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), nedan *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), nedan *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,

RP 179/2025 rd
KoUB 6/2026 rd
RSv 55/2026 rd

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 (1377/2025).

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 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 på det sätt som föreskrivs i 1 mom. lämna ut eller röja annan än i 1 mom. avsedd information som den fått vid skötseln av uppgifter enligt cyberresiliensförordningen, 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 föreskrivs för den anmälande myndigheten 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 en person anställd 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 §

Tillsyn över förvaltare av programvara med fri och öppen källkod

Marknadskontrollmyndigheten kan ge en förvaltare av programvara med fri och öppen källkod anvisningar om de skyldigheter som föreskrivs i cyberresiliensförordningen samt föreslå praktiska förbättringar i innehållet eller arrangemangen i ett programvaruprojekt med öppen källkod som drivs av en förvaltare av programvara.

Marknadskontrollmyndigheten kan ålägga en förvaltare av programvara med fri och öppen källkod att inom skälig tid avhjälpa av myndigheten observerade brister i fullgörandet av de skyldigheter som föreskrivs i cyberresiliensförordningen. Marknadskontrollmyndigheten kan offentliggöra uppgifter om brister som den observerat eller informera om saken, om de brister som observerats inte avhjälps inom skälig tid.

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.

En förutsättning 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 utfärdandet 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 cybersäkerhetscertifikat utan separat godkännande från myndigheten för cybersäkerhetscertifiering.

I avtalet med ett organ för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering ska det åtminstone 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 organet för bedömning av överensstämmelse som anmälts för cybersäkerhetscertifiering inte längre uppfyller kraven för det eller om organet väsentligt försummar fullgörandet av de uppgifter som det 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 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 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 punkten,

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 om den medför ytterligare kostnader för dem i strid med den 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 i enlighet med 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 den förordningen eller den information som avses i artikel 13.17 andra stycket i den förordningen,

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 den förordningen 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 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 den förordningen,

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 tillsammans 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 i den förordningen,

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 i den förordningen,

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 den förordningen,

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 punkten,

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 lämna en underrättelse till tillverkaren och marknadskontrollmyndigheten enligt andra stycket i den punkten,
3) försummar att på motiverad begäran av marknadskontrollmyndigheten ge myndigheten den information och dokumentation som avses i artikel 20.5 i cyberresiliensförordningen,
4) försummar att lämna 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 annars försummar den skyldighet som föreskrivs i den 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 i den förordningen informera andra anmälda organ om de omständigheter som avses i den 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 den akten,

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 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 vilket av dessa belopp som är störst.

En 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 vilket av dessa belopp som är störst.

En 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 vilket av dessa belopp som är störst.

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 påförs 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 samt 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 måste anses 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 tidsfristen 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 genom en lagakraftvunnen dom har dömts för samma gärning. Den som har påförts påföljdsavgift enligt 31—36 § för en överträdelse som gäller cybersäkerhetscertifiering får inte för samma gärning 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 ett 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 1 juni 2026.

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.

Helsingfors den 29 maj 2026

Republikens President

Alexander Stubb

Kommunikationsminister Lulu Ranne