Cybersäkerhetscenter inte expertis om marknadskontroll eller de nuvarande marknadskontrolluppgifterna.

Säkerhets- och kemikalieverket har etablerat kunnande om produktsäkerhetsakterna och ordnande av marknadskontroll. Säkerhets- och kemikalieverket har även kunnande om och erfarenhet från samarbete inom marknadskontrollen mellan EU-medlemsstaterna. Samarbetsgruppen för marknadskontroll och samordningskontoret för marknadskontroll verkar i anslutning till Säkerhets- och kemikalieverket Säkerhets- och kemikalieverket har även tilldelats uppgiften som kontrollmyndighet enligt cybersäkerhetslagen för vissa näringsgrenar utifrån cybersäkerhetslagen, som trädde i kraft den 8 april 2025. Å andra sidan har Säkerhets- och kemikalieverket dock inte existerande expertis om egenskaper som påverkar programvarors och enheters cybersäkerhet eller om bedömning av dessa.

Med tanke på ordnandet av övervakningen enligt cyberresiliensförordningen bedömer man att det är ett kostnadseffektivare alternativ att samla kunnande om marknadskontroll till en myndighet jämfört med att kunnande om cybersäkerhet samlas till en myndighet som har kunskap om marknadskontroll. I beredningen har man dessutom bedömt att det är mer motiverat att i stället för kunnande om marknadskontroll centralisera marknadskontrolluppgiften utifrån expertisen om den produktakt som kontrollen gäller, det vill säga i detta fall om omständigheter som påverkar cybersäkerheten för en produkt. Således har man i beredningen beslutat sig för ett förslag där den uppgift som gäller marknadskontroll enligt cyberresiliensförordningen tilldelas Transport- och kommunikationsverket på ett så centraliserat sätt som möjligt. Med anledning

av artikel 52 i cyberresiliensförordningen ska marknadskontrolluppgiften dock i fråga om AI-system med hög risk nationellt fördelas mellan de myndigheter som övervakar dessa.

Till den del som det handlar om AI-system med hög risk enligt EU:s förordning om artificiell intelligens (EU) 2024/1689, har det nationella handlingsutrymmet för att ordna marknadskontrollen begränsats i cyberresiliensförordningen. Enligt cyberresiliensförordningen övervakar marknadskontrollmyndigheterna enligt förordningen om artificiell intelligens nämligen i detta fall även cybersäkerhetskraven enligt cyberresiliensförordningen i fråga om dessa AI-system. Till denna del beror den marknadskontrollmodell som genomförs med andra ord på de lösningar för anordnandet av övervakningen enligt förordningen om artificiell intelligens vilka gjorts i samband med det nationella genomförandet av förordningen om artificiell intelligens.

### 5.1.2 Anmälande myndighet

Vid beredningen av propositionen har man som ett alternativ gjort en bedömning av en situation där Säkerhets- och kemikalieverket Tukes och Transport- och kommunikationsverket innehar uppgiften som anmälande myndighet. Transport- och kommunikationsverkets Cybersäkerhetscenter har för närvarande uppgifter som stödjer verksamheten även som anmälande myndighet enligt cyberresiliensförordningen. Dessutom får centraliseringen av den befogenhet som gäller marknadskontrollen i huvudsak till Transport- och kommunikationsverket stöd av att även uppgiften som anmälande myndighet tilldelas Transport- och kommunikationsverket.

### 5.1.3 Påföljdsregleringen

I propositionen har man inte beslutat sig för att föreslå straffrättsliga påföljder för överträdelser av eller försummelser som gäller cyberresiliensförordningen eller cybersäkerhetsakten. På grund av den straffrättsliga ultima ratio-principen ska straffrättsliga påföljder användas som det sista möjliga alternativet för att sanktionera överträdelser eller försummelser. Vid beredningen av propositionen har man inte bedömt att det finns något vägande samhälleligt behov av att påföra straffrättsliga påföljder, utan att överträdelser av förordningarna kan sanktioneras genom administrativa påföljder.

I propositionen föreslås att bestämmelser utfärdas om det undantag som tillåts i det nationella handlingsutrymmet i artikel 64.7 i cyberresiliensförordningen i fråga om påföljdsavgifter för den offentliga förvaltningen på så sätt att administrativa böter kan påföras för myndigheter eller offentliga organ. Inte heller en påföljdsavgift som anknyter till cybersäkerhetscertifieringen kan påföras för myndigheten. Cybersäkerhetsakten ger möjlighet för den nationella lagstiftaren att fastställa lämpliga påföljder inom ramen för effektivitets- och motsvarighetsprinciperna.

Cybersäkerhetsakten innehåller inte uttryckliga bestämmelser om en påföljdsavgift, utan förutsätter att medlemsstaterna utfärdar bestämmelser om effektiva, proportionella och avskräckande påföljder. I samband med beredningen har det bedömts att det i stället för en administrativ påföljdsavgift främst kan bli aktuellt med straffrättsliga påföljder, så att de i detta fall kan anses uppfylla kraven i förordningen. På ovan nämnda sätt har man i propositionen beslutat sig för att sanktionera överträdelser genom administrativa påföljder.

Under beredningen har man bedömt beloppet av den påföljdsavgift som ska föreskrivas för överträdelse av cybersäkerhetsakten. Beloppet av påföljdsavgifterna varierar i Finland avsevärt beroende på regleringssambandet. Regleringsprinciperna för administrativa sanktioner omfattar att man ska förhålla sig reserverat till reglering som gäller påföljdsavgifter av ett avsevärt

maximibelopp i lagstiftning som uteslutande baserar sig på nationell prövning, förutom om det finns särskilda grunder för sådan reglering i anknytning till det ärende som är föremål för förslaget.

I situationer som baserar sig på nationell prövning har beloppet av påföljdsavgiften ofta varierat från några hundra euro till omkring hundra tusen euro. De nuvarande påföljdsavgifterna enligt lagen om tjänster inom elektronisk kommunikation är 1 000–1 000 000 euro. Högre påföljdsavgifter enligt lagen om tjänster inom elektronisk kommunikation påförs av marknadsdomstolen. Påföljdsavgiften för utövare av televisions- eller radioverksamhet enligt 334 § i lagen om tjänster inom elektronisk kommunikation, vilken anknyter till genomförandet av EU:s dataförvaltningsakt, är å sin sida 1 000–100 000 euro och den påförs av Transport- och kommunikationsverket. Den påföljdsavgift som påförs enligt lagen om åtgärder mot spridning av terrorisminnehåll online (99/2023) för en juridisk person är å sin sida minst 1 000 euro och högst 100 000 euro.

Den reglering som baserar sig på EU-rätten innehåller å sin sida avsevärt höga påföljdsavgifter. Vid sidan om ovan behandlade reglering kring påföljdsavgifter i cyberresiliensförordningen är maximinivån på påföljdsavgiften flera miljoner euro till exempel i Europaparlamentets och rådets förordning (EU) 2022/2065 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) och förordningen om artificiell intelligens. Påföljdskollegiet vid dataombudsmannens byrå har påfört flera påföljdsavgifter för överträdelse av dataskyddsförordningen. Likaså innehåller den nationella regleringen (cybersäkerhetslagen) för genomförande av EU:s cybersäkerhetsdirektiv (NIS 2-direktivet) höga påföljdsavgifter.

En hög påföljdsavgift för överträdelse av cybersäkerhetsakten kan motiveras med att överträdelse av cybersäkerhetscertifieringen kan ha likadana allvarliga konsekvenser som överträdelser av cyberresiliensförordningen eller cybersäkerhetslagen. Sverige har ansett att 10 000–15 000 000 kronor, det vill säga omkring 1 300–1 300 000 euro, är en lämplig nivå för påföljdsavgiften. I Tyskland är beloppet på en administrativ bot å sin sida högst 500 000 euro. Däremot är den påföljdsavgift som kan påföras en juridisk person i Estland högst 20 000 euro. Med andra ord varierar påföljdsavgiften stort i jämförelseländerna.

Åtminstone tillsvidare är avsikten att europeiska cybersäkerhetscertifieringar ska basera sig på frivillighet. Till den del som cybersäkerhetscertifiering används för att visa överensstämmelse med cyberresiliensförordningen och en överträdelse av certifieringen på samma gång även innebär att kraven i cyberresiliensförordningen inte möts, leder detta till att gärningen omfattas av regleringen kring påföljdsavgifter enligt cyberresiliensförordningen. På grund av detta har man vid beredningen bedömt att utgångspunkten för nivån på den påföljdsavgift som fogas till överträdelser som gäller cybersäkerhetscertifieringen kan utgöras av nivån på de påföljdsavgifter som baserar sig på nationell prövning. En påföljdsavgift av ett maximibelopp av högst 100 000 euro kan således anses vara effektiv, proportionell och avskräckande för överträdelse av regleringen kring cybersäkerhetscertifiering. Påföljdsavgiften hänförs till de viktigaste skyldigheter som ingår i cybersäkerhetsakten.

Avgränsning av påföljdsavgiften till 100 000 euro möjliggör att det inte är behövligt att tilldela ett kollegium till uppgift att fatta beslut om en påföljdsavgift. En sådan påföljdsavgift jämställs med de administrativa påföljder som Transport- och kommunikationsverket redan för närvarande kan påföra. Inte heller de övriga rättsskyddsaspekterna förutsätter i detta fall att ett kollegium tilldelas till uppgift att fatta beslut om en påföljdsavgift. Det bedöms inte att påförande av en påföljdsavgift i typfallet ger upphov till besvärliga situationer som förutsätter

att de olika grundläggande fri- och rättigheterna vägs sinsemellan. Eftersom denna nivå på påföljdsavgiften kan anses vara måttlig i förhållande till övriga påföljdsavgifter enligt den övriga EU-regleringen kring cybersäkerhet, finns det ett behov av att följa de framtida erfarenheterna från tillämpningen av cybersäkerhetsakten i Finland och i de olika medlemsstaterna och hur de olika medlemsstaternas reglering eventuellt harmoniseras i framtiden.

I propositionen föreslås inte att man sanktionerar en situation där en marknadsaktör ger en felaktig anmälan om att en produkt, en tjänst eller en process har ett cybersäkerhetscertifikat. En sådan situation kan bli föremål för bedömning till exempel som olämpligt förfarande i näringsverksamhet eller som vilseledande marknadsföring enligt konsumentskyddslagen. När man med gärningen strävar efter ekonomisk vinning eller med den orsakar ekonomisk skada för den som vilseletts, kan gärningen bedömas även som bedrägeri. I förordningen föreslås inte heller att man sanktionerar falskt uppträdande som ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering till kommissionen i enlighet med cybersäkerhetsakten. Yttranden med koppling till certifieringen av en sådan aktör har enligt förslaget inte rättsverkningar. Gärningen kan likaså bedömas som ett bedrägeri och gärningen kan eventuellt även uppfylla rekvisitet för något annat brott, såsom usurpation av tjänstemannabefogenheter. Således ska det med tanke på artikel 65 i cybersäkerhetsakten vara behövligt att utfärda bestämmelser om att de beskrivna förfarandena omfattas av en administrativ påföljdsavgift.

Cyberresiliensförordningen innehåller inte nationellt handlingsutrymme i fråga om maximibeloppet av påföljdsavgiften i fråga om de gärningar som föreskrivits i 64 § 2–4 punkten.

### 5.1.4 Passivitetsbesvär

Enligt artikel 64.1 b i cybersäkerhetsakten ska fysiska och juridiska personer ha rätt till effektiva rättsmedel avseende underlåtenhet att vidta åtgärder med anledning av ett klagomål (en begäran om åtgärder) som lämnats in till myndigheten för cybersäkerhetscertifiering eller i vissa fall till ett organ för bedömning av överensstämmelse. På grund av detta har man i bedömningen bedömt att det finns ett behov av att utfärda bestämmelser om så kallade passivitetsbesvär.

Införande av separata passivitetsbesvär föreslås inte i propositionen. I Finland har passivitetsbesvär inkluderats i dataskyddslagen (21 §) då EU:s dataskyddsförordning genomfördes nationellt. Riksdagens lagutskott har ansett att passivitetsbesvär är exceptionella i det finländska rättssystemet. Den gällande lagstiftningen innehåller vissa exempel på rättsskyddsmedel som gäller situationer med dröjsmål hos en myndighet. De gäller dock situationer där myndigheterna föreskrivits en tidsfrist för att avgöra ärendet (LaUU 15/2023 rd). Ingen sådan tidsfrist är förknippad med cybersäkerhetsakten, varför man bedömt om det finns något behov av att möjliggöra passivitetsbesvär för att fullgöra de skyldigheter som följer av unionslagstiftningen.

För det första har riksdagens lagutskott ansett att en möjlighet att klaga till laglighetsövervakarna är ett effektivt rättsskyddsmedel, eftersom de har till uppgift att vidta behövliga åtgärder med anledning av en klagan (LaUU 5/2018 rd). För det andra är det möjligt att förstå ”underlåtenhet att vidta åtgärder med anledning av ett klagomål” (”a failure to act on a complaint”; ”valituksen käsittelemättä jättäminen”) på så sätt att det handlar om att avvisa en begäran om undersökning eller om ett avslag på ett krav, det vill säga ett avgörande om att myndigheten inte vidtar åtgärder med anledning av klagomålet. Sådana avgöranden är överklagbara förvaltningsbeslut.

Med beaktande av ovan nämnda omständigheter föreslås inte att passivitetsbesvär inkluderas som ett separat rättsskyddsmedel, eftersom en medborgare har möjlighet att klaga hos den högsta laglighetsövervakaren. På samma sätt kan möjligheten att överklaga ett avgörande om att avvisa eller avslå en överklagan redan anses uppfylla det behov av skydd som artikel 64.1 b i cybersäkerhetsakten förutsätter.

## 5.2 Planerade och genomförda metoder i andra medlemsstater

### 5.2.1 Cyberresiliensförordningen

Reglering som kompletterar cyberresiliensförordningen bereds samtidigt även i andra medlemsstater. Under beredningen av regeringens proposition fanns det inte tillgänglig information om hur de uppgifter som gäller marknadskontrollen enligt cyberresiliensförordningen eller kontrollen av anmälda organ enligt den ordnas i de andra medlemsstaterna.

I Sverige har marknadskontrolluppgifterna enligt de olika produktsäkerhetsakterna tilldelats sammanlagt 17 myndigheter. Marknadskontroll har tilldelats enligt produkt till den myndighet vars bransch de kontrollerade produkterna hänför sig till. Varje produktsäkerhetsakt övervakas med vissa undantag av en myndighet. Marknadskontrollmyndigheterna deltar i det nationella Marknadskontrollrådet, inom vilket samarbete förs och utbyte av uppgifter mellan myndigheterna görs i anknytning till marknadskontrollen. Den svenska och finska modellen för anordnandet av marknadskontrolluppgifterna i de olika produktsäkerhetsakterna motsvarar i huvudsak varandra. Sverige har planerat att på ett centraliserat sätt tilldela marknadskontrollen av cyberresiliensförordningen till myndigheten Post- och telestyrelsen.

I Danmark är marknadskontrollen av produktsäkerhetsakterna mer centraliserad än i Finland och Sverige. Största delen av marknadskontrolluppgifterna enligt produktsäkerhetsakterna har tilldelats myndigheten för teknologisäkerhet (Danish Safety Tehnology Authority). Vissa produkter har tilldelats de branschspecifika myndigheterna, såsom kemikaliesäkerhetstjänsten vid miljöverket. Varje produktsäkerhetsakt övervakas av en myndighet, med undantag för leksaker, vars övervakning har delats till två myndigheter.

I Tyskland är marknadskontrollen av produktsäkerhetsakterna fördelad mellan förbundsrepublikens och delstaternas myndigheter. Huvudansvaret för genomförandet av marknadskontroll innehas av myndigheterna i delstaterna i Tyskland, men en del av ansvaren har även delats mellan förbundsmyndigheterna. I Tyskland är marknadskontrollen således avsevärt mer utspridd än i Finland och Sverige. Tyskland har dock planerat att på ett centraliserat sätt tilldela uppgiften för marknadskontrollen enligt cyberresiliensförordningen till myndigheten Bundesamt für Sicherheit in der Informationstechnik (BSI).

I Estland är marknadskontrollen enligt produktsäkerhetsakterna mer centraliserad än i Finland och Sverige. Största delen av marknadskontrolluppgifterna enligt de olika produktsäkerhetsakterna har tilldelats myndigheten för reglering kring konsumentskydd och teknik (Consumer Protection and Techical Regulatory Authority). Vissa produkter har tilldelats de branschspecifika myndigheterna, såsom hälsonämnden eller sjöfartsmyndigheten. Varje produktsäkerhetsakt övervakas med vissa undantag av en myndighet.

Nederländerna har planerat att tilldela marknadskontrollen enligt cyberresiliensförordningen och uppgiften för den anmälande myndigheten på centraliserat sätt till en myndighet. Enligt planerna kommer uppgiften att skötas av ämbetsverket för digital infrastruktur (”Dutch

Authority for Digital Infrastructure”). Även uppgiften som nationell myndighet för cybersäkerhetscertifiering har förlagts till verket.

På Europeiska kommissionens webbplats finns det information om alla nationella marknadskontrollmyndigheter enligt de olika produktsäkerhetsakterna. Länk: https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/market-surveillance/organisation_en.

Regleringen kring marknadskontrollen i Sverige, Danmark, Estland och Tyskland har bedömts även i avsnitt 5.2 i regeringens proposition RP 195/2022 rd.

### 5.2.2 Cybersäkerhetsakten

*Sverige*

I Sverige ingår de nationella bestämmelser som kompletterar cybersäkerhetsakten i lag 2021:553 (lag med kompletterande bestämmelser till EU:s cybersäkerhetsakt). I lagen föreskrivs att den nationella myndigheten för cybersäkerhetscertifiering har de befogenheter som avses i artikel 58.8 i cybersäkerhetsakten. Den kan förena sitt beslut med vite och den har rätt att få handräckning av Kronofogden. Myndigheten för cybersäkerhetscertifiering har rätt att återkalla ett cybersäkerhetscertifikat som utfärdats av den eller ett organ för bedömning av överensstämmelse i enlighet med artikel 56.6 i cybersäkerhetsakten, om det inte uppfyller kraven i cybersäkerhetsakten eller i en europeisk ordning för cybersäkerhetscertifiering. Försvarets materielverk fungerar som denna myndighet på så sätt att Swedac (Styrelsen för ackreditering och teknisk kontroll) övervakar organen för bedömning av överensstämmelse. Lagen innehåller bestämmelser om ackrediteringen av organ för bedömning av överensstämmelse i anknytning till cybersäkerhetscertifiering. Regeringen har ett bemyndigande att utfärda närmare bestämmelser om ackrediteringskraven.

Sverige har bedömt att det är ändamålsenligt att förena iakttagandet av lagen med en administrativ påföljdsavgift, vars maximibelopp ska vara tillräckligt avskräckande, eftersom överträdelserna kan påverka samhällets vitala funktioner och orsaka allvarliga skador för statens säkerhet (Prop. 2020/21:186, s. 31–32, 37–38). Enligt lagen är beloppet av påföljdsavgiften 10 000–15 000 000 kronor, det vill säga omkring 1 300–1 300 000 euro. I regeringens proposition ansågs påföljdsavgiften i anknytning till vitala samhällsfunktioner och digitala tjänster, vilken uppgick till högst 10 miljoner kronor, vara jämställbar med den. I princip är det obligatoriskt att påföra en påföljdsavgift och den täcker en relativt stor grupp av olika gärningar.

En administrativ påföljdsavgift påförs den som gett en EU-försäkran om överensstämmelse utifrån artikel 53.2 i cybersäkerhetsakten, trots att IKT-produkterna, IKT-tjänsterna eller IKT-processerna inte är förenliga med kraven i ordningen för cybersäkerhetscertifiering. En påföljdsavgift påförs även för lämnande av felaktiga eller bristfälliga uppgifter i en ansökan som gäller cybersäkerhetscertifiering. En påföljdsavgift påförs även om en certifikatinnehavare försummar att lämna ut information enligt artikel 56.8 i cybersäkerhetsakten om sårbarhet eller oriktigheter som rör säkerheten och som kan påverka överensstämmelsen med de krav som sammanhänger med certifieringen eller om tillverkaren eller tillhandahållarna av certifierade IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse getts inte ger de uppgifter som artikel 55 förutsätter, om det kan orsaka en förhöjd exponering för dataskyddshot eller risk för skador. Dessutom påförs en påföljdsavgift för den som bryter mot vissa villkor för ett europeiskt cybersäkerhetscertifikat eller använder ett certifikat, som har återkallats i enlighet med artikel 58.8 samt för den som bryter mot ett förbud som getts i ett tillsynsbeslut med stöd av 5 § i lagen. Lagen innehåller bestämmelser om

omständigheter som ska beaktas i påförandet av en påföljdsavgift och om sänkning och uteblivet påförande om det finns ett särskilt skäl till det eller om det vore orimligt att påföra avgiften.

Myndigheten har rätt att ta ut avgifter för sin verksamhet enligt cybersäkerhetsakten. Dessutom innehåller lagen bestämmelser om rätten att söka ändring i beslut av myndigheten eller organet för bedömning av överensstämmelse.

*Estland*

De centrala bestämmelserna om cybersäkerhetscertifiering ingår i cybersäkerhetslagen (küberturvalisuse seadus). Den estländska myndigheten för regleringen av konsumentskydd och teknisk reglering (Tarbijakaitse ja Tehnilise Järelevalve Amet) fungerar som nationell myndighet för cybersäkerhetscertifiering. En administrativ påföljdsavgift kan även påföras om en EU-försäkran om överensstämmelse inte uppfyller förutsättningarna i artikel 53.2 i cybersäkerhetsakten eller om tillverkaren eller leverantören av de IKT-produkter, IKT-tjänster och IKT-processer som har certifierats eller för vilka en EU-försäkran om överensstämmelse har getts inte uppfyller förutsättningarna för att lämna ut uppgifter enligt artikel 55.2. Den påföljdsavgift som kan påföras en juridisk person är högst 20 000 euro.

*Tyskland*

Den nationella reglering som kompletterar cybersäkerhetsakten ingår i lagen om förbundsrepublikens verk för IT-säkerhet (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik), det vill säga BSI-lagen. Lagens 14 § innehåller bestämmelser om en administrativ sanktionsavgift, som kan vara högst 500 000 euro. En sanktionsavgift kan påföras för vissa överträdelser av cybersäkerhetsakten eller för att ett organ för bedömning av överensstämmelse verkar inom cybersäkerhetsaktens tillämpningsområde utan att säkerhetsverket gett rätt till det. I fråga om överträdelse av förordningen sanktioneras försummelser av skyldigheten att lämna ut uppgifter enligt artikel 55.1 eller skyldigheten att lämna ut uppgifter avseende en certifikatinnehavare enligt artikel 56.8.

### 5.2.3 Registrarer

*Sverige*

Genomförandet av NIS 2-direktivet pågår i Sverige. Regeringens proposition med förslag till genomförandelagstiftning har lämnats den 9 oktober 2025 (Regeringens proposition 2025/26:28: Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag). Enligt utkastet anses direktivet förutsätta att skyldigheten att föra ett toppdomänregister gäller såväl förvaltare av ett toppdomänregister som registrarer (s. 186). Enligt 2 kap. 11 § i utkastet till cybersäkerhetslag, ska en aktör som är förvaltare av ett toppdomänregister eller som erbjuder domännamnsregistreringstjänster föra ett register över domännamn och säkerhetskopior av det. I paragrafen uppräknas de uppgifter som ett register ska täcka enligt artikel 28.2 i NIS-direktivet. Enligt förslaget innehåller 2 kap. 12 § bestämmelser om att tillträde ges avgiftsfritt till uppgifterna i toppdomänregistret utan att avskilja situationer där uppgifter begärs av en förvaltare av ett toppdomänregister eller en registrar.

*Tyskland*

Förbundsrepubliken Tyskland har gett ett lagförslag om genomförande av NIS 2-direktivet (Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung), enligt vilket

49–51 § i BSI-lagen framöver innehåller bestämmelser om skyldigheten för de som förvaltar ett toppdomänregister och registrarer att föra ett domänregister och ge tillträde till uppgifterna samt om aktörernas samarbetsskyldighet. Skyldigheterna gäller bägge typer av aktörer. Enligt motiveringarna till lagförslaget (s. 186) är syftet dock inte att fullgöra skyldigheterna dubbelt, utan att genomföra dessa enligt en viss arbetsfördelning i ett lagstadgat samarbete, vilket i hög grad redan är fallet i praktiken. Genom samarbetsskyldigheten enligt lagutkastet genomförs artikel 28.6 i NIS-direktivet och samarbetsskyldigheten gäller enligt motiveringarna till lagförslaget inte bara insamling av registreringsuppgifter, utan alla föreskrivna skyldigheter. I utkastet konstateras även att dubbel administrering av uppgifterna kan innebära att uppgifter överförs till områden utanför EU i avsevärd mån.

## 6 Remissvar

Uppgifterna om remissbehandlingen beskrivs ovan i avsnitt 1.2.2. En sammanfattning av remissvaren finns i statsrådets projektportal under projektkoden LVM014:00/2024.

I remissvaren understödde man att uppgifterna som marknadskontrollmyndighet och anmälande myndighet tilldelas Transport- och kommunikationsverket. I flera utlåtandena betonades behoven av resursallokering på grund av de nya uppgifterna för såväl Transport- och kommunikationsverket som de andra myndigheterna. I utlåtandena gjorde man även detaljerade anmärkningar om den föreslagna regleringen. i synnerhet i fråga om förslagen om myndigheternas befogenheter och domännamn.

Med anledning av Tullens utlåtande kompletterades motiveringarna till bestämmelsen om regulatoriska sandlådor för cyberresiliens med tanke på rollen för de andra marknadskontrollmyndigheterna än Transport- och kommunikationsverket. I propositionen inkluderades inte något krav på att en regulatorisk sandlåda ska vara avgiftsfri för små och medelstora företag på det sätt som Centralhandelskammaren föreslog, eftersom cyberresiliensförordningen inte förutsätter detta och eftersom ett krav på att en regulatorisk sandlåda ska vara avgiftsfri i praktiken kan hindra möjligheten att den genomförs inom ramen för Transport- och kommunikationsverkets nuvarande anslag.

På grund av utlåtandena gjordes små preciseringar i bestämmelserna om påförande av en påföljdsavgift och motiveringarna till dessa. I propositionen gjordes dock inte ändringar på det sätt som föreslagits i ett utlåtande, enligt vilket regleringslösningen ska ändras så att en administrativ påföljdsavgift inte kan påföras myndigheter. Till denna del baserar sig propositionen på grundlagsutskottets utlåtandepraxis om randvillkoren för att påföra administrativa påföljdsavgifter och den motsvarar de gällande bestämmelserna om en administrativ påföljdsavgift till exempel i cybersäkerhetslagen och dataskyddslagen.

Den i vissa utlåtanden föreslagna ändringen, enligt vilken CSIRT-enheten tilldelas en skyldighet att anmäla vidareöverlåtelse av en handling eller uppgift som den fått, gjordes inte i propositionen. Vid beredningen har det bedömts att sekretessen för de anmälningsskyldigas affärshemligheter tryggas med stöd av offentlighetslagen och den övriga tillämpliga allmänna lagstiftningen. Även ett eventuellt behov av att höra en part om överlåtelse av en handling fastställs utifrån den allmänna lagstiftningen, såsom offentligslagen och förvaltningslagen.

På grund av remissvaren gjordes ändringar i 7 § 2 mom., som gäller utlämnande av uppgifter mellan CSIRT-enheten och marknadskontrollmyndigheten och motiveringarna till det, så att förslaget på ett noggrannare sätt motsvarar regleringen i cyberresiliensförordningen. På samma gång ändrades 9 § och motiveringarna till den.

Motiveringarna till lagstiftningsordningen i propositionen har preciserats och utvidgats till vissa delar. På grund av justitieministeriets utlåtande gjordes preciseringar i de avsnitt som innehåller en bedömning av propositionens förhållande till grundlagen med tanke på tilldelande av en offentlig förvaltningsuppgift och näringsfriheten. I utlåtandet från justitieministeriet och i vissa andra utlåtanden riktades uppmärksamhet på befogenheterna att göra inspektioner i hemfridsskyddade objekt och motiveringarna och bestämmelserna om detta ändrades. I fråga om marknadskontrollen enligt cyberresiliensförordningen gjordes tillägg som säkerställer regleringens proportionalitet i 19 § i förslaget. I fråga om befogenheterna för myndigheten för cybersäkerhetscertifiering avgränsades i 25 § utrymmen som används för boende av permanent natur från tillämpningsområdet för inspektionsrätten på samma gång som en möjlighet att dra in ett certifikat av hög assuransnivån fogades till förslaget för det fallet att man i övervakningen inte får nödvändig information från certifikatinnehavaren.

Med anledning av remissvaren gjordes flera preciseringar i fråga om ändringarna och tilläggen i fråga om domännamn och registrarer i lagen om tjänster inom elektronisk kommunikation. En teknisk precisering gjordes i definitionen av ett domännamn. Definitionen av en registrar ströks från 3 § som en onödig definition och bestämmelsen om tillämpningsområdet för nya 21 a kap. i lagen förtydligades med tanke på aktörer som verkar för registrarers räkning. För att säkerställa täckningen av genomförandet av NIS 2-direktivet fogades till förslaget en liknande utvidgning av tillämpningsområdet även till tillämpningsområdet för den gällande lagens 21 kap., som gäller domännamn som slutar med fi och ax. Till förslaget fogades även övergångsbestämmelser om nya skyldigheter som gäller domännamn.

På grund av remissvaren om insamling och offentliggörande av registreringsuppgifter om domännamn kompletterades och preciserades bedömningen av nuläget i propositionen och de föreslagna bestämmelserna om ärendet och motiveringarna till dessa. Till lagförslaget fogades en bestämmelse som baserar sig på NIS 2-direktivet om samarbetsskyldigheten för aktörer och därtill gjordes en precisering av motiveringarna om att en ändamålsenlig arbetsfördelning kan iakttas då registreringsuppgifter samlas in, administreras och tillgängliggörs för att undvika överlappningar på det sätt som beskrivs i skäl 109 i ingressen till NIS 2-direktivet. Paragrafen om förteckningen över registrarer preciserades för att på ett noggrannare sätt överensstämma med direktivet och regleringen i cybersäkerhetslagen och i överensstämmelse med detta fogades ett bemyndigande att utfärda föreskrifter till paragrafen. Ett omnämnande om att tillträdet till domännamnsuppgifter är avgiftsfritt inkluderades i specialmotiveringen.

Till propositionen fogades däremot inte förslaget i Tekijänoikeuden tiedotus- ja valvontakeskus ry:s utlåtande om en skyldighet att i fråga om företag samla in kontaktinformation som uttryckligen gäller en fysisk person såväl till förteckningen över registrarer som till databasen över registreringsuppgifter om domännamn för företag som registrerat ett domännamn. Vid den fortsatta beredningen av propositionen har det bedömts att artikel 28 i NIS 2-direktivet inte förutsätter att ett sådant krav ställs. Genom propositionen förutsätts att registreringsuppgifter om domännamn enligt artikel 28 i NIS 2-direktivet samlas in och administreras. Även om det inte förutsätts att kontaktinformation som uttryckligen gäller fysiska personer samlas in, kräver propositionen att uppgifter som behövs för att identifiera en innehavare av ett domännamn och kontakta innehavaren samlas in. I enlighet med skäl 111 till NIS 2-direktivet bör registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster, i synnerhet, verifiera minst ett av registrantens kontaktsätt. . Därtill preciserades inte förutsättningarna för en berättigad begäran som gäller registreringsuppgifter om domännamn i propositionen, eftersom det handlar om tillämpningen av annan EU-lagstiftning än den som kompletteras genom den aktuella propositionen. Tilldelande av åtkomst till registreringsuppgifter om domännamn behandlas även i skälen 109–112 till NIS 2-direktivet.

Propositionens konsekvensbedömning har vid den fortsatta beredningen kompletterats med anledning av de bedömningar som lagts fram under remissbehandlingen, i synnerhet i fråga om myndighetskonsekvenserna. På grund av remissvaren har även andra, mindre och lagstiftningstekniska ändringar, preciseringar och kompletteringar gjorts i propositionen. Därtill inkluderas till propositionen en paragraf om beslut som ska ges i övervakningen beträffande förvaltare av programvara med fri och öppen källkod.

## 7 Specialmotivering

### 7.1 Lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering

#### 1 kap. – Allmänna bestämmelser

**1 §.** *Lagens syfte.* Det föreslås att lagen innehåller nationella bestämmelser som kompletterar och preciserar tillämpningen av cyberresiliensförordningen. Dessutom innehåller lagen bestämmelser om genomförandet av de europeiska ordningarna för cybersäkerhetscertifiering.

Paragrafens *1 mom.* innehåller bestämmelser om lagens mål och preciserar och kompletterar cyberresiliensförordningen och dess nationella tillämpning.

Det finns bestämmelser om tillämpningsområdet för cyberresiliensförordningen i artiklarna 1–3 i förordningen. Lagen tillämpas på produkter som omfattas av cyberresiliensförordningen. Cyberresiliensförordningens tillämpningsområde omfattar i artikel 2.1 avsedda produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät. Det finns bestämmelser om avgränsningarna av tillämpningsområdet för cyberresiliensförordningen i dess artikel 2.2–2.7 och om definitionen av en produkt med digitala element i artikel 3 i förordningen.

De produkter som omfattas av cyberresiliensförordningens tillämpningsområde är till exempel smartklockor, säkerhetskameror, tv-apparater, leksaker, hemroutrar, brandväggar, spel och programvaror. Tillämpningsområdet täcker i bred grad IoT-enheter och programvaror, oberoende av om enheten eller programvaran är avsedd att användas av en konsument, ett företag eller den offentliga förvaltningen. Cyberresiliensförordningen tillämpas på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät i enlighet med artikel 2 i förordningen och med undantagen i den.

Paragrafens *2 mom.* innehåller bestämmelser om lagens mål och preciserar och kompletterar även cybersäkerhetsakten och dess nationella tillämpning. Målet är att komplettera genomförandet av de europeiska certifieringssystemen för cybersäkerhet enligt cybersäkerhetsakten. Med detta avses övervakning av certifieringsordningarna och utfärdande av cybersäkerhetscertifikat. Genom cybersäkerhetsakten har man inrättat ett regelverk för certifiering, som ställer krav på de europeiska certifieringsordningar som ska inrättas för IKT-produkter, IKT-tjänster och IKT-processer samt för förfarandena för att inrätta dessa.

**2 §.** *Definitioner.* Det föreslås att paragrafen innehåller definitioner som motsvarar definitionerna i cyberresiliensförordningen och cybersäkerhetsakten.

Momentets *1 punkt* innehåller en definition av produkt med digitala element. Definitionen motsvarar definitionen i artikel 3.1 i cyberresiliensförordningen, enligt vilken definitionen

täcker även programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat. I enlighet med artikel 3.2 i cyberresiliensförordningen avses med fjärrbehandling av data databehandling på distans för vilken programvaran utformats och utvecklats av tillverkaren eller under tillverkarens ansvar, och vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner. Det finns bestämmelser om definitionen av en programvara, hårdvara och komponent i punkterna 4–6 i artikel 3 i cyberresiliensförordningen.

Momentets *2 punkt* innehåller en definition av ett anmält organ. I enlighet med kapitel IV i cyberresiliensförordningen avses med anmält organ ett i Finland etablerat organ för bedömning av överensstämmelse som utsetts av en finsk myndighet och anmälts till Europeiska kommissionen.

Momentets *3 punkt* innehåller bestämmelser om definitionen av en distributör. I överensstämmelse med artikel 3.17 i cyberresiliensförordningen avses med distributör en sådana annan fysisk eller juridisk person i leveranskedjan än tillverkaren eller importören som tillhandahåller en produkt med digitala element på Europeiska unionens marknad utan att påverka dess egenskaper.

Momentets *4 punkt* innehåller bestämmelser om definitionen av en importör. I överensstämmelse med artikel 3.16 i cyberresiliensförordningen avses med importör en fysisk eller juridisk person som är etablerad i Europeiska unionen och som på marknaden släpper ut en produkt med digitala element vilken bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad utanför Europeiska unionen.

Momentets *5 punkt* innehåller bestämmelser om definitionen av en tillverkare. I överensstämmelse med artikel 13 i cyberresiliensförordningen avses med tillverkare en fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, vare sig mot betalning, i förvärvssyfte eller kostnadsfritt.

Momentets *6 punkt* innehåller en definition av tillverkarens representant. I överensstämmelse med artikel 2.15 i cyberresiliensförordningen avses med tillverkarens representant en fysisk eller juridisk person som är etablerad i unionen och som enligt skriftlig fullmakt från en tillverkare har rätt att i tillverkarens ställe utföra särskilda uppgifter.

Momentets *7 punkt* innehåller en definition av en ekonomisk aktör. Med ekonomisk aktör avses i 3–7 punkten definierade tillverkare, tillverkarens representanter, importörer, distributörer eller andra fysiska eller juridiska personer vilka omfattas av skyldigheterna enligt cyberresiliensförordningen i anknytning till produkter med digitala element eller tillhandahållande på marknaden. Definitionen motsvarar definitionen i artikel 3.12 i cyberresiliensförordningen.

Momentets *8 punkt* innehåller bestämmelser om definitionen av en förvaltare av programvara med fri och öppen källkod. Definitionen av en förvaltare av programvara med fri och öppen källkod av motsvarar definitionen i artikel 3.14 i cyberresiliensförordningen. Det finns bestämmelser om en programvara med fri och öppen källkod i artikel 3.48 i cyberresiliensförordningen.

Momentets *9 punkt* innehåller bestämmelser om definitionen av ett organ för bedömning av överensstämmelse. Med organ för bedömning av överensstämmelse avses ett organ som utför kalibrering, testning, certifiering och inspektioner och som på andra sätt bedömer överensstämmelse. Definitionen motsvarar definitionen i artikel 2.13 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 (nedan NLF-förordningen), som ligger till grund för motsvarande definitioner i artikel 3.28 i cyberresiliensförordningen och artikel 2.18 i cybersäkerhetsakten.

Momentets *10 punkt* innehåller bestämmelser om definitionen av ackreditering. Med ackreditering avses ett intyg från ett nationellt ackrediteringsorgan om att ett organ för bedömning av överensstämmelse uppgifter vissa krav för bedömning av överensstämmelse som fastställs genom harmoniserade standarder samt vid behov de krav som fastställs i sektorsspecifika program och eventuella ytterligare krav.

Momentets *11 punkt* innehåller bestämmelser om definitionen av en CSIRT-enhet. Med CSIRT-enhet avses en CSIRT-enhet enligt 19 § i cybersäkerhetslagen.

Momentets *12 punkt* innehåller bestämmelser om definitionen av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering, vilket i enlighet med artikel 61 i cybersäkerhetsakten avser ett organ för bedömning av överensstämmelse som anmälts till Europeiska kommissionen. Ett organ för bedömning av överensstämmelse definieras ovan i 9 punkten på ett sätt som motsvarar NLF-förordningen, till vilken motsvarande definition i cybersäkerhetsakten även hänvisar. När ett organ för bedömning av överensstämmelse som anmälts till kommissionen inom cyberresiliensförordningens område verkar som ett anmält organ enligt 2 punkten inom ramen för NLF-regelverket, handlar cybersäkerhetsakten inte om harmoniserad gemenskapslagstiftning och det organ för bedömning av överensstämmelse som ska anmälas till kommissionen verkar inte med stöd av den inom ramen för NLF-regelverket, även om krav enligt NLF-förordningen på grund av hänvisningen till cybersäkerhetsakten tillämpas till exempel på ackrediteringen av dessa. Anmälda organ och organ för bedömning av överensstämmelse som anmälts med stöd av cybersäkerhetsakten är föremål för likadana, men i viss mån lite olika krav. För att klargöra denna skillnad används i den föreslagna lagen begreppet organ för bedömning av överensstämmelse som anmäls för cybersäkerhetscertifiering i sammanhang som gäller verksamhet i anknytning till cybersäkerhetsakten. I praktiken är det dock möjligt att ett visst organ för bedömning av överensstämmelse gör en ansökan för att verka i bägge roller, som kan stödja varandra.

**3 §.** *Förhållande till annan lagstiftning.* Paragrafen innehåller informativa hänvisningar till marknadskontrollförordningen och marknadskontrollagen, vilka tillämpas vid sidan om vad som föreskrivs i den föreslagna lagen vid övervakningen enligt cyberresiliensförordningen.

Paragrafens *1 mom.* innehåller en informativ hänvisning till marknadskontrollförordningen. Marknadskontrollförordningen tillämpas med stöd av artikel 52.1 i cyberresiliensförordningen på marknadskontrollen av produkter med digitala element.

Paragrafens 2 mom. innehåller en informativ hänvisning till lagen om marknadskontrollen av vissa produkter (nedan *marknadskontrollagen*). Marknadskontrollagen tillämpas på marknadskontrollen av produkter med digitala element i enlighet med de ändringar som föreslås genom lagförslag 2. Marknadskontrollagen innehåller bestämmelser om marknadskontrollen av produkter, tillsynsmyndigheternas befogenheter och tillsynsmetoder samt om sökande av ändring i myndigheternas beslut.

Paragrafens *3 mom.* innehåller en informativ hänvisning till lagen om konsumentprodukters säkerhet och EU:s förordning om allmän produktsäkerhet. I enlighet med artikel 2 i EU:s förordning om allmän produktsäkerhet tillämpas förordningen på produkter som släpps ut eller tillhandahålls på marknaden i den mån det inte föreligger särskilda bestämmelser med samma

syfte enligt unionsrätten som reglerar säkerheten hos de berörda produkterna. När de särskilda säkerhetskrav som fastställts i unionslagstiftningen tillämpas på produkterna, tillämpas förordningen endast på de omständigheter och risker eller riskkategorier som dessa krav inte täcker.

Paragrafens *4 mom.* innehåller en informativ hänvisning till EU:s förordning om artificiell intelligens och lagen om tillsyn över vissa system för artificiell intelligens, som föreslås i regeringens proposition till riksdagen med förslag om lagstiftning som kompletterar EU:s förordning om artificiell intelligens (RP 46/2025 rd). Förordningen om artificiell intelligens och den nationella reglering som kompletterar den innehåller bestämmelser om kraven på AI-system och övervakningen av dessa i fråga om de produkter som omfattas av tillämpningsområdet för förordningen om artificiell intelligens.

Paragrafens *5 mom.* innehåller en informativ hänvisning till vad som föreskrivs annanstans i lagen om CSIRT-enhetens uppgifter. CSIRT-enhetens uppgifter och samordning av sårbarheter regleras i cybersäkerhetslagen, med undantag för de uppgifter och den behandling av rapporter som avses i cyberresiliensförordningen. Artiklarna 14–17 i cyberresiliensförordningen innehåller bestämmelser om sårbarheter som ingår i en produkt med digitala element och om obligatoriska och frivilliga anmälningar som ska göras om vissa omständigheter samt om handläggningen av dessa. Enligt förslaget tar CSIRT-enheten emot och handlägger rapporter på det nationella planet. Bestämmelsernas innehåll har beskrivits mer ingående i avsnitt 2.1.3.1.

CSIRT-enheten tar emot även andra än frivilliga rapporter om sårbarheter enligt cyberresiliensförordningen som en del av skötseln av dess befintliga uppgifter enligt cybersäkerhetslagen. Detta behandlas även i motiveringarna till 8 §. CSIRT-enhetens uppgift som gäller sårbarhetssamordning enligt 22 § i cybersäkerhetslagen täcker sårbarhetsanmälningar om produkter och tjänster som lämnar utanför tillämpningsområdet för cyberresiliensförordningen och sårbarhetsanmälningar som gäller verksamheten vid organisationerna.

**2 kap. – Överensstämmelse och anmälningar**

**4 §.** *Överensstämmelse för produkter med digitala element.* Paragrafen innehåller en informativ hänvisning till de krav som ställts på produkter med digitala element med stöd av cyberresiliensförordningen.

Med stöd av artikel 6 i cyberresiliensförordningen får produkter med digitala element tillhandahållas på marknaden endast om den uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I i förordningen, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen kan förutses och, i tillämpliga fall, att de nödvändiga säkerhetsuppdateringarna har installerats. En ytterligare förutsättning är att de processer som införs av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II i förordningen.

Det finns bestämmelser om skyldigheterna för en ekonomisk aktör och kraven på en produkt med digitala element i 2 kap. i förordningen och bilaga I och bilaga II till den samt i 3 kap. om påvisande av överensstämmelse i förordningen.

**5 §.** *Ej färdigställda produkter.* Artikel 4.2 och artikel 4.3 i cyberresiliensförordningen innehåller bestämmelser om situationer där medlemsstaterna inte får hindra att produkter med digitala element som inte uppfyller kraven i cyberresiliensförordningen visas, används eller tillhandahålls på marknaden. Med stöd av principen om prioriteten för EU-rätten är det inte

möjligt att en nationell norm i strid med artikel 4 blir tillämplig. För att tydliggöra regleringen och precisera rättsläget i synnerhet med tanke på förslagen om den administrativa påföljdsavgiften i 6 kap. föreslås att separata bestämmelser utfärdas om att tillåta att ej färdigställda produkter enligt artikel 4.2 och 4.3 visas, används eller släpps ut på marknaden.

I paragrafen utfärdas bestämmelser om möjligheten att visa, använda eller på marknaden släppa ut en produkt med digitala element, då de inte uppfyller kraven i cyberresiliensförordningen. I enlighet med artikel 4.2 i cyberresiliensförordningen får medlemsstaterna inte förhindra att sådana produkter med digitala element som inte uppfyller kraven i förordningen visas eller används vid mässor, utställningar och demonstrationer eller liknande evenemang, inbegripet prototyper, förutsatt att produkten visas med en synlig märkning som tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden förrän den gör det. I enlighet med artikel 4.3 i cyberresiliensförordningen får medlemsstaterna inte förhindra att en ej färdigställd programvara som inte uppfyller kraven i förordningen tillhandahålls på marknaden, under förutsättning att programvaran tillhandahålls endast under den begränsade tid som krävs för testningsändamål och med en synlig märkning som tydligt anger att den inte uppfyller kraven i förordningen och att den inte kommer att tillhandahållas på marknaden för andra ändamål än testning.

För klarhetens skull konstateras att ett hinder som orsakas av den övriga regleringen dock kan uppkomma för användningen av en produkt med digitala element. Till exempel om radioutrustning är en produkt med digitala element, kan ett radiotillstånd krävas för att använda den. Bestämmelsen gäller visning av en produkt med digitala element, även om överensstämmelsen med kraven enligt cyberresiliensförordningen inte uppfylls. Syftet med bestämmelsen är inte att bilda en grund för att avvika från de krav som ställs på produkten i den övriga regleringen, om sådana är tillämpliga på produkten.

**6 §.** *Produkter med digitala element vid offentlig upphandling.* Paragrafen innehåller bestämmelser för en upphandlande enhet att beakta efterlevnad av de cybersäkerhetskrav som fastställts i bilaga I till cyberresiliensförordningen, inbegripet tillverkarnas förmåga att effektivt behandla sårbarheter då föremålet för den offentliga upphandlingen är en produkt med digitala element. Genom bestämmelsen kompletteras artikel 5.2 i cyberresiliensförordningen, vilken förutsätter att medlemsstaterna, utan att det påverkar tillämpningen av direktiven 2014/24/EU och 2014/25/EU, när produkter med digitala element som omfattas av denna förordnings tillämpningsområde upphandlas, ska säkerställa att överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till denna förordning, inbegripet tillverkarnas förmåga att ändamålsenligt hantera sårbarheter, beaktas i upphandlingsprocessen. I praktiken kan en upphandlande enhet beakta efterlevnad av kraven på cybersäkerhet till exempel vid beredningen av en upphandling eller en anbudsbegäran, vid prövningen av de krav som ställs på upphandlingsobjektet eller vid fastställande av lämplighetskriterierna för en kandidat eller leverantör. Bestämmelsen är avsedd att tillämpas för upphandlingar som omfattas av tillämpningsområdet för lagen om offentlig upphandling och koncession, där föremålet för upphandlingen är en produkt på vilken kraven i cyberresiliensförordningen tillämpas.

**7 §.** *Tillverkarens anmälningsskyldighet.* Paragrafens *1 mom.* innehåller en informativ hänvisning till skyldigheten enligt artikel 14 i cyberresiliensförordningen att anmäla en aktivt utnyttjad sårbarhet i en produkt med digitala element eller en incident som påverkar dataskyddet för en produkt med digitala element. Anmälan ska göras via den gemensamma rapporteringsplattformen enligt artikel 16 i cyberresiliensförordningen till CSIRT-enheten och och Europeiska unionens cybersäkerhetsbyrå Enisa. Det finns bestämmelser om definitionen av en aktivt utnyttjad sårbarhet i artikel 3.40 och artikel 3.42 i förordningen och om definitionen av en allvarlig incident i artikel 3.43, artikel 3.44 och artikel 14.5 i förordningen. Anmälningar

ska göras enligt de tidsfrister och de uppgiftsinnehåll som föreskrivs i artikel 14.2 och artikel 14.4 i förordningen. CSIRT-enheten vid Transport- och kommunikationsverket kan i enlighet med artikel 14.6 i cybersäkerhetsakten vid behov med en delrapport begära ytterligare information om situationen för en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar dataskyddet för en produkt med digitala element. Dessutom ska tillverkaren i enlighet med artikel 14.8 ge produktanvändarna information. Anmälningsskyldigheterna tillämpas dessutom även på förvaltare av programvara med fri och öppen källkod med stöd av artikel 24.3 i förordningen.

Paragrafens *2 mom.* innehåller för klarhetens skull bestämmelser om samarbetet mellan CSIRT-enheten och marknadskontrollmyndigheten. Momentet innehåller en informativ hänvisning till artikel 16.3 i cyberresiliensförordningen, enligt vilken de CSIRT-enheter som utsetts till samordnare ska förse marknadskontrollmyndigheterna i sina respektive medlemsstater med den anmälda information som gäller en aktivt utnyttjad sårbarhet eller en allvarlig incident och som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina skyldigheter enligt denna förordning CSIRT-enhetens skyldighet att lämna ut uppgifter hänför sig i praktiken till de uppgiftstyper som specificerats i artikel 14 i cyberresiliensförordningen, vilka en tillverkare ska inkludera i sin anmälan. Med anledning av bestämmelserna i artikel 16.3 i cyberresiliensförordningen har marknadskontrollmyndigheten rätt att få även de sekretessbelagda uppgifter som den behöver utifrån ett meddelande. Rätten för CSIRT-enheten att lämna ut sekretessbelagda uppgifter föreskrivs nedan i 9 § 1 punkten. Marknadskontrollmyndigheten kan anses behöva alla uppgifter som förutsätts av cyberresiliensförordningen och som ingår i en sårbarhets- eller incidentsanmälan.

**8 §.** *Frivillig anmälan*. Paragrafen innehåller bestämmelser om frivilliga anmälningar enligt artikel 15 i cyberresiliensförordningen, vilka CSIRT-enheten i enlighet med *1 mom.* tar emot från tillverkarna och andra aktörer utöver Europeiska unionens cybersäkerhetsbyrå Enisa. En frivillig anmälan enligt artikel 15.1 eller artikel 15.2 i cyberresiliensförordningen kan gälla 1) sårbarhet i en produkt med digitala element, 2) cyberhot som kan påverka riskprofilen för en produkt med digitala element eller 3) eventuella incidenter som påverkar dataskyddet för en produkt med digitala element samt tillbud som kunde ha lett till en sådan incident.

Frivilliga anmälningar ska behandlas enligt det förfarande som föreskrivs i artikel 15 och artikel 16 i cyberresiliensförordningen. Om någon annan än en tillverkare anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar dataskyddet för en produkt med digitala element, ska den CSIRT-enhet som utsetts till samordnare utan dröjsmål anmäla den till tillverkaren. CSIRT-enheten kan prioritera behandlingen av obligatoriska anmälningar, det vill säga anmälningar enligt artikel 14 i cyberresiliensförordningen, i förhållande till frivilliga anmälningar.

För klarhetens skull konstateras att de sårbarhetsanmälningar som CSIRT-enheten tar emot, då tillämpningen av bestämmelserna om sårbarhetsanmälningar i cyberresiliensförordningen börjar, kan delas in i tre kategorier: 1) obligatoriska rapporter om sårbarheter enligt artikel 14 i cyberresiliensförordningen, 2) frivilliga rapporter om sårbarheter enligt artikel 15 i cyberresiliensförordningen, och 3) andra frivilliga sårbarhetsanmälningar. På behandlingen av anmälningar enligt kategorierna 1 och 2 tillämpas åtgärder enligt cyberresiliensförordningen, såsom skyldigheten att underrätta övriga medlemsstater om sårbarhetsanmälningar. På behandlingen av frivilliga rapporter om sårbarheter enligt kategori 3 tillämpas inte regleringen i cyberresiliensförordningen, utan bestämmelserna i 22 § i cybersäkerhetslagen tillämpas på sårbarhetssamordningen i fråga om dessa.

Således är det möjligt att till CSIRT-enhetem frivilligt anmäla sårbarheter, cyberhot, avvikelser och tillbud som en annan än en frivillig anmälan enligt artikel 15 i cyberresiliensförordningen. Sådana anmälningar omfattas inte av tillämpningsområdet för bestämmelsen eller skyldigheterna avseende behandlingen av anmälningar i cyberresiliensförordningen.

Med stöd av paragrafens *2 mom.* får information som på frivillig basis lämnats ut till CSIRT-enheten enligt artikel 15 i cyberresiliensförordningen inte utan samtycke av den som lämnat ut informationen användas i brottsutredningar eller vid administrativt eller annat beslutsfattande som gäller den som lämnat ut informationen. I enlighet med artikel 15.5 i cyberresiliensförordningen får, utan att det påverkar förebyggandet, utredningen, avslöjandet och lagföringen av brott, frivillig rapportering inte leda till att den anmälande fysiska eller juridiska personen åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in anmälan. Syftet med bestämmelsen är att skydda frivilliga anmälare och uppmuntra till frivillig anmälning för att förbättra säkerheten.

**9 §.** *CSIRT-enhetens rätt att lämna ut sekretessbelagd information.* I paragrafen regleras CSIRT-enhetens rätt att trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information lämna ut en handling som den fått eller upprättat i samband med skötseln av dess uppgifter enligt artiklarna 14–17 i cyberresiliensförordningen samt röja sekretessbelagd information, om det är nödvändigt för skötseln av uppgifterna. Bestämmelsen är behövlig för att sköta de uppgifter som tilldelats CSIRT-enheten genom cyberresiliensförordningen. Artiklarnas innehåll beskrivs mer ingående i avsnitt 2.1.3.1. Med stöd av paragrafen kan CSIRT-enheten överlåta uppgifter på eget initiativ för att sköta uppgifterna i anknytning till behandlingen av dessa sårbarhetsanmälningar och incidentanmälningar i enlighet med cyberresiliensförordningen.

Rätten att lämna ut uppgifter är nödvändig, eftersom CSIRT-enheten i enlighet med artikel 16.2 i cyberresiliensförordningen kan förmedla anmälningar som den tagit emot i anmälningstjänsten till andra CSIRT-enheter som utsetts till samordnare i ett område där tillverkaren har meddelat att den släppt ut en produkt med digitala element. Anmälningarna blir i princip tillgängliga samtidigt även för Enisa, då de görs till en CSIRT-enhet. Det är dock möjligt att skjuta upp förmedlingen av en anmälan i en sådan undantagssituation som föreskrivs i artikel 16.2 i cyberresiliensförordningen.

Tillämpningsområdet för paragrafens *1 mom.* är avgränsat till de obligatoriska uppgiftstyperna i sårbarhets- och incidentsanmälningar vilka specificerats i artikel 14.2, 14.4 och 14.6 i cyberresiliensförordningen och motsvarande uppgifter som ingår i frivilliga anmälningar som getts med stöd av artikel 15. Rätten att lämna ut information är bunden till behovsförutsättningen och gäller således för uppgifter som ingår i obligatoriska tidiga varningar, anmälningar om en incident, anmälningar om en sårbarhet och eventuella delrapporter och slutrapporter vilka CSIRT-enheten tagit emot, liksom även frivilliga anmälningar om sårbarheter, incidenter och tillbud.

De uppgiftstyper som ingår i obligatoriska anmälningar har specificerats i artikel 14. Med stöd av artikel 2 ges en tidig varning om en sårbarhet (med andra ord information om att en sårbarhet existerar och att information kommer att ges om den). I den anmäls vid behov de de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits. I den egentliga sårbarhetsanmälan ges allmänna uppgifter om den berörda produkten med digitala element, den allmänna karaktären av utnyttjandet och sårbarheten i fråga samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta. En slutrapport om en sårbarhet ska å sin sida innehålla en beskrivning av sårbarheten och dess allvarlighetsgrad och konsekvenser, i

förekommande fall information om en fientlig aktör som har utnyttjat eller som utnyttjar sårbarheten, detaljer om säkerhetsuppdateringen eller andra korrigerande åtgärder som har gjorts tillgängliga för att avhjälpa sårbarheten. Med stöd av artikel 4 som gäller incidenter ska tillverkaren i en tidig varning å sin sida inkludera information om den misstänker att incidenten orsakats av olagliga eller fientliga handlingar, och i tillämpliga fall även ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits. Den egentliga incidentsanmälan ska innehålla allmänna uppgifter om arten av incidenten, en första bedömning av incidenten samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta. En slutrapport om en incident ska å sin sida innehålla en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst incidenten och tillämpade och pågående riskreducerande åtgärder. Med stöd av punkt 6 i artikeln kan CSIRT-enheten begära att tillverkarna lämnar en delrapport om relevanta statusuppdateringar om den aktivt utnyttjade sårbarheten eller allvarliga incidenten som påverkar säkerheten för produkten med digitala element. Delrapporten innehåller med andra ord en uppdatering av de uppgifter som getts med stöd av punkt 2 och 4.

I fråga om frivilliga anmälningar är det möjligt att till CSIRT-enheten anmäla eventuella sårbarheter eller cyberhot som kan påverka riskprofilen för en produkt med digitala element eller eventuella incidenter som påverkar dataskyddet för en produkt med digitala element samt tillbud som kunde ha lett till en sådan incident. I förslaget preciseras de uppgiftstyper som ska lämnas genom att förutsätta att det handlar om en uppgift som motsvarar de uppgifter som nämns i punkterna 2, 4 och 6 i artikeln, så att det står klart att lämnandet av uppgiften kan bindas till behovsförutsättningen.

Det föreslås att paragrafens *2 mom.* dessutom innehåller bestämmelser om möjligheten att lämna även andra än ovan nämnda specificerade uppgifter som CSIRT-enheten fått då den skött uppgifter enligt cyberresiliensförordningen. I så fall kan uppgifterna enligt momentet lämnas endast till de aktörer som avses i 1 mom. Förutsättningen är att det med avvikelse från 1 mom. är nödvändigt att lämna ut information för att utföra de uppgifter som föreskrivs i artiklarna 14–17 i cyberresiliensförordningen. Förslaget är behövligt eftersom det är möjligt att sådan anknuten information som inte nödvändigtvis hör till de uppgifter som specificeras i artiklarna 14 och 15 i cyberresiliensförordningen uppkommer i behandlingen av anmälningarna. Enligt huvudregeln lämnas information på det sätt som föreskrivs i 1 mom. och 2 mom. är avsett att tillämpas endast i undantagsfall.

I enlighet med artikel 15.5 i cyberresiliensförordningen ska den CSIRT-enhet som utsetts till samordnare och Enisa säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls frivilligt av den anmälande fysiska eller juridiska personen. Så som bedömts i avsnitt 3.1.4 kan det i fråga om CSIRT-enheten anses att bestämmelserna i offentlighetslagen säkerställer sekretessen för dessa till den del som det är befogat. Då CSIRT-enheten lämnar anmälningsuppgifter som den fått frivilligt, ska den behandla uppgifterna så att dessa intressen inte äventyras. De aktörer till vilka det enligt förslaget är möjligt att lämna ut information binds av en sekretesskyldighet enligt offentlighetslagen eller av denna samma skyldighet enligt cyberresiliensförordningen.

En sekretessbestämmelse eller en annan begränsning av utlämnade av information, från vilken man gör undantag med stöd av den föreslagna bestämmelsen, kan gälla till exempel en privat affärshemlighet eller skyddsarrangemangen i informations- och kommunikationssystem. Information om en sårbarhet eller incident kan även vara föremål för andra sekretessgrunder enligt offentlighetslagen, såsom 24 § 1 mom. 9 punkten i offentlighetslagen (handlingar som

gäller upprätthållande av statens säkerhet) eller 17 punkten (offentliga samfunds företagshemligheter). Information som gäller en näringsidkare som är etablerad i en annan medlemsstat kan i vissa förhållanden vara sekretessbelagd även med stöd av 24 § 1 mom. 2 punkten i offentlighetslagen.

Paragrafens *1 punkt* innehåller bestämmelser om utlämnande av information till den behöriga marknadskontrollmyndigheten i Finland i övervakningen enligt cyberresiliensförordningen. Det finns bestämmelser om tilldelningen av marknadskontrolluppgifterna i 15 och 16 § i den föreslagna lagen. Punkten kompletterar artikel 16.3 i cyberresiliensförordningen, som reglerar skyldigheten för CSIRT-enheter att förse marknadskontrollmyndigheterna i dess medlemsstater de uppgifter som anmälts i en sårbarhetsanmälan eller en incidentanmälan, vilka marknadskontrollmyndigheterna behöver för att fullgöra sina skyldigheter enligt förordningen. Uppgifter kan även lämnas ut i fråga om uppgifter som ingår i en delrapport eller slutrapport.

Paragrafens *2 punkt* reglerar å sin sida bestämmelser om utlämnande av uppgifter till Europeiska unionens cybersäkerhetsbyrå Enisa och *3 punkten* till en CSIRT-enhet som utsetts till samordnare i en annan medlemsstat. Det finns bestämmelser om skyldigheten för en CSIRT-enhet att förmedla anmälningar till Enisa och andra CSIRT-enheter i artikel 16 i cyberresiliensförordningen. Därtill kan det från fall till fall vara behövligt att utbyta upplysningar med Enisa, då avsikten är att informera allmänheten om en incident på det sätt som avses i artikel 17.2 i cyberresiliensförordningen.

Paragrafen begränsar inte CSIRT-enhetens rätt att lämna ut dessa uppgifter inom ramen för klausulerna om skadeförutsättningar i offentlighetslagen och inte heller utlämnade av uppgifter utifrån en grund som föreskrivits i någon annan lag, såsom i cybersäkerhetslagen eller 319 § i lagen om tjänster inom elektronisk kommunikation.

**10 §.** *Regulatorisk sandlåda för cyberresiliens*. Paragrafen innehåller bestämmelser om inrättande av en regulatorisk sandlåda enligt artikel 33.2 i cyberresiliensförordningen. Bestämmelsen ålägger inte att inrätta en regulatorisk sandlåda för cyberresiliens, utan möjliggör att en regulatorisk sandlåda inrättas vid behov utifrån ett beslut av Transport- och kommunikationsverket. Bestämmelsen avgränsar inte antalet regulatoriska sandlådor för cyberresiliens som inrättas. Vid behov kan det finnas flera regulatoriska sandlådor, till exempel för att testa olika produkter eller förhållanden. Transport- och kommunikationsverket kan pröva om en regulatorisk sandlåda ska inrättas. För en ekonomisk aktör är det frivilligt att utnyttja en regulatorisk sandlåda i produktutvecklingen och i princip även avgiftsbelagt i enlighet med vad som bestäms i lagen om grunderna för avgifter till staten. Utnyttjande av en regulatorisk sandlåda är avsett som ett temporärt stöd för en ekonomisk aktörs utvecklingsarbete då en produkt med digitala element eller en del av den inte är tillgänglig på marknaden.

Med stöd av *1 mom.* i paragrafen inrättas en regulatorisk sandlåda av Transport- och kommunikationsverket. Ett beslut ska fattas om inrättande av en regulatorisk sandlåda, i vilket man fastställer giltighetstiden för sandlådan och platsen eller en tillämplig teknisk avgränsning samt det testobjekt som lämpar sig för sandlådan. Till exempel en produktgrupp eller -typ kan fastställas som testobjekt utifrån produktens användningsändamål eller egenskaper eller något annat lämpligt sätt. Det är även möjligt att avgränsa testobjektet till exempel till en viss komponent, en viss egenskap, ett visst användningsändamål eller en viss programvara. I verksamhetsplanen är det möjligt att precisera kapaciteten och resursallokeringen för den regulatoriska sandlådan. I beslutet är det även möjligt att ställa villkor för den regulatoriska sandlådan, vilka behövs för att ordna dess verksamhet eller för dess säkerhet. Villkoren kan gälla till exempel den tidsmässiga avgränsningen av testningen eller säkerhetsarrangemangen för testningen. Villkoren ska vara jämbördiga för de ekonomiska aktörerna och behövliga med

tanke på den regulatoriska sandlådan eller säkerheten. En regulatorisk sandlåda kan inrättas även i anslutning till en regulatorisk sandlåda enligt förordningen om artificiell intelligens, om det är ändamålsenligt på grund av testningen, såsom på grund av testning som gäller AI-system med hög risk. Avsikten är att föreslå bestämmelser om regulatoriska sandlådor för regleringen kring artificiell intelligens i lagen om vissa system för artificiell intelligens som en del av genomförandet av fas II av förordningen om artificiell intelligens (VN/31658/2024).

Med stöd av *2 mom.* i paragrafen beviljar Transport- och kommunikationsverket på ansökan rätt till en ekonomisk aktör att bedriva verksamhet, det vill säga testning i en regulatorisk sandlåda. Inrättande eller förekomst av en regulatorisk sandlåda bildar således inte någon rätt för en ekonomisk aktör att ta i drift en sådan utan separat ansökan. De uppgifter som behövs för behandlingen ska läggas fram i ansökan. Transport- och kommunikationsverket ska på ansökan bevilja rätt att bedriva verksamhet i en regulatorisk sandlåda, såvida en i momentet avsedd grund för att inte bevilja en sådan rätt föreligger. Transport- och kommunikationsverket ska behandla de ekonomiska aktörerna jämlikt, så som 6 § i förvaltningslagen förutsätter.

Den informativa hänvisningen i paragrafens *3 mom.* redogör för att Transport- och kommunikationsverket i enlighet med artikel 33.2 i cyberresiliensförordningen har en skyldighet att ge information om inrättandet av en regulatorisk sandlåda till Europeiska kommissionen och till övriga marknadskontrollmyndigheter via samarbetsgruppen. Dessutom innehåller paragrafen bestämmelser om verkets uppgift att övervaka och styra verksamheten i en regulatorisk sandlåda. Om cyberresiliensen för AI-system med hög risk testats, får den myndighet som ansvarar för marknadskontrollen av systemet delta i styrningen av verksamheten i den regulatoriska sandlådan inom ramen för dess befogenheter och resurser, men förslaget innehåller inte någon skyldighet till detta. Avsikten är att utfärda bestämmelser om uppgifterna för de myndigheter som ansvarar för marknadskontrollen av AI-system i lagen om tillsyn över vissa system för artificiell intelligens.

Med stöd av paragrafens *4 mom.* kan närmare bestämmelser om den tekniska organiseringen av och verksamheten hos regulatoriska sandlådor för cyberresiliens samt om ansökan av en ekonomisk aktör utfärdas genom föreskrift av Transport- och kommunikationsverket.

**3 kap. – Anmälda organ**

**11 §.** *Anmälande myndighet.* Det föreslås att paragrafen innehåller bestämmelser om uppgiften för den i artikel 36 i cyberresiliensförordningen avsedda myndigheten som ansvarar för anmälan, vilken tilldelas Transport- och kommunikationsverket. Den anmälande myndigheten har till uppgift att sköta de uppgifter som föreskrivits för den i kapitel IV i cyberresiliensförordningen. Den anmälande myndigheten ansvarar således för att upprätta och genomföra de behövliga förfarandena, som gäller bedömningen, utseendet och anmälan i anknytning till organen för bedömning av överensstämmelse samt att övervaka dessa. I enlighet med artikel 41 i cyberresiliensförordningen omfattar uppgifterna även att övervaka anmälda organ då de anlitar underleverantörer eller dotterbolag. Den anmälande myndigheten ansvarar även för att anmäla de uppgifter som avses i artikel 35.1, artikel 38.1 och artikel 46.2 i cyberresiliensförordningen till kommissionen och till övriga medlemsstater då medlemsstaten har en skyldighet att anmäla dessa. Den anmälande myndigheten ska i verksamheten uppfylla de krav som föreskrivs i artikel 37 i cyberresiliensförordningen.

**12 §.** *Ansökan om anmälan.* Med stöd av paragrafen adresseras en ansökan som gäller anmälan som ett anmält organ enligt cyberresiliensförordningen till den anmälande myndigheten, det vill säga till Transport- och kommunikationsverket. Ett organ för bedömning av överensstämmelse

som inte är etablerat i Finland ska i enlighet med artikel 42.1 i cyberresiliensförordningen ansöka om anmälan från den medlemsstat där organet för bedömning är etablerat.

De uppgifter som avses i artikel 42 i cyberresiliensförordningen ska fogas till ansökan. Dessa uppgifter är en beskrivning av åtgärderna för att bedöma överensstämmelse, förfarandet eller förfarandena för bedömning av överensstämmelse och av en eller flera produkter med digitala element för vilka organet anser sig vara kompetent samt från fall till fall ett ackrediteringsintyg, som det nationella ackrediteringsorganet har utfärdat, i vilket det styrks att organet för bedömning av överensstämmelse uppfyller de krav som föreskrivits i artikel 39 i cyberresiliensförordningen. Med stöd av 2 a § i lagen om Säkerhets- och kemikalieverket (1261/2010) verkar Säkerhets- och kemikalieverkets ackrediteringsenhet (ackrediteringstjänsten FINAS) som nationellt ackrediteringsorgan i Finland.

Fogande av ett ackrediteringsintyg till ansökan är avsett som det huvudsakliga och primära förfarandet vid en ansökan om utseende till anmält organ. Cyberresiliensförordningen innehåller dock även bestämmelser om ett alternativt förfarande som kan tillämpas om det exceptionellt inte är möjligt att skaffa ett ackrediteringsintyg. Om man till ansökan inte kan foga ett ackrediteringsintyg från ackrediteringstjänsten FINA över att ett organ för bedömning av överensstämmelse uppfyller kraven i cyberresiliensförordningen, ska organet för bedömning av överensstämmelse i enlighet med artikel 42.3 i cyberresiliensförordningen till Transport- och kommunikationsverket överlämna alla behövliga underlag som möjliggör kontroll, erkännande och regelbunden tillsyn över att det uppfyller de krav som föreskrivits i artikel 39 i cyberresiliensförordningen.

**13 §.** *Utseende av ett anmält organ samt begränsning eller återkallelse av ett utseende.* Med stöd av paragrafens *1 mom.* utser Transport- och kommunikationsverket på ansökan ett organ för bedömning av överensstämmelse till ett anmält organ, om det uppfyller kraven enligt cyberresiliensförordningen i fråga om kompetensområde. En ytterligare förutsättning för att sköta uppgifterna för ett anmält organ är att inga invändningar enligt artikel 43.5 i cyberresiliensförordningen har gjorts. Det föreslås att ett organ för bedömning av överensstämmelse utses till ett anmält organ för att bedöma överensstämmelsen för de produkter med digitala element för vilka organet för bedömning har ansökt om anmälning och påvisat att det uppfyller kraven. Den finns bestämmelser om anmälningsförfarandet i artikel 43 i cyberresiliensförordningen. Det finns bestämmelser om kraven på anmälda organ i artikel 39 i cyberresiliensförordningen.

Paragrafens *2 mom.* innehåller bestämmelser om innehållet i ett beslut om utseende av ett anmält organ. Vid sidan om vad som bestäms i 44 § i förvaltningslagen ska beslutet ange kompetensområdet för bedömningsorganet och fastställa tillsynsarrangemangen. I beslutet är det dessutom möjligt att vid behov ställa krav, begränsningar och villkor i fråga om organets verksamhet, med vilka det säkerställs att uppgifterna enligt cyberresiliensförordningen utförs på ett ändamålsenligt sätt.

Paragrafens *3 mom.* innehåller en informativ hänvisning till bestämmelserna i artikel 45 i cyberresiliensförordningen om begränsning och återkallelse av ett beslut om utseende till anmält organ.

Med stöd av paragrafens *4 mom.* tillämpas på personer anställda vid ett anmält organ och ett dotterbolag och en underleverantör som organet använder bestämmelserna om straffrättsligt tjänsteansvar när personal utför i cyberresiliensförordningen avsedda uppgifter som hör till ett anmält organ. Bestämmelsen behövs, eftersom skötseln av uppgifterna handlar om en offentlig förvaltningsuppgift. Momentet innehåller även en informativ hänvisning till skadeståndslagen.

Dessutom ska ett anmält organ eller ett dotterbolag eller en underleverantör som det använder, då det sköter en offentlig förvaltningsuppgift, iaktta de allmänna förvaltningslagarna, det vill säga förvaltningslagen (434/2003), lagen om offentlighet i myndigheters verksamhet (621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003), lagen om informationshantering inom den offentliga förvaltningen (906/2019) och lagen om om tillhandahållande av digitala tjänster (306/2019) även utan uttrycklig hänvisning till de allmänna lagarna. Det finns bestämmelser om möjligheten för ett anmält organ att lägga ut uppgifter på underentreprenad eller att anlita ett dotterbolag i artikel 41.

**14 §.** *Den anmälande myndighetens och anmälda organs rätt att lämna ut sekretessbelagd information.* Paragrafen innehåller bestämmelser om den anmälande myndighetens och anmälda organs rätt att lämna ut information då det behövs för att utföra de uppgifter som tilldelats dem med stöd av cyberresiliensförordningen.

I paragrafens *1 mom.* föreskrivs rätten för den anmälande myndigheten att lämna ut en handling som den fått eller upprättat samt röja sekretessbelagd information om grunderna för anmälan av organ för bedömning av överensstämmelse och om dess övriga kompetens, om det behövs för att fullgöra den anmälande myndighetens skyldigheter enligt cyberresiliensförordningen. Det handlar främst om affärshemligheter eller andra näringshemligheter som gäller organ för bedömning av överensstämmelse. Det är behövligt att lämna ut sekretessbelagd information till exempel i en sådan situation som avses i artikel 43.4 i cyberresiliensförordningen, där anmälningen av organet baserar sig på någon annan utredning än ett ackrediteringsintyg. I så fall ska den anmälande myndigheten till kommissionen och de andra medlemsstaterna överlämna underlag, med vilka det är möjligt att bevisa att ett organ för bedömning av överensstämmelse har kompetens och använder arrangemang med vilka det kan säkerställas att organet övervakas regelbundet och att det fortfarande uppfyller de krav som föreskrivs i artikel 39. Det är sannolikt behövligt att lämna ut sekretessbelagd information även i en situation där ett anmält organs kompetens bestrids i enlighet med artikel 46 i cyberresiliensförordningen. I så fall ska den medlemsstat som gjort anmälan, det vill säga den anmälande myndigheten med stöd av 11 § 2 mom. i enlighet med artikel 46.2 i cyberresiliensförordningen på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

I paragrafens *2 mom.* föreskrivs å sin sida rätten för ett anmält organ att lämna ut eller röja en handling eller information som den fått eller upprättat och som gäller bedömning av överensstämmelse och resultaten av kontroller till Europeiska kommissionen, medlemsstater i Europeiska unionen och andra anmälda organ, om det behövs för att fullgöra det anmälda organets skyldigheter enligt cyberresiliensförordningen. I en sådan situation handlar det i regel om affärshemligheter för tillverkaren i anknytning till den bedömda produkten eller andra sekretessbelagda uppgifter som gäller produkten. En förutsättning för att lämna ut information är att de behövs för att fullgöra en skyldighet för ett anmält organ vilken föreskrivits med stöd av cyberresiliensförordningen. Det kan vara behövligt att lämna ut information för att fullgöra skyldigheten för ett anmält organ enligt artikel 49.2 i cyberresiliensförordningen. Enligt den ska de anmälda organen ge de andra organ som anmälts enligt denna förordning, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter med digitala element, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse. Dessutom har ett anmält organ en skyldighet att överlämna kopior av den tekniska dokumentationen i anknytning till EU-typkontrollen och resultaten av kontroller som gjorts av det anmälda organet till kommissionen eller en annan medlemsstat med stöd av punkt 9 i del II i bilaga VIII till cyberresiliensförordningen.

**4 kap. – Marknadskontroll**

**15 §.** *Marknadskontrollmyndighet*. Paragrafen innehåller bestämmelser om uppgiften som marknadskontrollmyndighet enligt cyberresiliensförordningen. I Finland fungerar i regel Transport- och kommunikationsverket som marknadskontrollmyndighet för kraven enligt cyberresiliensförordningen i fråga om de produkter med digitala element som omfattas av förordningens tillämpningsområde. Marknadskontrollmyndigheten ansvarar för de uppgifter som den tilldelas i cyberresiliensförordningen. Marknadskontrollmyndighetens uppgifter och befogenheter föreskrivs dessutom i marknadskontrollförordningen och marknadskontrollagen.

**16 §.** *Marknadskontroll av AI-system med hög risk*. Paragrafen innehåller bestämmelser om marknadskontrollen av produkter med digitala element då en produkt är ett AI-system med hög risk enligt förordningen om artificiell intelligens. Med avvikelse från vad som föreskrivs i 15 § ovan utgörs marknadskontrollmyndigheten för AI-system med hög risk även i fråga om kraven i cyberresiliensförordningen av den myndighet som övervakar AI-system hög risk med stöd av 3 § i lagen om tillsyn över vissa system för artificiell intelligens.

Artikel 52.14 i cyberresiliensförordningen förutsätter att till den del det handlar om AI-system med hög risk enligt EU:s förordning om artificiell intelligens (EU) 2024/1689, ska produkterna med stöd av förordningen om artificiell intelligens övervakas av den behöriga myndigheten även i fråga om kraven enligt cyberresiliensförordningen. Denna fråga är inte förenad med något nationellt handlingsutrymme. På grund av detta fungerar den behöriga myndigheten enligt 3 § i lagen om tillsyn över vissa system för artificiell intelligens som marknadskontrollmyndighet för AI-system med hög risk, till den del som de omfattas av kraven i cyberresiliensförordningen.

Artikel 52.15 i cyberresiliensförordningen innehåller bestämmelser om inrättande av en Adco-grupp. Adco-gruppen består av företrädare för de utsedda marknadskontrollmyndigheterna och, om så är lämpligt, företrädare för de centrala samordningskontoren. Representanten till Adco-gruppen utnämns av Transport- och kommunikationsverket, eftersom marknadskontrolluppgiften samlas till den, med undantag för undantaget i 16 §. I det fallet att det är möjligt att utnämna flera än en representant från Finland till samarbetsgruppen, är det möjligt att utnämna även en marknadskontrollmyndighet enligt 16 § som representant, om det är ändamålsenligt för marknadskontrollen enligt cyberresiliensförordningen.

**17 §.** *Expertstöd för marknadskontroll*. Det föreslås att paragrafen innehåller bestämmelser om tillhandahållande av expertstöd från Transport- och kommunikationsverket till en annan myndighet för marknadskontrollen och påförandet av en administrativ påföljdsavgift. Transport- och kommunikationsverket kan på begäran ge expertstöd som gäller marknadskontroll, bedömning av överensstämmelse och bedömning av cybersäkerhetsrisker enligt cyberresiliensförordningen till de marknadskontrollmyndigheter som avses i 16 § samt till den som är behörig att påföra påföljdsavgifter enligt 6 kap. Stöd kan således ges till en annan myndighet i praktiken för marknadskontrollen av AI-system med hög risk eller påförande av en administrativ påföljdsavgift som hänför sig till dessa.

Möjligheten att använda experthjälp behövs i praktiken för att säkerställa att man i kontrollen förmår iaktta enhetliga grunder för att bedöma produkternas överensstämmelse. Karaktären på experthjälpen kan vara till exempel informativt eller tekniskt stöd för bedömningar av överensstämmelsen samt stöd för att rikta kontrollåtgärderna. Stödet kan gälla det förfarande som avses i artikel 54 i cyberresiliensförordningen, där en eventuell betydande cybersäkerhetsrisk enligt artikel 54 i cyberresiliensförordningen bedöms. Den föreslagna lagens 18 § innehåller bestämmelser om informationsutbytet i anknytning till expertstöd.

På samarbetet mellan marknadskontrollmyndigheterna tillämpas i övrigt vad som bestäms i marknadskontrollagen, marknadskontrollförordningen och cyberresiliensförordningen.

**18 §.** *Marknadskontrollmyndighetens rätt att lämna ut sekretessbelagd information.* Paragrafen innehåller bestämmelser om den rätt att lämna ut sekretessbelagd information vilken förutsätts för marknadskontrollen enligt cyberresiliensförordningen.

Bestämmelserna tillämpas som specialbestämmelser utöver vad som annanstans i lagen bestäms om rätten att lämna ut information för marknadskontrollmyndigheten. Marknadskontrollagens 11 § innehåller bestämmelser bland annat om rätten för marknadskontrollmyndigheten att lämna ut information till Tullen och 13 § i marknadskontrollagen innehåller bestämmelser om rätten att lämna ut information till vissa andra finländska och utländska myndigheter och till internationella organ. De uppgiftstyper som räknats upp i marknadskontrollagen (uppgifter om ett företags och en sammanslutnings ekonomiska ställning, affärshemligheter och en enskild persons personliga förhållande) är inte tillräckliga för det samarbete som cyberresiliensförordningen förutsätter (se avsnitt 3.1.2), även om utlämnande av även dessa uppgifter blir aktuellt. I paragrafens kompletteras dessa bestämmelser genom att utfärda en bestämmelse om rätten att lämna ut även vissa andra uppgifter och om utlämnandet av uppgifter till sådana myndigheter som inte nämns i marknadskontrollagen.

I paragrafens *1 mom.* utvidgas de uppgiftstyper som med stöd av 11 och 13 § i marknadskontrollagen omfattas av rätten att lämna ut information att även gälla information om överensstämmelse, säkerhetsarrangemang och sårbarhet i fråga om produkter med digitala element och uppgifter om incidenter som påverkar dataskyddet. Dessa uppgifter kan vara sekretessbelagda i synnerhet i egenskap av i 24 § 1 mom. 7 punkten i offentlighetslagen avsedda handlingar som gäller säkerhetsarrangemangen i informations- och kommunikationssystem och som påverkar genomförandet av dessa. Dessa uppgifter är i princip sekretessbelagda utifrån sekretesspresumtionen. Det är nödvändigt att inkludera uppgifterna i informationsutbytet, eftersom skyldigheterna i cyberresiliensförordningen hänför sig till dessa uppgifters föremål. Marknadskontrollmyndigheten kan lämna ut information på eget initiativ eller på begäran.

Paragrafens *2 mom.* innehåller bestämmelser om marknadskontrollmyndighetens rätt att lämna ut sekretessbelagd information till de instanser som avses i 1–6 punkten och med vilka det är behövligt för marknadskontrollmyndigheten att samarbeta för att fullgöra dess föreskrivna uppgifter, men vilka inte ingår i 11 och 13 § i marknadskontrollagen. Marknadskontrollmyndigheten kan lämna ut information på eget initiativ eller på begäran.

Momentets *1 punkt* innehåller bestämmelser om utlämnande av information till ackrediteringstjänsten FINAS, om utlämnandet av information är nödvändigt för att bedöma kompetensen för organ för bedömning av överensstämmelse. Enligt artikel 5.3 om ackreditering i NLF-förordningen ska de nationella ackrediteringsorganen övervaka de organ för bedömning av överensstämmelse till vilka det utfärdat ett ackrediteringsintyg. I punkt 4 i artikeln föreskrivs att om ett nationellt ackrediteringsorgan bedömer att ett organ för bedömning av överensstämmelse som erhållit ett ackrediteringsintyg inte längre har nödvändig kompetens för att bedriva specifik verksamhet inom bedömning av överensstämmelse, eller allvarligt underlåtit att uppfylla sina skyldigheter, ska ackrediteringsorganet inom rimlig tid vidta alla lämpliga åtgärder för att begränsa, eller tillfälligt eller helt återkalla ackrediteringsintyget.

Momentets *2 punkt* innehåller bestämmelser om utlämnande av uppgifter till den nationella myndigheten för cybersäkerhetscertifiering, om utlämnandet av information är nödvändigt för att myndigheten i fråga ska kunna utföra sina tillsynsuppgifter. Marknadskontrollmyndigheterna ska enligt artikel 52.4 i cyberresiliensförordningen när så är

lämpligt samarbeta med de nationella myndigheter för cybersäkerhetscertifiering som utsetts med stöd av cybersäkerhetsakten och regelbundet utbyta information med dessa. Med stöd av 21 § i den föreslagna lagen fortsätter Transport- och kommunikationsverket med uppgiften. Information kan därtill lämnas ut till en myndighet som sköter en motsvarande uppgift i en annan medlemsstat. På det föreslagna sättet kan det vara nödvändigt att lämna ut information till exempel om det i kontrollen framkommer en incident som gäller cybersäkerhetscertifieringen, mot vilken myndigheten för cybersäkerhetscertifiering ska rikta kontrollåtgärder.

Momentets *3 punkt* innehåller bestämmelser om utlämnande av information till en sådan tillsynsmyndighet som avses i 26 § i cybersäkerhetslagen och 18 h § i lagen om informationshantering inom den offentliga förvaltningen (906/2019), Finansinspektionen eller en motsvarande myndighet i en annan medlemsstat, om en produkt med digitala element med fog kan bedömas utgöra en betydande cybersäkerhetsrisk på grund av icke-tekniska riskfaktorer. Detta hänvisar till en situation enligt artikel 54.2 i cyberresiliensförordningen. I den föreskrivs att om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, med stöd av artikel 8 i NIS 2-direktivet underrätta den utsedda eller inrättade behöriga myndigheten om detta samt vid behov föra samarbete med dessa myndigheter. Nationellt utgörs de behöriga myndigheterna enligt artikel 8 i NIS 2-direktivet av tillsynsmyndigheterna enligt 26 § i cybersäkerhetslagen och 18 h § i informationshanteringslagen samt Finansinspektionen med stöd av 50 p § i lagen om Finansinspektionen (878/2008). Utlämnandet av sekretessbelagda information ska vara nödvändigt för att fullgöra anmälningsskyldigheten enligt artikel 54.2 i cyberresiliensförordningen.

Momentets 4 punkt innehåller för det första bestämmelser om utlämnandet av information till Europeiska unionens cybersäkerhetsbyrå (Enisa) och CSIRT-enheten, som verkar vid Transport- och kommunikationsverkets Cybersäkerhetscenter, om det är nödvändigt för att fullgöra en samarbetsskyldighet eller genomföra rådgivning eller en utredning enligt artiklarna 52.4, 52.5 och 54.1 i cyberresiliensförordningen. Dessutom innehåller momentet bestämmelser om utlämnande av information till CSIRT-enheten, om det är nödvändigt för att utföra de uppgifter som CSIRT-enheten ska utföra enligt cybersäkerhetslagen.

I artikel 52.4 i cyberresiliensförordningen föreskrivs att när det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 14 i cyberresiliensförordningen, ska de utsedda marknadskontrollmyndigheterna samarbeta och regelbundet utbyta information med de CSIRT-enheter som utsetts till samordnare och med Enisa. Enligt artikel 52.5 i cyberresiliensförordningen får marknadskontrollmyndigheterna be en CSIRT-enhet som utsetts till samordnare eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av denna förordning När marknadskontrollmyndigheterna gör en undersökning enligt artikel 54 kan de begära den CSIRT-enhet som utsetts till samordnare eller Enisa att lägga fram en analys till stöd för bedömningarna av överensstämmelsen för produkter med digitala element.

Artikel 54 i cyberresiliensförordningen innehåller bestämmelser om förfaranden på nationell nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk. I punkt 1 i artikeln föreskrivs att om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning.

För det andra innehåller punkten bestämmelser om rätten att lämna ut information även i andra fall till CSIRT-enheten i det fallet att det är nödvändigt för skötseln av de uppgifter som föreskrivits för den i cybersäkerhetslagen. Med tanke på de uppgifter som föreskrivits för CSIRT-enheten i cybersäkerhetslagen kan utlämnande av information vara nödvändigt till exempel för att föra en lägesbild av cybersäkerheten, ge en tidig varning, för sårbarhetssamordningen eller för sårbarhetskartläggningen. Rätten att lämna ut information handlar till denna del om en bestämmelse som förbättrar det nationella samarbetet och utbytet av information, vilken marknadskontrollen enligt cyberresiliensförordningen inte direkt förutsätter. Sannolikt är det dock möjligt att marknadskontrollmyndigheten upptäcker eller i sitt uppdrag tar emot uppgifter som är nödvändiga för att sköta de uppgifter för CSIRT-enheten vilka föreskrivs i 20 § i lagen om cybersäkerhet. Det kan till exempel handla om uppgifter som är behövliga för att föra en lägesbild över cybersäkerheten till exempel i situationer där skyldigheterna i cyberresiliensförordningen fullgjorts bristfälligt, vilka marknadskontrollmyndigheten anser att CSIRT-enheten ska underrättas om, eller till exempel om sårbarhets- och hotuppgifter som kommit till marknadskontrollmyndighetens kännedom och som behövs för att sköta CSIRT-enhetens uppgift som gäller sårbarhetssamordning eller för att ge en tidig varning eller uppgifter som gör att CSIRT-enheten kan genomföra en sårbarhetskartläggning. Genom bestämmelsen stöds samarbetet och utbytet av information mellan de nationella myndigheterna med tanke på cyberincidenter.

Paragrafens *5 punkt* innehåller bestämmelser om utlämnande av information till dataombudsmannen, om det är nödvändigt att lämna ut informationen för skötseln av dataombudsmannens lagstadgade tillsynsuppgifter. Enligt artikel 52.7.1 i cyberresiliensförordningen ska marknadskontrollmyndigheterna vid behov samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddsrätt. I detta samarbete ingår att underrätta dessa myndigheter om alla iakttagelser av betydelse för deras fullgörande av sina befogenheter, inbegripet utfärdande av vägledning och råd enligt artikel 52.10 om vägledningen och råden rör behandling av personuppgifter. Punkten möjliggör att information lämnas ut på eget initiativ i dessa fall. Utlämnandet av information ska avgränsas till det som är nödvändigt med tanke på informationen om observationer. Dataombudsmannen ska ha rätt att begära även andra uppgifter i anknytning till ärendet enligt vad som bestäms nedan.

Momentets *6 punkt* innehåller bestämmelser om utlämnande av nödvändig information för tillsynen av konkurrenslagstiftningen till Europeiska kommissionen, Konkurrens- och konsumentverket eller den nationella konkurrensmyndigheten i en annan medlemsstat i Europeiska unionen. I artikel 52.13 i cyberresiliensförordningen föreskrivs att de utsedda marknadskontrollmyndigheterna utan dröjsmål till kommissionen och berörda nationella konkurrensmyndigheter ska rapportera all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrensrätt.

Paragrafens *3 mom.* innehåller bestämmelser om utbyte av information mellan en i 17 § avsedd myndighet som begär och tar emot expertstöd. Myndigheterna kan utan hinder av sekretessplikterna lämna ut information som är nödvändig för expertstödet till varandra. Tillhandahållande av expertstöd är en separat uppgift i förhållande till Transport- och kommunikationsverkets tillsynsuppgift, varför det för klarhetens skull finns ett behov av att utfärda separata bestämmelser om rätten att lämna ut information även för tillhandahållandet av expertstöd.

**19 §.** *Marknadskontrollmyndighetens rätt att utföra inspektioner och ta programvaror för undersökning*. Det föreslås att paragrafens *1 mom.* innehåller bestämmelser om marknadskontrollmyndighetens rätt att göra inspektioner i utrymmen som används för boende

av permanent natur och som en ekonomisk aktör använder för syfte i anknytning till dess närings- eller yrkesverksamhet. Bestämmelsen kompletterar bestämmelsen om marknadskontrollmyndighetens inspektionsrätt i 9 § i marknadskontrollagen, vilken till övriga delar tillämpas på marknadskontrollmyndighetens rätt att göra inspektioner. Marknadskontrollagens 9 § 2 mom. förutsätter att separata bestämmelser vid behov utfärdas om inspektion av utrymmen som används för boende av permanent natur.

Cyberresiliensförordningens tillämpningsområde omfattar produkter som kan utvecklas och tillverkas och i anknytning till vilka det i viss mån även är möjligt att bedriva verksamhet i hemfridsskyddade utrymmen vid sidan om företagets separata verksamhetslokaler. Närings- eller yrkesverksamhet som omfattas av cyberresiliensförordningens tillämpningsområde, såsom programvaruutveckling eller montering av enheter, kan bedrivas och det är även vanligt att sådan bedrivs i hemfridsskyddade utrymmen. I så fall är det möjligt att det uppkommer situationer där den enda möjligheten att göra en inspektion som gäller ett företag är att göra den i områden som i sig är hemfridsskyddade och som en ekonomisk aktör använder i sin näringsverksamhet, där de system och den dokumentation som används i verksamheten finns. Regleringen möjliggör därför att inspektionen utsträcks även till hemfridsskyddade utrymmen, då det är nödvändigt för att utreda omständigheter som är föremål för inspektionen.

En inspektion som omfattas av hemfridsskyddet är möjlig endast om den är nödvändig för att utreda omständigheter som är föremål för inspektionen, det vill säga att myndigheten inte kan skaffa uppgifter som är nödvändiga för övervakningen med stöd av sin rätt att få uppgifter eller genom att göra inspektionen annanstans än i ett utrymme som används för boende av permanent natur.

Externa experter kan vid behov delta i en inspektion som hjälp till marknadskontrollmyndigheten på det sätt som föreskrivs i 14 § 2 mom. i marknadskontrollagen. En självständig inspektion av en extern expert är inte möjlig med stöd av bestämmelsen. Eftersom bestämmelsen innehåller en hänvisning till 9 § i marknadskontrollagen, handlar en inspektion av ett utrymme som används för boende av permanent natur på det sätt som avses i det nämnda momentet om en inspektion enligt marknadskontrollagen. På grund av hänvisningen blir även 39 § i förvaltningslagen tillämplig vid inspektioner enligt bestämmelsen.

I momentet förutsätts att myndigheten har motiverade och specificerade skäl att misstänka att det har skett eller sker en sådan överträdelse av bestämmelserna i cyberresiliensförordningen eller bestämmelser som utfärdats med stöd av den att påföljden kan vara en påföljdsavgift enligt den föreslagna lagen. Således får en inspektion utföras i ett utrymme som används för boende av permanent natur endast om myndigheten i förväg har ändamålsenliga grunder att misstänka att regleringen överträds. Överträdelsens allvar uttrycks av att det är möjligt att påföra en administrativ påföljdsavgift av straffkaraktär för den. Om det är uppenbart att den gärning som utreds inte leder till att någon påföljdsavgift påförs på grund av att den är ringa eller någon annan motsvarande orsak, kan inte heller någon inspektion göras. Proportionaliteten för inspektionen säkerställs dessutom av förutsättningen i momentet om att den misstänkta överträdelsen handlar om en produkt med digitala element eller en process i anknytning till den, såsom hanteringen av sårbarheter, överensstämmelse med kraven eller att det handlar om en situation som avses i artikel 57 i cyberresiliensförordningen, där produkten trots överensstämmelsen med kraven orsakar en avsevärd cybersäkerhetsrisk samt en annan i artikeln avsedd risk som ska hänföra sig till människornas hälsa eller säkerhet, efterlevnad av skyldigheter för att skydda de grundläggande fri- och rättigheterna enligt unionsrätten eller den nationella lagstiftningen, dataskyddet för centrala aktörer enligt NIS 2-direktivet eller andra aspekter som gäller skyddet av ett allmänt intresse. Således kan inspektionsrätten utövas i

hemfridsskyddade utrymmen endast i misstänkta fall av överträdelse som är allvarliga i den månen att dessa förutsättningar uppfylls.

Paragrafens 2 mom. innehåller enligt förslaget bestämmelser om upptagning för undersökning inom marknadskontrollen. Momentet innehåller en informativ hänvisning till marknadskontrollagen. Dessutom innehåller momentet bestämmelser om ett avgränsat undantag till skyldigheten enligt marknadskontrollagen att ersätta en produkt som tagits för undersökning till en ekonomisk aktör.

Marknadskontrollmyndighetens 10 § innehåller bestämmelser om marknadskontrollmyndighetens rätt att ta produkter för undersökning, om det behövs för kontrollen av produkternas överensstämmelse med kraven. Enligt 10 § 2 mom. i marknadskontrollagen ska marknadskontrollmyndigheten på yrkande från en ekonomisk aktör ersätta en produkt enligt gängse pris, förutsatt att det inte framgår att produkten inte överensstämmer med kraven. Eftersom även programvaruprodukter och produktlösningar för fjärrbehandling av data, inbegripet programvaru- och hårdvarukomponenter som släpps ut på marknaden oberoende av varandra, kan omfattas av tillämpningsområdet för cyberresiliensförordningen, lämpar sig behörigheten enligt marknadskontrollagen även för dessa. Om en programvaruprodukt tas för undersökning, orsakar detta för den ekonomiska aktören inte någon skada på grund av att det exemplar som tas för undersökning inte kan säljas jämfört med vad en fysisk produkt på motsvarande sätt kan orsaka, eftersom programvaruprodukter i regel är i digitalt format. Således ska marknadskontrollmyndigheten inte betala någon ersättning enligt 10 § i marknadskontrollen för tagande av en programvara för undersökning till en ekonomisk aktör, oberoende av om programvaran konstateras överensstämma med kraven. Bestämmelsen gäller inte för ersättning som tas ut av Tullen med stöd av 10 § 2 mom. i marknadskontrollagen.

**20 §.** *Tillsynsbeslut som meddelas en förvaltare av programvara med fri och öppen källkod*. Paragrafens *1 mom.* innehåller bestämmelser om möjligheten att ge en förvaltare av programvara med fri och öppen källkod ett åläggande förordnande om att inom utsatt tid avhjälpa brister i fullgörandet av dess skyldigheter enligt cyberresiliensförordningen Det finns bestämmelser om skyldigheterna för en förvaltare av programvara i artikel 24 i cyberresiliensförordningen (se avsnitt 2.1.3.3). Behovet av reglering som kompletterar marknadskontrollagen har bedömts i avsnitt 3.1.2. Det kan handla till exempel om en skyldighet att åtgärda en brist i de riktlinjer för cybersäkerhet som utarbetats av en förvaltare av programvara eller att göra en incidents- eller sårbarhetsanmälan som fattas. Genom skyldigheten är det även möjligt att effektivisera en myndighets begäran om att överlämna de dokumenterade riktlinjerna för cybersäkerheten vilka utarbetats av en förvaltare av programvara, om de inte överlämnas till den frivilligt, liksom en myndighets begäran om att föra det samarbete som cyberresiliensförordningen förutsätter för att lindra cybersäkerhetsriskerna i vissa fall, om begäran inte iakttas i övrigt.

Paragrafens *2 mom.* innehåller bestämmelser om möjligheten för tillsynsmyndigheten att förena ett beslut som den har fattat med vite. Bestämmelser om föreläggande och verkställande av vite finns i viteslagen.

## 5 kap. – Cybersäkerhetscertifiering

**21 §.** *Nationell myndighet för cybersäkerhetscertifiering*. I paragrafens *1 mom.* tilldelas uppgifterna enligt cybersäkerhetsakten för den nationella myndighet som utfärdar cybersäkerhetscertifiering till Transport- och kommunikationsverket, som även för närvarande sköter uppgiften med stöd av lagen om tjänster inom elektronisk kommunikation. Med stöd av

artikel 58 i cybersäkerhetsakten omfattar myndighetsuppgifterna att bemyndiga organ för bedömning av överensstämmelse, tillsyn och uppföljning, kontroll av överensstämmelse och utfärdande av cybersäkerhetscertifikat av hög assuransnivå.

På ett sätt som avviker från den svenskspråkiga versionen av cybersäkerhetsakten används i förslaget begreppet myndighet för cybersäkerhetscertifiering, vilket även i praktiken har tillägnats i myndighetens kommunikation. I den svenskspråkiga versionen av cybersäkerhetsakten används begreppet nationell myndighet som utfärdar cybersäkerhetscertifiering, även om denna myndighets uppgifter, utöver att utfärda europeiska cybersäkerhetscertifikat, i vissa fall även omfattar tillsynsverksamhet i anknytning till cybersäkerhetsakten. I förordningen krävs att dessa verksamheter avskiljs från varandra. Det begrepp som använts i den finskspråkiga versionen är ”kansallinen kyberturvallisuussertifioinnin myöntävä viranomainen”, medan ”national cybersecurity certification authority” används i den engelskspråkiga versionen. Det föreslagna begreppet redogör bättre än den svenskspråkiga versionen för att myndighetens uppgifter, utöver att utfärda europeiska cybersäkerhetscertifikat, omfattar tillsynsverksamhet i anknytning till cybersäkerhetsakten.

Paragrafens *2 mom.* innehåller på det sätt som förordningen förutsätter bestämmelser om avskiljandet av utfärdandet av cybersäkerhetscertifikat och tillsynsverksamheten i anknytning till cybersäkerhetsakten. Enligt förordningen ska medlemsstaterna 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.

Transport- och kommunikationsverket ska organisatoriskt ordna sin verksamhet så att beslutsfattandet i anknytning till utfärdande av cybersäkerhetscertifikat har avskilts från beslutsfattandet i anknytning till cybersäkerhetscertifieringen på så sätt att samma personer inte kan rikta administrativ handledning såväl på utfärdande av certifikat som på kontrollverksamheten. I praktiken kan uppgifterna tilldelas de enheter som verkar vid de olika avdelningarna vid Transport- och kommunikationsverkets Cybersäkerhetscenter. Detta hindrar dock inte att myndighetspersonalens expertis utnyttjas i olika uppgifter.

Cybersäkerhetsakten och föreslagna 24 § möjliggör att uppgiften att delegera utfärdandet av certifikat av hög assuransnivå hos myndigheten för cybersäkerhetscertifiering delegeras till organet för bedömning av överensstämmelse. Enligt tolkningen av Europeiska gruppen för cybersäkerhetscertifiering utgör ett förhandsgodkännande enligt artikel 56.6 a i cybersäkerhetsakten, vilket getts av en myndighet för utfärdande av enskilda certifikat till organ för bedömning av överensstämmelse, utfärdande av certifiering, som ska avskiljas från tillsynsmyndighetens verksamhet. Allmän delegering i förväg enligt artikel 56.6 b i förordningen är inte lika problematiskt i förhållande till skötseln av tillsynsuppgifter, eftersom myndigheten inte spelar någon roll i utfärdandet av certifikat. Även till denna del är det möjligt att anse att delegeringen organisatoriskt sett är en naturligare del av utfärdandet av certifikat, med den skillnaden att det i fråga om anmälning och bemyndigande av ett bedömningsorgan och tillsynsuppgifterna i princip finns möjlighet att pröva om man överhuvudtaget ska delegera uppgifterna och till vilka organ för bedömning av överensstämmelse de delegeras. Myndigheternas tillsynsuppgifter omfattar å sin sida på entydigt sätt den i artikel 58.7 f i cybersäkerhetsakten nämnda behandlingen av klagomål som gjorts av utomstående i anknytning till certifikat som utfärdats utifrån delegering av organ för bedömning av överensstämmelse.

**22 §.** *Anmälan och bemyndigande av organ för bedömning av överensstämmelse för cybersäkerhetscertifiering*. Paragrafens *1 mom.* är en informativ hänvisning till uppgiften för myndigheten för cybersäkerhetscertifiering att anmäla ett organ för bedömning av överensstämmelse till kommissionen för cybersäkerhetscertifiering efter att organet ackrediterats. På samma sätt som i 11 § i den föreslagna lagen i fråga om cyberresiliensförordningen utfärdas ackrediteringen av Säkerhets- och kemikalieverkets ackrediteringsenhet (ackrediteringstjänsten FINAS). En ytterligare förutsättning för anmälan är i vissa fall ett bemyndigande som getts av myndigheten för cybersäkerhetscertifiering till bedömningsorganet, vilket behövs vid fastställandet av särskilda krav eller tilläggskrav enligt artikel 54.1 f, vilka bedömningsorganet ska uppfylla. Sådana krav på bemyndigande kan ingå i de certifieringsordningar som kommissionen har godkänt. För närvarande förutsätter EUCC-genomförandeförordningen (kommissionens genomförandeförordning (EU) 2024/482 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska ordningen för cybersäkerhetscertifiering (EUCC) som baserar sig på gemensamma kriterier) bemyndigande för utfärdande av certifikat av hög assuransnivå utifrån den.

På ackreditering och jämställbar kompetensbedömning tillämpas lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005). På de krav som gäller ett organ för bedömning av överensstämmelse tillämpas bilagan till förordningen med stöd av hänvisningen i artikel 60.1 i cybersäkerhetsakten. Det nationella ackrediteringsorganet utfärdar ackreditering endast om kraven uppfylls. Myndigheten för cybersäkerhetscertifiering har uppgifter enligt cyberresiliensförordningen och behörighet att övervaka att organen för bedömning av överensstämmelse iakttar kraven i förordningen. Dessutom följer ackrediteringsenheten bedömningsorganets kompetens och den kan dra in en ackreditering, om förutsättningarna för ackreditering inte längre är uppfyllda.

I paragrafens *2 mom.* föreskrivs att förutsättningen för anmälan och bemyndigande för cybersäkerhetscertifiering är att organet för bedömning av överensstämmelse av ackrediteringstjänsten FINAS har beviljats ett ackrediteringsintyg över att organet för bedömning av överensstämmelse uppfyller kraven i cybersäkerhetsakten. Den föreslagna ordalydelsen möjliggör att myndigheten för cybersäkerhetscertifiering kan inleda bedömningen i anknytning till bemyndigandet då ackrediteringsförfarandet fortfarande pågår, om myndigheten finner det motiverat.

**23 §.** *Skyldigheter för organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering*.

Paragrafens *1 mom.* innehåller bestämmelser om skyldigheten för ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering att utföra bedömningar av överensstämmelse på det sätt som förutsätts i fråga om förfarandena för bedömning av överensstämmelse enligt cyberresiliensförordningen och de rättsakter som getts med stöd av den, liksom även andra uppgifter som föreskrivits i ovan avsedda rättsakter. Förslaget motsvarar delvis 14 § 1 mom. i lagen om anmälda organ för vissa produktgrupper. Den nämnda lagen blir inte tillämplig på organ för bedömning av överensstämmelse som anmälts med stöd av cybersäkerhetsakten, varför det finns ett behov av att inkludera vissa bestämmelser om bedömningsorganens skyldigheter.

Paragrafens *2 mom.* innehåller bestämmelser om skyldigheten för ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering att till myndigheten för cybersäkerhetscertifiering anmäla alla ändringar som påverkar uppfyllandet av förutsättningarna för anmälan eller bemyndigande. Dessa förutsättningar föreskrivs i

cybersäkerhetsakten och i de certifieringsordningar som godkänts med stöd av den. I 25 § i lagförslaget föreskrivs rätten för myndigheten för cybersäkerhetscertifiering att få även andra uppgifter från organet för bedömning av överensstämmelse.

På ett sätt som motsvarar ovan nämnda situation i fråga om 13 §, innehåller paragrafens *3 mom.* bestämmelser om det straffrättsliga tjänsteansvaret med anledning av skötseln av en offentlig förvaltningsuppgift för en person anställd vid ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och vid ett dotterbolag och en underleverantör som organet använder. Dessutom innehåller momentet en informativ hänvisning till skadeståndslagen. På det sätt som nämns ovan i samband med motiveringarna till 13 § blir de allmänna förvaltningslagarna tillämpliga även utan separat hänvisning. I en bilaga till cybersäkerhetsakten (krav på organ för bedömning av överensstämmelse) finns det även krav som gäller användning av dotterbolag eller underleverantörer.

**24 §.** *Överföring av uppgifter i anslutning till utfärdande av cybersäkerhetscertifikat*. Paragrafens *1 mom.* innehåller bestämmelser om att myndigheten för cybersäkerhetscertifiering kan överföra, det vill säga delegera, utfärdandet av cybersäkerhetscertifikat av hög assuransnivå till ett organ för bedömning av överensstämmelse. Denna möjlighet regleras i artikel 56.5 i cybersäkerhetsakten, vilken möjliggör två olika delegeringssätt. Uppgiften kan överföras antingen så att myndigheten i förväg godkänner utfärdandet av varje enskilt certifikat separat eller allmänt i förväg så att organet för bedömning av överensstämmelse självständigt utfärdar de europeiska cybersäkerhetscertifikat som beviljas inom ramen för någon viss europeisk ordning för cybersäkerhetscertifiering. I bägge fall kan bedömningsorganet anses förfara självständigt och fatta beslut om beviljande i eget namn, det vill säga att det inte handlar om en myndighetsassisterande roll. En certifieringsordning som getts genom en genomförandeförordning av kommissionen kan ställa randvillkor på delegeringen eller förutsätta sådana. Till exempel artikel 17.4 i EUCC-genomförandeförordningen möjliggör endast ett förfarande där myndigheten godkänner varje enskild certifieringsprocess i förväg. I samband med 21 § ovan görs en granskning av avskiljandet av delegeringsuppgifterna hos myndigheten för cybersäkerhetscertifiering från tillsynsuppgifterna.

Det är möjligt att lagen om offentlig upphandling och koncession (1397/2016) från fall till fall blir tillämplig på upphandling av en tjänst från ett organ för bedömning av överensstämmelse i anknytning till överföringen av uppgiften. Om en myndighet för uppgiften godkänner alla organ för bedömning av överensstämmelse som uppfyller de lagstadgade förutsättningarna, handlar det inte om offentlig upphandling, varvid upphandlingslagstiftningen inte heller tillämpas (se på motsvarande sätt RP 108/2016 rd, s. 75). Om endast en del av organen för bedömning av överensstämmelse kan delta i utfärdandet av certifikat enligt lagförslag 1, kan situationen å sin sida komma att bedömas som en tjänstekoncession. I lagen om offentlig upphandling och koncession avses med tjänstekoncession ”ett sådant skriftligt avtal mot ett ekonomiskt vederlag genom vilket en eller flera upphandlande enheter överför tillhandahållandet och administreringen av andra tjänster än sådana som gäller byggkoncession och verksamhetsrisken i samband med den på en eller flera leverantörer, och där vederlaget för överföringen utgörs antingen av enbart rätten att utnyttja tjänsterna eller gemensamt av en sådan rätt och en betalning”. När en tjänsteleverantör tar en risk i anknytning till efterfrågan på tjänsten och certifieringsmyndigheten å sin sida drar nytta av att den inte behöver sköter uppgiften själv, kan definitionen uppfyllas.

Paragrafens *2 mom.* innehåller bestämmelser om omständigheter som åtminstone ska överenskommas i det avtal som ska ingås med ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering. Avtalet ska för det första innehålla en närmare beskrivning av de uppgifter som delegeras. Det är även möjligt att avgränsa uppgifterna

noggrannare än endast till ett visst certifieringssystem. För det andra är det möjligt att i avtalet inkludera de särskilda krav som myndigheten för cybersäkerhetscertifiering bedömt vara behövliga i fråga om kompetensen för organet för bedömning av överensstämmelse och säkerheten i dess verksamhet, såsom skötseln av dataskyddet och den fysiska säkerheten, om de krav som följer av den tillämpliga ordningen för cybersäkerhetscertifiering inte anses vara tillräckliga. För det tredje ska avtalet innehålla ett ställningstagande till avtalsperioden, inledandet av verksamheten och avslutande av avtalet under avtalsperioden, såsom den eventuella rätten för myndigheten eller bedömningsorganet att säga upp ett avtal om delegering mitt under avtalsperioden. För det fjärde ska avtalet innehålla ett omnämnande om förvaring och arkivering av handlingar i anslutning till verksamheten hos organet för bedömning av överensstämmelse i synnerhet med tanke på avtalets slut. För det femte ska avtalet innehålla en överenskommelse om påföljder för brister och försummelser i verksamheten hos organet för bedömning av överensstämmelse.

Behandling av personuppgifter eller avgifter nämns inte separat i momentet. Ett organ för bedömning av överensstämmelse anses fungera som självständig personuppgiftsansvarig till den del som skötseln av certifieringsuppgifter omfattar till exempel behandling av personuppgifter som gäller den som ansöker om ett certifikat. Syftet är att skötseln av den delegerade uppgiften finansieras med avgifter som organet för bedömning tar ut utifrån kommersiella grunder av de som ansöker som certifiering.

Enligt paragrafens *3 mom.* får myndigheten för cybersäkerhetscertifiering säga upp eller häva ett avtal om delegering, om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte längre uppfyller de allmänna kraven för bedömningsorganet eller om det väsentligt försummar fullgörandet av de uppgifter som överenskommits i avtalet eller annars bryter mot avtalet eller väsentligen eller upprepade gånger handlar lagstridigt. Förslaget möjliggör att delegering återkallas, om de delegerade uppgifterna försummas på väsentligt sätt eller om organet för bedömning inte längre är kvalificerat för sina uppgifter. Vid behov är det möjligt att rikta även tillsynsåtgärder på ett organ för bedömning av överensstämmelse i ett separat förfarande i enlighet med den föreslagna lagen, men återkallelse av delegering är i princip inte beroende av hur tillsynsprocessen framskrider.

**25 §.** *Rätt att få information och utföra inspektioner för myndigheten för cybersäkerhetscertifiering.* Paragrafens *1 mom.* innehåller bestämmelser om rätten att få information för myndigheten för cybersäkerhetscertifiering. Myndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av EU-försäkringar om överensstämmelse få den information som är nödvändig för skötseln av dess uppgifter enligt denna lag och cybersäkerhetsakten och för tillsynen över efterlevnaden av cybersäkerhetsakten, bestämmelser som utfärdats med stöd av den och denna lag. Uppgifterna ska lämnas ut utan obefogat dröjsmål, i den form som myndigheten begärt och avgiftsfritt.

Förslaget kompletterar artikel 58.8 a i cybersäkerhetsakten, enligt vilken myndigheten ska ha befogenheter att 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 (eng. ”requires”) för att kunna fullgöra sin uppgift. Uttrycket kan anses överensstämma med den föreslagna förutsättningen som gäller nödvändigheten.

De befogenheter som regleras i paragrafen förutsätter inte att det handlar om ett organ för bedömning av överensstämmelse som har anmälts för myndighetscertifiering, eftersom rätten

att få information gäller även för en situation där bedömningsorganet bara har ansökt om anmälan och å andra sidan även de situationer, där bedömningsorganet på begäran av medlemsstaten redan har avförts från den förteckning över anmälningar som kommissionen upprätthåller.

Den föreslagna paragrafens *2 mom.* innehåller bestämmelser om inspektionsrätten för myndigheten för cybersäkerhetscertifiering. I enlighet med artikel 58.7 b i cybersäkerhetsakten kan en inspektion göras hos organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare en EU-försäkran om överensstämmelse. Föremålet för inspektionen är omständigheter som anknyter till övervakningen av efterlevnaden av cybersäkerhetsakten, de akter som utfärdats med stöd av den och den föreslagna lagen. Det föreslås att vad som föreskrivs i 39 § i förvaltningslagen (434/2003) iakttas vid inspektioner.

Paragrafens *3 mom.* innehåller bestämmelser om rätten för myndigheten för cybersäkerhetscertifiering att låta en oberoende expert utföra en inspektion. Den som utför inspektionen och de som deltar i den ska ha sådan utbildning och erfarenhet som behövs för att utföra inspektionen. Det är möjligt att skaffa den erfarenhet som behövs till exempel genom att tjänstgöra för ett organ för bedömning av överensstämmelse. Momentet innehåller bestämmelser om det straffrättsliga tjänsteansvaret med en informativ hänvisning till skadeståndslagen.

Det föreslås att paragrafens *4 mom.* innehåller bestämmelser om att myndigheten för cybersäkerhetscertifiering och oberoende experter när de utför inspektionen har rätt att få tillträde till alla lokaler där verksamhet som avses i cybersäkerhetsakten bedrivs samt till alla lokaler och informationssystem där uppgifter som är av betydelse för tillsynen förvaras eller behandlas. Med uppgifter som behandlas i informationssystem avses till exempel ärendehanterings- och arkiveringssystem, där uppgifter om en produkt som varit föremål för bedömning av bedömningsorganet förvaras eller system hos innehavaren av cybersäkerhetscertifikatet, där man förvarar uppgifter om produkten. Inspektionen är inte avsedd att utsträckas till exempelvis e-postsystem eller andra liknande informationssystem som används för kommunikation mellan företagets personal, eftersom de uppgifter som behandlas i dessa generellt på det sätt som avses i bestämmelsen inte anses vara betydelsefulla för tillsynen över skyldigheterna enligt cybersäkerhetsakten.

I momentet föreskrivs att inspektioner dock inte får utsträckas till utrymmen som används för boende av permanent natur. Även om verksamhet som omfattas av cybersäkerhetsaktens tillämpningsområde kan utövas i utrymmen som används för boende av permanent natur och en cybersäkerhetsinnehavare kan vara en fysisk person, föreslås i propositionen i motsats till i fråga om 17 § ovan att inspektionen till denna del utsträcks till hemfridsskyddet. Till denna del anses cybersäkerhetsakten innehålla nationellt handlingsutrymme och därtill möjliggör regleringen att giltigheten för ett certifikat avbryts eller dras in i det fallet att certifikatinnehavaren inte fullgör sin informationsskyldighet. Således anses möjligheten att utsträcka inspektioner till hemfridsskyddet inte vara nödvändigt.

**26 §.** *Rätt för myndigheten för cybersäkerhetscertifiering att lämna ut sekretessbelagd information.* Det föreslås att paragrafen innehåller bestämmelser om rätten för myndigheten för cybersäkerhetscertifiering att lämna ut sekretessbelagd information på begäran eller på eget initiativ. Bestämmelserna i paragrafen tillämpas vid sidan om vad som bestäms i offentlighetslagen och i andra delar av lagen, varför det inte föreslås att bestämmelser utfärdas om utlämnande av information för till exempel förundersökning. Uppgiftstyperna specificeras inte, men i paragrafpunkterna har utlämnandet av information inte bundits till nödvändighet

med tanke på en viss uppgift. I praktiken kan informationen gälla till exempel ett samfunds affärshemligheter och skyddsarrangemangen för informations- och kommunikationssystem.

Paragrafens *1 punkt* innehåller bestämmelser om utlämnande av sekretessbelagd information för det första till marknadskontrollmyndigheten enligt 4 § i marknadskontrollagen. Förslaget behövs med anledning av artikel 58.7 a i cybersäkerhetsakten, eftersom den förutsätter tillsynssamarbete med de relevanta marknadskontrollmyndigheterna. Även i artikel 28.2 i EUCC-genomförandeförordningen förutsätts att myndigheten för cybersäkerhetscertifiering anmäler överensstämmelse med kraven till marknadskontrollmyndigheten. Likaså förutsätter led h i denna punkt informationsutbyte med övriga myndigheter om eventuella fall, där de certifierade nyttigheterna inte svarar mot kraven i förordningen eller enskilda europeiska ordningar för cybersäkerhetscertifiering. För det andra möjliggör punkten utlämnande av uppgifter till Säkerhets- och kemikalieverkets ackrediteringsenhet eller till en annan medlemsstats nationella ackrediteringsorgan, om utlämnande av uppgiften är nödvändigt för att utföra den aktuella myndighetens uppgifter. Detta förslag behövs på grund av artikel 58.7 c i cybersäkerhetsakten, eftersom den förutsätter att myndigheten biträder och stödjer de nationella ackrediteringsorganen.

Paragrafens *2 punkt* innehåller å sin sida bestämmelser om utlämnande av information till andra nationella myndigheter för cybersäkerhetscertifiering, andra medlemmar i Europeiska gruppen för cybersäkerhetscertifiering, Europeiska unionens cybersäkerhetsbyrå Enisa och Europeiska kommissionen, om det är nödvändigt för att fullgöra en skyldighet som myndigheten för cybersäkerhetscertifiering har enligt cybersäkerhetsakten eller med stöd av den. Till denna del kompletterar den föreslagna bestämmelsen i synnerhet artikel 58.7 g och 58.7 h samt artikel 58.9, vilka gäller samarbetet med Enisa, kommissionen, Europeiska gruppen för cybersäkerhetscertifiering och andra nationella myndigheter som utfärdar cybersäkerhetscertifiering. Till exempel artikel 38 i EUCC-genomförandeförordningen förutsätter att myndigheten för cybersäkerhetscertifiering delar vissa uppgifter om sårbarheter med andra nationella myndigheter för cybersäkerhetscertifiering och med Enisa. Dessutom kan utlämnande av information vara behövligt i samband med kollegial bedömning enligt artikel 59 i cybersäkerhetsakten.

Paragrafens *3 punkt* innehåller å sin sida bestämmelser om utlämnande av vissa uppgifter till den tillsynsmyndighet som avses i 26 § i cybersäkerhetslagen och 18 h § i lagen om informationshantering inom den offentliga förvaltningen, Finansinspektionen och CSIRT-enheten, om utlämnandet är nödvändigt för skötseln av deras lagstadgade uppgifter. Det finns bestämmelser om Finansinspektionens uppgifter i anknytning till cybersäkerhet i lagen om Finansinspektionen och i den så kallade DORA-förordningen (Europaparlamentets och rådets förordning (EU) 2022/554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011). Punkten kompletterar artikel 58.7 h i cybersäkerhetsakten, enligt vilken myndigheten för cybersäkerhetscertifiering ska 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. Dessa uppgifter liksom sårbarhetsuppgifter om dessa kan vara behövliga till exempel för en uppgift som gäller bevakningen av cyberhot vid CSIRT-enheten, vilken föreskrivits i cybersäkerhetslagen. Uppgifter om brister i en certifierad produkt eller tjänst kan vara behövliga även med tanke på övervakningen av efterlevnaden av riskhanteringsskyldigheterna enligt cybersäkerhetslagen eller DORA-förordningen för användarna av dessa.

**27 §.** *Tillsynsbeslut.* Paragrafens *1 mom.* innehåller bestämmelser om befogenheten för myndigheten för cybersäkerhetscertifiering att meddela ett förpliktande beslut för att avhjälpa verksamhet som strider mot skyldigheterna enligt den föreslagna lagen eller cybersäkerhetsakten eller de bestämmelser som utfärdats med stöd av den, såsom kraven enligt den tillämpliga europeiska ordningen för cybersäkerhetscertifiering. Genom ett beslut kan myndigheten ålägga ett organ för bedömning av överensstämmelse, innehavaren av ett europeiskt cybersäkerhetscertifikat eller en utfärdare av EU-försäkringar om överensstämmelse att inom utsatt tid avhjälpa en brist, om fel, försummelser eller andra brister i fullgörandet av de föreskrivna skyldigheterna upptäcks i tillsynen. Myndigheten kan till exempel ålägga en aktör att avhjälpa de observerade bristerna eller försummelserna, avsluta verksamhet i strid med regleringen och att avhålla sig från sådan verksamhet framöver samt förordna att aktören uppfyller sin skyldighet att lämna ut information på det förordnade sätt och inom den föreskrivna tiden.

Paragrafens *2 mom.* innehåller bestämmelser om möjligheten för myndigheten för cybersäkerhetscertifiering att förena ett beslut som den har fattat med vite, hot om tvångsutförande eller hot om avbrytande. Bestämmelser om föreläggande och verkställande av administrativa sanktioner finns i viteslagen.

**28 §.** *Återkallande av cybersäkerhetscertifikat*. Det föreslås att paragrafen innehåller bestämmelser om rätten för myndigheterna för cybersäkerhetscertifiering återkalla ett europeiskt cybersäkerhetscertifikat som den har utfärdat eller som i enlighet med artikel 56.6 i cybersäkerhetsakten har utfärdats av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering för det första i det fallet att certifikatet inte uppfyller de krav som föreskrivs i cybersäkerhetsakten eller kraven i den europeiska ordningen för cybersäkerhetscertifiering i fråga. Artikel 58.8 e i cybersäkerhetsakten förutsätter att nationella bestämmelser om en sådan befogenhet utfärdas. Förutsättningen är att bristen inte avhjälps inom en skälig tid, om det är möjligt att avhjälpa bristen. Tidsfristen kan ingå i ett tillsynsbeslut enligt 25 §, om beslutet föregås av återkallande av ett certifikat. Alternativt kan återkallandet av ett certifikat behandlas som ett separat ärende, varvid den tidsfrist som förutsätts för anmälan om bristen eller avhjälpandet kan anmälas med en annan än en överklagbar handling av myndigheten innan det överklagbara avgörandet om återkallandet av certifikatet.

Enligt artikel 56.6 i cybersäkerhetsakten ska myndigheten för cybersäkerhetscertifiering i princip utfärda certifikat av hög assuransnivå. Organet för bedömning av överensstämmelse utfärdar dock ett certifikat av hög assuransnivå då myndigheten i förväg delegerat denna uppgift till organet antingen allmänt eller för ett enskilt fall. Dessutom kan myndigheten för cybersäkerhetscertifiering exceptionellt utfärda även certifikat som avser assuransnivå ”grundläggande” eller ”betydande” då ordningen för certifieringen så anger (artikel 56.4). Förslaget möjliggör att certifikatet återkallas i ovan nämnda fall. I fall där certifikat av assuransnivå ”grundläggande” eller ”betydande” har utfärdats av ett organ för bedömning av överensstämmelse, föreskrivs däremot inte bestämmelser om befogenheten att återkalla ett certifikat. Detta behövs inte, eftersom ansvaret för att återkalla ett certifikat ligger hos det organ för bedömning av överensstämmelse som utfärdat det i enlighet med föreskrifterna för den tillämpliga certifieringsordningen. I princip har nämligen det organ för bedömning av överensstämmelse som beviljat certifikatet till uppgift att återkalla det, vilket även framgår av artikel 14 i den så kallade EUCC-genomförandeförordningen och därtill kan ett bedömningsorgan avbryta giltigheten för ett certifikat utifrån dess artikel 30. Befogenheten att återkalla certifikat för den nationella myndigheten för cybersäkerhetscertifiering kompletterar bedömningsorganets befogenhet att återkalla certifikat i ovan nämnda situationer.

För det andra möjliggör förslaget att ett certifikat återkallas i det fallet att innehavaren av ett cybersäkerhetscertifikat inte ger myndigheten för cybersäkerhetscertifiering de i 26 § 1 mom. avsedda uppgifter som den begärt eller försummar skyldigheten att rätta uppgifterna inom skälig tid. Till denna del förutsätts regleringen dock inte direkt av cybersäkerhetsakten. EUCC-genomförandeförordningen möjliggör dock liknande åtgärder, det vill säga att giltigheten för ett certifikat dras av bedömningsorganet i det fallet att innehavaren av certifikatet kontinuerligt eller upprepat bryter sin förbindelse att lämna ut uppgifter (artikel 29 och artikel 9.1) eller inte för samarbete (artikel 28.4). Det kan i sista hand bli aktuellt att använda den föreslagna befogenheten till exempel i fall där nödvändiga uppgifter inte ges frivilligt och inte kan skaffas med en inspektion enligt 26 § på grund av att dessa utrymmen omfattas av hemfridsskyddet eller finns utomlands.

**29 §.** *Avbrytande, begränsning eller återkallande av bemyndigande för eller anmälan av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering.* Paragrafens *1 mom.* innehåller bestämmelser om möjligheten att återkalla, avbryta eller begränsa en anmälan eller ett bemyndigande för ett organ för bedömning av överensstämmelse samt lämna in en begäran om att stryka ett organ för bedömning av överensstämmelse från förteckningen över anmälda organ för bedömning av överensstämmelse. Myndigheten för cybersäkerhetscertifiering ska vid behov vidta dessa åtgärder för det första om organet för bedömning inte åtgärdat sin verksamhet på det sätt som förutsätts i tillsynsbeslutet och det handlar om en väsentlig överträdelse eller försummelse. För det andra ska åtgärder vidtas vid behov, om organet för bedömning av överensstämmelse inte uppfyller de krav som föreskrivits för det eller om dess ackreditering begränsas, om ackrediteringen återkallas eller om ackrediteringen avbryts. Åtgärder ska vidtas även i det fallet att beslutet inte ännu vunnit laga kraft, om det är verkställbart trots sökande av ändring. Överträdelsens, bristens eller försummelsens karaktär och eventuellt avhjälpande av den innan beslutet fattas ska beaktas i bedömningen av den typ av åtgärd som är behövlig.

Förslaget är behövligt med anledning av artikel 58.7 e i cybersäkerhetsakten, där det föreskrivs att myndigheten har en skyldighet att begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden, om organen för bedömning av överensstämmelse inte uppfyller kraven i cybersäkerhetsakten. Dessutom kompletterar den artikel 61.1 och 61.4 i cybersäkerhetsakten. På grund av det ovan nämnda ska de nationella myndigheterna för cybersäkerhetscertifiering utan oskäligt dröjsmål till kommissionen anmäla alla ändringar i ackrediteringarna och befogenheter för organen för bedömning. I den sist nämnda punkten förskrivs å sin sida att den nationella myndighet som utfärdar cybersäkerhetscertifiering kan framföra en begäran till kommissionen om att avföra ett av denna myndighet anmält organ för bedömning av överensstämmelse från den förteckning över organ för bedömning av överensstämmelse vilken anmälts till certifieringsordningen enligt punkt 2. En sådan begäran ska enligt förslaget läggas fram, om förutsättningarna för anmälan inte längre är uppfyllda.

Det som föreskrivs i momentet tillämpas endast om inte något annat följer av det beslut som getts med stöd av cybersäkerhetsakten. Kommissionens genomförandeförordning (EU) 2024/3143 innehåller bestämmelser om fastställandet av förhållanden, formkrav och förfaranden för anmälningar enligt artikel 61.5 i cybersäkerhetsakten, medan dess artikel 4.2 innehåller bestämmelser om skyldigheten för myndigheten för cybersäkerhetscertifiering att vid behov vidta ovan nämnda åtgärder beroende på hur allvarligt underlåtenheten att fullgöra dessa krav eller skyldigheter varit. Dessutom kan en certifieringsordning som meddelas genom en genomförandeförordning av kommissionen innehålla mer detaljerad reglering om återkallande av ett bemyndigande eller en anmälan som gäller ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering. Sådan reglering ingår i artikel 22.6 i EUCC-genomförandeförordningen.

Föreslagna *2 mom.* motsvarar till denna del 6 § 4 mom. i lagen om anmälda produkter för vissa produktgrupper. Den innehåller bestämmelser om en situation där ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering har lagt ner sin verksamhet eller avförs från kommissionens förteckning. I så fall ska myndigheten för cybersäkerhetscertifiering vidta ändamålsenliga åtgärder för att säkerställa att handlingarna för det aktuella organet för bedömning av överensstämmelse behandlas av ett annat organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering eller att handlingarna i övrigt hålls tillgängliga för myndigheten för cybersäkerhetscertifiering och myndigheterna med ansvar för marknadskontroll. Myndigheten ska se till att handlingarnas konfidentialitet bibehålls i enlighet med cybersäkerhetsakten och de akter som getts med stöd av den samt offentlighetslagen.

**30 §.** *Handräckning av polisen.* Enligt den föreslagna paragrafen är polisen skyldig att ge myndigheten för cybersäkerhetscertifiering handräckning för tillsynen över efterlevnaden och verkställigheten av de skyldigheterna som föreskrivits i den föreslagna lagen och cybersäkerhetsakten eller de med stöd av den. Det kan bli aktuellt att ge handräckning till exempel om en myndighet hindras från att utöva sina inspektionsbefogenheter. Paragrafen innehåller en informativ hänvisning till polislagen (872/2011), som innehåller bestämmelser om handräckning som ges av polisen.

**6 kap. – Påföljdsavgifter**

**31 §.** *Påföljdsavgift för tillverkare.* Det föreslås att paragrafen innehåller bestämmelser om en administrativ påföljdsavgift, som kan påföras för en tillverkare utifrån överträdelse av cyberresiliensförordningen.

Paragrafens *1 mom.* innehåller på det sätt som artikel 64.2 i cyberresiliensförordningen förutsätter bestämmelser om att uteblivet fullgörande av de väsentliga cybersäkerhetskrav som fastställs i bilaga I till cyberresiliensförordningen och de skyldigheter som regleras i artiklarna 13 och 14 är en grund för en administrativ påföljdsavgift. Momentets bestämmelser täcker även på det sätt som artikel 64.3 förutsätter överträdelse av artikel 31.1–31.4, överträdelse av artikel 32.1–32.3 och överträdelse av artikel 33.5.

Paragrafens *2 mom.* innehåller på det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter bestämmelser om att överträdelse av en skyldighet som föreskrivits för en tillverkare är en grund för att påföra en administrativ påföljdsavgift då skyldigheterna för tillverkarna tillämpas med stöd av artikel 21 på en importör eller distributör eller med stöd av artikel 22 på en annan sådan fysisk person eller juridisk person än en tillverkare, importör eller distributör.

**32 §.** *Påföljdsavgift för tillverkarens representant.* Det föreslås att paragrafen innehåller bestämmelser om en administrativ påföljdsavgift, som kan påföras för tillverkarens representant utifrån överträdelse av cyberresiliensförordningen. På det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter innehåller paragrafen bestämmelser om överträdelse av artikel 18 i förordningen. Med tillverkarens representant avses en fysisk eller juridisk person som enligt skriftlig fullmakt från en tillverkare har rätt att i tillverkarens ställe utföra vissa särskilda uppgifter, som annars hör till tillverkaren. Det finns bestämmelser om skyldigheterna för tillverkarens representant i artikel 18 i cyberresiliensförordningen. När tillverkarens representant inte utsetts med ett skriftligt uppdrag av tillverkaren eller när försummelsen inte omfattas av uppdraget, kan ingen administrativ påföljdsavgift påföras utifrån ansvaret för tillverkarens representant.

**33 §.** *Påföljdsavgift för importörer.* Det föreslås att paragrafen innehåller bestämmelser om en administrativ påföljdsavgift, som kan påföras för en importör utifrån överträdelse av cyberresiliensförordningen. På det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter innehåller paragrafen bestämmelser om överträdelse av artikel 19 i förordningen.

**34 §.** *Påföljdsavgift för distributörer.* Det föreslås att paragrafen innehåller bestämmelser om en administrativ påföljdsavgift, som kan påföras för en distributör utifrån överträdelse av cyberresiliensförordningen. På det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter innehåller paragrafen bestämmelser om överträdelse av artikel 20 i förordningen.

**35 §.** *Påföljdsavgift för anmälda organ.* Paragrafen innehåller bestämmelser om den administrativa påföljdsavgift som kan påföras ett anmält organ utifrån överträdelse av cyberresiliensförordningen då den agerar i strid med cyberresiliensförordningen i sitt uppdrag. På det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter innehåller paragrafen bestämmelser om den administrativa påföljdsavgift som påförs för överträdelse av artikel 39, 41, 47 eller 49 i förordningen.

**36 §.** *Andra påföljdsavgifter i anslutning till cyberresiliensförordningen.* Paragrafen innehåller bestämmelser om den administrativa påföljdsavgift som kan påföras en ekonomisk aktör utifrån överträdelse av cyberresiliensförordningen i andra än de situationer som avses i 31–35 §. På det sätt som artikel 64.3 i cyberresiliensförordningen förutsätter innehåller paragrafen bestämmelser om den administrativa påföljdsavgift som påförs för överträdelse av artikel 23, 30 eller 53 i förordningen. Paragrafen innehåller på det sätt som artikel 64.4 i cyberresiliensförordningen förutsätter bestämmelser om en administrativ påföljdsavgift för en ekonomisk aktör för felaktiga, bristfälliga eller vilseledande uppgifter som lämnats som svar på en begäran av anmälda organ eller marknadskontrollmyndigheterna.

**37 §.** *Påföljdsavgift som gäller cybersäkerhetscertifiering*. Paragrafen innehåller bestämmelser om gärningar i anknytning till överträdelse av cybersäkerhetsakten, för vilka en administrativ påföljdsavgift kan påföras. I syfte att genomföra artikel 65 i cybersäkerhetsakten innehåller paragrafen bestämmelser om den administrativa påföljdsavgift som ska påföras utifrån överträdelse av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering enligt denna del i förordningen.

I paragrafens *1 punkt* föreskrivs att det är möjligt att med en påföljdsavgift sanktionera en situation där en tillverkare eller leverantör av IKT-produkter, IKT-tjänster eller IKT-processer utfärdar en sådan EU-försäkran om överensstämmelse som avses i artikel 53.2 i cybersäkerhetsakten trots att dessa nyttigheter inte uppfyller kraven enligt den europeiska ordningen för cybersäkerhetscertifiering i fråga. Syftet med en EU-försäkran om överensstämmelse är att visa att de krav som definierats i ordningen är uppfyllda. Om en tillverkare eller leverantör gett en EU-försäkran om överensstämmelse på felaktiga grunder, är det möjligt att påföra en påföljdsavgift för detta. För att säkerställa att förtroendet för EU-försäkringar om överensstämmelse är det viktigt att missbruk av dessa har sanktionerats så att aktörerna har ändamålsenliga incitament att se till att de krav som ställs i cyberresiliensförordningen är uppfyllda.

I paragrafens *2 punkt* sanktioneras en försummelse att ge myndigheten för cybersäkerhetscertifiering den information som avses i artikel 53.3 i cybersäkerhetsakten eller en försummelse att lämna in en kopia av EU-försäkran om överensstämmelse till myndigheten för cybersäkerhetscertifiering och Europeiska unionens cybersäkerhetsbyrå Enisa.

Enligt denna punkt i cybersäkerhetsakten ska tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller hanterade säkerhetstjänster, under en period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering, ge den nationella myndigheten för cybersäkerhetscertifiering tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas, IKT-tjänsternas eller de hanterade säkerhetstjänsternas överensstämmelse med ordningen. Dessutom ska en kopia av EU-försäkran om överensstämmelse lämnas in till den nationella myndighet som utfärdar cybersäkerhetscertifiering och till Europeiska unionens cybersäkerhetsbyrå Enisa. För de först nämnda är det möjligt att påföra en sanktion, om de relevanta uppgifterna inte ges på begäran av myndigheten för cybersäkerhetscertifiering, om de inte är tillgängliga på annat sätt. I fråga om de sist nämnda är det möjligt att påföra en påföljdsavgift, om en tillverkare eller leverantör försummar att överlämna kopian på eget initiativ.

I paragrafens *3 punkt* föreskrivs att påföljdsavgiften omfattar situationer där certifikatinnehavaren bryter mot de villkor för ett cybersäkerhetscertifikat som ställts i en europeisk ordning för cybersäkerhetscertifiering. Enligt artikel 54.1 k i cybersäkerhetsakten kan sådana villkor ställas för utfärdande, bibehållande, fortsättande och förnyelse av certifikat samt villkor för utvidgning eller inskränkning av tillämpningsområdet för certifiering. Med tanke på certifikatens tillförlitlighet kan det anses att det är centralt att villkoren iakttas.

I paragrafens *4 punkt* föreskrivs att påföljdsavgiften omfattar situationer där en tillverkare eller leverantör av IKT-produkter, IKT-tjänsterna eller IKT-processer försummar att offentliggöra den information som avses i artikel 55.1 i cybersäkerhetsakten på det sätt som föreskrivs i artikel 55.2 i cybersäkerhetsakten. Punkten gäller situationer där dessa produkter, tjänster eller processer är certifierade eller för vilka en EU-försäkran om överensstämmelse har getts. Aktören ska i så fall offentliggöra de uppgifter som räknas upp i punkten, vilka på olika sätt främjar att cybersäkerheten för produkten, processen eller tjänsten upprätthålls. Enligt 2 punkten i artikeln ska uppgifterna tillgängliggöras i elektroniskt format och finnas tillgängliga och vid behov uppdateras åtminstone fram till dess att motsvarande europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse löper ut.

Förslaget innehåller inte någon närmare begränsning av de uppgifter som kan leda till påförande av en påföljdsavgift om de inte lämnas. Överträdelsens karaktär beaktas dock inom ramen för föreslagna 40 §, med stöd av vilken en påföljdsavgift inte påförs till exempel om den är ringa.

I *5 punkten* i paragrafen sanktioneras en situation där felaktig, vilseledande eller bristfällig information ges till myndigheten för cybersäkerhetscertifiering eller organet för bedömning av överensstämmelse. Sanktioneringen gäller i synnerhet en situation där en aktör lämnar in IKT-produkter, IKT-tjänster eller IKT-processer eller informationssäkerhetstjänster för certifiering. Artikel 56.7 i cybersäkerhetsakten innehåller bestämmelser om skyldigheten att vid en ansökan om certifiering göra alla uppgifter som behövs för att genomföra certifieringsförfarandet tillgängliga för myndigheten eller bedömningsorganet. I den föreslagna punkten förutsätts att informationen gäller omständigheter som är betydelsefulla för att sköta en uppgift enligt den föreslagna lagen eller cybersäkerhetsakten, varför ett oväsentligt fel inte leder till att en påföljdsavgift påförs. Syftet med sanktioneringen är att se till att beviljandet av ett certifikat inte sker utifrån felaktig information. Uteblivet uppfyllande av kraven kan ha allvarliga skadliga konsekvenser för användarna av en produkt, tjänst eller process.

Sådant utlämnade av felaktig information kan även bli föremål för bedömning av ingivande osant intyg till myndighet enligt 16 kap. 8 § i strafflagen. I så fall kan man vid behov beakta vad som föreskrivs om förbudet mot dubbel straffbarhet i 40 § 3 mom.

Paragrafens *6 punkt* innehåller bestämmelser om en påföljdsavgift där en innehavare av ett europeiskt cybersäkerhetscertifikat försummar att lämna ut information enligt artikel 56.8 i cybersäkerhetsakten om en sårbarhet eller oriktighet som gäller säkerheten för en IKT-produkt, IKT-tjänst eller IKT-process, vilken kan påverka överensstämmelsen med kraven i anknytning till certifieringen. Anmälan görs till myndigheten för cybersäkerhetscertifiering eller organet för bedömning av överensstämmelse, beroende på vilken aktör som utfärdat certifikatet.

I paragrafens *7 punkt* sanktioneras en situation där en instans använder ett europeiskt cybersäkerhetscertifikat som har återkallats eller vars giltighet har löpt ut. Med sådan certifikatanvändning avses att en IKT-produkt, IKT-tjänst eller IKT-process eller dataskyddstjänst marknadsförs som certifierad eller något annat förfarande, där en tidigare certifikatinnehavare hänvisar till certifikatnyttigheten som en säkerhetsgaranti, även om detta certifikat har återkallats eller gått ut.

I vissa situationer kan myndigheten för cybersäkerhetscertifiering återkalla ett certifikat i enlighet med 28 § i den föreslagna lagen. Det finns bestämmelser om denna möjlighet till återkallande i artikel 58.8 e i cybersäkerhetsakten. I övrigt återkallas ett cybersäkerhetscertifikat av det organ för bedömning av överensstämmelse som utfärdat det aktuella europeiska cybersäkerhetscertifikatet. Efter återkallandet gäller certifikatet inte längre. Certifikaten har dessutom en viss giltighetstid som fastställs inom ramen för certifieringsordningen, efter vilken certifikatet inte längre är giltigt. I synnerhet i säkerhetskritiska samband är det viktigt att felaktig information inte ges om certifieringsstatus för produkterna, tjänsterna och processerna.

**38 §.** *Påföljdsavgiftens belopp.* Paragrafen innehåller bestämmelser om beloppet av den administrativa påföljdsavgift som påförs med stöd av 31–37 §. För att påföljden ska ha en tillräckligt förebyggande effekt, ska avgiftens storlek vara tillräcklig. Den myndighet som påför en påföljd ska säkerställa att sanktionen och dess belopp står i proportion till gärningen med beaktande av ratio i cyberresiliensförordningen och cybersäkerhetsakten. Genom paragrafen genomförs artikel 64 i cyberresiliensförordningen och för egen del artikel 65 i cybersäkerhetsakten.

Paragrafens *1 mom.* innehåller bestämmelser om maximibeloppet av den administrativa påföljdsavgift som påförs för överträdelse av 31 § 1 mom., det vill säga i huvudsak artikel 13 eller artikel 14 i cyberresiliensförordningen. Maximibeloppet är 15 000 euro eller då tillverkaren är ett företag, två och en halv procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är högst. Maximibeloppet av den administrativa påföljdsavgiften motsvarar den nivå som förutsätts i artikel 64.2 i cyberresiliensförordningen.

Paragrafens *2 mom.* innehåller bestämmelser om maximibeloppet av den påföljdsavgift som påförs med stöd av 36 § 2 punkten, 32–35 § eller 36 § 1–3 punkten för överträdelse av cyberresiliensförordningen. Maximibeloppet är 10 000 000 euro eller då tillverkaren är ett företag, två procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är högst. Maximibeloppet är i praktiken tillämpligt på överträdelser av cyberresiliensförordningen av andra ekonomiska aktörer än tillverkare och på anmälda organ. Maximibeloppet av den administrativa påföljdsavgiften motsvarar den nivå som förutsätts i artikel 64.3 i cyberresiliensförordningen.

Paragrafens *3 mom.* innehåller bestämmelser om maximibeloppet av den påföljdsavgift som påförs med stöd av 36 § 4 punkten för överträdelse av cyberresiliensförordningen. Maximibeloppet är 5 000 000 euro eller då tillverkaren är ett företag, en procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är

högst. Maximibeloppet omfattar en situation där information som avsiktligen är felaktig, bristfällig eller vilseledande lämnas till ett anmält organ eller marknadskontrollmyndigheten på ett sätt som är av betydelse för skötseln av en uppgift för det anmälda organet eller marknadskontrollmyndigheten. Maximibeloppet av den administrativa påföljdsavgiften motsvarar den nivå som förutsätts i artikel 64.4 i cyberresiliensförordningen.

Paragrafens *4 mom.* innehåller bestämmelser om maximibeloppet av en påföljdsavgift som gäller cybersäkerhetscertifiering, vilken är 100 000 euro. Beloppet av den administrativa påföljdsavgift som påförs utifrån överträdelse av cybersäkerhetsakten motsvarar den nivå på vilken påföljden har en tillräcklig, effektivt och proportionell förebyggande effekt. Påföljdsavgiftens nivå bedöms och motiveras i avsnitt 5.1.3. Maximibeloppet av den administrativa påföljdsavgiften uppfyller förutsättningarna i artikel 65 i cybersäkerhetsakten.

I *5 mom.* i paragrafen finns det bestämmelser om en samlad bedömning av påföljdsavgiften. Fastställandet av påföljdsavgiftens storlek ska basera sig på en samlad bedömning av överträdelsens allvar och förfarandets klandervärdhet. När beloppet av påföljdsavgiften bedöms ska man beakta förfarandets art, allvar och längd och dess återkommande karaktär, den skada som överträdelsen orsakat och aktörens storlek samt dess eventuella tidigare överträdelser i anknytning till tillämpningsområdet för den föreslagna lagen. Aktörens storlek ska beaktas, eftersom de skyldigheter som omfattas av lagens tillämpningsområde kan hänföra sig till organisationer av väldigt olika storlekar.

Även artikel 64.5 i cyberresiliensförordningen innehåller bestämmelser om de omständigheter som ska beaktas då en administrativ påföljdsavgift påförs. Dessa omständigheter ska tillämpas på påförande av en administrativ påföljdsavgift med stöd av 31–36 §. I artikel 64.5 i cyberresiliensförordningen föreskrivs att då beslut fattas om beloppet av en administrativ sanktionsavgift, ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn tas till följande omständigheter:

a) överträdelsens art, allvarlighetsgrad och varaktighet samt dess konsekvenser,

b) huruvida administrativa sanktionsavgifter redan har påförts av samma eller andra marknadskontrollmyndigheter på samma ekonomiska aktör för en liknande överträdelse,

c) storleken på, särskilt när det gäller mikroföretag, små och medelstora företag, inbegripet uppstartsföretag, och marknadsandelen för den ekonomiska aktör som begått överträdelsen.

**39 §.** *Påförande av påföljdsavgift.* Paragrafen innehåller bestämmelser om påförande av en administrativ påföljdsavgift.

Med stöd av *1 mom.* påförs en administrativ påföljdsavgift med stöd av 31–34 § och 36 § av marknadskontrollmyndigheten. Transport- och kommunikationsverket fungerar som marknadskontrollmyndighet med stöd av 15 §. I fråga om AI-system med hög risk, som omfattas av cyberresiliensförordningens tillämpningsområde, fungerar den behöriga tillsynsmyndigheten enligt lagen om tillsyn över vissa system för artificiell intelligens som marknadskontrollmyndighet med stöd av 16 §. När den behöriga marknadskontrollmyndigheten utgörs av marknadskontrollmyndigheten enligt 3 § i lagen om tillsyn över vissa system för artificiell intelligens, påförs den administrativa påföljdsavgiften i den ordning som föreskrivs i 13 § i den nämnda lagen. I så fall påför den behöriga aktören med andra ord en påföljdsavgift enligt den föreslagna lagen med stöd av lagen om tillsyn över vissa system för artificiell

intelligens. Gärningarna handlar om överträdelser av cyberresiliensförordningen av en ekonomisk aktör.

När beloppet av en administrativ påföljdsavgift som omfattas av Transport- och kommunikationsverkets befogenhet är över 100 000 euro, ska påföljdsavgiften påföras i ett förfarande enligt 7 a § i lagen om Transport- och kommunikationsverket, det vill säga i påföljdskollegiet.

Med stöd av paragrafens *2 mom.* meddelar den anmälande myndigheten, det vill säga Transport- och kommunikationsverket, beloppet av den administrativa påföljdsavgiften för en gärning enligt 35 §. Gärningarna handlar om överträdelser av cyberresiliensförordningen av ett anmält organ.

När beloppet av en administrativ påföljdsavgift som omfattas av Transport- och kommunikationsverkets befogenhet är över 100 000 euro, ska påföljdsavgiften påföras i ett förfarande enligt 7 a § i lagen om Transport- och kommunikationsverket, det vill säga i påföljdskollegiet.

Med stöd av paragrafens *3 mom.* meddelar myndigheten för cybersäkerhetscertifiering, det vill säga Transport- och kommunikationsverket, beloppet av den administrativa påföljdsavgiften för en gärning enligt 37 §. Gärningarna handlar om förseelser som gäller cybersäkerhetscertifiering.

Paragrafens *4 mom.* innehåller bestämmelser om rätten för den myndighet som påför påföljdsavgiften att avgiftsfritt och utan hinder av sekretessbestämmelserna få uppgifter som är nödvändiga för att påföra en påföljdsavgift eller för att bedöma dess belopp från en ekonomisk aktör eller från en annan myndighet. Rätten att få information är nödvändig för att behandla och avgöra ett ärende som gäller påförande av en administrativ påföljdsavgift. Rätten att få information begränsar sig till uppgifter som är nödvändiga för att fastställa påföljdsavgiften i det ärende som behandlas, det vill säga för att bedöma dess grund eller belopp.

**40 §.** *Avstående från påförande av påföljdsavgift.* I paragrafen finns det bestämmelser om när påföljdsavgift inte påförs.

Enligt *1 mom.* ska påföljdsavgift inte påföras, om

1) aktören på eget initiativ vidtagit tillräckliga åtgärder för att avhjälpa överträdelsen eller försummelsen omedelbart efter att den upptäckts och utan dröjsmål underrättat tillsynsmyndigheten om den samt samarbetat med tillsynsmyndigheten, och överträdelsen eller försummelsen inte är allvarlig eller återkommande,

2) överträdelsen eller försummelsen ska anses vara ringa, eller

3) påförande av påföljdsavgift ska anses vara uppenbart oskäligt på andra grunder än de som avses i 1 eller 2 punkten.

Grundlagsutskottet har i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden till prövning så att påföljdsavgift inte påförs om de villkor som anges i lag är uppfyllda (GrUU 49/2017 rd och GrUU 39/2017 rd).

Syftet med bestämmelsen är att säkerställa att en påföljdsavgift inte påförs i situationer där det är oskäligt antingen utifrån de omständigheter som avses i 1 mom. 1 eller 2 punkten eller i övrigt uppenbart oskäligt utifrån en annan eller flera andra motsvarande omständigheter.

I *2 mom.* i paragrafen finns det bestämmelser om preskriberingen av rätten att påföra en påföljdsavgift. Påföljdsavgift får inte påföras, om det har förflutit mer än fem år sedan överträdelsen eller försummelsen har skett. Om förseelsen eller försummelsen har varit av vilseledande karaktär, räknas tidsfristen från det att förseelsen eller försummelsen upphört.

I paragrafens *3 mom.* föreskrivs att påföljdsavgift inte kan påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom. Dessutom får en påföljdsavgift som gäller cybersäkerhetscertifiering inte påföras för den som för samma gärning påförts en strängare påföljdsavgift utifrån överträdelse av cyberresiliensförordningen. Bestämmelserna motsvarar den så kallade ne bis in idem-principen, det vill säga förbudet mot dubbel straffbarhet.

I paragrafens *4 mom.* föreskrivs ett förbud att påföra en påföljdsavgift för statliga myndigheter, statliga affärsverk, välfärdsområden eller välfärdssammanslutningar, kommunala myndigheter, självständiga offentligrättsliga inrättningar, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland eller ortodoxa kyrkan i Finland och de två sistnämndas församlingar, kyrkliga samfälligheter eller övriga organ.

Paragrafens *5 mom.* innehåller bestämmelser om förbudet att påföra en påföljdsavgift för ett mikroföretag eller litet företag på den grunden att företaget har överskridit tidsfristen på 24 timmar för anmälan av en händelse enligt artikel 14.1 eller 14.3 i cyberresiliensförordningen. Skyldigheten enligt artikel 14 i cyberresiliensförordningen att anmäla aktivt utnyttjade sårbarheter eller en allvarlig incident som påverkar en produkts dataskydd blir trots punkten även tillämplig på mikroföretag och små företag enligt vad som bestäms i artikel 14 i cyberresiliensförordningen och en påföljdsavgift kan påföras utifrån försummelse av de tidsfrister som avses i artikel 14.2, artikel 14.4 c och artikel 14.4 c. Punkten motsvarar definitionen i strecksats a i artikel 64 i cyberresiliensförordningen.

Paragrafens *6 mom.* innehåller ett förbud att påföra en påföljdsavgift för en förvaltare av programvara med fri och öppen källkod. Definitionen av en förvaltare av programvara med fri och öppen källkod fastställs i 2 § 8 punkten i lagen och den motsvarar definitionen i artikel 3.14 i cyberresiliensförordningen. Punkten motsvarar definitionen i strecksats b i artikel 64 i cyberresiliensförordningen.

**41 §.** *Verkställighet av påföljdsavgift.* Det föreslås att paragrafen reglerar verkställigheten av påföljdsavgifter. En påföljdsavgift som påförts med stöd av lag verkställs i den ordning som föreskrivs i lagen om verkställighet av böter (672/2002). Rättsregistercentralen svarar för verkställigheten av påföljdsavgiften. Med stöd av 4 b § i den nämnda lagen (lag 416/2025) förfaller en påföljdsavgift fem år efter den dag då det lagakraftvunna avgörandet har getts. Dröjsmålsränta tas inte ut på en påföljdsavgift.

**7 kap – Särskilda bestämmelser**

**42 §.** *Begäran om omprövning.* Det föreslås att paragrafen innehåller beslut som kan vara föremål för i förvaltningslagen avsedd omprövning. Omprövning får begäras i ett beslut av ett anmält organ, i ett beslut av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och i ett beslut som gäller en avgift som tas ut för en myndighetsprestation.

Föremålet för en begäran om omprövning kan vara ett förvaltningsbeslut av ett organ för bedömning av överensstämmelse som anmälts för myndighetscertifiering, vilket ges utifrån

denna lag, cyberresiliensförordningen eller cybersäkerhetsakten. Föremålet för begäran om omprövning kan således vara till exempel ett beslut om att utfärda eller inte utfärda en försäkran om överensstämmelse av ett anmält organ. Föremålet för begäran om omprövning kan även vara ett myndighetsbeslut som gäller den avgift som tas ut för en myndighetsprestation.

Förvaltningslagen tillämpas på behandlingen av en begäran om omprövning. Det är möjligt att överklaga ett beslut om en begäran om omprövning hos förvaltningsdomstolen i den ordning som föreskrivs i lagen om rättegång i förvaltningsärenden. I 43 § 5 mom. nedan finns det en särskild bestämmelse om verkställbarheten för ett beslut om en begäran om omprövning.

Bestämmelsen motsvarar förutsättningen i artikel 48 i cyberresiliensförordningen om det tillgängliga förfarandet för ändringssökande i beslut av ett anmält organ.

**43 §.** *Ändringssökande.* Paragrafens *1 mom.* innehåller en informativ hänvisning till att sökande av ändring hos förvaltningsdomstolen regleras i lagen om rättegång i förvaltningsärenden. Föremålet för ändringssökande kan vara ett beslut av till exempel den anmälande myndigheten, marknadskontrollmyndigheten och myndigheten för cybersäkerhetscertifiering. Föremålet för ändringssökande kan även vara ett beslut om en administrativ påföljdsavgift av en sådan myndighet eller ett beslut om avgiftsbelagdhet för en myndighets avgift, vilket getts med anledning av en begäran om omprövning.

Paragrafens *2–5 mom.* innehåller bestämmelser om verkställbarheten för ett förvaltningsbeslut som getts med stöd av lagen, då beslutet inte vunnit laga kraft.

I paragrafens 2 mom. föreskrivs att ett beslut av marknadskontrollmyndigheten som gäller annat än påförande av påföljdsavgift får verkställas trots ändringssökande. Huvudregeln för verkställbarheten för ett beslut motsvarar 29 § i lagen om marknadskontroll. I enlighet med regleringsprincipen för administrativa sanktioner är ett beslut om en administrativ påföljd dock verkställbart först utifrån ett lagakraftvunnet beslut.

Paragrafens *3–5 mom.* innehåller uttömmande bestämmelser om beslut som kan förordnas att verkställas trots ändringssökande.

Paragrafens 3 mom. innehåller bestämmelser om verkställbarheten för ett beslut av den anmälande myndigheten. Den anmälande myndigheten kan i ett beslut om utseende av ett anmält organ eller om avgränsning eller indragning av utseendet av ett anmält organ förordna att beslutet ska iakttas trots ändringssökande. Genom förslaget säkerställs att om ett anmält organ inte längre uppfyller förutsättningarna för utseende, kan den anmälande myndigheten på det sätt som cyberresiliensförordningen förutsätter vidta effektiva åtgärder trots ändringssökandet.

I paragrafens 4 mom. föreskrivs å sin sida möjligheten för myndigheten för cybersäkerhetscertifiering att förordna att ett beslut ska iakttas trots ändringssökande.

I paragrafens 5 mom. föreskrivs att ett beslut av ett anmält organ eller ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering kan verkställas då beslutet gäller de korrigerande åtgärder som krävs av tillverkaren av en produkt som innehåller digitala element eller innehavaren av ett europeiskt cybersäkerhetscertifikat eller som gäller återkallande av ett intyg om överensstämmelse för en produkt med digitala element eller ett europeiskt cybersäkerhetscertifikat. Föremålet för sökande av ändring kan vara ett beslut som getts om en begäran om omprövning. Syftet med detta förslag är att säkerställa att dessa reparativa åtgärder är effektiva då allvarliga brister har konstaterats.

Enligt 123 § i lagen om rättegång i förvaltningsärenden kan förvaltningsdomstolen under den tid ett besvärsärende är anhängigt förbjuda att beslutet verkställs, förordna att verkställigheten ska avbrytas eller förordna om något annat som gäller verkställigheten av beslutet På grund av detta innehåller paragrafen inte separata bestämmelser om möjligheten för en besvärsmyndighet att förbjuda verkställighet av ett sådant beslut som av den beslutsfattande myndigheten förordnats att verkställas trots ändringssökande. Den nämnda bestämmelsen tillämpas vid sidan om paragrafens 2–5 mom.

Paragrafens *6 mom.* innehåller en informativ hänvisning till viteslagen. Vid sökande av ändring i beslut som gäller föreläggande och utdömande av vite samt föreläggande och verkställighet av hot om tvångsutförande eller hot om avbrytande tillämpas dock viteslagen (1113/1990).

**44 §.** *Avgifter.* Enligt paragrafen finns bestämmelser om de allmänna grunderna för när myndigheters prestationer ska vara avgiftsbelagda och för storleken av de avgifter som uppbärs för prestationerna och om övriga grunder för avgifterna i lagen om grunderna för avgifter till staten (150/1992). Paragrafen är av informativ karaktär. Med stöd av lagen om grunderna för avgifter till staten är det möjligt att ta ut avgifter för prestationer av den anmälande myndigheten och myndigheten för cybersäkerhetscertifiering, vilket avser i synnerhet anmälning och övervakning av organ för bedömning av överensstämmelse samt utfärdande av cybersäkerhetscertifikat. Dessutom kan avgifter tas ut för användning av regulatoriska sandlådor i enlighet med grunderna i lagen om grunderna för avgifter till staten. Befogenheten i 8 § i lagen om grunderna för avgifterna till staten att besluta om bland annat avgiftsbelagdheten för en prestation innehas enligt förslaget av kommunikationsministeriet i fråga om Transport- och kommunikationsverkets prestationer.

**45 §.** *Ikraftträdande.* I *1 mom*. finns det bestämmelser om lagens ikraftträdande. Paragrafens *2–4 mom.* innehåller graderingar för början av tillämpningen, vilka motsvarar graderingarna för de tidpunkter då cyberresiliensförordningen börjar tillämpas.

Med stöd av 2 mom. i paragrafen tillämpas bestämmelserna i 3 kap. om anmälda organs och den anmälande myndighetens uppgifter och bestämmelserna i 35 § om påföljdsavgiften för anmälda organ den 11 juni 2026. Början för tillämpningen motsvarar artikel 7.1.2 i cyberresiliensförordningen.

Med stöd av paragrafens 3 mom. börjar anmälningen enligt artikel 14 i cyberresiliensförordningen och påföljdsavgiften för tillverkare i fråga om anmälningen tillämpas den 11 september 2026. Början för tillämpningen motsvarar artikel 71.2.2 i cyberresiliensförordningen.

Med stöd av paragrafens 4 mom. börjar bestämmelserna om skyldigheterna för ekonomiska aktörer enligt cyberresiliensförordningen och om överträdelse av dessa samt om administrativa påföljdsavgifter tillämpas den 11 december 2027 Början för tillämpningen motsvarar artikel 71.2.1 i cyberresiliensförordningen.

### 7.2 Lagen om marknadskontrollen av vissa produkter

**1 §.** *Tillämpningsområde*. Det föreslås att paragrafens *1 mom.* ändras på så sätt att lagförslag 1 fogas som en ny punkt till momentets lista över de lagar vars tillämpningsområde omfattar produkter på vilka marknadskontrollagen tillämpas. Med anledning av tillägget görs en teknisk ändring i den föregående punkten.

Lagen om marknadskontrollen av vissa produkter tillämpas även på marknadskontrollen av produkter som omfattas av cyberresiliensförordningen till den del som inte annat bestäms i den föreslagna lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering. Lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering är således en specialbestämmelse i förhållande till marknadskontrollagen. Med produkt som omfattas av lagens tillämpningsområde avses produkter som omfattas av cyberresiliensförordningens tillämpningsområde. En produkt som omfattas av lagens tillämpningsområde avser således inte en produkt för vilken cybersäkerhetscertifiering utfärdats, om produkten inte omfattas av cyberresiliensförordningens tillämpningsområde.

**4 §.** *Tillsynsmyndigheter*. Det föreslås att paragrafens *4 mom.* ändras så att man till momentet fogar produkter som omfattas av tillämpningsområdet för lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering till listan över produkter för vilka Transport- och kommunikationsverket fungerar som marknadskontrollmyndighet. Avsikten är inte att ändra momentet till andra delar.

I enlighet med 15 § i den hänvisade lagen fungerar således Transport- och kommunikationsverket som marknadskontrollmyndighet för de produkter som omfattas av cyberresiliensförordningens tillämpningsområde. Med stöd av 16 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering är det möjligt att även den behöriga tillsynsmyndigheten enligt 3 § i lagen om tillsyn över system för artificiell intelligens undantagsvis fungerar som marknadskontrollmyndighet då marknadskontrollen hänför sig till ett AI-system med hög risk enligt artikel 6 i förordningen om artificiell intelligens, vilket även omfattas av cyberresiliensförordningens tillämpningsområde. Det nämnda undantaget baserar sig på artikel 52.14 i cyberresiliensförordningen.

### 7.3 Cybersäkerhetslagen

**20 §.** *CSIRT-enhetens uppgifter.* Till listan över CSIRT-enhetens uppgifter i paragrafens *1 mom.* fogas en ny 10 punkt, som gäller de uppgifter som tilldelats CSIRT-enheten i cyberresiliensförordningen och lagförslag 1. CSIRT-enhetens centrala uppgift är att ta emot och behandla i artikel 14 i cyberresiliensförordningen avsedda anmälningar om aktivt utnyttjade sårbarheter och allvarliga incidenter vilka påverkar dataskyddet för en produkt med digitala element. Tillverkarna är skyldiga att göra anmälningar på det sätt som föreskrivs i cyberresiliensförordningen. CSIRT-enheten har även till uppgift att behandla frivilliga anmälningar enligt artikel 15 i cyberresiliensförordningen.

De andra uppgifter som tilldelats CSIRT-enheten är bland annat att biträda marknadskontrollmyndigheten vid behov. I artikel 52.5 i cyberresiliensförordningen får marknadskontrollmyndigheterna be en CSIRT-enhet som utsetts till samordnare eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av denna förordning. När marknadskontrollmyndigheterna gör en undersökning enligt artikel 54 kan de begära den CSIRT-enhet som utsetts till samordnare eller Enisa att lägga fram en analys till stöd för bedömningarna av överensstämmelsen för produkter med digitala element. På motsvarande sätt föreskrivs i artikel 54.1 att om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i förordning. CSIRT-enheten ska vid behov sköta uppgifterna enligt cyberresiliensförordningen i samarbete med övriga myndigheter.

**28 §.** *Rätt att få information*. Det föreslås att paragrafens ändras så att rätten att lämna ut information för en myndighet som övervakar vad som föreskrivs i *4 mom.* i den kan tillämpas även på utlämnande av information till Finansinspektionen för dess uppgift som behörig myndighet enligt 50 p § 1 och 2 mom. i lagen om Finansinspektionen. Enligt dessa bestämmelser fungerar Finansinspektionen som behörig myndighet enligt artikel 46 i EU:s DORA-förordning och behörig myndighet enligt artikel 8.1 i NIS 2-direktivet i fråga om verksamhetsområdena 3 och 4 i bilaga I till det nämnda direktivet. Detta innebär att tillsynsmyndigheten enligt cybersäkerhetslagen utan hinder av sekretessbestämmelserna, den tystnadsplikt som föreskrivs i 28 § 2 mom. och andra begränsningar som gäller utlämnande av information kan lämna ut en handling som den fått eller upprättat i samband med skötseln av dess uppgifter enligt cybersäkerhetslagen och röja sekretessbelagd information även till Finansinspektionen, om det är nödvändigt för dess uppgift som behörig myndighet enligt 50 p § 1 och 2 mom. i lagen om Finansinspektionen. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt.

Cybersäkerhetslagen innehåller inte bestämmelser om Finansinspektionens uppgifter och informationsutbyte mellan den och de tillsynsmyndigheter som definieras i 26 § i cybersäkerhetslagen, eftersom DORA-förordningen är en branschspecifik unionsakt enligt artikel 4 i NIS 2-direktivet, och medlemsstaterna inte bör tillämpa bestämmelserna i NIS 2-direktivet inom dess område, om de gäller hantering av cybersäkerhetsrisker och rapporteringsskyldigheten samt tillsyn och verkställighet (RP 57/2024 rd, 33).

I 50 p § i lagen om Finansinspektionen finns det på ett sätt som kan jämställas med 26 § i cybersäkerhetslagen bestämmelser om att Finansinspektionen fungerar som behörig myndighet enligt artikel 8.1 i NIS 2-direktivet i fråga om verksamhetsområdena 3 och 4 i bilaga I till direktivet. I 71 § 1 mom. i den nämnda lagen finns det bestämmelser om Finansinspektionens rätt att utan hinder av sekretessbestämmelserna lämna ut uppgifter om störningar och hot i anknytning till informations- och kommunikationsteknik till Transport- och kommunikationsverket för genomförande av det samarbete som avses i 3 f 3 mom. Enligt den sista nämnda bestämmelsen ska Finansinspektionen samarbeta med Transport- och kommunikationsverket i skötseln av uppgifter enligt NIS 2-direktivet.

Cybersäkerhetslagens 28 § innehåller dock för närvarande inte bestämmelser om rätten för tillsynsmyndigheterna att lämna ut information till Finansinspektionen. Med stöd av 318 § 2 mom. i lagen om tjänster inom elektronisk kommunikation (i lag 703/2025) har Transport- och kommunikationsverket, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut en handling som den fått eller upprättat i samband med skötseln av dess lagstadgade uppgifter samt röja den sekretessbelagda informationen för Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket samt livskraftscentralen, om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerhet. Bestämmelsens bakgrund utgörs av genomförandet av NIS-direktivet, som numera har upphävts, och den möjliggör att information lämnas ut från Transport- och kommunikationsverket till Finansinspektionen även inom NIS 2-direktivets tillämpningsområde. Med stöd av 318 § 5 mom. kan bestämmelsen dock inte tillämpas på uppgifter om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter eller förekomsten av och innehållet i förtrolig radiokommunikation, även om Transport- och kommunikationsverket i egenskap av tillsynsmyndighet kan få även dessa uppgifter med stöd av 28 § 2 mom. Således är det motiverat att utvidga regleringen kring utlämnande av information i 28 § 4 mom. i cybersäkerhetslagen att gälla även Finansinspektionen, så att alla behöriga myndigheter enligt NIS 2-direktivet till denna del har samma ställning.

### 7.4 Lagen om tjänster inom elektronisk kommunikation

#### 1 kap. – Lagens mål och definitioner

**3 §.** *Definitioner.* Paragrafens 35 punkt ändras så att avgränsningen till domännamn med den nationella toppdomänen fi och toppdomänen för landskap ax stryks från definitionen av ett domännamn. Med domännamn avses med andra ord framöver i lagen en adressuppgift i namnform som används på Internet, oberoende av under vilken toppdomän (eng. top-level domain, TLD) domännamnet lyder. Ändringen behövs för att foga nya 21 a kap., eftersom bestämmelserna i det gäller andra domännamn än de som slutar med fi eller ax. Dessutom motsvarar definitionen bättre definitionen av termen i allmänspråket.

Trots ändringen tillämpas 21 kap. även framöver endast på adressuppgifter som omfattas av Finlands nationella domännamn fi och domänen för landskap ax för Åland. Tillämpningsbegränsningen gällande 21 kap. i lagen bibehålls i oförändrad form i 163 §. Syftet med ändringen är inte att utvidga de nuvarande bestämmelserna om domännamn i lagen till andra domännamn än de som omfattas av den nationella domänen fi och domänen för landskap ax.

Till definitionen av domännamn görs dessutom en teknisk precisering enligt rådande tolkningspraxis om att domännamn avser en adressuppgift av andra graden av formen domain.fi. Detta motsvarar vad som föreskrivs i den hävda lagen om domännamn (228/2003). Genom ändringen förtydligas att ett domännamn inte avser delen före den första punkten till exempel i adressen undersida.domain.fi, som den aktör som administrerar en adressuppgift av andra graden enkelt kan fastställa.

Till paragrafen fogas nya 35 a punkten, som definierar den som förvaltar ett toppdomänregister på samma sätt som i 2 § i cybersäkerhetslagen. Definitionen motsvarar även definitionen av ett toppdomänregister i artikel 6.21 i NIS 2-direktivet. Med den som förvaltar ett toppdomänregister avses en part som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av parten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av parten endast för dess eget bruk.

Med den som förvaltar ett toppdomänregister avses således en förvaltare av ett domännamnsregister på högsta nivå (Top-Level Domain Registry). Toppdomäner delas in i två grupper, som är nationella toppdomän (ccTLD) och generiska toppdomäner (gTLD). Syftet med definitionen är inte att avgränsa dess tillämpning till ett visst geografiskt område.

#### 21 kap. – Domännamn för Finland och Åland

Kapitlets rubrik preciseras så att den redogör för bestämmelsernas tillämpningsområde i förhållande till föreslagna nya 21 a kap.

**164 §.** *Transport- och kommunikationsverkets domännamnsverksamhet och förmedling av domännamn.* I paragrafens 2 mom. görs en teknisk ändring, eftersom begreppet registrar framöver i nya 21 a kap. används även för sådana registrarer som inte gjort någon i 165 § i lagen avsedd anmälan som gäller förmedling av domäner som slutar på fi och ax. Framöver kan anteckningar i domänregistret således göras endast av en i 165 § avsedd registrar som gjort en

anmälan. Den ansvarar med andra ord för anteckningarna även då de görs på det sätt som nämns i 167 § 1 mom. i lagen av en aktör som handlar för en registrars räkning.

Dessutom fogas till paragrafen ett nytt *4 mom.* som på det sätt som genomförandet av NIS 2-direktivet förutsätter innehåller bestämmelser om tillämpningen av vissa skyldigheter enligt 21 kap. även på aktörer som tillhandahåller registreringstjänster för domännamn för registrarers räkning. De skyldigheter som föreskrivits i NIS 2-direktivet gäller aktörer som tillhandahåller registreringstjänster för domännamn, vilket enligt artikel 6.22 i direktivet utöver registrarer avser även entiteter som verkar som ombud för en registrar, såsom leverantörer eller återförsäljare av integritets- eller förmedlingstjänster. Eftersom en domän enligt 167 § i lagen ska antecknas i användarens namn med användarens riktiga uppgifter, blir det dock inte aktuellt att tillhandahålla alla sådana tjänster i fråga om domäner som slutar med fi och ax.

I det föreslagna momentet föreskrivs för det första att anmälningsskyldigheten enligt 165 § tillämpas på aktörer som agerar för registrarers räkning. Genom det genomförs artikel 3.3 och 3.4 i NIS 2-direktivet och artikel 27.2–27.4 i fråga om dessa aktörer. För det andra innehåller momentet bestämmelser om tillämpningen av de skyldigheter som gäller tillgången till uppgifter enligt 170 § i lagen på dessa aktörer i den omfattning som förutsätts för att genomföra artikel 27.3–5 i direktivet på miniminivå. Genom 1 mom. 2 punkten i paragrafen genomförs för egen del även artikel 28.1. Till exempel de särskilda nationella dataskyddsskyldigheterna som inte baserar sig på NIS 2-direktivet tillämpas dock inte på aktörer som agerar för registrarers räkning. För det tredje innebär 171 § i lagen att Transport- och kommunikationsverket vid överträdelse av lagen kan utöva sina i lagen föreskrivna befogenheter även i fråga om aktörer som verkar för registrarers räkning. Förslaget leder även till att föreskrifter som Transport- och kommunikationsverket har utfärdat med stöd av 165 § 3 mom. och 170 § 2 mom. i lagen kan kan tillämpas också på dessa aktörer.

**21 a kap. – Andra domännamn**

**172 a §.** *Kapitlets tillämpningsområde.* Med stöd av paragrafens *1 mom.* tillämpas nya 21 a kap. på andra domännamn än de som omfattas av tillämpningsområdet för 21 kap. och förmedling av dessa.

Nya 21 a kap. är avsett att allmänt gälla för toppdomänregister och förmedlingsverksamhet som gäller domännamn i Finland till den del som verksamheten inte omfattas av tillämpningsområdet för specialbestämmelserna om domännamn som slutar på fi och ax i 21 kap. Kapitlet tillämpas inte på domännamn som omfattas av tillämpningsområdet för 21 kap. eller på anknuten domännamnsverksamhet eller förmedling av domännamn. Nya 21 a kap. tillämpas således på andra domännamn än de som slutar med fi eller ax och förmedlingen av dessa, oberoende av domännamnets ändelse.

Paragrafens *2 mom.* innehåller en bestämmelse om det territoriella tillämpningsområdet för kapitlet. Kapitlet tillämpas på registrarer vars huvudsakliga verksamhetsställe eller en utsedd representant i Europeiska unionen finns i Finland. Om en registrar som är etablerad utanför Europeiska unionen inte har utsett någon representant i unionen, men tillhandahåller tjänster i Finland, omfattas registraren även av kapitlets tillämpningsområde. Bestämmelsen motsvarar artikel 26.2 och artikel 26.3 i NIS 2-direktivet om det territoriella tillämpningsområdet för skyldigheterna i direktivet.

I paragrafens 3 mom. föreskrivs att vad som i detta kapitel föreskrivs om registrarer tillämpas också på på aktörer som tillhandahåller registreringstjänster för domännamn för registrarers räkning, när de utövar förmedling av domännamn. Omnämnandet motsvarar

tillämpningsområdet för de skyldigheter som förutsätts i artikel 28 i NIS 2-direktivet, eftersom även aktörer som handlar för registrarers räkning utöver registrarer definieras som entiteter som tillhandahåller domännamnsregistreringstjänster i artikel 6.22 i NIS 2-direktivet. De aktörer som agerar för registrarer kan vara till exempel tillhandahållare eller återförsäljare av integritets- eller förmedlingstjänster.

**172 b §.** *Registrarens anmälan*. Paragrafen innehåller bestämmelser om de uppgifter som en registrar ska anmäla till Transport- och kommunikationsverket. Genom paragrafen kompletteras genomförandet av artikel 3.3 och 3.4 och artikel 27 i NIS 2-direktivet i fråga om sådana registrarer som förmedlar andra domännamn än de som omfattas av tillämpningsområdet för 21 kap. En registrar ska till Transport- och kommunikationsverket anmäla namn, adress, e-postadress, telefonnummer och andra uppdaterade kontaktuppgifter, sin IP-adressdomän och en förteckning över de medlemsstater i Europeiska unionen där den tillhandahåller sina tjänster. Dessutom ska den anmäla kontaktuppgifterna för sina verksamhetsställen och företrädare i Europeiska unionen. En registrar ska utan dröjsmål anmäla förändringar i de uppgifter som avses i 1 mom. inom den tidsfrist på två veckor eller tre månader som förutsätts i direktivet beroende på den förändrade uppgiften. Transport- och kommunikationsverket kan utfärda närmare föreskrifter om anmälan av uppgifter på samma sätt som för den motsvarande anmälningsskyldighet föreskrivits i 41 § i cybersäkerhetslagen, vilken bland annat gäller den som förvaltar ett toppdomänregister. Den gemensamma kontaktpunkt som avses i 18 § i cybersäkerhetslagen ansvarar för att göra anmälningar enligt artikel 27.4 i NIS 2-direktivet, varför Transport- och kommunikationsverket ska överlämna de uppgifter som behövs för att göra anmälan till den gemensamma kontaktpunkten. Den gemensamma kontaktpunkten finns vid Transport- och kommunikationsverket.

**172 c §.** *Registreringsuppgifter om domännamn.* Paragrafen innehåller bestämmelser om skyldigheten för den som förvaltar ett toppdomänregister och en registrar att samla in och upprätthålla registreringsuppgifter om domännamn. Det föreslås att uppgifter ska samlas in och administreras på det sätt som artikel 28 i NIS 2-direktivet förutsätter. I uppgifterna enligt artikel 28.2 i NIS 2-direktivet ska man inkludera domännamn, registreringsdatum, registrantens namn, e-postadress och telefonnummer och e-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet om dessa inte är desamma som för registranten. Skyldigheten hänför sig till bägge aktörstyper, men samarbetsskyldigheten enligt 172 § ska iakttas i fullgörandet av den. Den som förvaltar ett toppdomänregister och registrarer ska dessutom införa och offentligt tillgängliggöra de riktlinjer och förfarandena med vilka de säkerställer att registreringsuppgifterna om domännamn är exakta och korrekta. Genom paragrafen genomförs artikel 28.2 och 28.3 i NIS 2-direktivet i fråga om andra registrarer än de som omfattas av tillämpningsområdet för 21 kap.

**172 d §.** *Tillgång till registreringsuppgifter om domännamn.* Paragrafen innehåller bestämmelser om att tillträde beviljas till registreringsuppgifter om domännamn på det sätt som artikel 28.4 och 28.5 i NIS 2-direktivet förutsätter och att det samarbete som förutsätts i 6 punkten ska föras.

Paragrafens *1 mom.* innehåller bestämmelser om den offentliga tillgängligheten för registreringsuppgifter om domännamn till den del som uppgifterna inte är personuppgifter. Med stöd av momentet ska andra registreringsuppgifter om domännamn än personuppgifter göras offentligt tillgängliga utan oskäligt dröjsmål efter registreringen av ett domännamn. Skyldigheten hänför sig till bägge aktörstyper, men den föreslagna samarbetsskyldigheten enligt 3 mom. ska iakttas i fullgörandet av den.

Paragrafens *2 mom.* innehåller bestämmelser om utlämnande av registreringsuppgifter om domännamn till den del som uppgifterna är personuppgifter. Med stöd av momentet ska tillgång ges till registreringsuppgifterna om domännamn, om den som begär tillgång till uppgifterna och är berättigad till det lägger fram en lagenlig och behörigt motiverad begäran. En begäran ska besvaras utan oskäligt dröjsmål och senast inom 72 timmar från det att begäran tagits emot. Skyldigheten möjliggör inte att en avgift tas ut för lämnade av uppgifter. Dessutom ska ett toppdomänregister och en registrar göra deras riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.

Paragrafens *3 mom.* innehåller bestämmelser om skyldigheten för de som förvaltar ett toppdomänregister och registrarer att samarbeta för att fullgöra de skyldigheter som föreskrivs i 172 c § och i 172 d § och för att undvika insamling av överlappande registreringsuppgifter Genom momentet genomförs artikel 28.6 i NIS 2-direktivet, enligt vilken efterlevnad av de skyldigheter som föreskrivits i 1–5 punkten inte får leda till överlappningar i insamlingen av registreringsuppgifter om domännamn. För detta ska medlemsstaterna förutsätta att toppdomänregister och de entiteter som tillhandahåller domännamnsregistreringstjänster ska samarbeta med varandra. Det är dock möjligt att anse att det samarbete som direktivet förutsätter inte begränsar sig på begränsat sätt till insamling av uppgifter, utan att det mer generellt är behövligt för att fullgöra de skyldigheter som direktivet förutsätter.

Det finns olika verksamhetsmodeller för att registrera domännamn och publicera registreringsuppgifter. Syftet med föreslagna 172 c § och 172 d § är att möjliggöra olika motiverade sätt för att genomföra insamlingen, verifieringen, administreringen och tillträdet till uppgifterna och en ändamålsenlig arbetsfördelning i ett samarbete mellan de olika aktörerna i mån av möjlighet inom de ramar som bästa avtalsbaserad praxis som uppkommit i det internationella samarbetet möjliggör, under förutsättning att det slutresultat som NIS 2-direktivet förutsätter uppnås. Beroende på fallet är det möjligt att till exempel en registrar i praktiken ansvarar för att tillgängliggöra uppgifterna i enlighet med den skyldighet som föreskrivs i 1 mom. i denna paragraf till den del som de uppgifter som direktivet förutsätter inte ingår i de uppgifter som hålls tillgängliga av förvaltaren av ett toppdomänregister, medan förvaltaren av ett toppdomänregister kan ansvara för att uppgifterna om grundande av ett domännamn och tillgången till uppgifterna om denna registrar är tillgängliga. Om ett toppdomsänsregister å sin sida offentliggör alla uppgifter som förutsätts, är det inte befogat att förutsätta att registraren offentliggör uppgifterna på nytt. Det är inte heller ändamålsenligt att aktörer som handlar för en rergistrars räkning, på vilka skyldigheten även tillämpas, på egen hand ska offentliggöra uppgifterna på nytt, om de offentliggjorts av en förvaltare av ett toppdomänregister eller registrar.

Paragrafens *4 mom.* innehåller en informativ hänvisning till den allmänna dataskyddsförordningen som gäller skyddet för personuppgifter och till dataskyddslagen.

**304 §.** Det föreslås att 304 § 1 mom. 14 punkten, som gäller genomförandet av cybersäkerhetsakten och Transport- och kommunikationsverkets särskilda uppgifter som nationell myndighet för cybersäkerhetscertifiering, upphävs i lagen om tjänster inom elektronisk kommunikation. Framöver utfärdas bestämmelser om Transport- och kommunikationsverkets uppgift som nationell myndighet för cybersäkerhetscertifiering i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering. Således föreslås att bestämmelsen upphävs, eftersom den är överlappande med den föreslagna lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering.

### 7.5 Lagen om verkställighet av böter

**1 §.** *Lagens tillämpningsområde*. Rättsregistercentralen verkställer försummelse- och påföljdsavgifter som påförs med stöd av olika lagar genom att iaktta det förfarande som förskrivits för verkställighet av böter. Det föreslås att nya 37 punkten fogas till paragrafens *2 mom.*, med stöd av vilken en påföljdsavgift enligt 31–37 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering verkställs enligt ordningen i lagen. Med anledning av ändringen görs en teknisk ändring i 36 punkten.

## 8 Bestämmelser på lägre nivå än lag

Det föreslås att 10 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering innehåller bestämmelser om möjligheten att inrätta en regulatorisk sandlåda. Med stöd av föreslagna 10 § 4 mom. kan närmare tekniska bestämmelser om organiseringen av och verksamheten hos regulatoriska sandlådor för cyberresiliens och om ansökan av en ekonomisk aktör utfärdas genom föreskrift av Transport- och kommunikationsverket. Det handlar om tekniska föreskrifter om verksamheten i regulatoriska sandlådor och det är ändamålsenligt att ge den myndighet som inrättar en regulatorisk sandlåda befogenheter att utfärda dessa föreskrifter. I verksamhet i en regulatorisk sandlåda är det möjligt att det framkommer ett behov av att ändra de tekniska föreskrifterna för verksamheten med beaktande av till exempel utvecklingen för hotmiljön för cybersäkerheten eller andra särdrag i anknytning till cybersäkerheten.

De grundläggande bestämmelserna som gäller avgiftsbelagdheten för de statliga myndigheternas prestationer och beloppet av dessa ingår i lagen om grunderna för avgifter till staten. Även om propositionen innehåller förslag som gäller avgiftsbelagdheten för statliga myndigheters prestationer, innehåller propositionen inte i fråga om dessa förslag nya bemyndiganden att utfärda förordningar. Bemyndigandet att utfärda förordning om avgiftsbelagdheten för statliga myndigheters prestationer baserar sig på 8 § i lagen om grunderna för avgifter till staten, sådan den lyder i gällande form.

I 172 b § 2 mom. som fogas till lagen om tjänster inom elektronisk kommunikation föreskrivs att Transport- och kommunikationsverket har rätt att utfärda närmare tekniska föreskrifter om utlämnande av uppgifter för förteckningen över registrarer, vilket motsvarar motsvarande reglering i cybersäkerhetslagen. Dessutom är ändringen av 164 § i lagen, vilken påverkar tillämpningsområdet för 21 kap., betydelsefull med tanke på bemyndigandena att utfärda föreskrifter enligt 165 § och 170 § i lagen.

## 9 Ikraftträdande

Det föreslås att lagarna träder i kraft den 1 juni 2026, med undantag för de föreslagna ändringarna i anknytning till genomförandet av NIS 2-direktivet i lagen om tjänster inom elektronisk kommunikation, vilka föreslås träda i kraft så fort som möjligt.

Det föreslås att tillämpningen av den föreslagna lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering i fråga om vissa bestämmelser tillämpas på graderat sätt på ett sätt som motsvarar början för tillämpningen av cyberresiliensförordningen. I enlighet med artikel 71 tillämpas cyberresiliensförordningen från och med den 11 december 2027. Kapitel IV som gäller anmälda organ tillämpas från och med den 11 juni 2026 och artikel 14 som gäller rapporteringsskyldigheterna från och med den 11 september 2026.

Övergångsbestämmelser på tre månader föreslås till vissa delar för de ändringar som gäller toppdomänregister och förmedling av domännamn i lagen om tjänster inom elektronisk kommunikation. Inom övergångstiden ska de anmälningar om tillhandahållande av registreringstjänster för domännamn vilka förutsätts av den föreslagna lagen göras och de riktlinjer och förfarande som direktivet förutsätter ska offentliggöras.

## 10 Verkställighet och uppföljning

Artikel 70 i cyberresiliensförordningen innehåller en skyldighet som gäller översyn av förordningen för Europeiska kommissionen. Senast den 1 december 2030 och därefter vart fjärde år överlämnar kommissionen till Europaparlamentet och rådet en offentlig berättelse om utvärderingen och översynen av cyberresiliensförordningen.

Artikel 52 i cyberresiliensförordningen innehåller uppgifter för marknadskontrollmyndigheterna, vilka stödjer genomförandet och uppföljningen av regleringen. Marknadskontrollen ska bland annat årligen rapportera resultaten av de relevanta marknadskontrollåtgärderna till kommissionen och följa hur tillverkarna tillämpat de kriterier som avses i artikel 13.8 i cyberresiliensförordningen då de fastställer stödtiden för produkter med digitala element.

Med stöd av cyberresiliensförordningen grundas därtill en administrativ samarbetsgrupp mellan de olika medlemsstaternas marknadskontrollmyndigheter. Denna Adco-grupp ska i en allmänt tillgänglig och användarvänlig form offentliggöra relevant statistik om kategorier av produkter med digitala element, inbegripet genomsnittliga stödperioder, vilka fastställs av tillverkaren enligt artikel 13.8, samt tillhandahålla vägledning som inbegriper vägledande stödperioder för kategorier av produkter med digitala element.

Även cybersäkerhetsakten innehåller bestämmelser som förutsätter att kommissionen ger en utvärderingsberättelse om förordningen för första gången år 2024. En översyn av förordningen pågår fortfarande i kommissionen och den kan leda till att ett ändringsförslag läggs fram.

## 11 Förhållande till andra propositioner

Lagförslag 1 innehåller hänvisningar till den föreslagna lagen om tillsyn över vissa system för artificiell intelligens. Förslaget om denna lag ingår i regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s förordning om artificiell intelligens RP 46/2025 rd. Genom propositionen föreslås även att lagen om marknadskontrollen av vissa produkter och lagen om verkställighet av böter ändras, vilket är av betydelse även för ändringarna i lagförslag 2 och 5 i denna proposition. Behandlingen av denna proposition pågår ännu i riksdagen.

Flera regeringspropositioner som innehåller förslag om att ändra 1 § 2 mom. i lagen om verkställighet av böter är anhängiga hos riksdagen. Dessa propositioner utgörs utöver vad som nämnts i det föregående avsnittet av regeringens proposition till riksdagen med förslag till lag om karens i anslutning till uppdraget som medlem av statsrådet och lag om ändring av 1 § i lagen om verkställighet av böter (RP 90/2024 rd), regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU-förordningen om transparens och inriktning när det gäller politisk reklam (RP 57/2025 rd), regeringens proposition till riksdagen med förslag till lag om underlättande av utbyggnad av nät med mycket hög kapacitet och till lagar om ändring av 249 och 303 § i lagen om tjänster inom elektronisk kommunikation och 1 § i lagen om verkställighet av böter (RP 74/2025 rd), riksdagens proposition till riksdagen med förslag till lag om tillsyn över skyldigheterna och om påföljder enligt EU:s avskogningsförordning samt till lagar som har samband med den (RP 77/2025 rd), regeringens proposition till riksdagen med

förslag till lagstiftning som kompletterar EU:s dataförordning (RP 128/2025 rd) och regeringens proposition till riksdagen om godkännande och sättande i kraft av överenskommelsen med Norge om internationell taxitrafik på väg och med förslag till vissa andra lagar (RP 134/2025 rd).

## 12 Förhållande till grundlagen samt lagstiftningsordning

Propositionen innehåller förslag som är betydelsefulla med tanke på grundlagen i förhållande till bestämmelserna i grundlagen om lagbundenheten för utövning av offentligt makt enligt 2 § 3 mom., skyddet för privatliv, hemfrid och personuppgifter enligt 10 §, egendomsskyddet enligt 15 §, näringsfriheten enligt 18 §, utfärdande av förordningar och delegering av lagstiftningsbehörighet enligt 80 § och överföring av förvaltningsuppgifter på andra än myndigheter enligt 124 §.

### 12.1 Myndighetsuppgifter

I cyberresiliensförordningen åläggs medlemsstaterna att utse en marknadskontrollmyndighet och att anmäla myndigheten. Skyldigheten att utse en myndighet kommer direkt från förordningen. Huruvida en eller flera myndigheter ska utses och vilka dessa myndigheter är hör till den nationella prövningsrätten.

Grundlagsutskottet har när det bedömt bestämmelser om myndigheternas befogenheter även utgått från att regleringen av myndigheters befogenheter är betydelsefull med tanke på rättsstatsprincipen i grundlagens 2 § 3 mom. (GrUU 51/2006 rd, s. 2/I). Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag och i all offentlig verksamhet ska lag noggrant iakttas. Utgångspunkten är att den som utövar offentlig makt alltid ska ha en behörighetsgrund som i sista hand återgår på en av riksdagen stiftad lag. För lagar gäller det allmänna kravet på att en lag ska vara exakt och noga avgränsad. (GrUU 19/2021 rd, punkt 15 med hänvisningar). Den behöriga beslutsfattaren ska entydigt framgå av lagen (GrUU 18/2021 rd, punkt 2). Enligt utskottets uppfattning är reglering kring behörigheter i allmänhet betydelsefull även med tanke på de grundlagstryggade grundläggande fri- och rättigheterna (se GrUU 10/2016 rd, s. 3). När en myndighet ges nya uppgifter ska de lämpa sig för myndigheten (se GrUU 32/2020 rd, s. 5).

I fråga om sakinnehåll lämpar sig uppgifterna enligt cyberresiliensförordningen på det föreslagna sättet för Transport- och kommunikationsverkets uppgifter. Vilken myndighet som har till uppgift att övervaka AI-system med hög risk fastställs utifrån lagen om tillsyn över vissa system för artificiell intelligens och EU:s förordning om artificiell intelligens, eftersom de marknadskontrollmyndigheter som utsetts för förordningen om artificiell intelligens även ansvarar för de marknadskontrollåtgärder som krävs med stöd av cyberresiliensförordningen, och till denna del finns det inte något nationellt handlingsutrymme för att ordna marknadskontrollen. Innehållet i uppgifterna fastställs i huvudsak utifrån cyberresiliensförordningen. Regleringen i cyberresiliensförordningen kompletteras av bestämmelser i de nationella allmänna lagarna om förvaltning, marknadskontrollagen och bestämmelserna i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering bland annat om utbyte av uppgifter. Myndigheternas nya uppgifter baserar sig på lagen och på den direkt tillämpliga EU-förordningen. Uppgifterna för den behöriga myndigheten har definierat noggrant och exakt i den föreslagna lagen.

### 12.2 Överföring av offentliga förvaltningsuppgifter på andra än myndigheter

Enligt 124 § i grundlagen kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock anförtros endast myndigheter.

Enligt grundlagsutskottets tolkningspraxis är en förutsättning för att anförtro skötseln av en offentlig förvaltningsuppgift någon annan än en myndighet att lagen, åtminstone på ett allmänt sätt, fastställer den kompetens eller behörighet som förutsätts av den som sköter uppgiften (bland annat GrUU 28/2001 rd och GrUU 48/2001 rd). I sin tolkningspraxis har grundlagsutskottet ansett att det för att kraven på rättssäkerhet och god förvaltning ska anses vara uppfyllda i den bemärkelse som avses i 124 § i grundlagen krävs att ärendena behandlas i enlighet med de allmänna förvaltningslagarna och att de som behandlar ärendena handlar under tjänsteansvar (GrUU 33/2004 rd, s. 7/II, GrUU 46/2002 rd, s. 10). De allmänna förvaltningslagarna tillämpas, med stöd av sina bestämmelser om tillämpningsområde, myndighetsdefinition eller skyldigheten för en enskild att betjäna på ett visst språk, även på enskilda när de fullgör offentliga förvaltningsuppgifter (GrUU 42/2005 rd, s. 3/II). Bestämmelserna om straffrättsligt tjänsteansvar tillämpas även på dem som är anställda hos bolaget när de utför offentliga förvaltningsuppgifter (GrUU 26/2017 rd, s. 55–56, GrUU 16/2016 rd, s. 2–3, GrUU 8/2014 rd, s. 5/I).

De anmälda organen enligt cyberresiliensförordningen utför uppgifter för att bedöma överensstämmelsen, vilka handlar om en offentlig förvaltningsuppgift. I artikel 39.2 i cyberresiliensförordningen konstateras att ett organ för bedömning av överensstämmelse ska ha inrättats enligt den nationella lagstiftningen i en medlemsstat och att det ska vara en juridisk person. Dessutom innehåller artikel 39 detaljerade och noggranna bestämmelser om kraven i skötseln av uppgift som organ för bedömning av överensstämmelse. Om ett organ för bedömning av överensstämmelse låter en underleverantör utföra vissa uppgifter i anknytning till bedömningen av överensstämmelse eller använder dotterbolag, ska organet för bedömning av överensstämmelse med stöd av artikel 41 i cyberresiliensförordningen säkerställa att underleverantören eller dotterbolaget uppfyller även de krav som föreskrivs i artikel 39 i cyberresiliensförordningen och anmäla detta till myndigheten. Även situationer där verksamheten vid ett anmält organ för bedömning av överensstämmelse ska begränsas eller återkallas har reglerats närmare i artikel 45 i förordningen. Den direkt tillämpliga detaljerade regleringen i cyberresiliensförordningen kan med tanke på 124 § i grundlagen anses bilda en tillräcklig författningsgrund för kompetensen och behörigheten för den som sköter uppgiften. Uppgifterna vid ett anmält organ handlar inte om betydande utövning av offentlig makt.

På kraven på organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och som sköter uppgifter enligt cybersäkerhetsakten tillämpas å sin sida bilagan till förordningen på grund av hänvisningen till artikel 60.1 i cybersäkerhetsakten. Även denna uppgift handlar om en offentlig förvaltningsuppgift. Kraven överensstämmer med motsvarande krav i cyberresiliensförordningen. Ett organ för bedömning av överensstämmelse ska ha inrättats enligt nationell lagstiftning och det ska vara en juridisk person. Bilagan innehåller detaljerade krav på bedömningarna och med dessa säkerställs oberoendet och utesluts intressekonflikter. Organen för bedömning av överensstämmelse ska säkerställa att deras dotterbolags och underleverantörers åtgärder inte påverkar tillförlitligheten, objektiviteten eller opartiskheten i de åtgärder som de vidtagit för att bedöma överensstämmelsen. Den direkt tillämpliga detaljerade regleringen i cybersäkerhetsakten kan med tanke på 124 § i grundlagen

anses bilda en tillräcklig författningsgrund för kompetensen och behörigheten för den som sköter uppgiften. Uppgiften handlar inte om betydande utövning av offentlig makt.

Dessutom möjliggör lagförslag 1 att uppgifter i anknytning till cybersäkerhetscertifiering vilka tilldelats myndigheten för cybersäkerhetscertifiering delegeras till ett organ för bedömning av överensstämmelse på ett sätt som överensstämmer med regleringen i cybersäkerhetsakten. Uppgifterna är likadana som i övrigt för uppgifterna för organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering med stöd av cybersäkerhetsakten och de handlar om utövning av offentlig makt, dock inte om utövning av avsevärd offentlig makt. Skillnaden är att det handlar om utfärdande av certifikat av hög assuransnivå, vilken i cybersäkerhetsakten i princip är en uppgift som reserverats för myndigheter. Hög assuransnivå på certifieringen gör dock i sig inte uppgiften till en sådan betydande utövning av offentlig makt som inte kan tilldelas någon utanför myndighetsmaskineriet. Delegering kan vara behövligt i synnerhet på grund av det specialkunnande av hög nivå som förutsätts i uppgiften. Förslaget möjliggör att exaktare kompetenskrav fastställs i avtalet om delegering, om det är behövligt med tanke på det tillämpliga certifieringssystemet. Det föreslås att lagen innehåller bestämmelser om de allmänna kraven på organ för bedömning av överensstämmelse med ackreditering och eventuella bemyndiganden, vilka med tanke på 124 § i grundlagen på tillräcklig nivå säkerställer att den som sköter uppgiften har kompetens även i fråga även om den delegerade uppgiften.

Ett anmält organ och ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering anses i sin uppgift fungera som en självständig personuppgiftsansvarig i förhållande till dess anmälande myndighet.

*Tillgodoseende av de grundläggande fri- och rättigheterna, rättsskyddet och andra krav på god förvaltning* Ytterligare ett villkor för att offentliga förvaltningsuppgifter ska kunna anförtros andra än myndigheter är att det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. I 118 § i grundlagen finns bestämmelser om ansvaret för ämbetsåtgärder. Tjänsteansvaret omfattar såväl ett skadeståndsrättsligt som ett straffrättsligt ansvar. När det genom lag utfärdas att skötseln av en offentlig förvaltningsuppgift anförtros någon annan än en myndighet, ska man enligt grundlagsutskottets vedertagna tolkning genom bestämmelser säkerställa att samma bestämmelser som tillämpas på den som sköter uppgiften med tjänsteansvar tillämpas på den som sköter uppgiften (GrUU 5/2010 rd, GrUU 3/2009 rd, GrUU 1/2008 rd). Den föreslagna lagen innehåller den bestämmelse om tjänsteansvar som grundlagsutskottet förutsätter i sin tolkningspraxis. Bestämmelserna om straffrättsligt ansvar tillämpas på ett anmält organ enligt cybersäkerhetsakten och ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering eller på personalen i dotterbolag eller underleverantörer som de anlitar då de sköter de uppgifter som avses i cybersäkerhetsakten, cyberresiliensförordningen eller den föreslagna lagen. De allmänna förvaltningslagarna blir tillämpliga även utan separat hänvisning. Det är även möjligt att göra en begäran om omprövning eller söka ändring i ett beslut som fattats av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering, vilket tryggar tillgodoseendet av det rättsskydd som föreskrivits i 21 § i grundlagen.

*Tillståndsplikten för uppgifterna för ett anmält organ och ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och begränsning eller indragning av uppgifterna* Enligt den föreslagna regleringen ska ett organ för bedömning av överensstämmelse göra en ansökan om utseende som ett anmält organ enligt cyberresiliensförordningen och anmälan till Transport- och kommunikationsverket. Ett bedömningsorgan som uppfyller kraven i artikel 39 i cyberresiliensförordningen i fråga om de produkter med digitala element för vilka bedömningsorganet har kompetens utses som ett

anmält organ. På motsvarande sätt förutsätter certifieringsverksamhet enligt cybersäkerhetsakten i fråga om ett organ för bedömning av överensstämmelse att Transport- och kommunikationsverket anger det för cybersäkerhetscertifiering till kommissionen. Anmälning förutsätter ackreditering av ackrediteringstjänster FINAS och att de förutsättningar som ställs i bilagan till cybersäkerhetsakten och i den tillämpliga certifieringsordningen är uppfyllda.

Anmälda organ enligt cyberresiliensförordningen och organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering enligt cybersäkerhetsakten utför uppgifter för att bedöma överensstämmelse, vilka handlar om en offentlig förvaltningsuppgift. Grundlagsutskottet har i sin praxis ansett att skötseln av förvaltningsuppgifter som i princip ankommer på en myndighet omfattas av den näringsfrihet som tryggats i 18 § 1 mom. i grundlagen (GrUU 23/2013 rd, GrUU 20/2006 rd, s. 3/I). Grundlagsutskottet har dock ansett att det med tanke på proportionaliteten för regleringen kring rättigheterna och skyldigheterna för en enskild aktör som inte hör till någon myndighetsorganisation är nödvändigt att möjligheten att återkalla ett godkännande binds till allvarliga och väsentliga överträdelser eller försummelser och till att anmärkningar och varningar som getts till en enskild aktör inte lett till att bristerna i verksamheten åtgärdats (GrUU 23/2013 rd, GrUU 20/2006 rd, s. 3/I, GrUU 27/2010 rd, s. 3/II).

Cyberresiliensförordningen innehåller bestämmelser om avgränsning och återkallelse av utseendet. Om ett anmält organ inte längre uppfyller de föreskrivna kraven eller inte fullgör sina skyldigheter, är det behövligt att den myndighet som ansvarar för anmälningen begränsar anmälan eller återkallar den tillsvidare eller i sin helhet, beroende på hur allvarligt underlåtenheten att fullgöra kraven eller iaktta skyldigheterna varit. Till denna del finns det inte något nationellt handlingsutrymme. De genomförandeakter som getts med stöd av cybersäkerhetsakten fastställer för egen del förutsättningarna för att en myndighet på olika sätt ska begränsa rätten för ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering att utföra uppgifterna enligt de aktuella akterna. Till den del som EU-rätten inte innehåller andra bestämmelser om ärendet, innehåller den föreslagna lagen bestämmelser om befogenheterna för myndigheten att i sista hand återkalla ett utseende, om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte åtgärdat sin verksamhet inom den utsatta tiden och det handlar om en väsentlig överträdelse eller försummelse eller om det inte uppfyller de krav som ställts på det eller om dess ackreditering begränsas, återkallas eller avbryts.

I förslaget föreskrivs dessutom att myndigheten för cybersäkerhetscertifiering får säga upp eller häva ett avtal om delegering, om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte längre uppfyller de allmänna kraven för det eller om organet väsentligt åsidosätter fullgörandet av de uppgifter man kommit överens om i avtalet eller annars bryter mot avtalet eller väsentligen eller upprepade gånger handlar lagstridigt.

Förslaget bedöms uppfylla de krav som grundlagsutskottet i praktiken ställt för återkallande av godkännande av verksamheten.

*Anlitande av experter vid inspektioner* Förslaget möjliggör att myndigheten för cybersäkerhetscertifiering kan låta en oberoende expert med behövlig utbildning och erfarenhet utföra en inspektion. Enligt förslaget tillämpas i så fall bestämmelserna om straffrättsligt tjänsteansvar på experter, och därtill tillämpas de allmänna förvaltningslagarna även utan uttryckligt omnämnande, vilket tryggar att kraven på god förvaltning iakttas. Rollen för externa experter är kompletterande. Myndigheten anses då fungera som personuppgiftsansvarig och experten som personuppgiftsbiträde. Däremot fattar myndigheten eventuella administrativa

beslut utifrån observationerna vid inspektionen. På grund av behovet av särskild expertis i övervakningen och tryggandet av effektiv användning av myndigheternas resurser ska möjligheten att använda en extern expert anses vara ändamålsenlig. Således är det inte med tanke på 124 § i grundlagen problematiskt att använda en extern expert.

### 12.3 Egendomsskydd

Bestämmelsen i 19 § 1 2 mom. i lagförslag 1, enligt vilken ingen ersättning betalas till en ekonomisk aktör för att en programvara tas för undersökning, är betydelsefull för det grundlagstryggade egendomsskyddet. Enligt 15 § i grundlagen är vars och ens egendom tryggad. Enligt grundlagsutskottets etablerade utlåtandepraxis omfattar egendomsskyddet utöver den principiella rätten för en ägare att disponera och använda sin egendom på önskat sätt också rätten att råda över den (GrUU 41/2006 rd, s. 2, GrUU 49/2005 rd, s. 2, GrUU 15/2005 rd, s. 2). Ägarens rättigheter kan begränsas genom lag, förutsatt att regleringen uppfyller de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna.

Den föreslagna bestämmelsen omfattas av det nationella handlingsutrymmet. Det handlar om ett undantag till regleringen i marknadskontrollagen enligt vilken marknadskontrollmyndigheten enligt 10 § 2 mom. i marknadskontrollagen på yrkande från en ekonomisk aktör ska ersätta en produkt som tagits för undersökning enligt gängse pris, förutsatt att det inte framgår att produkten inte överensstämmer med kraven. Grunden för undantaget är att tagande för undersökning av en programvara i digitalt format, det vill säga i praktiken överlämnande av en elektronisk kopia, i motsats till en fysisk produkt, för den ekonomiska aktören inte orsakar sådana försäljningsförluster och inte heller andra skador att ersätta vilka ska ersättas enligt programvarans gängse värde. Eftersom sådant tagande för undersökning inte begränsar möjligheten för tillverkaren av programvaran eller en annan ekonomisk aktör att använda sin egendom eller tillverka nya kopior av den och inte orsakar någon ekonomisk skada som är större än ett litet besvär, bedöms förslaget inte vara problematiskt med tanke på egendomsskyddet.

### 12.4 Anmälningsskyldigheten för registrarer

Nya 21 a kap. 172 b § i lagen om tjänster inom elektronisk kommunikation innehåller bestämmelser om anmälningsskyldigheten för registrarer och dem som agerar för deras räkning. Dessutom utvidgas anmälningsskyldigheten enligt 21 kap. till dem som agerar för registrarers räkning. Förslaget innebär i praktiken att en aktör som omfattas av tillämpningsområdet har en skyldighet att anmäla sin verksamhet till Transport- och kommunikationsverket och det är således betydelsefullt med tanke på den näringsfrihet som tryggats i 18 § i grundlagen.

Genomförandet av artikel 27 i NIS 2-direktivet förutsätter att uppgifter enligt anmälningsskyldigheten samlas in från registrarerna. Dessutom innebär anmälningsskyldigheten att Transport- och kommunikationsverket får information om de registrarer som omfattas endast av tillämpningsområdet för nya 21 a kap., vilket är en förutsättning för att rikta tillsynen på registrarer. De uppgifter som ska anmälas utgörs av aktörens kontaktuppgifter och den kan således rimligen anmälas och uppdateras.

Grundlagsutskottet har inte ansett att anmälningsskyldigheten är problematisk med tanke på näringsfriheten, då en utebliven anmälan inte inneburit ett förbud att bedriva verksamhet (GrUU 16/2009 rd, s. 3/I) eller då en myndighet inte förutsätts fatta något beslut med anledning av anmälan (GrUU 54/2002 rd, s. 3/I). Det förutsätts inte att Transport- och kommunikationsverket fattar något beslut på grund av anmälan. En utebliven anmälan innebär i sig inte något förbud

att erbjuda en tjänst eller att bedriva verksamhet. Förslaget bedöms således inte vara problematiskt med tanke på näringsfriheten.

### 12.5 Skyddet för hemfrid

Med stöd av föreslagna 19 § kan marknadskontrollmyndigheten under vissa förutsättningar göra en inspektion i ett utrymme som används för boende av permanent natur. Förslaget är av betydelse med avseende på skyddet för hemfriden, som tryggas i 10 § i grundlagen.

Enligt 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Enligt 10 § 3 mom. i grundlagen kan det genom lag föreskrivas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas eller för att brott ska kunna utredas. Enligt artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Enligt artikel 52 i stadgan ska varje begränsning i utövandet av dessa rättigheter vara föreskriven i lag och får endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Enligt grundlagsutskottets utlåtandepraxis omfattar hemfridsskyddet enligt 10 § i grundlagen i princip alla utrymmen som används för boende av permanent natur, det vill säga även sådana lokaler för näringsidkare som finns till exempel i näringsidkarens bostad. Enligt utskottet kommer själva kärnan i hemfriden dock inte nödvändigtvis i riskzonen när man inspekterar lokaler där det utövas närings- eller yrkesverksamhet (se till exempel GrUU 17/2018 rd, s. 5, GrUU 54/2014 rd, s. s. 2/II, GrUU 21/2010 rd och GrUU 6/2019).

I sin utlåtandepraxis om myndigheternas inspektionsrätt i anknytning till genomförandet av EU-regleringen har grundlagsutskottet ansett att den inte har något konstitutionellt att anmärka om regleringen kring inspektioner som omfattas av EU-förordningens tillämpningsområde och förutsätts av EU-regleringen (GrUU 12/2019 rd och GrUU 6/2019 rd). Grundlagsutskottet har riktat uppmärksamhet på att det i Europeiska unionens stadga om de grundläggande rättigheterna tryggade hemfridsskyddet inte till alla delar är enhetligt med 10 § 3 mom. i grundlagen. I grundlagsutskottets utlåtanden har man riktat uppmärksamhet på att stadgan om de grundläggande rättigheterna inte innehåller något likadant kvalificerat lagförbehåll som den finländska grundlagen, varför det ibland kan vara svårt att utan problem samordna EU-reglering som även är enhetlig med stadgan om de grundläggande rättigheterna med Finland konstitution (se till exempel GrUU 6/2019 rd och GrUU 39/2016 rd). Dessutom har grundlagsutskottet ansett att det är viktigt att det, i den mån som EU-lagstiftningen kräver reglering på det nationella planet eller möjliggör sådan, tas hänsyn till de krav som de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ställer när det nationella handlingsutrymmet utnyttjas (GrUU 25/2005 rd). Grundlagsutskottet har till denna del ansett att om inspektionsbefogenheten på hemfridsskyddade platser inte till alla delar krävs i EU-förordningen, måste befogenheten att utföra inspektioner i utrymmen som omfattas av hemfriden begränsas till vad som är nödvändigt med avseende på förordningen (till exempel GrUU 6/2019 rd).

Den föreslagna befogenhetsregleringen kring kontroller förutsätts av EU-regleringen och den beaktar de krav som grundlagsutskottet ställt i praktiken.

Enligt artikel 52 i cyberresiliensförordningen tillämpas på marknadskontrollen av produkter vid sidan om de produkter som omfattas av förordningens tillämpningsområde även förordning (EU) 2019/1020 (den så kallade marknadskontrollförordningen). I artikel 14.4 i marknadskontrollförordningen föreskrivs det om de minimibefogenheter som

marknadskontrollmyndigheterna i medlemsstaterna ska ha tillgång till. Enligt artikel 14.4 e i marknadskontrollförordningen ska marknadskontrollmyndigheterna ha befogenhet att få tillträde till lokaler, mark eller transportmedel som den berörda ekonomiska aktören använder för ändamål som har samband med den ekonomiska aktörens näringsverksamhet, affärsverksamhet, hantverk eller yrke, i syfte att identifiera bristande överensstämmelse och erhålla bevis.

Marknadskontrollförordningen kompletteras nationellt av lagen om marknadskontroll. Enligt 9 § 1 mom. i marknadskontrollagen har marknadskontrollmyndigheten med tanke på kontrollen rätt att få tillträde till alla lokaler där det bedrivs sådan verksamhet som avses i de lagar som nämns i 1 § 1 mom. eller där det förvaras uppgifter som är betydelsefulla för kontrollen, och utföra sådana inspektioner som behövs för kontrollen. Det är dock inte tillåtet att utsträcka inspektioner till utrymmen som används för boende av permanent natur. Vid inspektionerna följs bestämmelserna i 39 § i förvaltningslagen (434/2003). Enligt paragrafens 2 mom. utfärdas bestämmelser om marknadskontrollmyndighetens rätt att utsträcka inspektioner till utrymmen som används för boende av permanent natur vid behov separat i de lagar som nämns i 1 § 1 mom.

Marknadskontrollförordningen förutsätter att marknadskontrollmyndighetens befogenheter är tillgängliga i övervakningen av alla produkter som omfattas av cyberresiliensförordningens tillämpningsområde. Enligt marknadskontrollagen ska inspektioner kunna utsträckas till alla utrymmen som en ekonomisk aktör använder i sin närings- eller yrkesverksamhet. Bestämmelserna om en myndighets rätt att göra inspektioner i utrymmen som är avsedda för boende av permanent natur föreskrivs dock inte i marknadskontrollagen, utan i sektorslagstiftningen. I förarbetena till marknadskontrollagen bedöms att när befogenheten att göra inspektioner i utrymmen som används för boende av permanent natur är behövlig inom någon produktsektor på grund av dess särdrag, ska bestämmelser om denna befogenhet utfärdas separat genom en sektorlag (RP 139/2021 rd, s. 12). Flera produktlagar innehåller bestämmelser om utsträckande av inspektionsrätten även till utrymmen som används för boende av permanent natur med vissa randvillkor (till exempel lagen om konsumentprodukters säkerhet, elsäkerhetslagen, lagen om kosmetiska produkter och lagen om gödselmedel). En sådan situation som är aktuell med tanke på övervakningen enligt cybersäkerhetsakten är en sådan situation som beskrivits i förarbetena till marknadskontrollagen.

Verksamhet som omfattas av cyberresiliensförordningens tillämpningsområde, såsom programvaruutveckling, kan bedrivas och det är även vanligt att sådan bedrivs i hemfridsskyddade utrymmen. Sådan verksamhet kan vara företagsverksamhet som huvud- eller bisyssla för personen. I så fall är det möjligt att det uppkommer situationer där den enda möjligheten att göra en inspektion av en tillverkare eller en annan ekonomisk aktör är att utföra den i det aktuella hemfridsskyddade utrymme som används i näringsverksamheten, men som även omfattas av hemfridsskyddet. Det är även möjligt att enheter monteras i samband med bostadsutrymmen. Således anses det att marknadskontrollförordningen förutsätter att en inspektion, i syfte att övervaka cyberresiliensförordningen, i begränsad utsträckning ska kunna utsträckas även till hemfridsskyddade utrymmen i sådana situationer.

Grundlagsutskottet har på etablerats sätt betonat att ordalydelsen i 10 § 3 mom. i grundlagen förutsätter att en inspektion som sträcker sig till en hemfridsskyddad plats binds till kravet på nödvändighet och förutsatt att det i befogenhetsbestämmelserna skrivs in att inspektioner i till exempel bostäder bara får förrättas om det är nödvändigt för att utreda de frågor som inspektionen avser (se till exempel GrUU 54/2014 rd, s. 3 och de utlåtanden till vilka det hänvisats i det).

Grundlagsutskottet har i sin praxis ansett att en åtgärd som inskränker på hemfridsskyddet är godtagbara ”i syfte att utreda brott”, om åtgärden binds till att det finns en konkret och specificerad orsak att misstänka att lagen överträtts eller kommer att överträdas (GrUU 14/2013 rd, s. 3 och GrUU 69/2002 rd, s. 2). Från proportionalitetssynpunkt har utskottet ansett att hemfridsskyddet inte får åsidosättas för utredning av mindre förseelser för vilka kan följa högst böter. (GrUU 40/2002 rd, s. 2). Grundlagsutskottet har å andra sidan ansett att inspektioner som inskränker hemfriden för att kontrollera hur stöd och bidrag som beviljats av offentliga medel används som beviljats är acceptabla också om det finns grundad anledning att misstänka sådana straffbara förseelser som allra högst ger ett bötesstraff (GrUU 69/2002 rd, s. 2–3). Inspektionsrätten kan genom en vanlig lag vara sammankopplad med ett förfarande som är sanktionerat med en straffavgift (GrUU 7/2004 rd, GrUU 39/2005 rd och GrUU 14/2013 rd).

Marknadskontrollagens 9 § innehåller en hänvisning till 39 § i förvaltningslagen, så som grundlagsutskottet förutsatt för reglering kring inspektioner av tillsynskaraktär (GrUU 11/2013 rd, s. 2).

Rätten att göra inspektioner i hemfridsskyddade områden är avgränsad till utrymmen som en ekonomisk aktör använder för ändamål i anknytning till deras närings- eller yrkesverksamhet. Enligt förslaget får en inspektion i ett utrymme som används för boende av permanent natur göras endast om den den är nödvändig för att utreda omständigheter som gäller föremålet för inspektionen. Detta innebär att förutsättningen är att den misstänkta överträdelsen inte kan utredas på annat sätt, såsom med rätten att få uppgifter eller genom att göra en inspektion i ett objekt som inte omfattas av hemfridsskyddet. Rätten att göra inspektioner i utrymmen som omfattas av hemfridsskyddet hänför sig till uppgifter som är nödvändiga för att sköta övervakningsuppgifter som anknyter till överträdelser av de skyldigheter som baserar sig på cyberresiliensförordningen eller lagförslag 1 i propositionen. Det är dock inte möjligt att på uttömmande sätt räkna upp de uppgifter som det är nödvändigt att skaffa för att göra en inspektion i utrymmen som omfattas av hemfridsskyddet.

Åtgärdens proportionalitet har säkerställts genom en bestämmelse. Förutsättningen är för det första att det finns ett motiverat och specificerat skäl till att cyberresiliensförordningen har överträtts eller överträds på ett sätt som kan leda till en administrativ påföljdsavgift enligt förslaget. Maximibeloppet av den påföljdsavgift som föreskrivs för överträdelse av cyberresiliensförordningen är avsevärt och det handlar om en sanktion av straffnatur. En ytterligare förutsättning är att den misstänkta överträdelsen ska handla om att en produkt eller process med digitala element inte överensstämmer med kraven eller om en annan situation med avsevärd cybersäkerhetsrisk enligt artikel 57 i cyberresiliensförordningen, vilken beskrivits närmare i motiveringarna till bestämmelsen. Syftet med cyberresiliensförordningen är att förbättra cybersäkerheten för produkter med digitala element såväl för konsumenter som för företag. Produkterna kan orsaka allvarliga cybersäkerhetsrisker och en risk till exempel för människornas hälsa eller säkerhet. Därför är det proportionellt att en inspektion i ovan nämnda situationer kan göras även i utrymmen som används för boende av permanent natur. Dessa förutsättningar innebär att en inspektion inte får göras i hemfridsskyddade objekt i sådana situationer med smärre överträdelser, för vilka en påföljdsavgift inte kan påföras eller som handlar om de sist nämnda omständigheterna.

Proportionaliteten säkerställs även av tillämpningen av 39 § i förvaltningslagen. Enligt den ska en inspektion förrättas utan att inspektionsobjektet eller dess innehavare orsakas oskälig olägenhet. Proportionaliteten säkerställs därtill bland annat av 6 § i förvaltningslagen, enligt vilken myndigheternas åtgärder ska använda sina befogenheter enbart för syften som är godtagbara enligt lag och åtgärderna ska vara opartiska och stå i rätt proportion till sitt syfte.

Den föreslagna lagen uppfyller således de förutsättningar som grundlagsutskottet fastställt i praktiken, då den förutsätter nödvändighet och ett konkret och specificerat skäl samt då inspektionsrätten är kopplad till verksamhet som kan leda till en administrativ påföljdsavgift av straffkaraktär, och därtill säkerställs i detta att åtgärden är proportionell.

Enligt 14 § 2 mom. i marknadskontrollagen får oberoende experter assistera marknadskontrollmyndigheten vid sådana inspektioner som avses i denna lag En extern expert har således inte någon självständig roll i en inspektion. Lagen innehåller även bestämmelser om det straffrättsliga tjänsteansvaret för en expert. Grundlagsutskottet har inte ansett att det finns något hinder till att bestämmelser utfärdas genom lag om rätten för ett organ som utsetts utanför myndighetsmaskineriet att biträda då en inspektion förrättas (GrUU 42/2005 rd och GrUU 46/2001 rd).

Med beaktande av det ovan angivna bedöms förslagen om inspektionsrätten uppfylla de randvillkor som följer av grundlagsutskottets praxis i fråga om en inspektion inom ramen för hemfridsskyddet.

### 12.6 Myndigheternas rätt att få och lämna ut information samt integritetsskyddet

*Myndigheternas rätt att få och lämna ut information.* Grundlagsutskottet har ofta bedömt omfattningen, exaktheten och innehållet i fråga om bestämmelserna om de uppgifter som ska fås och lämnas ut trots sekretessen (se till exempel GrUU 89/2022 rd, stycke 12). Myndigheternas rätt att få och möjlighet att lämna ut uppgifter kan enligt utskottet gälla behövliga uppgifter för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om informationsinnehållen å andra sidan inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på ”att informationen är nödvändig” för ett visst ändamål (se till exempel GrUU 8/2021 rd, stycke 24 och de utlåtanden som nämns där).

Grundlagsutskottet har upprepade gånger understrukit att det vid en särskiljning mellan behövlighet respektive nödvändighet att få eller lämna ut uppgifter är frågan inte bara om omfattningen av innehållet i uppgifterna utan också att den myndighet som är berättigad till uppgifterna i och med sina egna behov åsidosätter de grunder och intressen som är skyddade med hjälp av den sekretess som gäller myndigheten som innehar uppgifterna. Ju mer generella bestämmelserna om rätten att få information är, desto större är risken att sådana intressen kan åsidosättas per automatik. Ju mer fullständigt rätten att få uppgifter är kopplad till de sakliga förutsättningarna i bestämmelserna, desto mer sannolikt är det att en enskild begäran om information i praktiken måste motiveras. I så fall är det även möjligt för den som lämnar ut uppgifterna att bedöma begäran med tanke på de lagliga förutsättningarna för utlämnandet. Den som lämnar ut uppgifter kan dessutom genom att vägra att de facto lämna ut uppgifter åstadkomma en situation där skyldigheten att lämna ut uppgifter, det vill säga tolkningen av bestämmelserna, ska prövas av en extern myndighet. Denna möjlighet är viktig då det gäller att anpassa tillgången till information och sekretessintressena till varandra (se till exempel GrUU 7/2019 rd, s. 7 och GrUU 48/2018 rd, s. 5 och de utlåtanden till vilka det hänvisats i det).

Lagförslag 1 och 3 i den propositionen innehåller bestämmelser om myndigheternas rätter att få och lämna ut uppgifter, vilka kan gälla sekretessbelagd information, såsom affärshemligheter eller information om säkerhetsarrangemangen för informations- och kommunikationssystem. Uppgifterna kan undantagsvis även gälla omständigheter som omfattas av skyddet för privatlivet. Således ska propositionen bedömas med tanke på egendomsskyddet som föreskrivs i 15 § i grundlagen och skyddet för privatlivet som föreskrivs i 10 §.

De föreslagna rätterna att få och lämna ut uppgifter förutsätts i huvudsak av de uppgifter som definieras i cyberresiliensförordningen och cybersäkerhetsakten.

I 9 § i lagförslag 1 utfärdas bestämmelser om CSIRT-enhetens rätt att lämna ut vissa sekretessbelagda uppgifter som den fått i samband med skötseln av uppgifter enligt cyberresiliensförordningen i syfte att utföra dessa uppgifter. Rätten att lämna ut information är i regel bunden till behovsförutsättningen på så sätt att de uppgiftstyper som rätten att lämna ut information täcker har sitt ursprung i artikel 14.2, 14.4 och 14.6 i cyberresiliensförordningen. Utlämnandet av andra uppgifter som eventuellt fåtts vid skötseln av dessa uppgifter är bundet till nödvändighetsförutsättningen. I 14 § i lagförslaget finns det å sin sida bestämmelser om rätten för den anmälande myndigheten och ett anmält organ att lämna ut sekretessbelagd information. Rätten att lämna ut information för en anmälande myndighet är bunden till nödvändighet med tanke på skötseln av de uppgifter som fastställts i paragrafen. Rätten att lämna ut information för ett anmält organ är å sin sida bunden till behovsförutsättningen på så sätt att de uppgifter som lämnas ut har fastställts att gälla bedömningen av överensstämmelsen och kontrollresultaten. I 18 § 1 mom. i förslaget utsträcks marknadskontrollmyndighetens rätt att lämna ut information enligt 11 och 13 § i marknadskontrollagen att gälla även rätten att lämna ut information om överensstämmelse, säkerhetsarrangemang och sårbarhet i fråga om produkter med digitala element och uppgifter om incidenter som påverkar säkerheten. Marknadskontrollagen har stiftats med samverkan av grundlagsutskottet (GrUU 36/2016 rd, EkUB 19/2016 rd). Den föreslagna utvidgningen till uppgiftstyper som rätten att lämna ut information täcker är nödvändig, eftersom skyldigheterna i cyberresiliensförordningen hänför sig till deras område. I 18 § 2 mom. i förslaget finns det bestämmelser om rätten för marknadskontrollmyndigheten att lämna ut information till vissa finländska och utländska myndigheter för deras föreskrivna uppgifter. Rätten att lämna ut information är bunden till nödvändighet med tanke på skötseln av de uppgifter som fastställts i paragrafen. I föreslagna 26 § föreskrivs å sin sida rätten för myndigheten för cybersäkerhetscertifiering att lämna ut sekretessbelagda information. I fråga om 1 och 2 punkten i paragrafen är rätten att lämna ut information för en anmälande myndighet bunden till nödvändighet med tanke på skötseln av de uppgifter som fastställts i dessa punkter. I fråga om paragrafens 3 punkt är rätten att lämna ut information å sin sida bunden till behovsförutsättningen med tanke på uppgifterna för den mottagande myndigheten, på så sätt att de uppgiftstyper som lämnas ut har räknats upp i punkten. Förslagen om utlämnande av uppgifter till CSIRT-enheten för att den ska kunna sköta sina uppgifter enligt cybersäkerhetslagen förutsätts inte direkt av cyberresiliensförordningen eller cybersäkerhetsakten, men en ändamålsenlig skötsel av CSIRT-enhetens uppgifter kan anses förutsätta en möjlighet att utlämna dessa uppgifter till den, eftersom det främjar tillgodoseendet av cybersäkerheten.

Likaså är rätten att lämna ut information på grund av ändringen av 28 § i cybersäkerhetslagen i enlighet med lagförslag 3 bunden till nödvändighet med tanke på vissa av Finansinspektionens uppgifter, vilka föreskrivits i lagen om Finansinspektionen. Detta förslag granskas nedan separat med tanke på skyddet för konfidentiell kommunikation.

Det föreslås att 25 § i lagförslag 1 i propositionen innehåller bestämmelser om rätten för myndigheten för cybersäkerhetscertifiering att få information, vilken har begränsats till skötseln av dess uppgifter enligt den föreslagna lagen och cybersäkerhetsakten och för att övervaka de uppgifter som är nödvändiga för att övervaka efterlevnaden av cybersäkerhetsakten, de bestämmelser som utfärdats med stöd av den samt denna lag. Rätten att få information hänför sig till organen för bedömning av överensstämmelse, innehavaren av ett europeiska cybersäkerhetscertifikat och de som ger EU-försäkringar om överensstämmelse. Det är inte ändamålsenligt att räkna upp uppgiftstyperna på ett uttömmande sätt eller begränsa dessa till vissa situationer, eftersom myndigheterna kan ha många olika former av behov av att få

information. Dessutom fogas till 39 § 4 mom. i förslaget bestämmelser om rätten för den myndighet som påför en påföljdsavgift att få de uppgifter som är nödvändiga för att påföra en påföljdsavgift eller bedöma dess belopp.

Således kan den föreslagna regleringen anses uppfylla grundlagsutskottets förutsättningar för reglering kring rätt att få och lämna ut information till denna del.

*Skyddet för personuppgifter.* Enligt 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Närmare bestämmelser om skyddet för personuppgifter utfärdas genom lag. Inskränkningar i skyddet för privatlivet ska i det aktuella lagstiftningssammanhanget bedömas utifrån de allmänna villkoren för inskränkningar i de grundläggande fri- och rättigheterna (till exempel GrUU 42/2016 rd, s. 2–3). Enligt artikel 8 i stadgan om de grundläggande rättigheterna ska personuppgifter behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Enligt artikel 52.1 i stadgan om de grundläggande rättigheterna ska varje begränsning i utövandet av rättigheterna och friheterna som erkänns i stadgan om de grundläggande rättigheterna vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

De föreslagna bestämmelserna om rätten att lämna ut och få information enligt lagförslag 1 och 3 i propositionen lämnar inte personuppgifter utanför rätten att lämna ut eller få information, även om föremålet för utlämnandet av information i huvudsak är tekniska uppgifter i stället för personuppgifter. Personuppgifter kan dock förvaras till exempel för utredningar som begärs av ett organ för bedömning av överensstämmelse, vilka kan gälla uppfyllandet av de krav som ställs på bedömningsorganets personal. Till den del som personuppgifter behandlas i samband med utövningen av rätten att få och lämna ut uppgifter, ska dataskyddslagstiftningen, såsom allmänna dataskyddsförordningen och dataskyddslagen, iakttas i behandlingen av personuppgifter.

Enligt grundlagsutskottet bör skyddet för personuppgifter i första hand tillgodoses med stöd av allmänna dataskyddsförordningen och den nationella allmänna lag som stiftas med stöd av den. Den nationella speciallagstiftningen bör vara avgränsad till nödvändiga bestämmelser inom ramen för det nationella handlingsutrymme som dataskyddsförordningen medger (se GrUU 14/2018 rd).

I fråga om dessa rätter att få och lämna ut information utgörs rättsgrunden för behandlingen av personuppgifter i princip av en lagstadgad förpliktelse för en myndighet enligt artikel 6.1 c i dataskyddsförordningen. Propositionen innehåller kompletterande reglering om behandlingen av personuppgifter i förhållande till den allmänna dataskyddsförordningen och dataskyddslagen. I den föreslagna lagen används det nationella handlingsutrymme som artikel 6.2 och 6.3 i allmänna dataskyddsförordningen tillåter genom att fastställa rättsgrunden för behandlingen av personuppgifter och de organ och ändamål för vilka personuppgifter kan lämnas ut. Personuppgifter kan lämnas ut endast då det är nödvändigt för fallet eller i fråga om de fastställda uppgiftstyperna behövligt för att sköta lagstadgade uppgifter för en myndighet eller en privat aktör som sköter en offentlig förvaltningsuppgift. Dessa uppgifter baserar sig i huvudsak på unionslagstiftningen. Således uppfyller den föreslagna regleringen förutsättningen i artikel 6.3 i den allmänna dataskyddsförordningen att medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

*Konfidentiell kommunikation*. Enligt 2 mom. i grundlagen är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Enligt paragrafens 4 mom. kan genom lag föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten.

Genom lagförslag 3 ändras rätten att lämna ut information enligt 28 § 4 mom. i cybersäkerhetslagen till att gälla utlämnande av information även till Finansinspektionen utöver de tillsynsmyndigheter som fastställts i 26 § i cybersäkerhetslagen. Rätten att lämna ut information gäller även förmedlingsuppgifter, lokaliseringsuppgifter och information om meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, vilka tillsynsmyndigheten haft rätt att få på grund av att informationen varit nödvändig för fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapporteringen av betydande incidenter, Grundlagsutskottet har ansett denna reglering är möjlig med tanke på de randvillkor som 10 § i grundlagen ställer, eftersom meddelanden som innehåller ett skadligt datorprogram eller kommando kan anses falla helt utanför tillämpningsområdet för hemligheten för förtroliga meddelanden i 10 § i grundlagen och att den aktuella rätten att få information om förmedlingsuppgifter kan anses vara ett relativt begränsat inkräktande på skyddet för hemligheten för förtroliga meddelanden, utan att den bildar något problem med tanke på de allmänna förutsättningarna att begränsa grundläggande fri- och rättigheter (GrUU 62/2024 rd).

Förslaget om att i detta hänseende jämställa Finansinspektionen med de fastställda tillsynsmyndigheterna enligt cybersäkerhetslagen är motiverat, så att alla behöriga myndigheter enligt NIS 2-direktivet till denna del är i samma ställning. För närvarande innehåller cybersäkerhetslagen inte bestämmelser om Finansinspektionens uppgifter eller informationsutbyte mellan de tillsynsmyndigheter som föreskrivits i 26 § i cybersäkerhetslagen, eftersom även om det NIS 2-direktiv som den verkställt innehåller reglering som hänför sig till de verksamhetsområden som Finansinspektionen övervakar, är EU:s DORA-förordning i fråga om aktörernas skyldigheter en specialakt i förhållande till NIS 2-direktivet. I enlighet med lagen om Finansinspektionen fungerar Finansinspektionen dock som behörig myndighet enligt NIS 2-direktivet och som behörig myndighet enligt DORA-förordningen.

Utifrån det ovan angivna bedöms förslagen om myndigheternas informationsutbyte och rätt att lämna ut information vara förenliga med de randvillkor som grundlagen ställer.

### 12.7 Påföljdsregleringen

Det föreslås att 6 kap. i lagförslag 1, på det sätt som cyberresiliensförordningen förutsätter, innehåller bestämmelser om att en administrativ påföljdsavgift påförs för den som inte fullgör de skyldigheter som cyberresiliensförordningen fastställer. Dessutom innehåller kapitlet en påföljdsavgift för överträdelse av cybersäkerhetsakten till den del som propositionen innehåller nationellt handlingsutrymme. De föreslagna påföljdsavgifterna handlar om en administrativ påföljdsavgift som påförs för en lagstridig gärning, vilken kan vara av ett avsevärt belopp.

Enligt grundlagsutskottets utlåtandepraxis ska de allmänna grunderna för administrativa påföljder i enlighet med 2 § 3 mom. i grundlagen fastställas i lag. Dessutom är det fråga om betydande utövning av offentlig makt, som endast kan anförtros myndigheter. Lagen måste exakt och tydligt föreskriva om grunderna för betalningsskyldigheten och avgiftens storlek, rättsskyddet för den betalningsskyldige och grunderna för verkställigheten av lagen. Utskottet

har också ansett att även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen, som framgår av grundlagens 8 §, inte direkt gäller administrativa påföljder kan det allmänna kravet på exakthet ändå inte åsidosättas i ett sådant sammanhang (GrUU 43/2013 rd, GrUU 14/2012 rd, GrUU 32/2012 rd och de utlåtanden som nämns där).

Grundlagsutskottets hävdvunna tolkning har varit att administrativa påföljdsavgifter är administrativa påföljder av sanktionskaraktär som påförs för en lagstridig gärning. I sak har utskottet i sina utlåtanden jämställt en ekonomisk påföljd av straffkaraktär med en straffrättslig påföljd (GrUU 17/2012 rd, s. 6, GrUU 9/2012 rd, s. 2). En administrativ påföljdsavgift handlar enligt grundlagsutskottet om avsevärd utövning av offentlig makt (GrUU 34/2012 rd, s. 3, GrUU 17/2012 rd, s. 6, och GrUU 9/2012 rd, s. 2). Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag. Enligt sista meningen i 124 § i grundlagen får uppgifter som innebär betydande utövning av offentlig makt ges endast myndigheter. I förslaget om påförande av påföljdsavgift har grundlagsutskottets utlåtandepraxis beaktats. Lagen innehåller exakta, noggrant avgränsade och uttömmande bestämmelser om de gärningar eller försummelser som kan ligga till grund för påförande av påföljdsavgiften för en aktör.

Grundlagsutskottet har i sin bedömning av den allmänna dataskyddsförordningen konstaterat att rättssäkerhetsintresset i fråga om administrativa påföljdsavgifter är starkt accentuerat, med hänsyn till att påföljdsavgiften är sträng och har karaktär av sanktion. Grundlagsutskottet har förutsatt att för att säkerställa att ett förfarande är ändamålsenligt, oberoende och opartiskt på det sätt som krävs i 21 § i grundlagen, ska beslut om en påföljdsavgift fattas av ett kollegialt organ för att förslaget ska kunna behandlas i vanlig lagstiftningsordning (GrUU 14/2018 rd).

Enligt grundlagsutskottet ska förvaltningsmyndigheten vid behandlingen av ett ärende iaktta garantierna för god förvaltning enligt 21 § 2 mom. i grundlagen, vilka är bland annat offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring. Enligt grundlagen ska garantier för god förvaltning tryggas genom lag.

Enligt förslaget påförs en påföljdsavgift på grund av överträdelse av cyberresiliensförordningen av Transport- och kommunikationsverket. Enligt 7 a § i lagen om Transport- och kommunikationsverket har Transport- och kommunikationsverket ett påföljdskollegium som har till uppgift att påföra påföljdsavgifter som omfattas av verkets behörighet i sådana fall när påföljdsavgiften överstiger 100 000 euro. Påföljdskollegiet fattar beslut efter föredragning. Lagen innehåller bestämmelser om kollegiets förtrogenhet, expertis, oberoende och opartiskhet. Dessutom, när den behöriga marknadskontrollmyndigheten exceptionellt utgörs av marknadskontrollmyndigheten enligt 3 § i lagen om tillsyn över vissa system för artificiell intelligens, påförs den administrativa påföljdsavgiften enligt förslaget i den ordning som föreskrivs i 13 § i den nämnda lagen. Detta innebär att påförandet av en påföljdsavgift i fråga om vissa påföljdsavgifter som överskrider det belopp i euro som föreskrivs i den aktuella lagen styrs till ett kollegium för påföljdsavgifter för kontrollen av AI-system eller till det påföljdskollegium som avses i dataskyddslagen. Till denna del uppfyller förslaget de krav som grundlagsutskottet i praktiken ställt på förfarandet.

Transport- och kommunikationsverket påför också överträdelseavgiften i anknytning till cybersäkerhetscertifiering i rollen som nationell myndighet för cybersäkerhetscertifiering. Eftersom maximibeloppet av påföljdsavgiften i så fall är 100 000 euro, omfattas en sådan påföljdsavgift med stöd av 7 a § i lagen om Transport- och kommunikationsverket inte av påföljdskollegiets beslutsbehörighet. Det kan bedömas att denna påföljdsavgift inte förutsätter att den styrs för att avgöras av ett kollegium, eftersom den ska anses vara av högt maximibelopp och avsevärt kännbar, med beaktande av att det handlar om näringsverksamhet och att certifiering i princip är frivilligt.

Enligt grundlagsutskottet ska det i lag exakt och tydligt föreskrivas om grunderna för betalningsskyldigheten och avgiftsbeloppet samt om den betalningsskyldiges rättssäkerhet och om grunderna för verkställandet av lagen (GrUU 14/2013 rd, s. 2, GrUU 34/2012 rd, s. 3, GrUU 17/2012 rd, s. 6). Förslagets bestämmelser om dessa omständigheter bedöms hålla en tillräcklig nivå.

Eftersom i synnerhet de påföljdsavgifter som förutsätts i cyberresiliensförordningen är betydande, måste man enligt grundlagsutskottet fästa särskild uppmärksamhet vid kraven på rättssäkerhet (GrUU 14/2018 rd, s. 18) Påföljdsavgiftens maximibelopp fastställs i 38 § i lagförslag 1. Påföljdsavgiftens belopp grundar sig enligt 38 § på en helhetsbedömning där de omständigheter som anges i paragrafen ska beaktas. Ändring i ett beslut om påföljdsavgift får sökas genom besvär på det sätt som föreskrivs för rättegång i förvaltningsärenden. Grundlagsutskottet har i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden till prövning så att påföljdsavgift inte påförs om de villkor som anges i lag är uppfyllda (GrUU 49/2017 rd, s. 5–6, GrUU 39/2017 rd, s. 4). Detta har beaktats i 40 § i förslaget, vars syfte är att säkerställa att ingen påföljdsavgift påförs i situationer där det är uppenbart oskäligt. Ett beslut om en påföljdsavgift kan inte förordnas att iakttas med stöd av 43 § i förslaget trots ändringssökande. Det kan bedömas att detta tryggar att rättsskyddsarrangemangen är ändamålsenliga (GrUU 4/2004 rd, s. 7–8).

Enligt artikel 65 i cybersäkerhetsakten ska medlemsstaterna fastställa regler om sanktioner vid överträdelse av denna avdelning och överträdelser av europeiska ordningar för cybersäkerhetscertifiering, och de ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I övrigt ges medlemsstaterna nationellt handlingsutrymme i fråga om påföljdsbestämmelserna, förutsatt att de allmänna krav för genomförande av unionsrätten som följer av principen om lojalt samarbete uppfylls (likvärdighets- och effektivitetsprincipen). Detta innebär bland annat att medlemsstaterna i princip kan besluta om påföljderna genomförs som administrativa påföljder eller som straffrättsliga straff. Förslaget innehåller bestämmelser om en administrativ påföljdsavgift som kan påföras för överträdelser som gäller cybersäkerhetscertifieringen (37 § i lagförslag 1).

*Acceptabilitet och sistahandskaraktär.* Syftet med de europeiska ordningarna för cybersäkerhetscertifiering är att öka nivån på cybersäkerheten i unionen. Deras syfte är att fastställa att de bedömda IKT-produkterna, IKT-tjänsterna och IKT-processerna är förenliga med de säkerhetskrav som fastställts för dem, så att det är möjligt att skydda uppgifternas, funktionernas eller tjänsternas användarvänlighet, autenticitet, integritet och konfidentialitet under hela deras livslängd (skäl 95 till och artikel 46 i cybersäkerhetsakten). Cybersäkerhetsrisker som gäller produkterna kan bland annat äventyra konfidentialiteten för personuppgifterna och kommunikationen. Dessa mål har en koppling till skyddet för privatlivet som tryggats i 10 § i grundlagen. De är godtagbara mål med tanke på utfärdandet av påföljdsbestämmelser. De talar också för att det nationella handlingsutrymmet utnyttjas för att föreskriva om påföljder. Syftet med de föreslagna bestämmelserna är att säkerställa att bestämmelserna iakttas och att skyldigheterna i fråga om bedrivande av verksamhet fullgörs. Bestämmelserna främjar specialprevention och allmän prevention. Med tanke på övervakningens effektivitet och funktion kan lindrigare påföljder inte anses vara tillräckliga, med beaktande av ovan nämnda godtagbara mål och cybersäkerhetens centrala roll i samhället.

I enlighet med ultima ratio-principen ska ett straffrättsligt straff tillgripas som ett sista medel. I valet av den nationella påföljdsarten ska den så kallade likvärdighetsprincipen iakttas. Enligt principen ska medlemsstaterna sörja för att en påföljd för överträdelse av EU-rätten i fråga om

grunder och förfaranden fastställs på samma sätt som en överträdelse av den nationella rätten av samma karaktär och med ett jämställbart allvar.

Ovan i avsnitt 5.1.35.1.2 beskrivs de grunder som ligger till grund för det föreslagna maximibeloppet av sanktioneringen av överträdelse av cybersäkerhetscertifieringen. Vid beredningen har man ansett att en administrativ sanktion är en lösning som är förenlig med likvärdighetsprincipen och en lämpligare påföljd än en straffrättslig påföljd för överträdelse av cybersäkerhetsakten.

*Självinkrimineringsskyddet*. Enligt Europadomstolens praxis är självinkrimineringsskyddet inte något hinder eller någon begränsning för sådana lagstadgade administrativa tillsynsförfaranden där en person förutsätts lämna ut information eller utredningar till exempel för beskattning, näringstillsynen eller miljöskyddet (GrUU 39/2014).

*Oskuldspresumtionen*. Förslaget är inte problematiskt med tanke på oskuldspresumtionen, eftersom det inte grundar sig på ansvar oberoende av vållande (se GrUU 9/2018 rd, s. 4). En förutsättning för att påföra en påföljdsavgift är att den gärning eller försummelse som bryter mot cyberresiliensförordningen eller cybersäkerhetsakten beror på ett förfarande av uppsåt eller oaktsamhet av aktören.

*Förbudet mot dubbel straffbarhet.* Den föreslagna påföljdsavgiften är inte problematisk med tanke på förbudet mot dubbel straffbarhet. Enligt ne bis in idem-regeln får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan har blivit slutligt frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat (GrUU 9/2012 rd, s. 3, GrUU 14/2013 rd, s. 2). Enligt Europadomstolens avgörandepraxis omfattar förbudet också administrativa påföljder av straffkaraktär (GrUU 9/2012 rd, s. 3). Förbudet mot dubbel straffbarhet gäller som allmän rättsprincip, och det finns inget behov av att föreskriva särskilt om det. Möjligheten till överlappande förfaranden enligt olika bestämmelser kan dock inte helt uteslutas. Enligt unionsdomstolen är möjligheten att förfaranden och påföljder är överlappande förenlig med det väsentliga innehållet i artikel 50 i stadgan om de grundläggande rättigheterna, under förutsättning att den nationella lagstiftningen inte tillåter att ett förfarande inleds och påföljder påförs för samma gärningar utifrån samma överträdelse eller för att uppnå samma mål, utan att den uteslutande reglerar att överlappande förfaranden och påföljder är möjliga med stöd av olika bestämmelser (mål C-117/20 bpost, punkt 43 och mål C- 412/21 Dual Prod SRL, punkt 63). Dessutom ska det finnas tydliga och exakta regler utifrån vilka det är möjligt att förutse vilka åtgärder och försummelser som kan vara föremål för överlappning av förfaranden och påföljder (mål C-117/20 bpost, punkt 51, mål C-412/21 Dual Prod SRL, punkt 67 och mål C-205/23 Engie Romania, punkt 66).

I propositionens lagförslag 1 har regeln beaktats i 40 § 3 mom., enligt vilket påföljdsavgift inte får påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom.

En påföljdsavgift som gäller cybersäkerhetscertifiering får enligt förslaget inte påföras heller för den som för samma gärning påförts en påföljdsavgift för överträdelse av cyberresiliensförordningen. Cybersäkerhetsakten begränsar inte tillämpningen av cyberresiliensförordningen eller exempelvis dataskyddsregleringen inklusive påföljder. Cyberresiliensförordningens och cybersäkerhetsaktens mål kan anses vara likadana i den mån att det är motiverat att inom ramen för det nationella handlingsutrymmet och på det föreslagna sättet utfärda bestämmelser om att en annan påföljdsavgift inte kan påföras utifrån samma gärning för en överträdelse som gäller cybersäkerhetscertifiering. Den föreslagna bestämmelsen

är tydlig och exakt och utifrån den är det möjligt att förutse vilka åtgärder och försummelser som kan vara föremål för överlappningar när det gäller förfaranden och påföljder.

Målen i den allmänna dataskyddsförordningen kan i vissa situationer gå i samma riktning som cybersäkerhetsakten, eftersom den allmänna dataskyddsförordningen förutsätter att den personuppgiftsansvarige säkerställer att behandlingen av personuppgifter är säker (artikel 32) och de innehåller bestämmelser om certifieringsmekanismer och -märken, vars syfte är att visa att de personuppgiftsansvariga och personuppgiftsbiträdena iakttar denna förordning då de genomföra behandlingsuppgifter, så som konstateras i skäl 74 till cybersäkerhetsakten. Enligt det sist nämnda begränsar cybersäkerhetsakten inte certifiering av informationsbehandlingsfunktioner i enlighet med förordning (EU) 2016/679, inte heller då åtgärderna har inkluderats i IKT-produkter, IKT-tjänster och IKT-processer. I princip kan det dock anses att certifieringsmekanismerna enligt cybersäkerhetsakten och dataskyddsförordningen dock har egna särskilda mål. Från fall till fall ska det dock säkerställas att de förfaranden som myndigheterna infört har mål som kompletterar varandra och som gäller de olika dimensionerna för ifrågavarande samma straffbara gärning (mål C-117/20 bpost, punkt 50).

*Påföljder för myndigheterna*. Enligt regeringens proposition med förslag till dataskyddslag är en administrativ påföljdsavgift som påförs en myndighet ett förfarande som är främmande för vår allmänna rättsordning. Rättsordningen ställer andra specialkrav på den offentliga förvaltningen, vilka för sin del motiverar denna regleringslösning (RP 14/2018 rd, s. 19). Grundlagsutskottet har ansett att en utvidgning av bestämmelserna om påföljdsavgift till myndighetsverksamhet inte är problemfri i konstitutionellt hänseende (se GrUU 14/2018 rd och GrUU 13/2023 rd). Grundlagsutskottet har i sin bedömning av statsrådets skrivelse om förslaget till förordning om artificiell intelligens betonat betydelsen av att man i fråga om administrativa påföljder bör sträva efter att säkerställa ett tillräckligt nationellt handlingsutrymme, särskilt för att beakta att myndigheterna i Finland inte kan påföras administrativa påföljdsavgifter, eftersom endast straffrättsliga påföljder kan påföras myndigheterna (se GrUU 37/2021 rd, stycke 40). Således innehåller 40 § 4 mom. i propositionen bestämmelser om de offentligrättsliga aktörer som kan påföras påföljdsavgifter.

*Proportionalitet*. Grundlagsutskottet har ansett att de bestämmelser som är relevanta för proportionaliteten gäller sanktionernas storlek i euro, men också de omständigheter som ska beaktas vid fastställandet av påföljdens storlek och avstående från påföljdsavgift. Utskottet har också i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden till prövning så att påföljdsavgift inte påförs om de villkor som anges i lag är uppfyllda. (GrUU 46/2021 rd, punkt 17 med hänvisningar). Den föreslagna paragrafen om en påföljdsavgift i anknytning till cybersäkerhetscertifiering är proportionell. I fråga om cyberresiliensförordningen fastställs maximibeloppen av påföljdsavgifterna i denna förordning.

Förslaget innehåller bestämmelser om maximibeloppet av påföljdsavgiften och även om de omständigheter som ska beaktas i påföljdsprövningen. Stränghetsgraden för den påföljdsavgift som gäller cybersäkerhetscertifiering har bestämts i förhållande till gärningarnas klandervärdhet och skyddsintresset, och påföljdsavgiften hänför sig till näringsidkare, i praktiken juridiska personer. Påförande av en påföljdsavgift handlar om sådan behandling av ett förvaltningsärende på vilken förvaltningslagen tillämpas (GrUU 32/2005 rd, s. 3/II). I föreslagna 40 § föreskrivs också när en påföljdsavgift inte ska påföras.

*Exakthet.* Grundlagsutskottet har ansett att även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen i grundlagens 8 § inte som sådant gäller bestämmelserna om administrativa sanktioner, kan det allmänna kravet på exakthet ändå inte förbigås i ett sammanhang som detta

(GrUU 9/2012 rd, GrUU 74/2002 rd och GrUU 57/2010 rd). De föreslagna bestämmelserna om påföljdsavgifter innehåller beskrivningar av de sanktionerade gärningarnas och försummelsernas natur och de redogör entydigt för vilka lagstridiga gärningar eller försummelser som kan leda till en sanktion.

Förslaget om administrativa påföljdsavgifter bedöms uppfylla förutsättningarna för administrativa påföljder enligt grundlagsutskottets utlåtandepraxis och de regleringsprinciper för administrativa påföljdsavgifter vilka härletts ur dessa.

### 12.8 Ålands ställning och relation till självstyrelse

Propositionen fördelar sig dels mellan rikets, dels mellan landskapets lagstiftningsbehörighet. I 18 och 27 § i självstyrelselagen för Åland (1144/1991) föreskrivs om behörighetsfördelningen mellan riket och landskapet Åland. I de utlåtanden som mottagits från högsta domstolen (13.6.2025 KKO-HD/442/2025) och Ålandsdelegationen (26.5.2025 Nr 22/25) i samband med lagstiftningskontrollen vid föredragningen av åländska landskapslagar för republikens president den 27 juni 2025 har det konstaterats att cybersäkerhet eller ett motsvarande begrepp inte nämns i fördelningen av lagstiftningsbehörigheten mellan landskapet och riket i självstyrelselagen. Lagstiftningsbehörigheten ska bedömas med tanke på de rättsområden som landskapslagstiftningen gäller. I 59 b § i självstyrelselagen för Åland finns det bestämmelser om genomförande av beslut som har fattats inom Europeiska unionen. I självstyrelselagen fördelar sig ansvaret för att genomföra unionslagstiftning enligt den behörighetsindelning som föreskrivits i självstyrelselagen. Landskapet ansvarar för genomförande av unionsakter till den del som ärendet omfattas av dess behörighet enligt självstyrelselagen.

I 59 b § 3 mom. i självstyrelselagen för Åland föreskrivs att får medlemsstaterna enligt gemenskapsrätten i något fall där både landskapet och riket har behörighet utse endast en förvaltningsmyndighet, utser riket denna myndighet. När denna myndighet fattar ett beslut som annars skulle höra till landskapets behörighet, ska beslutet fattas i enlighet med landskapsregeringens ståndpunkt. I den tidigare bedömningen har utseendet av den nationella cybersäkerhetscertifieringsmyndigheten ansetts höra till rikets behörighet utifrån den grunden att cybersäkerhetsakten hade förutsatt att en nationell myndighet utses (regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den RP 98/2020 rd, s. 326) Eftersom cybersäkerhetsakten liksom även cyberresiliensförordningen dock möjliggör att flera än en myndighet utses, kan fördelningen av statens och landskapets behörighet dock inte avgöras utifrån 59 b § 3 mom. i självstyrelselagen.

Standardisering omfattas av rikets lagstiftningsbehörighet (27 § 19 punkten i självstyrelselagen). Till den del som rättsakterna innehåller myndighetsuppgifter som gäller standardisering hör de därför till landskapets lagstiftningsbehörighet.

Med vissa begränsningar omfattar rikets lagstiftningsbehörighet enligt 18 § 22 punkten i självstyrelselagen ärenden som gäller näringsverksamhet. Enligt 25 punkten omfattar behörigheten ärenden som gäller beläggande med straff och storleken av straff inom rättsområden som hör till landskapets lagstiftningsbehörighet, medan 26 punkten gäller utsättande och utdömande av vite samt användning av andra tvångsmedel inom rättsområden som hör till landskapets lagstiftningsbehörighet. Cybersäkerheten och informationssäkerheten hänför sig till den lagstiftningsbehörighet till vilken lagstiftningsbehörigheten för respektive sektor hör (på motsvarande sätt i RP 57/2024 rd, s. 275). Myndighetsuppgifterna och påföljderna i anknytning till kontroll och certifiering enligt cyberresiliensförordningen och cybersäkerhetsakten kan således i princip anses omfattas av landskapets behörighet.

Cyberresiliensförordningens och cybersäkerhetsaktens horisontella tillämpningsområden är i detta hänseende dock problematiska i fråga om fastställandet av rikets och landskapets lagstiftningsbehörighet.

Konsumentskydd (27 § 10 punkten i självstyrelselagen) hör till rikets lagstiftningsbehörighet. Konsumentskyddsaspekterna är dock inte avsevärda i cyberresiliensförordningen och inte heller i cybersäkerhetsakten och ingendera av dessa rättsakter begränsar sig till konsumentskyddets område. Med de väsentliga cybersäkerhetskrav som regleras i cyberresiliensförordningen skyddas dock konsumenter och organisationer mot cybersäkerhetsrisker, och dessa har även som mål att förbättra skyddet för personuppgifter och integriteten för enskilda personer (skäl 32). På motsvarande sätt konstateras i cybersäkerhetsakten till exempel att företag och enskilda konsumenter ska ha exakta uppgifter om den nivå på vilka säkerheten för IKT-produkter, IKT-tjänster och IKT-processer har certifierats (skäl 10). Certifieringsordningarna kan i princip hänföra sig såväl till företagsprodukter som till konsumentprodukter.

Konsumentskyddsärenden har å sin sida ansetts hör till rikets lagstiftningsbehörighet, då det handlar om konsumentprodukternas produktsäkerhet (RP 195/2022 rd, s. 48). Regleringen kring konsumentsäkerhet har ansetts gälla frågor som enligt 18 § 6 punkten (allmän ordning och säkerhet), 12 punkten (hälso- och sjukvård) och 22 punkten (näringsverksamhet) i självstyrelselagen hör till landskapet Ålands lagstiftningsbehörighet. Trots det horisontella tillämpningsområdet och den typ av regleringsobjekt som är ny för marknadskontrollakter har cyberresiliensförordningen en karaktär av en produktsäkerhetsakt, varför den åtminstone utifrån denna grund i princip kan anses omfattas av rikets lagstiftningsbehörighet. Europeiska cybersäkerhetscertifikat och försäkringar om överensstämmelse enligt cyberresiliensförordningen kommer enligt bedömningen att vara viktiga även för att uppfylla kraven i cyberresiliensförordningen. Cyberresiliensförordningen innehåller även liknande särdrag som i marknadskontrollregleringen, varför den i princip bedöms omfattas av landskapets lagstiftningsbehörighet utifrån samma grunder som produktsäkerhetsregleringen, eftersom det kan anses handla om omständigheter som gäller den allmänna ordning och säkerhet och i synnerhet näringsverksamhet.

Undantaget utgörs dock av situationer som handlar om reglering kring näringsverksamhet som omfattas av rikets lagstiftningsbehörighet. Enligt 27 § 40 punkten i självstyrelselagen har riket lagstiftningsbehörighet i ärenden som gäller televerksamhet. I fråga om 30 kap. i lagen om tjänster inom elektronisk kommunikation (radioutrustnings överensstämmelse med kraven och marknadskontroll) har det ansetts att regleringen kring radioutrustning i egenskap av televerksamhet med stöd av 27 § 40 punkten i självstyrelselagen omfattas av rikets lagstiftningsbehörighet (RP 79/2023 rd, s. 31), även om utsläppande eller tillhandahållande på marknaden inte är egentlig televerksamhet. På grund av detta ska det på motsvarande sätt anses att genomförandet av cyberresiliensförordningen och cybersäkerhetsakten, i fråga om radioutrustning men också andra enheter i anknytning till televerksamhet, i Finland omfattas av rikets behörighet.

Även ärenden som gäller domännamn anses höra till rikets lagstiftningsbehörighet (regeringens förslag till riksdagen med förslag till lag om ändring av lagen om domännamn RP 151/2005 rd, s. 2).

### 12.9 Delegering av lagstiftningsbehörigheten till en myndighet

Enligt 80 § 2 mom. i grundlagen kan även myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning.

Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat. Enligt grundlagsutskottets utlåtandepraxis är en särskild orsak till att utfärda bestämmelser om bemyndigandet att utfärda föreskrifter för en myndighet bland annat reglering som är teknisk och innehåller lite detaljer (GrUU 52/2001 rd och GrUU 46/2001 rd) och som inte omfattar någon avsevärd utövning av prövningsrätt (GrUU 43/2000 rd).

Enligt artikel 33.2 i cyberresiliensförordningen kan medlemsstaterna vid behov inrätta regulatoriska sandlådor för cyberresiliens. I 10 § i lagförslaget om genomförandet av cyberresiliensförordningen regleras att Transport- och kommunikationsverket har ett bemyndigande att utfärda föreskrifter om inrättande av en regulatorisk sandlåda. De föreslagna bemyndigandena att utfärda föreskrifter handlar om teknisk reglering som inte omfattar någon avsevärd användning av prövningsrätt. Myndigheten kan pröva inrättande av regulatoriska sandlådor och det är frivilligt för en ekonomisk aktör att delta i dessa. Regleringens sakmässiga betydelse förutsätter inte heller i övrigt att ärenden föreskrivs genom lag eller förordning.

Föreslagna nya 21 a kap. i lagen om tjänster inom elektronisk kommunikation innehåller ett bemyndigande att utfärda förordningar i anknytning till anmälningen av uppgifter till förteckningen över registrarer. Förslaget är av samma innehåll som bemyndigandet att utfärda föreskrifter i 41 § 4 mom. i cybersäkerhetslagen, vars förhållande till grundlagen har bedömts i regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet (RP 57/2024 rd, s. 266–267) och som föreskrivits med grundlagsutskottets medverkan (GrUU 62/2024 rd). På grund av de andra ändringarna omfattas även aktörer som verkar för registrarers räkning framöver av bemyndigandena att utfärda föreskrifter i gällande 21 kap., vilket inte anses ha någon konsekvens för den konstitutionella bedömningen av bemyndigandet att utfärda föreskrifter.

De föreslagna bestämmelserna om bemyndigande är noggrant avgränsade, detaljerade och i fråga om tillämpningsområde exakt avgränsade och de uppfyller förutsättningar i 80 § 2 mom. i grundlagen.

På de grunder som anges ovan kan förslagen behandlas i vanlig lagstiftningsordning.

*Kläm*

Eftersom cyberresiliensförordningen och cybersäkerhetsakten innehåller bestämmelser som enligt förslaget kompletteras genom lag och eftersom NIS 2-direktivet innehåller bestämmelser som enligt förslaget verkställs genom lag, föreläggs riksdagen följande lagförslag:

**1.**

# Lag

**om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering**

I enlighet med riksdagens beslut föreskrivs:

1 kap.

**Allmänna bestämmelser**

1 §

*Lagens syfte*

Genom denna lag preciseras och kompletteras Europaparlamentets och rådets förordning (EU) 2024/2847 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (*cyberresiliensförordningen*) och dess nationella tillämpning.

Genom denna lag preciseras och kompletteras 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*) och dess nationella tillämpning.

2 §

*Definitioner*

I denna lag avses med

1) *produkt med digitala element* en programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data,

2) *anmält organ* ett i Finland etablerat organ för bedömning av överensstämmelse som utsetts av en finsk myndighet och anmälts till Europeiska kommissionen enligt artikel 43 i cyberresiliensförordningen,

3) *distributör* en annan sådan fysisk eller juridisk person i leveranskedjan än tillverkaren eller importören, som tillhandahåller en produkt med digitala element på Europeiska unionens marknad utan att påverka dess egenskaper,

4) *importör* en fysisk eller juridisk person som är etablerad i Europeiska unionen och som på marknaden släpper ut en produkt med digitala element vilken bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad utanför Europeiska unionen,

5) *tillverkare* en fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, vare sig mot betalning, för monetarisering eller kostnadsfritt,

6) tillverkarens representant en fysisk eller juridisk person som är etablerad inom Europeiska unionen och som enligt skriftlig fullmakt från tillverkaren har rätt att i dennes ställe utföra särskilda uppgifter,

7) *ekonomisk aktör* tillverkaren, tillverkarens representant, importören, distributören eller en annan fysisk eller juridisk person som omfattas av skyldigheter avseende tillverkning av produkter med digitala element eller avseende tillhandahållande av produkter med digitala element på marknaden i enlighet med cyberresiliensförordningen,

8) *förvaltare av programvara med fri och öppen källkod* en juridisk person, annan än en tillverkare som har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av specifika produkter med digitala element, vilka klassificeras som programvara med fri och öppen källkod enligt artikel 3.48 i cyberresiliensförordningen och är avsedda för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft,

9) *organ för bedömning av överensstämmelse* organ som utför bedömningar av överensstämmelse, bland annat kalibrering, provning, certifiering och kontroll,

10) *ackreditering* en förklaring från ett nationellt ackrediteringsorgan om att ett organ för bedömning av överensstämmelse uppfyller kraven i harmoniserade standarder och, i förekommande fall, eventuella ytterligare krav, bland annat de som fastställs i sektorsspecifika program, för att utföra specifika bedömningar av överensstämmelse,

11) *CSIRT-enheten* den enhet som avses i 19 § i cybersäkerhetslagen (124/2025),

12) *organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering* ett organ för bedömning av överensstämmelse som anmälts till Europeiska kommissionen i enlighet med artikel 61 i cybersäkerhetsakten.

3 §

*Förhållande till annan lagstiftning*

Bestämmelser om en ram för marknadskontrollen, för samarbetet med ekonomiska aktörer och för kontrollen av produkter som förs in på Europeiska unionens marknad finns i Europaparlamentets och rådets förordning (EU) 2019/1020 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011, nedan *marknadskontrollförordningen*.

Bestämmelser om marknadskontrollmyndigheternas behörighet, yttre gränskontroll enligt artiklarna 25–28 i marknadskontrollförordningen och sökande av ändring i marknadskontrollmyndighetens beslut finns i lagen om marknadskontrollen av vissa produkter (1137/2016), nedan *marknadskontrollagen*.

Bestämmelser om konsumentprodukters säkerhet finns i Europaparlamentets och rådets förordning (EU) 2023/988 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG samt i lagen om konsumentprodukters säkerhet (184/2025).

Bestämmelser om krav på system för artificiell intelligens finns i Europaparlamentets och rådets förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) och i lagen om tillsyn över vissa system för artificiell intelligens ( / ).

Bestämmelser om CSIRT-enhetens uppgifter och behandlingen av andra rapporter om sårbarheter än de som avses i cyberresiliensförordningen finns i cybersäkerhetslagen.

2 kap.

**Överensstämmelse och anmälningar**

4 §

*Överensstämmelse för produkter med digitala element*

Bestämmelser om överensstämmelse för produkter med digitala element finns i cyberresiliensförordningen.

5 §

*Ej färdigställda produkter*

Produkter med digitala element som inte uppfyller kraven i cyberresiliensförordningen får visas eller användas på det sätt som föreskrivs i artikel 4.2 i cyberresiliensförordningen. En ej färdigställd programvara som inte uppfyller kraven i cyberresiliensförordningen får tillhandahållas på marknaden för testning under en begränsad tid enligt vad som föreskrivs i artikel 4.3 i cyberresiliensförordningen.

6 §

*Produkter med digitala element vid offentlig upphandling*

Vid en upphandling som omfattas av tillämpningsområdet för lagen om offentlig upphandling och koncession (1397/2016), där föremålet för upphandlingen är en produkt med digitala element, ska den upphandlande enheten ta i beaktande vad som i artikel 5.2 i cyberresiliensförordningen föreskrivs om överensstämmelse med kraven och tillverkarens förmåga att ändamålsenligt hantera sårbarheter.

7 §

*Tillverkarens anmälningsskyldighet*

Bestämmelser om tillverkarens skyldighet att anmäla aktivt utnyttjade sårbarheter i en produkt med digitala element och allvarliga incidenter som påverkar säkerheten för produkten finns i artikel 14 i cyberresiliensförordningen.

Bestämmelser om CSIRT-enhetens skyldighet att efter att ha mottagit en anmälan om en händelse med stöd av artikel 14 i cyberresiliensförordningen anmäla den till marknadskontrollmyndigheten finns i artikel 16.3 i cyberresiliensförordningen.

8 §

*Frivillig anmälan*

CSIRT-enheten tar emot frivilliga anmälningar enligt artikel 15 i cyberresiliensförordningen om eventuella sårbarheter i en produkt med digitala element, cyberhot, allvarliga incidenter som påverkar säkerheten för en produkt med digitala element och om tillbud.

Oberoende av vad som någon annanstans i lag föreskrivs om myndigheternas rätt att få information, får information som på frivillig basis lämnats ut till CSIRT-enheten enligt artikel 15 i cyberresiliensförordningen inte utan samtycke av den som lämnat ut informationen användas i brottsutredningar eller vid administrativt eller annat beslutsfattande som gäller den som lämnat ut informationen.

9 §

*CSIRT-enhetens rätt att lämna ut sekretessbelagd information*

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) och någon annanstans i lag har CSIRT-enheten rätt att på eget initiativ eller på begäran trots sekretessbestämmelserna och andra begränsningar av utlämnande av information lämna ut eller röja information som den fått med stöd av artikel 14.2, 14.4 och 14.6 i cyberresiliensförordningen eller motsvarande information som den fått med stöd av artikel 15 i den nämnda förordningen, om det behövs för skötseln av de uppgifter som föreskrivs i artiklarna 14–17 i cyberresiliensförordningen

1) till den marknadskontrollmyndighet som avses i 15 och 16 §,
2) till Europeiska unionens cybersäkerhetsbyrå Enisa,
3) till en CSIRT-enhet som utsetts till samordnare i en annan medlemsstat i Europeiska unionen.

CSIRT-enheten får också lämna ut eller röja annan än i 1 mom. avsedd information som den fått vid skötseln av uppgifter enligt cyberresiliensförordningen på det sätt som föreskrivs i 1 mom., om det är nödvändigt för skötseln av de uppgifter som föreskrivs i artiklarna 14–17 i cyberresiliensförordningen.

10 §

*Regulatorisk sandlåda för cyberresiliens*

Transport- och kommunikationsverket kan fatta beslut om att inrätta en regulatorisk sandlåda för cyberresiliens enligt artikel 33.2 i cyberresiliensförordningen. I beslutet om inrättande av en regulatorisk sandlåda för cyberresiliens ska den regulatoriska sandlådans giltighetstid och plats, lämplig teknisk avgränsning samt dessutom verksamhetsplan och lämpliga föremål för testningen fastställas. I beslutet kan det fastställas sådana villkor för den regulatoriska sandlådan som behövs med tanke på organiseringen av verksamheten eller säkerheten i verksamheten.

Transport- och kommunikationsverket beviljar på ansökan en ekonomisk aktör rätt att bedriva verksamhet i en regulatorisk sandlåda. Ansökan ska innehålla behövliga uppgifter om sökanden och sökandens verksamhet, andra parter som deltar i testningen, föremålet för testningen och testningens ändamål. Rätt beviljas inte, om föremålet för testningen eller den planerade verksamheten inte uppfyller villkoren i beslutet om inrättande av den regulatoriska sandlådan, om testningen orsakar oskälig olägenhet eller fara för andra aktörer eller om den ekonomiska aktören under de tre år som föregår ansökan har påförts en administrativ påföljdsavgift med stöd av denna lag. Rätten kan också vägras, om testningen på grund av de tillgängliga resurserna i den regulatoriska sandlådan inte är möjlig.

Transport- och kommunikationsverket svarar för att informera om inrättandet av en regulatorisk sandlåda i enlighet med artikel 33.2 i cyberresiliensförordningen samt för tillsyn över, vägledning av och stöd för de ekonomiska aktörerna i den regulatoriska sandlådan i samarbete med övriga marknadskontrollmyndigheter.

Närmare bestämmelser om den tekniska organiseringen av och verksamheten hos regulatoriska sandlådor för cyberresiliens samt om ansökan av en ekonomisk aktör får utfärdas genom föreskrift av Transport- och kommunikationsverket.

3 kap.

**Anmälda organ**

11 §

*Anmälande myndighet*

Transport- och kommunikationsverket är den anmälande myndighet som avses i artikel 36 i cyberresiliensförordningen (*anmälande myndighet*).

Den anmälande myndigheten utser organ för bedömning av överensstämmelse till anmälda organ, utövar tillsyn över de organ som den har anmält och svarar för andra uppgifter som den anmälande myndigheten föreskrivs i cyberresiliensförordningen. Den anmälande myndigheten svarar för att den information som avses i artiklarna 35.1, 38.1 och 46.2 i cyberresiliensförordningen anmäls till Europeiska kommissionen och de övriga medlemsstaterna i Europeiska unionen.

Bestämmelser om krav på den anmälande myndigheten finns i artikel 37 i cyberresiliensförordningen.

12 §

*Ansökan om anmälan*

Ett organ för bedömning av överensstämmelse som är etablerat i Finland ska ansöka om anmälan hos den anmälande myndigheten. Till ansökan ska fogas ett av Säkerhets- och kemikalieverkets ackrediteringsenhet (*ackrediteringstjänsten FINAS*) utfärdat ackrediteringsintyg över att organet för bedömning av överensstämmelse uppfyller kraven i cyberresiliensförordningen, samt andra uppgifter som avses i artikel 42 cyberresiliensförordningen. Om organet för bedömning av överensstämmelse ändå inte kan foga något ackrediteringsintyg till ansökan ska det ge den anmälande myndigheten alla uppgifter som behövs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i cyberresiliensförordningen.

13 §

*Utseende av ett anmält organ samt begränsning eller återkallelse av ett utseende*

Den anmälande myndigheten utser på ansökan ett organ för bedömning av överensstämmelse till anmält organ, om det uppfyller kraven enligt cyberresiliensförordningen.

I beslutet om utseende anges behörighetsområdet för det anmälda organet för bedömning av överensstämmelse, fastställs arrangemangen för tillsynen över organet och uppställs vid behov sådana krav, begränsningar och villkor för organets verksamhet med hjälp av vilka det säkerställs att uppgifterna utförs korrekt.

Bestämmelser om begränsning och återkallelse av utseenden finns i artikel 45 i cyberresiliensförordningen.

På personer anställda vid ett anmält organ eller ett dotterbolag eller en underleverantör som organet använder tillämpas bestämmelserna om straffrättsligt tjänsteansvar när personen utför uppgifter som avses i cyberresiliensförordningen. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

14 §

*Den anmälande myndighetens och anmälda organs rätt att lämna ut sekretessbelagd information*

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag får den anmälande myndigheten på eget initiativ eller på begäran trots sekretessbestämmelserna och andra begränsningar av utlämnande av information lämna ut eller röja en handling eller information som den fått eller upprättat och som gäller grunderna för anmälan av ett organ för bedömning av överensstämmelse och dess övriga kompetens till Europeiska kommissionen och andra medlemsstater i Europeiska unionen, om det behövs för att fullgöra den anmälande myndighetens skyldigheter enligt cyberresiliensförordningen.

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag får ett anmält organ på eget initiativ eller på begäran trots sekretessbestämmelserna och andra begränsningar av utlämnande av information lämna ut eller röja en handling eller information som den fått eller upprättat och som gäller bedömning av överensstämmelse och resultaten av kontroller till Europeiska kommissionen, medlemsstater i Europeiska unionen och andra anmälda organ, om det behövs för att fullgöra det anmälda organets skyldigheter enligt cyberresiliensförordningen.

4 kap.

## Marknadskontroll

15 §

*Marknadskontrollmyndighet*

Marknadskontrollmyndighet enligt artikel 52 i cyberresiliensförordningen är Transport- och kommunikationsverket.

16 §

*Marknadskontroll av AI-system med hög risk*

Med avvikelse från 15 § är den tillsynsmyndighet som är behörig med stöd av 3 § i lagen om tillsyn över vissa system för artificiell intelligens marknadskontrollmyndighet för sådana AI-system med hög risk som avses i artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) och som omfattas av tillämpningsområdet för cyberresiliensförordningen.

17 §

*Expertstöd för marknadskontroll*

Transport- och kommunikationsverket kan på begäran ge expertstöd som gäller marknadskontroll, bedömning av överensstämmelse och bedömning av cybersäkerhetsrisker enligt cyberresiliensförordningen till de marknadskontrollmyndigheter som avses i 16 § samt till den som är behörig att påföra påföljdsavgifter enligt 6 kap. Bestämmelser om samarbete mellan marknadskontrollmyndigheter finns i marknadskontrollagen.

18 §

*Marknadskontrollmyndighetens rätt att lämna ut sekretessbelagd information*

Vad som i 11 och 13 § i marknadskontrollagen föreskrivs om rätten att trots sekretessbestämmelserna lämna ut uppgifter tillämpas också på uppgifter om överensstämmelse, säkerhetsarrangemang och sårbarhet i fråga om produkter med digitala element och på uppgifter om incidenter som påverkar säkerheten. Marknadskontrollmyndigheten kan lämna ut uppgifter på eget initiativ eller på begäran.

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag har marknadskontrollmyndigheten rätt att på eget initiativ eller på begäran trots sekretessbestämmelserna och andra begränsningar av utlämnande av information lämna ut en handling som den fått eller upprättat i samband med skötseln av dess uppgifter till samt att röja sekretessbelagd information för

1) ackrediteringstjänsten FINAS och den anmälande myndigheten, om utlämnandet av information är nödvändigt för att bedöma kompetensen hos organ för bedömning av överensstämmelse,

2) den myndighet som avses i 21 § eller motsvarande myndighet i en annan medlemsstat i Europeiska unionen, om utlämnandet av information är nödvändigt för att myndigheten i fråga ska kunna utföra sina tillsynsuppgifter,

3) den tillsynsmyndighet som avses i 26 § i cybersäkerhetslagen och 18 h § i lagen om informationshantering inom den offentliga förvaltningen (906/2019), Finansinspektionen eller motsvarande myndighet i en annan medlemsstat i Europeiska unionen, om en produkt med digitala element med fog kan bedömas utgöra en betydande cybersäkerhetsrisk på grund av icke-tekniska riskfaktorer och utlämnandet av information är nödvändigt för fullgörandet av anmälningsskyldigheten enligt artikel 54.2 i cyberresiliensförordningen,

4) Europeiska unionens cybersäkerhetsbyrå Enisa och CSIRT-enheten, om det är nödvändigt för att fullgöra en samarbetsskyldighet eller genomföra rådgivning eller en utredning enligt artiklarna 52.4, 52.5 och 54.1 i cyberresiliensförordningen eller för att utföra de uppgifter som CSIRT-enheten ska utföra enligt cybersäkerhetslagen,

5) dataombudsmannen, om utlämnandet av information är nödvändigt för skötseln av dess lagstadgade tillsynsuppgifter,

6) Europeiska kommissionen, Konkurrens- och konsumentverket och den nationella konkurrensmyndigheten i en annan medlemsstat i Europeiska unionen, om det är nödvändigt för att ge information som är av betydelse för tillämpningen av Europeiska unionens konkurrensrätt för att fullgöra skyldigheten enligt artikel 52.13 i cyberresiliensförordningen.

Transport- och kommunikationsverket och den som begär expertstöd enligt 17 § har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att till varandra lämna ut handlingar som de fått eller upprättat i samband med skötseln av sina uppgifter samt att för varandra röja sekretessbelagd information, om det är nödvändigt för att ge expertstöd.

19 §

*Marknadskontrollmyndighetens rätt att utföra inspektioner och ta programvaror för undersökning*

Utöver vad som föreskrivs i 9 § 1 mom. i marknadskontrollagen får inspektioner också utföras i utrymmen som används för boende av permanent natur och som en ekonomisk aktör använder för ändamål som rör dess närings- eller yrkesverksamhet. I utrymmen som används för boende av permanent natur får inspektion utföras endast om det är nödvändigt för att utreda de omständigheter som är föremål för inspektion och om det finns motiverade och specificerade skäl att misstänka att det har skett eller sker en sådan överträdelse av bestämmelserna i cyberresiliensförordningen eller bestämmelser som utfärdats med stöd av den att påföljden kan vara påföljdsavgift enligt denna lag. Dessutom förutsätts det att den misstänkta överträdelsen gäller bristande överensstämmelse hos en produkt med digitala element eller en process i

anslutning till den eller att det är fråga om en i artikel 57 i cyberresiliensförordningen avsedd situation där produkten annars utgör en betydande cybersäkerhetsrisk.

Bestämmelser om marknadskontrollmyndighetens rätt att ta produkter för undersökning finns i marknadskontrollagen. Ekonomiska aktörer betalas ingen ersättning för programvaror som tas för undersökning.

20 §

*Tillsynsbeslut som meddelas en förvaltare av programvara med fri och öppen källkod*

Marknadskontrollmyndigheten kan ålägga en förvaltare av programvara med fri och öppen källkod att inom utsatt tid avhjälpa brister i fullgörandet av dess skyldigheter enligt cyberresiliensförordningen.

Marknadskontrollmyndigheten kan förena ett beslut som den fattat med stöd av denna paragraf med vite.

5 kap.

## Cybersäkerhetscertifiering

21 §

*Nationell myndighet för cybersäkerhetscertifiering*

Den nationella myndighet för cybersäkerhetscertifiering som avses i artikel 58 i cybersäkerhetsakten (*myndighet för cybersäkerhetscertifiering*) är Transport- och kommunikationsverket.

Transport- och kommunikationsverkets uppgifter i samband med utfärdande av europeiska cybersäkerhetscertifikat ska avskiljas från tillsynsverksamheten enligt artikel 58 i cybersäkerhetsakten och det ska säkerställas att dessa funktioner utförs oberoende av varandra.

22 §

*Anmälan och bemyndigande av organ för bedömning av överensstämmelse för cybersäkerhetscertifiering*

Bestämmelser om uppgifterna för myndigheten för cybersäkerhetscertifiering i anslutning till bemyndigande av organ för bedömning av överensstämmelse för cybersäkerhetscertifiering finns i artikel 60.3 i cybersäkerhetsakten och bestämmelser om anmälan av organ för bedömning av överensstämmelse som ackrediterats för cybersäkerhetscertifiering till Europeiska kommissionen finns i artikel 61 i cybersäkerhetsakten. Om den europeiska ordning för cybersäkerhetscertifiering som tillämpas förutsätter det, förutsätts för anmälan ett bemyndigande av myndigheten för cybersäkerhetscertifiering. Myndigheten för cybersäkerhetscertifiering utövar tillsyn över de organ för bedömning av överensstämmelse som den anmält för cybersäkerhetscertifiering.

Förutsättningen för anmälan och bemyndigande för cybersäkerhetscertifiering är att ackrediteringstjänsten FINAS över den ackreditering som avses i artikel 60.1 i cybersäkerhetsakten har beviljat organet för bedömning av överensstämmelse ett ackrediteringsintyg över att organet för bedömning av överensstämmelse uppfyller kraven i cybersäkerhetsakten.

23 §

*Skyldigheter för organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering*

Ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering ska utföra bedömningar av överensstämmelse på det sätts som förutsätts i förfarandena för bedömning av överensstämmelse enligt cybersäkerhetsakten och de bestämmelser som utfärdats med stöd av den. Dessutom ska ett organ för bedömning av överensstämmelse utföra övriga uppgifter som föreskrivs i cybersäkerhetsakten och de bestämmelser som utfärdats med stöd av den.

Ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering ska till myndigheten för cybersäkerhetscertifiering anmäla alla ändringar som påverkar uppfyllandet av förutsättningarna för anmälan eller bemyndigande.

På en person anställd vid ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering eller ett dotterbolag eller en underleverantör som organet använder tillämpas bestämmelserna om straffrättsligt tjänsteansvar när personen sköter uppgifter som avses i cybersäkerhetsakten och i denna lag. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

24 §

*Överföring av uppgifter i anslutning till utfärdande av cybersäkerhetscertifikat*

Myndigheten för cybersäkerhetscertifiering får i fråga om en viss europeisk ordning för cybersäkerhetscertifiering överföra uppgifter i anslutning till utfärdande av europeiska cybersäkerhetscertifikat på hög assuransnivå enligt artikel 52.7 i cybersäkerhetsakten till ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering

1) i de fall som avses i artikel 56.6 a i cybersäkerhetsakten så att myndigheten för cybersäkerhetscertifiering på förhand godkänner utfärdande av varje enskilt europeiskt cybersäkerhetscertifikat, eller

2) i de fall som avses i artikel 56.6 b i cybersäkerhetsakten på ett allmänt plan så att organet för bedömning av överensstämmelse utfärdar ett cybersäkerhetscertifikat utan separat godkännande från myndigheten för cybersäkerhetscertifiering.

I avtalet med ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering ska åtminstone följande avtalas om:

1) uppgifterna för organet för bedömning av överensstämmelse,

2) behövliga särskilda krav som ställs på kompetensen hos organet för bedömning av överensstämmelse och säkerheten i organets verksamhet,

3) avtalsperioden, inledandet av verksamheten och avslutande av avtalet under avtalsperioden,

4) förvaring och arkivering av handlingar i anslutning till verksamheten hos organet för bedömning av överensstämmelse,

5) påföljder för brister och försummelser i verksamheten hos organet för bedömning av överensstämmelse.

Myndigheten för cybersäkerhetscertifiering får säga upp eller häva avtalet, om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte längre uppfyller kraven för det eller om organet väsentligt försummar fullgörandet av de uppgifter som överenskommits om i avtalet eller annars bryter mot avtalet eller väsentligen eller upprepade gånger handlar lagstridigt.

25 §

*Rätt att få information och utföra inspektioner för myndigheten för cybersäkerhetscertifiering*

Myndigheten för cybersäkerhetscertifiering har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och i artikel 53.2 i cybersäkerhetsakten avsedda utfärdare av EU-försäkringar om överensstämmelse få den information som är nödvändig för skötseln av dess uppgifter enligt denna lag och cybersäkerhetsakten och för tillsynen över efterlevnaden av cybersäkerhetsakten, bestämmelser som utfärdats med stöd av den och denna lag. Informationen ska lämnas utan obefogat dröjsmål, i den form som myndigheten begär och avgiftsfritt.

Myndigheten för cybersäkerhetscertifiering har rätt att göra inspektioner som gäller organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat eller utfärdare av EU-försäkringar om överensstämmelse för att övervaka att cybersäkerhetsakten, de bestämmelser som utfärdats med stöd av den och denna lag iakttas. Vid inspektionerna ska bestämmelserna i 39 § i förvaltningslagen (434/2003) iakttas.

Myndigheten för cybersäkerhetscertifiering har rätt att anlita en oberoende expert för inspektionen. Den som förrättar inspektionen och den som deltar i inspektionen ska ha sådan utbildning och erfarenhet som behövs för inspektionen. På oberoende experter tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de utför uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

Myndigheten för cybersäkerhetscertifiering och oberoende experter har när de utför inspektionen rätt att få tillträde till alla lokaler där verksamhet som avses i cybersäkerhetsakten bedrivs samt till alla lokaler och informationssystem där uppgifter som är av betydelse för tillsynen förvaras eller behandlas. Inspektioner får emellertid inte utföras i utrymmen som används för boende av permanent natur.

26 §

*Rätt för myndigheten för cybersäkerhetscertifiering att lämna ut sekretessbelagd information*

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag har myndigheten för cybersäkerhetscertifiering rätt att på eget initiativ eller på begäran trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information lämna ut en handling som den fått eller upprättat i samband med skötseln av uppgifterna enligt denna lag eller cybersäkerhetsakten till samt röja sekretessbelagd information för

1) den marknadskontrollmyndighet som avses i 4 § i marknadskontrollagen och Säkerhets- och kemikalieverkets ackrediteringsenhet eller det nationella ackrediteringsorganet i en annan medlemsstat i Europeiska unionen, om utlämnandet av informationen är nödvändigt för att myndigheten i fråga ska kunna utföra sina uppgifter,

2) andra nationella myndigheter för cybersäkerhetscertifiering och andra medlemmar i Europeiska gruppen för cybersäkerhetscertifiering och Europeiska unionens cybersäkerhetsbyrå Enisa och Europeiska kommissionen, om det är nödvändigt för att fullgöra en skyldighet som myndigheten för cybersäkerhetscertifiering har enligt cybersäkerhetsakten eller med stöd av den,

3) den tillsynsmyndighet som avses i 26 § i cybersäkerhetslagen och 18 h § i lagen om informationshantering inom den offentliga förvaltningen, Finansinspektionen och CSIRT-enheten, om det är fråga om information om att en IKT-produkt, IKT-tjänst eller IKT-process eller en informationssäkerhetstjänst inte motsvarar kraven enligt cybersäkerhetsakten eller den europeiska ordningen för cybersäkerhetscertifiering samt information om sårbarheter som gäller

en sådan produkt, tjänst eller process eller informationssäkerhetstjänst, och om utlämnandet är nödvändigt för skötseln av deras lagstadgade uppgifter.

27 §

*Tillsynsbeslut*

Myndigheten för cybersäkerhetscertifiering kan ålägga ett organ för bedömning av överensstämmelse, innehavaren av ett europeiskt cybersäkerhetscertifikat eller en utfärdare av EU-försäkringar om överensstämmelse att inom utsatt tid avhjälpa brister i fullgörandet av dess skyldigheter enligt denna lag eller cybersäkerhetsakten eller bestämmelser som utfärdats med stöd av den.

Myndigheten för cybersäkerhetscertifiering kan förena ett beslut som den har fattat med stöd av denna paragraf med vite eller hot om att den verksamhet som strider mot skyldigheterna avbryts eller att den försummade åtgärden vidtas på bekostnad av organet för bedömning av överensstämmelse, innehavaren av ett europeiskt cybersäkerhetscertifikat eller utfärdaren av EU-försäkringar om överensstämmelse.

28 §

*Återkallande av cybersäkerhetscertifikat*

Myndigheten för cybersäkerhetscertifiering kan återkalla ett europeiskt cybersäkerhetscertifikat som den har utfärdat eller som i enlighet med artikel 56.6 i cybersäkerhetsakten har utfärdats av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering, om cybersäkerhetscertifikatet inte uppfyller kraven enligt cybersäkerhetsakten eller kraven för den europeiska ordningen för cybersäkerhetscertifiering i fråga eller om innehavaren av cybersäkerhetscertifikatet inte lämnar myndigheten för cybersäkerhetscertifiering den i 25 § 1 mom. avsedda information som myndigheten begär och bristen eller försummelsen inte avhjälps inom en skälig tid.

29 §

*Avbrytande, begränsning eller återkallande av bemyndigande för eller anmälan av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering*

Om inte något annat följer av vad som föreskrivs med stöd av cybersäkerhetsakten, ska myndigheten för cybersäkerhetscertifiering vid behov återkalla, avbryta eller begränsa ett bemyndigande för ett organ för bedömning av överensstämmelse enligt artikel 60.3 i cybersäkerhetsakten och en anmälan enligt artikel 61.1 i cybersäkerhetsakten samt lämna in en begäran om att stryka ett organ för bedömning av överensstämmelse från förteckningen i enlighet med artikel 61.4 i cybersäkerhetsakten, om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte har avhjälpt brister i sin verksamhet inom den tidsfrist som fastställts med stöd av 27 § och det är fråga om en väsentlig överträdelse eller försummelse eller om organet inte uppfyller de föreskrivna kraven eller om dess ackreditering begränsas, återkallas eller avbryts.

Om ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering har avslutat sin verksamhet eller om den stryks från Europeiska kommissionens förteckning, ska myndigheten för cybersäkerhetscertifiering vidta lämpliga åtgärder för att säkerställa att organets handlingar handläggs av ett annat organ för bedömning av överensstämmelse som

anmälts för cybersäkerhetscertifiering eller att handlingarna finns tillgängliga för myndigheten för cybersäkerhetscertifiering och de myndigheter som svarar för marknadskontrollen.

30 §

*Handräckning av polisen*

Polisen är skyldig att ge myndigheten för cybersäkerhetscertifiering handräckning för tillsynen över efterlevnaden och verkställigheten av denna lag och cybersäkerhetsakten och de skyldigheter som föreskrivs med stöd av den.

Bestämmelser om handräckning av polisen finns i polislagen (872/2011).

6 kap.

**Påföljdsavgifter**

31 §

*Påföljdsavgift för tillverkare*

En administrativ påföljdsavgift kan påföras en tillverkare som uppsåtligen eller av oaktsamhet

1) i strid med artikel 13.1 i cyberresiliensförordningen släpper ut en produkt med digitala element på marknaden utan att säkerställa att produkten har utformats, utvecklats och producerats i enlighet med de väsentliga cybersäkerhetskrav som fastställs i del I i bilaga I till cyberresiliensförordningen,

2) försummar att göra en bedömning av cybersäkerhetsrisker enligt artikel 13.2 i cyberresiliensförordningen eller att beakta resultaten av bedömningen,

3) försummar skyldigheten enligt artikel 13.3 i cyberresiliensförordningen att dokumentera bedömningen av cybersäkerhetsrisker eller försummar att uppdatera den,

4) försummar skyldigheten enligt artikel 13.4 i cyberresiliensförordningen att inkludera bedömningen av cybersäkerhetsrisker i den tekniska dokumentationen,

5) försummar skyldigheten enligt artikel 13.7 i cyberresiliensförordningen att dokumentera cybersäkerhetsaspekter eller försummar att uppdatera bedömningen av cybersäkerhetsrisker enligt den nämnda punkten,

6) integrerar komponenter som kommer från en tredje part i produkten på något annat sätt än i enlighet med artikel 13.5 i cyberresiliensförordningen eller försummar skyldigheten enligt artikel 13.6 i cyberresiliensförordningen att rapportera en sårbarhet i en integrerad komponent till den som tillverkar eller underhåller komponenten, att åtgärda eller avhjälpa sårbarheten eller försummar skyldigheten att dela information enligt den nämnda artikeln,

7) fastställer en stödperiod i strid med artikel 13.8 i cyberresiliensförordningen eller underlåter att meddela att stödperioden tar slut på det sätt som föreskrivs i artikel 13.19 i cyberresiliensförordningen,

8) försummar skyldigheten enligt artikel 13.8 i cyberresiliensförordningen att hantera sårbarheter effektivt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i del II i bilaga I till cyberresiliensförordningen under stödperioden,

9) försummar att säkerställa att säkerhetsuppdateringar som under stödperioden har gjorts tillgängliga för användarna förblir tillgängliga under den tidsperiod som föreskrivs i artikel 13.9 i cyberresiliensförordningen,

10) säkerställer efterlevnaden av det väsentliga cybersäkerhetskrav som avses i artikel 13.10 i cyberresiliensförordningen endast för den version som tillverkaren senast släppte ut på marknaden, om användningen av versionen inte är kostnadsfri för användarna eller medför ytterligare kostnader för dem i strid med den nämnda punkten,

11) försummar att upprätta den tekniska dokumentation som avses i artikel 31 i cyberresiliensförordningen innan en produkt med digitala element släpps ut på marknaden eller upprättar den tekniska dokumentationen i strid med artiklarna 31.1–31.4 eller 33.5 i cyberresiliensförordningen,

12) försummar skyldigheten enligt artikel 13.12 andra stycket i cyberresiliensförordningen att genomföra eller låta genomföra valda förfaranden för bedömning av överensstämmelse enligt artikel 32.1–32.5 i cyberresiliensförordningen,

13) försummar att upprätta en EU-försäkran om överensstämmelse i enlighet med artikel 28 i cyberresiliensförordningen eller försummar att fästa en CE-märkning på produkten enligt artikel 30 i cyberresiliensförordningen, när det genom ett förfarande för bedömning av överensstämmelse har visats att produkten uppfyller de väsentliga cybersäkerhetskrav som avses i artikel 13.12 tredje stycket i cyberresiliensförordningen,

14) försummar att hålla den tekniska dokumentationen om produkten och EU-försäkran om överensstämmelse tillgänglig för marknadskontrollmyndigheten under den tidsperiod som föreskrivs i artikel 13.13 i cyberresiliensförordningen,

15) försummar att använda de förfaranden eller ta hänsyn till de förändringar som avses i artikel 13.14 i cyberresiliensförordningen,

16) försummar att förse produkten, dess förpackning eller ett dokument som åtföljer med produkten med den identifieringsmärkning som avses i artikel 13.15 i cyberresiliensförordningen, den information som avses i artikel 13.16 i cyberresiliensförordningen eller den information som avses i artikel 13.17 andra stycket i cyberresiliensförordningen,

17) försummar att utse en i artikel 13.17 första stycket i cyberresiliensförordningen avsedd gemensam kontaktpunkt eller i strid med artikel 13.17 tredje stycket i cyberresiliensförordningen begränsar användarens kommunikationsmedel enbart till automatiserade verktyg,

18) försummar skyldigheten enligt artikel 13.18 i cyberresiliensförordningen att säkerställa att en produkt med digitala element åtföljs av den information och de instruktioner som ska ges användaren på det i den punkten avsedda sättet och som fastställs i bilaga II till den nämnda förordningen eller försummar att säkerställa att informationen och instruktionerna förblir tillgängliga för användarna och marknadskontrollmyndigheten under den tidsperiod som föreskrivs i artikel 13.18 i cyberresiliensförordningen,

19) försummar skyldigheten enligt artikel 13.20 i cyberresiliensförordningen att lämna in en kopia av EU-försäkran om överensstämmelse eller en förenklad EU-försäkran om överensstämmelse med produkten,

20) underlåter att vidta de korrigerande åtgärder som behövs i en situation som avses i artikel 13.21 i cyberresiliensförordningen,

21) försummar skyldigheten enligt artikel 13.22 i cyberresiliensförordningen att lämna information eller handlingar till marknadskontrollmyndigheten eller att samarbeta,

22) försummar skyldigheten enligt artikel 13.23 i cyberresiliensförordningen att underrätta om upphörande av verksamheten,

23) försummar skyldigheten enligt artikel 14.1 i cyberresiliensförordningen att anmäla aktivt utnyttjade sårbarheter i en produkt med digitala element eller försummar att i anmälan eller slutrapporten inkludera de uppgifter som avses i artikel 14.2,

24) försummar skyldigheten enligt artikel 14.3 i cyberresiliensförordningen att anmäla allvarliga incidenter som påverkar säkerheten för en produkt med digitala element eller försummar att lämna uppgifter enligt artikel 14.4,

25) försummar att lämna CSIRT-enheten de uppgifter som avses i artikel 14.6 i cyberresiliensförordningen, när CSIRT-enheten har begärt att tillverkaren lämnar en delrapport,

26) försummar skyldigheten enligt artikel 14.8 i cyberresiliensförordningen att underrätta drabbade användare av en produkt med digitala element och vid behov alla användare om en

aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element.

En administrativ påföljdsavgift kan på de grunder som anges i 1 mom. påföras någon annan aktör än tillverkaren, om aktören med stöd av artikel 21 eller 22 i cyberresiliensförordningen svarar för tillverkarens skyldigheter.

32 §

*Påföljdsavgift för tillverkarens representant*

En administrativ påföljdsavgift kan påföras tillverkarens representant, om representanten uppsåtligen eller av oaktsamhet

1) försummar att säkerställa att EU-försäkran om överensstämmelse och den tekniska dokumentationen finns tillgängliga för marknadskontrollmyndigheten under den tidsperiod som anges i artikel 18.3 a i cyberresiliensförordningen,

2) försummar att på begäran ge marknadskontrollmyndigheten de uppgifter som avses i det inledande stycket till artikel 18.3 i cyberresiliensförordningen eller de handlingar och uppgifter som avses i artikel 18.3 b eller att samarbeta i enlighet med artikel 18.3 c i cyberresiliensförordningen,

3) på något annat sätt än de som avses i 1 och 2 punkten försummar en uppgift som omfattas av den fullmakt som tillverkarens representant har fått av tillverkaren och som med stöd av cyberresiliensförordningen hör till tillverkarens skyldigheter.

33 §

*Påföljdsavgift för importörer*

En administrativ påföljdsavgift kan påföras en importör som uppsåtligen eller av oaktsamhet

1) släpper ut en produkt med digitala element på marknaden i strid med artikel 19.1–19.3 i cyberresiliensförordningen,

2) försummar att göra en anmälan till tillverkaren eller marknadskontrollmyndigheten när importören är skyldig att göra det med stöd av artikel 19.3 i cyberresiliensförordningen,

3) försummar att ange de uppgifter som avses i artikel 19.4 i cyberresiliensförordningen på det sätt som föreskrivs i den punkten,

4) försummar att vidta de åtgärder som avses i artikel 19.5 första stycket i cyberresiliensförordningen eller försummar att göra en underrättelse till tillverkaren och marknadskontrollmyndigheten enligt andra stycket i den nämnda punkten i cyberresiliensförordningen,

5) försummar att hålla en kopia av EU-försäkran om överensstämmelse tillgänglig för marknadskontrollmyndigheten eller säkerställa att marknadskontrollmyndigheten på begäran kan få tillgång till den tekniska dokumentationen under den tid som föreskrivs i artikel 19.6 i cyberresiliensförordningen,

6) försummar att på begäran ge marknadskontrollmyndigheten den information som avses i artikel 19.7 i cyberresiliensförordningen.

34 §

*Påföljdsavgift för distributörer*

En administrativ påföljdsavgift kan påföras en distributör som uppsåtligen eller av oaktsamhet

1) tillhandahåller en produkt med digitala element på marknaden i strid med artikel 20.1–20.3 i cyberresiliensförordningen,
2) försummar att vidta de åtgärder som avses i artikel 20.4 första stycket i cyberresiliensförordningen eller försummar att göra en underrättelse till tillverkaren och marknadskontrollmyndigheten enligt andra stycket i den nämnda punkten i cyberresiliensförordningen,
3) försummar att på motiverad begäran av marknadskontrollmyndigheten ge marknadskontrollmyndigheten den information och dokumentation som avses i artikel 20.5 i cyberresiliensförordningen,
4) försummar att ge marknadskontrollmyndigheten den underrättelse som avses i artikel 20.6 i cyberresiliensförordningen.

35 §

*Påföljdsavgift för anmälda organ*

En administrativ påföljdsavgift kan påföras ett anmält organ som uppsåtligen eller av oaktsamhet
1) agerar som anmält organ utan att uppfylla kraven i artikel 39 i cyberresiliensförordningen,
2) använder dotterbolag eller lägger ut uppgifter på underentreprenad på något annat sätt än i enlighet med artikel 41 i cyberresiliensförordningen,
3) utför en bedömning av överensstämmelse på något annat sätt än i enlighet med det förfarande som föreskrivs i artikel 47 i cyberresiliensförordningen eller försummar den skyldighet som föreskrivs i den nämnda artikeln,
4) försummar att underrätta den anmälande myndigheten om de omständigheter som avses i artikel 49.1 i cyberresiliensförordningen eller att i enlighet med artikel 49.2 informera andra anmälda organ om de omständigheter som avses i den nämnda punkten.

36 §

*Andra påföljdsavgifter i anslutning till cyberresiliensförordningen*

En administrativ påföljdsavgift kan påföras en ekonomisk aktör som uppsåtligen eller av oaktsamhet
1) försummar att på begäran lämna marknadskontrollmyndigheten den information som avses i artikel 23 i cyberresiliensförordningen, när den ekonomiska aktören är skyldig att lämna informationen,
2) fäster en CE-märkning på produkten på något annat sätt än i enlighet med artikel 30 i cyberresiliensförordningen,
3) försummar att på begäran ge marknadskontrollmyndigheten tillgång till de data som avses i artikel 53 i cyberresiliensförordningen, när de behövs för att bedöma om en produkt med digitala element och de processer som införts av tillverkaren uppfyller de väsentliga cybersäkerhetskraven enligt bilaga I till cyberresiliensförordningen,
4) lämnar ett anmält organ eller marknadskontrollmyndigheten information som är felaktig, bristfällig eller vilseledande och som är av betydelse för skötseln av en uppgift som avses i denna lag eller i cyberresiliensförordningen.

37 §

*Påföljdsavgift som gäller cybersäkerhetscertifiering*

En administrativ påföljdsavgift kan påföras den som uppsåtligen eller av oaktsamhet

1) utfärdar en sådan EU-försäkran om överensstämmelse som avses i artikel 53.2 i cybersäkerhetsakten trots att IKT-produkterna, IKT-tjänsterna eller IKT-processerna eller de utlokaliserade säkerhetstjänsterna inte uppfyller kraven enligt den europeiska ordningen för cybersäkerhetscertifiering i fråga,

2) försummar att ge myndigheten för cybersäkerhetscertifiering den information som avses i artikel 53.3 i cybersäkerhetsakten eller försummar att lämna in en kopia av EU-försäkran om överensstämmelse till myndigheten för cybersäkerhetscertifiering och Europeiska unionens cybersäkerhetsbyrå,

3) bryter mot de villkor för en europeisk ordning för cybersäkerhetscertifiering som avses i artikel 54.1 k i cybersäkerhetsakten,

4) försummar att offentliggöra den information som avses i artikel 55.1 i cybersäkerhetsakten på det sätt som föreskrivs i artikel 55.2 i cybersäkerhetsakten,

5) lämnar myndigheten för cybersäkerhetscertifiering eller ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering information som är felaktig, bristfällig eller vilseledande och som är av betydelse för skötseln av en uppgift som avses i denna lag eller i cybersäkerhetsakten,

6) försummar att lämna information enligt artikel 56.8 i cybersäkerhetsakten,

7) använder ett europeiskt cybersäkerhetscertifikat som har återkallats eller vars giltighetstid har löpt ut.

38 §

*Påföljdsavgiftens belopp*

En administrativ påföljdsavgift som med stöd av 31 § 1 mom. påförs en tillverkare är högst 15 000 000 euro eller två och en halv procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är högst.

En administrativ påföljdsavgift som påförs med stöd av 31 § 2 mom., 32–35 § eller 36 § 1–3 punkten är högst 10 000 000 euro eller två procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är högst.

En administrativ påföljdsavgift som påförs med stöd av 36 § 4 punkten är högst 5 000 000 euro eller en procent av företagets globala omsättning under den föregående räkenskapsperioden, beroende på vilken siffra som är högst.

En påföljdsavgift som påförs med stöd av 37 § är högst 100 000 euro.

Påföljdsavgiftens belopp ska baseras på en samlad bedömning. Vid bedömningen av påföljdsavgiftens belopp ska hänsyn tas till förfarandets art, allvar och varaktighet samt om det har upprepats, den skada som överträdelsen orsakat och aktörens storlek samt aktörens eventuella tidigare överträdelser som omfattas av denna lag. När påföljdsavgifter fastställs för överträdelser av cyberresiliensförordningen ska dessutom artikel 64.5 i cyberresiliensförordningen tas i beaktande.

39 §

*Påförande av påföljdsavgift*

De administrativa påföljdsavgifter som avses i 31–34 och 36 § påförs av marknadskontrollmyndigheten. När marknadskontrollmyndighet är den marknadskontrollmyndighet som avses i 3 § i lagen om tillsyn över vissa system för artificiell intelligens, påförs den administrativa påföljdsavgiften i den ordning som föreskrivs i 13 § i den lagen.

Den administrativa påföljdsavgift som avses i 35 § påförs av den anmälande myndigheten.

Den administrativa påföljdsavgift som avses i 37 § påförs av myndigheten för cybersäkerhetscertifiering.

Den myndighet som påför den administrativa påföljdsavgiften har trots sekretessbestämmelserna rätt att avgiftsfritt av ekonomiska aktörer och andra myndigheter få den information som är nödvändig för påförande av påföljdsavgiften eller för beräkning av dess belopp.

40 §

*Avstående från påförande av påföljdsavgift*

Påföljdsavgift påförs inte, om

1) aktören på eget initiativ vidtagit tillräckliga åtgärder för att avhjälpa överträdelsen eller försummelsen omedelbart efter att den upptäckts och utan dröjsmål underrättat tillsynsmyndigheten om den samt samarbetat med tillsynsmyndigheten, och överträdelsen eller försummelsen inte är allvarlig eller återkommande,

2) överträdelsen eller försummelsen ska anses vara ringa, eller

3) påförande av påföljdsavgift ska anses vara uppenbart oskäligt på andra grunder än de som avses i 1 eller 2 punkten.

Påföljdsavgift får inte påföras, om det har förflutit mer än fem år sedan överträdelsen eller försummelsen har skett. Om överträdelsen eller försummelsen har varit fortlöpande räknas tiden från det att överträdelsen eller försummelsen har upphört.

Påföljdsavgift får inte påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom. Den som har påförts påföljdsavgift enligt 31–36 § för en överträdelse som gäller cybersäkerhetscertifiering får inte påföras påföljdsavgift enligt 37 §.

Statliga myndigheter, statliga affärsverk, välfärdsområden eller välfärdssammanslutningar, kommunala myndigheter, självständiga offentligrättsliga inrättningar, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland eller ortodoxa kyrkan i Finland eller de två sistnämndas församlingar, kyrkliga samfälligheter och övriga organ får inte påföras påföljdsavgift.

En tillverkare som är ett mikroföretag eller litet företag enligt kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag får inte påföras påföljdsavgift på den grunden att företaget har överskridit tidsfristen för förhandsanmälan enligt artikel 14.2 a eller artikel 14.4 a i cyberresiliensförordningen.

Påföljdsavgift får inte påföras en förvaltare av programvara med fri och öppen källkod.

41 §

*Verkställighet av påföljdsavgift*

Bestämmelser om verkställighet av påföljdsavgifter som påförts med stöd av denna lag finns i lagen om verkställighet av böter (672/2002).

7 kap.

**Särskilda bestämmelser**

42 §

*Begäran om omprövning*

Omprövning får begäras i ett beslut av ett anmält organ, i ett beslut av ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och i ett beslut som gäller en avgift som tas ut för en myndighetsprestation. Bestämmelser om begäran om omprövning finns i förvaltningslagen.

43 §

*Ändringssökande*

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

Ett beslut av marknadskontrollmyndigheten som gäller annat än påförande av påföljdsavgift får verkställas trots ändringssökande.

Den anmälande myndigheten kan bestämma att ett beslut om utseende till anmält organ eller om begränsning eller återkallande av ett utseende ska iakttas trots ändringssökande.

Myndigheten för cybersäkerhetscertifiering kan i sitt beslut som gäller annat än påförande av påföljdsavgift bestämma att beslutet ska iakttas trots ändringssökande.

I ett sådant beslut som fattats med anledning av en begäran om omprövning och som fattats av ett anmält organ eller ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering och som gäller korrigerande åtgärder som krävs av tillverkaren av en produkt med digitala element eller innehavaren av ett europeiskt cybersäkerhetscertifikat, eller som gäller återkallande av ett intyg om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat för en produkt med digitala element kan det bestämmas att beslutet ska iakttas trots ändringssökande.

Vid sökande av ändring i beslut som gäller föreläggande och utdömande av vite samt föreläggande och verkställighet av hot om tvångsutförande eller hot om avbrytande tillämpas dock viteslagen (1113/1990).

44 §

*Avgifter*

Bestämmelser om de allmänna grunderna för när myndigheters prestationer ska vara avgiftsbelagda och för storleken av de avgifter som uppbärs för prestationerna och om övriga grunder för avgifterna finns i lagen om grunderna för avgifter till staten (150/1992).

45 §

*Ikraftträdande*

Denna lag träder i kraft den 20 .

Bestämmelserna i 3 kap. och 35 § tillämpas dock först från och med den 11 juni 2026.

Bestämmelserna i 7–9 § och 31 § 1 mom. 23–26 punkten tillämpas dock först från och med den 11 september 2026.

Bestämmelserna i 4–6 §, 31 § 1 mom. 1–22 punkten, 32–34 § och 36 § tillämpas dock först från och med den 11 december 2027.

---

**2.**

# Lag

**om ändring av 1 och 4 § i lagen om marknadskontrollen av vissa produkter**

I enlighet med riksdagens beslut

*ändras* i lagen om marknadskontrollen av vissa produkter (1137/2016) 1 § 1 mom. 32 punkten och 4 § 4 mom.,

sådana de lyder, 1 § 1 mom. 32 punkten i lag 186/2025 och 4 § 4 mom. i lag 103/2023, och

*fogas* till 1 § 1 mom., sådant det lyder i lag 186/2025, en ny 33 punkt som följer:

1 §

*Tillämpningsområde*

Denna lag tillämpas på marknadskontrollen av de produkter som omfattas av tillämpningsområdet för följande lagar, om inte något annat föreskrivs i de lagar som nämns:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

32) lagen om konsumentprodukters säkerhet (184/2025),

33) lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

4 §

*Tillsynsmyndigheter*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Med avvikelse från 1 mom. är Transport- och kommunikationsverket marknadskontrollmyndighet enligt denna lag när det gäller produkter som avses i luftfartslagen, fordonslagen, 24 a § 3 mom. i miljöskyddslagen, lagen om säkerhet och utsläppskrav för fritidsbåtar, lagen om tjänster inom elektronisk kommunikation, lagen om marin utrustning och lagen om tillgänglighetskrav för vissa produkter. Transport- och kommunikationsverket är marknadskontrollmyndighet enligt denna lag också när det gäller produkter som avses i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering, om inte något annat föreskrivs i den lagen.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

**3.**

# Lag

**om ändring av 20 och 28 § i cybersäkerhetslagen**

I enlighet med riksdagens beslut

*ändras* i cybersäkerhetslagen (124/2025) 20 § 1 mom. 9 punkten och 28 § 4 mom., av dem 28 § 4 mom. sådant det lyder i lag 369/2025, och

*fogas* till 20 § 1 mom. en ny 10 punkt som följer:

20 §

*CSIRT-enhetens uppgifter*

CSIRT-enheten har till uppgift att

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

9) ge anvisningar och rekommendationer om hantering av incidenter, krishantering inom cybersäkerheten och samordnad delgivning av information om sårbarheter,

10) ta emot och behandla anmälningar enligt artiklarna 14 och 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) och svara för övriga uppgifter som ankommer på CSIRT-enheten enligt den nämnda förordningen och lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

28 §

*Rätt att få information*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en CSIRT-enhet och en tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft samt Finansinspektionen, om det är nödvändigt för en uppgift som i denna lag eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft föreskrivits för myndigheten eller för uppgiften som behörig myndighet enligt 50 p § 1 och 2 mom. i lagen om Finansinspektionen (878/2008). Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

**4.**

# Lag

**om ändring av lagen om tjänster inom elektronisk kommunikation**

I enlighet med riksdagens beslut

*upphävs* i lagen om tjänster inom elektronisk kommunikation (917/2014) 304 § 1 mom. 14 punkten, sådan den lyder i lag 1211/2022,

*ändras* 3 § 35 punkten, rubriken för 21 kap. och 164 § 2 mom., av dem 164 § 2 mom. sådant det lyder i lag 1003/2018, och

*fogas* till 3 §, sådan den lyder delvis ändrad i lagarna 456/2016, 52/2019, 1207/2020, 1211/2022, 105/2023 och 661/2024, en ny 35 a punkt, till 164 §, sådan den lyder i lag 1003/2018, ett nytt 4 mom. och till lagen ett nytt 21 a kap. som följer:

3 §

*Definitioner*

I denna lag avses med

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

35) *domännamn* en adress på internet på andra nivån i form av ett namn som består av bokstäver, siffror eller andra tecken eller en kombination av dem,

35 a) *den som förvaltar ett toppdomänregister* en part som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, inbegripet registreringen av domännamn under den och den tekniska driften av den,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

21 kap.

**Domännamn för Finland och Åland**

164 §

*Transport- och kommunikationsverkets domännamnsverksamhet och förmedling av domännamn*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Endast registrarer som har lämnat in en anmälan enligt 165 § får göra registreringar i domännamnsregistret. Transport- och kommunikationsverket får emellertid för domännamnsförvaltningens behov avgiftsfritt registrera domännamn som består av endast ett tecken samt andra domännamn. Transport- och kommunikationsverket får också göra andra anteckningar i domännamnsregistret som behövs för att genomföra denna lag.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Vad som i 165 §, 170 § 1 mom. 2 och 8–11 punkten samt 171 § föreskrivs om registrarer, tillämpas också på aktörer som tillhandahåller registreringstjänster för domännamn för registrarers räkning.

21 a kap.

## Andra domännamn

172 a §

*Kapitlets tillämpningsområde*

Detta kapitel tillämpas på andra domännamn än domännamn under toppdomänen för Finland och toppdomänen för Åland och förmedling av dessa domännamn.

Detta kapitel tillämpas på registrarer och de som förvaltar ett toppdomänregister, om deras huvudsakliga etableringsställe eller deras utsedda företrädare i Europeiska unionen finns i Finland. Om en registrar inte är etablerad i en medlemsstat i Europeiska unionen men tillhandahåller sina tjänster i Finland eller inom en annan medlemsstat i Europeiska unionen, ska den utse en i artikel 26.3 i NIS 2-direktivet avsedd företrädare för Europeiska unionens medlemsstater. Detta kapitel tillämpas också på en registrar som inte är etablerad i en medlemsstat i Europeiska unionen eller inte har utsett en i artikel 26.3 i NIS 2-direktivet avsedd utsedd företrädare och som tillhandahåller tjänster i Finland.

Vad som i detta kapitel föreskrivs om registrarer, tillämpas också på aktörer som tillhandahåller registreringstjänster för domännamn för registrarers räkning.

172 b §

*Registrarens anmälan*

En registrar ska till Transport- och kommunikationsverket anmäla

1) sitt namn,

2) sin adress, sin e-postadress, sitt telefonnummer och andra aktuella kontaktuppgifter,

3) adress till sitt huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i Europeiska unionen eller, om registraren inte är etablerad i Europeiska unionen, adress, e-postadress, telefonnummer och annan aktuell kontaktinformation till registrarens utsedda företrädare i Europeiska unionen,

4) registrarens IP-adressintervaller,

5) en förteckning över de medlemsstater i Europeiska unionen där registraren tillhandahåller tjänster.

Registraren ska utan dröjsmål underrätta Transport- och kommunikationsverket om förändringar i de uppgifter som avses i 1 mom. Transport- och kommunikationsverket ska underrättas om förändringar inom två veckor från tidpunkten för förändringen. Om förändringar i de uppgifter som avses i 1 mom. 3 punkten ska dock underrättas inom tre månader från tidpunkten för förändringen. Transport- och kommunikationsverket kan meddela närmare föreskrifter om hur uppgifterna ska lämnas.

Transport- och kommunikationsverket ska lämna den gemensamma kontaktpunkt som avses i 18 § i cybersäkerhetslagen de uppgifter om registrarernas anmälningar som behövs för att göra en anmälan enligt artikel 27.4 i NIS 2-direktivet.

172 c §

*Registreringsuppgifter om domännamn*

De som förvaltar ett toppdomänregister och registrarer ska samla in och föra en förteckning över registreringsuppgifter om domännamn. En databas över registreringsuppgifter om

domännamn ska innehålla de uppgifter om domännamn som avses i artikel 28.2 i NIS 2-direktivet.

De som förvaltar ett toppdomänregister och registrarer ska ha riktlinjer och förfaranden för att säkerställa att uppgifterna i en databas över registreringsuppgifter om domännamn är exakta och korrekta. De som förvaltar ett toppdomänregister och registrarer ska göra de riktlinjer och förfaranden som de tillämpar offentligt tillgängliga.

172 d §

*Tillgång till registreringsuppgifter om domännamn*

De som förvaltar ett toppdomänregister och registrarer ska utan obefogat dröjsmål efter registreringen av ett domännamn göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga.

De som förvaltar ett toppdomänregister och registrarer ska ge tillgång till andra registreringsuppgifter om domännamn än de som avses i 1 mom., om den som legitimt begär tillgång till uppgifterna framställer en laglig och på tillbörligt sätt motiverad begäran. De som förvaltar ett toppdomänregister och registrarer ska besvara en begäran om tillgång till registreringsuppgifter om domännamn utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av begäran. De som förvaltar ett toppdomänregister och registrarer ska göra sina riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.

De som förvaltar ett toppdomänregister och registrarer ska samarbeta för att fullgöra de skyldigheter som föreskrivs i 172 c § och i denna paragraf och för att undvika insamling av överlappande registreringsuppgifter.

Bestämmelser om skydd för personuppgifter finns i 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 och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och i dataskyddslagen.

---

Denna lag träder i kraft den 20 . Upphävandet av 304 § 1 mom. 14 punkten träder dock i kraft först den 1 juni 2026.

En aktör som tillhandahåller registreringstjänster för domännamn för en registrars räkning ska göra den anmälan som avses i 165 § i lagen om tjänster inom elektronisk kommunikation inom tre månader från ikraftträdandet av denna lag.

Den anmälan som avses i 172 b § i denna lag ska göras inom tre månader från ikraftträdandet av denna lag.

De riktlinjer och förfaranden som avses i 172 c och 172 d § i denna lag ska göras offentligt tillgängliga inom tre månader från ikraftträdandet av denna lag.

---

**5.**

# Lag

**om ändring av 1 § i lagen om verkställighet av böter**

I enlighet med riksdagens beslut

*ändras* i lagen om verkställighet av böter (672/2002) 1 § 2 mom. 60 punkten, sådan den lyder i lag 860/2025, och

*fogas* till 1 § 2 mom., sådant det lyder i lagarna 416/2025 och 860/2025, en ny 61 punkt som följer:

1 §

*Lagens tillämpningsområde*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Denna lag innehåller bestämmelser om verkställighet av följande administrativa påföljder av straffkaraktär:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

60) avgift för trafikförseelse enligt 122 § i lagen om transport av farliga ämnen inom Försvarsmakten och Gränsbevakningsväsendet (849/2025),

61) en påföljdsavgift enligt 31–37 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

Helsingfors den 27 november 2025

**Statsminister**

**Petteri Orpo**

Kommunikationsminister Lulu Ranne

**2.**

# Lag

**om ändring av 1 och 4 § i lagen om marknadskontrollen av vissa produkter**

I enlighet med riksdagens beslut
*ändras* i lagen om marknadskontrollen av vissa produkter (1137/2016) 1 § 1 mom. 32 punkten och 4 § 4 mom.,
sådana de lyder, 1 § 1 mom. 32 punkten i lag 186/2025 och 4 § 4 mom. i lag 103/2023, och
*fogas* till 1 § 1 mom., sådant det lyder i lag 186/2025, en ny 33 punkt som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 1 § | 1 § |
| *Tillämpningsområde* | *Tillämpningsområde* |
| Denna lag tillämpas på marknadskontrollen av de produkter som omfattas av tillämpningsområdet för följande lagar, om inte något annat föreskrivs i de lagar som nämns: | Denna lag tillämpas på marknadskontrollen av de produkter som omfattas av tillämpningsområdet för följande lagar, om inte något annat föreskrivs i de lagar som nämns: |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| 32) lagen om konsumentprodukters säkerhet (184/2025), | 32) lagen om konsumentprodukters säkerhet (184/2025), |
| *(nya)* | *33) lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| 4 § | 4 § |
| *Tillsynsmyndigheter* | *Tillsynsmyndigheter* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| Med avvikelse från 1 mom. är Transport- och kommunikationsverket marknadskontrollmyndighet enligt denna lag när det gäller produkter som avses i luftfartslagen, fordonslagen, 24 a § 3 mom. i miljöskyddslagen, lagen om säkerhet och utsläppskrav för fritidsbåtar, lagen om tjänster inom elektronisk kommunikation, lagen om marin utrustning och lagen om tillgänglighetskrav för vissa produkter. | Med avvikelse från 1 mom. är Transport- och kommunikationsverket marknadskontrollmyndighet enligt denna lag när det gäller produkter som avses i luftfartslagen, fordonslagen, 24 a § 3 mom. i miljöskyddslagen, lagen om säkerhet och utsläppskrav för fritidsbåtar, lagen om tjänster inom elektronisk kommunikation, lagen om marin utrustning och lagen om tillgänglighetskrav för vissa produkter. *Transport- och kommunikationsverket är* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *marknadskontrollmyndighet enligt denna lag också när det gäller produkter som avses i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering, om inte något annat föreskrivs i den lagen.* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |

*Denna lag träder i kraft den 20 .*

**3.**

# Lag

**om ändring av 20 och 28 § i cybersäkerhetslagen**

I enlighet med riksdagens beslut

*ändras* i cybersäkerhetslagen (124/2025) 20 § 1 mom. 9 punkten och 28 § 4 mom., av dem 28 § 4 mom. sådant det lyder i lag 369/2025, och

*fogas* till 20 § 1 mom. en ny 10 punkt som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 20 § | 20 § |
| *CSIRT-enhetens uppgifter* | *CSIRT-enhetens uppgifter* |
| CSIRT-enheten har till uppgift att | CSIRT-enheten har till uppgift att |
| — — — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — — — |
| 9) ge anvisningar och rekommendationer om hantering av incidenter, krishantering inom cybersäkerheten och samordnad delgivning av information om sårbarheter. | 9) ge anvisningar och rekommendationer om hantering av incidenter, krishantering inom cybersäkerheten och samordnad delgivning av information om sårbarheter, |
| *(nya)* | *10) ta emot och behandla anmälningar enligt artiklarna 14 och 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) och svara för övriga uppgifter som ankommer på CSIRT-enheten enligt den nämnda förordningen och lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).* |
| — — — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — — — |
| 28 § | 28 § |
| *Rätt att få information* | *Rätt att få information* |
| — — — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — — — |
| Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av | Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en CSIRT-enhet och en tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft, om det är nödvändigt för en uppgift som i denna lag eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft föreskrivits för myndigheten. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt. | information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en CSIRT-enhet och en tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft *samt Finansinspektionen*, om det är nödvändigt för en uppgift som i denna lag eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft föreskrivits för myndigheten *eller för uppgiften som behörig myndighet enligt 50 p § 1 och 2 mom. i lagen om Finansinspektionen (878/2008*). Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt. |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| | *Denna lag träder i kraft den 20 .* |

**4.**

# Lag

**om ändring av lagen om tjänster inom elektronisk kommunikation**

I enlighet med riksdagens beslut

*upphävs* i lagen om tjänster inom elektronisk kommunikation (917/2014) 304 § 1 mom. 14 punkten, sådan den lyder i lag 1211/2022,

*ändras* 3 § 35 punkten, rubriken för 21 kap. och 164 § 2 mom., av dem 164 § 2 mom. sådant det lyder i lag 1003/2018, och

*fogas* till 3 §, sådan den lyder delvis ändrad i lagarna 456/2016, 52/2019, 1207/2020, 1211/2022, 105/2023 och 661/2024, en ny 35 a punkt, till 164 §, sådan den lyder i lag 1003/2018, ett nytt 4 mom. och till lagen ett nytt 21 a kap. som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 3 § | 3 § |
| *Definitioner* | *Definitioner* |
| I denna lag avses med | I denna lag avses med |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 35) *domännamn* en adress på internet *under den nationella toppdomänen fi eller toppdomänen ax för landskapet Åland* i form av ett namn som består av bokstäver, siffror eller andra tecken eller en kombination av dem, | 35) *domännamn* en adress på internet *på andra nivån* i form av ett namn som består av bokstäver, siffror eller andra tecken eller en kombination av dem, |
| *(nya)* | *35 a) den som förvaltar ett toppdomänregister en part som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, inbegripet registreringen av domännamn under den och den tekniska driften av den,* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 21 kap. | 21 kap. |
| **Domännamn** | ***Domännamn för Finland och Åland*** |
| 164 § | 164 § |
| *Transport- och kommunikationsverkets domännamnsverksamhet och förmedling av domännamn* | *Transport- och kommunikationsverkets domännamnsverksamhet och förmedling av domännamn* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| *Endast verksamhetsutövare som enligt 165 § har lämnat in en anmälan om* | *Endast registrarer som har lämnat in en anmälan enligt 165 § får göra registreringar* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| *registrarverksamhet (registrar) får göra registreringar i domännamnsregistret*. Transport- och kommunikationsverket får emellertid för domännamnsförvaltningens behov avgiftsfritt registrera domännamn som består av endast ett tecken samt andra domännamn. Transport- och kommunikationsverket får också göra andra anteckningar i domännamnsregistret som behövs för att genomföra denna lag. | *i domännamnsregistret.* Transport- och kommunikationsverket får emellertid för domännamnsförvaltningens behov avgiftsfritt registrera domännamn som består av endast ett tecken samt andra domännamn. Transport- och kommunikationsverket får också göra andra anteckningar i domännamnsregistret som behövs för att genomföra denna lag. |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| *(nya)* | *Vad som i 165 §, 170 § 1 mom. 2 och 8–11 punkten samt 171 § föreskrivs om registrarer, tillämpas också på aktörer som tillhandahåller registreringstjänster för domännamn för registrarers räkning.* |
| | 21 a kap. |
| *(nya)* | **Andra domännamn** |
| | *172 a §* |
| | *Kapitlets tillämpningsområde* |
| | *Detta kapitel tillämpas på andra domännamn än domännamn under toppdomänen för Finland och toppdomänen för Åland och förmedling av dessa domännamn.* |
| | *Detta kapitel tillämpas på registrarer och de som förvaltar ett toppdomänregister, om deras huvudsakliga etableringsställe eller deras utsedda företrädare i Europeiska unionen finns i Finland. Om en registrar inte är etablerad i en medlemsstat i Europeiska unionen men tillhandahåller sina tjänster i Finland eller inom en annan medlemsstat i Europeiska unionen, ska den utse en i artikel 26.3 i NIS 2-direktivet avsedd företrädare för Europeiska unionens medlemsstater. Detta kapitel tillämpas också på en registrar som inte är etablerad i en medlemsstat i Europeiska unionen eller inte har utsett en i artikel 26.3 i NIS 2-direktivet avsedd utsedd företrädare och som tillhandahåller tjänster i Finland.* |
| | *Vad som i detta kapitel föreskrivs om registrarer, tillämpas också på aktörer som* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *tillhandahåller registreringstjänster för domännamn för registrarers räkning.* |
| | *172 b §* |
| | *Registrarens anmälan* |
| | *En registrar ska till Transport- och kommunikationsverket anmäla*<br>*1) sitt namn,*<br>*2) sin adress, sin e-postadress, sitt telefonnummer och andra aktuella kontaktuppgifter,*<br>*3) adress till sitt huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i Europeiska unionen eller, om registraren inte är etablerad i Europeiska unionen, adress, e-postadress, telefonnummer och annan aktuell kontaktinformation till registrarens utsedda företrädare i Europeiska unionen,*<br>*4) registrarens IP-adressintervaller,*<br>*5) en förteckning över de medlemsstater i Europeiska unionen där registraren tillhandahåller tjänster.*<br>*Registraren ska utan dröjsmål underrätta Transport- och kommunikationsverket om förändringar i de uppgifter som avses i 1 mom. Transport- och kommunikationsverket ska underrättas om förändringar inom två veckor från tidpunkten för förändringen. Om förändringar i de uppgifter som avses i 1 mom. 3 punkten ska dock underrättas inom tre månader från tidpunkten för förändringen. Transport- och kommunikationsverket kan meddela närmare föreskrifter om hur uppgifterna ska lämnas.*<br>*Transport- och kommunikationsverket ska lämna den gemensamma kontaktpunkt som avses i 18 § i cybersäkerhetslagen de uppgifter om registrarernas anmälningar som behövs för att göra en anmälan enligt artikel 27.4 i NIS 2-direktivet.* |
| | *172 c §* |
| | *Registreringsuppgifter om domännamn* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *De som förvaltar ett toppdomänregister och registrarer ska samla in och föra en förteckning över registreringsuppgifter om domännamn. En databas över registreringsuppgifter om domännamn ska innehålla de uppgifter om domännamn som avses i artikel 28.2 i NIS 2-direktivet.*<br>*De som förvaltar ett toppdomänregister och registrarer ska ha riktlinjer och förfaranden för att säkerställa att uppgifterna i en databas över registreringsuppgifter om domännamn är exakta och korrekta. De som förvaltar ett toppdomänregister och registrarer ska göra de riktlinjer och förfaranden som de tillämpar offentligt tillgängliga.* |
| | *172 d §* |
| | *Tillgång till registreringsuppgifter om domännamn* |
| | *De som förvaltar ett toppdomänregister och registrarer ska utan obefogat dröjsmål efter registreringen av ett domännamn göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga.*<br>*De som förvaltar ett toppdomänregister och registrarer ska ge tillgång till andra registreringsuppgifter om domännamn än de som avses i 1 mom., om den som legitimt begär tillgång till uppgifterna framställer en laglig och på tillbörligt sätt motiverad begäran. De som förvaltar ett toppdomänregister och registrarer ska besvara en begäran om tillgång till registreringsuppgifter om domännamn utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av begäran. De som förvaltar ett toppdomänregister och registrarer ska göra sina riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.*<br>*De som förvaltar ett toppdomänregister och registrarer ska samarbeta för att fullgöra de skyldigheter som föreskrivs i 172 c § och i denna paragraf och för att undvika insamling av överlappande registreringsuppgifter.* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *Bestämmelser om skydd för personuppgifter finns i 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 och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och i dataskyddslagen.* |
| 304 § | 304 § |
| *Transport- och kommunikationsverkets särskilda uppgifter* | *Transport- och kommunikationsverkets särskilda uppgifter* |
| Utöver vad som föreskrivs någon annanstans i denna lag ska Transport- och kommunikationsverket | Utöver vad som föreskrivs någon annanstans i denna lag ska Transport- och kommunikationsverket |
| — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — |
| *14) vara nationell myndighet för cybersäkerhetscertifiering enligt 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)* | (*upphävs*) |
| — — — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — — — |
| | ———— |
| | *Denna lag träder i kraft den 20 . Upphävandet av 304 § 1 mom. 14 punkten träder dock i kraft först den 1 juni 2026.* |
| | *En aktör som tillhandahåller registreringstjänster för domännamn för en registrars räkning ska göra den anmälan som avses i 165 § i lagen om tjänster inom elektronisk kommunikation inom tre månader från ikraftträdandet av denna lag.* |
| | *Den anmälan som avses i 172 b § i denna lag ska göras inom tre månader från ikraftträdandet av denna lag.* |
| | *De riktlinjer och förfaranden som avses i 172 c och 172 d § i denna lag ska göras offentligt tillgängliga inom tre månader från ikraftträdandet av denna lag.* |
| | ———— |

**5.**

# Lag

**om ändring av 1 § i lagen om verkställighet av böter**

I enlighet med riksdagens beslut

*ändras* i lagen om verkställighet av böter (672/2002) 1 § 2 mom. 60 punkten, sådan den lyder i lag 860/2025, och

*fogas* till 1 § 2 mom., sådant det lyder i lagarna 416/2025 och 860/2025, en ny 61 punkt som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 1 § | 1 § |
| *Lagens tillämpningsområde* | *Lagens tillämpningsområde* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| Denna lag innehåller bestämmelser om verkställighet av följande administrativa påföljder av straffkaraktär: | Denna lag innehåller bestämmelser om verkställighet av följande administrativa påföljder av straffkaraktär: |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 60) avgift för trafikförseelse enligt 122 § i lagen om transport av farliga ämnen inom Försvarsmakten och Gränsbevakningsväsendet (849/2025), | 60) avgift för trafikförseelse enligt 122 § i lagen om transport av farliga ämnen inom Försvarsmakten och Gränsbevakningsväsendet (849/2025), |
| *(nya)* | *61) en påföljdsavgift enligt 31–37 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering ( / ).* |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |

———

*Denna lag träder i kraft den 20 .*

———