Cybersäkerhetslag

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om hantering av cybersäkerhetsrisker.

Genom denna lag genomförs 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 (*NIS 2-direktivet*).

Bestämmelser om genomförande av NIS 2-direktivet inom den i punkt 10 i bilaga I till det direktivet avsedda sektorn för offentlig förvaltning finns i lagen om informationshantering inom den offentliga förvaltningen (906/2019).

2 §

Definitioner

I denna lag avses med

1) *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,

2) *datacentraltjänst* en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

3) *leverantör av DNS-tjänster* en aktör som tillhandahåller allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

4) *sårbarhet* en svaghet, känslighet eller brist hos informations- och kommunikationstekniska produkter eller informations- och kommunikationstekniska tjänster som kan orsaka ett cyberhot eller en incident,

5) *leverantör av utlokaliserade driftstjänster* en aktör som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av i 17 punkten avsedda IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra kommunikationsnät och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

6) *kvalificerad tillhandahållare av betrodda tjänster* en sådan kvalificerad tillhandahållare av betrodda tjänster som avses i artikel 3.20 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan *eIDAS-förordningen*,

RP 57/2024 rd
KoUB 1/2025 rd
RSv 15/2025 rd

7) *cybersäkerhet* åtgärder som behövs för att skydda kommunikationsnät och informationssystem, deras användare och andra berörda personer mot cyberhot,

8) *cyberhot* en omständighet, händelse eller handling som när den förverkligas kan skada, störa eller på annat negativt sätt påverka kommunikationsnät eller informationssystem, användare av dessa system och andra personer,

9) *tillhandahållare av betrodda tjänster* en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i eIDAS-förordningen,

10) *molntjänst* en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma dataresurser,

11) *incident* en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem,

12) *incidenthantering* åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident,

13) *risk* risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en incident inträffar,

14) *nätverk för leverans av innehåll* ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

15) *leverantör av utlokaliserade säkerhetstjänster* en leverantör av utlokaliserade driftstjänster som agerar för att hantera cybersäkerhetsrisker eller tillhandahåller stöd för detta,

16) *IKT-tjänst* en IKT-tjänst som avses i artikel 2.13 i 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*),

17) *IKT-produkt* en IKT-produkt som avses i artikel 2.12 i cybersäkerhetsakten,

18) *tillsynsmyndighet* de myndigheter som anges i 26 §,

19) *plattform för sociala nätverkstjänster* en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll och kommunicera med andra via flera enheter,

20) *sökmotor* en sökmotor som avses i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster,

21) *internetbaserad marknadsplats* en i 6 kap. 8 § 4 punkten i konsumentskyddslagen (38/1978) avsedd internetbaserad marknadsplats,

22) *kommunikationsnät och informationssystem*

a) ett elektroniskt kommunikationsnät som avses i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation, nedan *teledirektivet*,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, och

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs i sådana system som avses i underpunkt a och b för att dessa system ska kunna drivas, användas, skyddas eller underhållas,

23) *säkerhet i kommunikationsnät och informationssystem* kommunikationsnäts och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nät och system,

24) *tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster* den som tillhandahåller kommunikationstjänster som avses i 3 § 37 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014) till en grupp av användare som inte har avgränsats på förhand,

25) *tillhandahållare av allmänna elektroniska kommunikationsnät* den som tillhandahåller nättjänster som avses i 3 § 34 punkten i lagen om tjänster inom elektronisk kommunikation.

3 §

Aktörer

Denna lag tillämpas på juridiska och fysiska personer (*aktörer*) som

1) bedriver verksamhet enligt bilaga I eller II eller är sådana aktörer som avses i nämnda bilagor, och

2) uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag och som tillhandahåller sina tjänster eller bedriver sin verksamhet i en medlemsstat i Europeiska unionen.

Denna lag tillämpas också på en aktör som oavsett storlek är

1) en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,

2) en tillhandahållare av betrodda tjänster,

3) den som förvaltar ett toppdomänregister, eller

4) en leverantör av DNS-tjänster.

Denna lag tillämpas dessutom på en sådan aktör, oavsett storlek, som bedriver verksamhet enligt bilaga I eller II eller som är en sådan aktör som avses i nämnda bilagor, om

1) aktören tillhandahåller en tjänst som är väsentlig för att upprätthålla kritiska samhälleliga eller ekonomiska funktioner och som inte tillhandahålls av andra aktörer,

2) en störning av den tjänst som aktören tillhandahåller skulle ha en betydande påverkan på allmän ordning, allmän säkerhet eller folkhälsa,

3) en störning av den tjänst som aktören tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser, eller

4) aktören är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i en medlemsstat i Europeiska unionen som är beroende av denna aktör.

Närmare bestämmelser om de kriterier som avses i 3 mom. får utfärdas genom förordning av statsrådet.

Artikel 3.4 i bilagan till den rekommendation som nämns i 1 mom. 2 punkten tillämpas inte på aktören.

4 §

Avgränsning av tillämpningsområdet

Bestämmelserna i 2 kap. tillämpas inte på verksamhet eller tjänster som tillhandahålls för tryggande av försvaret, den nationella säkerheten, allmän ordning och säkerhet eller förebyggande av brott, brottsutredning och väckande av åtal.

Denna lag tillämpas inte på aktörer som tillhandahåller endast sådan verksamhet eller sådana tjänster som avses i 1 mom.

Med avvikelse från 1 och 2 mom. tillämpas lagen på aktörer som är tillhandahållare av betrodda tjänster.

Denna lag tillämpas inte på aktörer på vilka Europaparlamentets och rådets förordning (EU) 2022/2554 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, nedan *DORA-förordningen*, inte tillämpas med stöd av artikel 2.4 i den förordningen.

Denna lag tillämpas inte på aktörer vars verksamhet enligt bilaga I eller II är sporadisk och ringa.

Denna lag tillämpas på en i kommunallagen (410/2015) avsedd kommun endast i fråga om verksamhet enligt bilaga I eller II.

De bestämmelser i denna lag som förpliktar att lämna ut information tillämpas inte om utlämnandet av informationen skulle äventyra försvaret eller den nationella säkerheten, eller strida mot ett viktigt intresse i samband därmed.

5 §

Förhållande till annan lagstiftning

Om det i någon annan lag eller i bestämmelser eller föreskrifter som utfärdats med stöd av någon annan lag finns krav som avviker från denna lag och som gäller hantering av cybersäkerhetsrisker eller anmälan av betydande incidenter, och kraven har minst samma verkan som motsvarande skyldigheter som fastställs i denna lag, ska de tillämpas i stället för motsvarande bestämmelser i denna lag.

Om det i en EU-förordning eller i en förordning av kommissionen som antagits med stöd av NIS 2-direktivet förutsätts att en aktör inför åtgärder för hantering av cybersäkerhetsrisker eller anmäler betydande incidenter, och kraven har minst samma verkan som motsvarande skyldigheter som fastställs i denna lag, ska dessa bestämmelser tillämpas i stället för 2, 4 och 5 kap. samt 41 § i denna lag.

Bestämmelser om datasäkerhet vid behandling av 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), nedan *den allmänna dataskyddsförordningen* och i dataskyddslagen (1050/2018).

Utöver vad som i denna lag föreskrivs om tillsynsmyndighetens befogenheter tillämpas bestämmelserna i 23 § 6 punkten i lagen om tillsyn över el- och naturgasmarknaden (590/2013), 109 a § i lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (390/2005) och 8 § 1 mom. 3 punkten i lagen om markstationer och vissa radaranläggningar (96/2023) på återkallande av tillstånd.

6 §

Jurisdiktion och territorialitet

Denna lag tillämpas på aktörer som är etablerade i Finland, om inte något annat föreskrivs i lag eller följer av Europeiska unionens lagstiftning eller internationella förpliktelser som är bindande för Finland.

Oberoende av i vilken stat aktören är etablerad tillämpas denna lag på tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster när de tillhandahåller sina tjänster i Finland.

Leverantörer av DNS-tjänster, de som förvaltar ett toppdomänregister, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster och leverantörer av utlokaliserade säkerhetstjänster, tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster omfattas av tillämpningsområdet för denna lag om deras huvudsakliga etableringsställe enligt artikel 26.2 i NIS 2-direktivet eller deras utsedda företrädare i Europeiska unionen enligt artikel 26.3 finns i Finland. Om en sådan aktör inte är etablerad i en medlemsstat i Europeiska unionen och aktören 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. Om en aktör 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 aktören tillhandahåller tjänster i Finland, omfattas aktören av tillämpningsområdet för denna lag.

Tillsynsmyndigheten kan vidta tillsyns- och efterlevnadskontrollåtgärder som riktar sig mot en aktör som är etablerad i en annan medlemsstat i Europeiska unionen på det sätt som föreskrivs i denna lag, om den behöriga myndigheten i en annan medlemsstat begär det och aktören tillhandahåller tjänster i Finland eller har ett kommunikationsnät eller informationssystem inom finskt territorium. En förutsättning är dessutom att tillsynsmyndigheten med stöd av denna lag skulle ha rätt att vidta motsvarande tillsyns- och efterlevnadskontrollåtgärder om aktören hade varit etablerad i Finland. Tillsynsmyndigheten kan avslå begäran om den inte med stöd av lag är behörig att tillhandahålla det begärda biståndet, det begärda biståndet inte står i proportion till tillsynsuppgifterna eller begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot Finlands intressen som gäller försvaret eller den nationella säkerheten. Innan tillsynsmyndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en medlemsstat i Europeiska unionen, med Europeiska kommissionen och Europeiska unionens cybersäkerhetsbyrå.

2 kap.

Riskhantering och anmälan av incidenter

7 §

Riskhantering

En aktör ska identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sin verksamhet eller för att tillhandahålla sina tjänster. Hanteringen av cybersäkerhetsrisker ska förhindra eller minimera incidenternas inverkan på verksamheten, driftskontinuiteten, tjänstemottagarna och andra tjänster.

Aktören ska vidta sådana riskhanteringsåtgärder som är aktuella, proportionella och tillräckliga i förhållande till riskerna för de kommunikationsnät och informationssystem som används i verksamheten och kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet och tillhandahållande av tjänster.

8 §

Handlingsmodell för hantering av cybersäkerhetsrisker

Aktören ska ha en uppdaterad handlingsmodell för hantering av cybersäkerhetsrisker för att skydda kommunikationsnät och informationssystem och deras fysiska miljö mot incidenter och deras verkningar.

I handlingsmodellen för hantering av cybersäkerhetsrisker ska de risker som hänför sig till kommunikationsnät och informationssystem och deras fysiska miljö identifieras med beaktande av ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen ska målen, förfarandena och ansvaren för hanteringen av cybersäkerhetsrisker samt de åtgärder enligt 9 § genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot cyberhot och incidenter (*hanteringsåtgärder*) fastställas och beskrivas.

9 §

Åtgärder för hantering av cybersäkerhetsrisker

Aktörerna ska vidta proportionella tekniska, driftsrelaterade eller organisatoriska hanteringsåtgärder i enlighet med handlingsmodellen för hantering av cybersäkerhetsrisker för att hantera sådana risker som hänför sig till säkerheten i kommunikationsnät och informationssystem samt förhindra eller minimera skadliga verkningar.

I handlingsmodellen och de hanteringsåtgärder som baserar sig på den ska åtminstone följande beaktas och hållas uppdaterat:

1) riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om hanteringsåtgärderna,

2) de riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem,

3) säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter,

4) den övergripande kvaliteten och resiliensen i leveranskedjan i fråga om direkta leverantörers produkter och tjänsteleverantörers tjänster, de hanteringsåtgärder som är inbyggda i dem samt cybersäkerhetspraxis hos direkta leverantörer och tjänsteleverantörer,

5) tillgångsförvaltningen och identifieringen av funktioner som är viktiga med tanke på dess säkerhet,

6) personalsäkerheten och utbildningen i cybersäkerhet,

7) förfarandena för åtkomsthantering och autentisering,

8) riktlinjerna och förfarandena för användning av krypteringsmetoder samt vid behov åtgärderna för användning av säker elektronisk kommunikation,

9) upptäckandet och hanteringen av incidenter i syfte att återställa och upprätthålla säkerheten och driftssäkerheten,

10) säkerhetskopieringen, katastrofhanteringen, krishanteringen och den övriga driftskontinuiteten och vid behov användningen av säkrade reservkommunikationssystem,

11) grundläggande praxis för informationssäkerhet för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet, samt

12) åtgärderna för att säkerställa den fysiska miljön, lokalsäkerheten och nödvändiga resurser i fråga om kommunikationsnät och informationssystem.

Åtgärderna ska ställas i relation till verksamhetens art och omfattning, de direkta konsekvenser som incidenten rimligtvis kan förutses ha, riskexponeringen i fråga om aktörens kommunikationsnät och informationssystem, sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, kostnaderna för åtgärderna samt de tekniska medel för att avvärja hot som med beaktande av den aktuella utvecklingen är tillgängliga.

Tillsynsmyndigheten kan inom sitt ansvarsområde meddela tekniska föreskrifter som preciserar riskhanteringsskyldigheterna om

1) sektorsspecifika särdrag som ska beaktas i handlingsmodellen för hantering av cybersäkerhetsrisker och i de delområden som avses i 2 mom. samt i förfarandena för riskhantering och hantering av informationssäkerheten i kommunikationsnät och informationssystem,

2) beaktandet av resultaten av de på unionsnivå samordnade riskbedömningarna av kritiska leveranskedjor i den sektorsspecifika riskhanteringen.

I riskhanteringen, handlingsmodellen för hantering av risker och hanteringsåtgärderna ska Europeiska kommissionens genomförandeakter som antas med stöd av artikel 21.5 i NIS 2-direktivet dessutom iakttas.

10 §

Ledningens ansvar

Aktörens ledning svarar för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av cybersäkerhetsrisker och utövar tillsyn över genomförandet av den. Aktörens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

Med ledning avses aktörens styrelse, förvaltningsråd och verkställande direktör samt någon annan i därmed jämförbar ställning som de facto leder dess verksamhet.

11 §

Incidentanmälningar till myndigheten

En aktör ska utan dröjsmål underrätta tillsynsmyndigheten om en betydande incident. Med en betydande incident avses en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för den berörda aktören, samt en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada.

En första anmälan ska göras inom 24 timmar från det att den betydande incidenten upptäcktes och en uppföljande anmälan inom 72 timmar från det att den betydande incidenten upptäcktes.

I den första anmälan ska uppges

1) att en betydande incident har upptäckts,

2) om den betydande incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar,

3) möjligheten och sannolikheten för gränsöverskridande verkningar och uppgifter om förväntad utveckling vad gäller gränsöverskridande verkningar.

I den uppföljande anmälan ska uppges

1) en bedömning av den betydande incidentens art, allvarlighetsgrad och konsekvenser,

2) i förekommande fall, tekniska angreppsindikatorer,

3) eventuella uppdateringar av uppgifterna i den första anmälan.

Tillsynsmyndigheten kan inom sitt ansvarsområde meddela närmare tekniska föreskrifter för att precisera typen av information i och det tekniska formatet och förfarandet för anmälningar, underrättelser, information eller rapporter som lämnas med stöd av 11—15 §.

Med avvikelse från 2 mom. ska en tillhandahållare av betrodda tjänster göra en uppföljande anmälan inom 24 timmar från det att den betydande incidenten upptäcktes, om den betydande incidenten påverkar tillhandahållandet av de betrodda tjänsterna.

Utöver vad som avses i 1 mom. avses med betydande incident en situation som specificeras i en genomförandeakt som antagits av Europeiska kommissionen med stöd av artikel 23.11 i NIS 2-direktivet och i vilken incidenten anses vara betydande.

12 §

Delrapport om incident

Aktören ska på begäran av tillsynsmyndigheten lämna ytterligare information eller en delrapport om statusuppdateringar som gäller den betydande incidenten och om hur hanteringen framskrider.

Om den betydande incidenten är långvarig, ska aktören lämna in en delrapport senast en månad efter lämnandet av den uppföljande anmälan.

13 §

Slutrapport om incident

Aktören ska lämna tillsynsmyndigheten en slutrapport om en betydande incident inom en månad från det att den uppföljande anmälan lämnades in eller, om det är fråga om en långvarig incident, inom en månad från det att hanteringen av den avslutades.

Slutrapporten ska innehålla

1) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser,

2) en redogörelse för den typ av hot eller grundorsak som sannolikt har utlöst incidenten,

3) en redogörelse för tillämpade och pågående åtgärder för att begränsa konsekvenserna av incidenten, och

4) en redogörelse för eventuella gränsöverskridande konsekvenser.

14 §

Rapportering om incidenter och cyberhot till andra än myndigheter

En aktör ska utan dröjsmål underrätta mottagarna av sina tjänster om en betydande incident, om den betydande incidenten sannolikt inverkar negativt på tillhandahållandet av aktörens tjänster.

En aktör ska utan dröjsmål underrätta de mottagare av sina tjänster som kan påverkas av ett betydande cyberhot om ett betydande cyberhot och om de åtgärder som står till buds för att hantera cyberhotet.

Om det ligger i allmänt intresse att det informeras om en betydande incident, kan tillsynsmyndigheten ålägga aktören att informera om saken eller själv informera om saken.

15 §

Frivillig underrättelse

Aktörer kan på frivillig basis underrätta tillsynsmyndigheten om andra än i 11 § avsedda incidenter, cyberhot och tillbud.

Tillsynsmyndigheten ska inom sitt ansvarsområde ta emot frivilliga underrättelser om betydande incidenter, incidenter, cyberhot och tillbud också av andra än de aktörer som avses i denna lag.

Tillsynsmyndigheten ska informera den i 18 § avsedda gemensamma kontaktpunkten om underrättelser enligt denna paragraf.

16 §

Mottagande av incidentanmälan

Tillsynsmyndigheten ska utan dröjsmål svara den part som gjort en incidentanmälan. Svaret ska innehålla initial återkoppling om den betydande incidenten samt vägledning om hur den ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet.

Tillsynsmyndigheten får prioritera besvarandet av anmälningar som avses i 11 § och hanteringen av dem enligt 17 § i förhållande till frivilliga underrättelser.

17 §

Hantering av incidentanmälningar

Tillsynsmyndigheten ska omedelbart lämna de anmälningar, underrättelser och rapporter som avses i 11—13 och 15 § till CSIRT-enheten. CSIRT-enheten ger på begäran av en aktör vägledning och operativa råd om begränsande åtgärder.

Om en betydande incident har lett till en sådan i artikel 33 i den allmänna dataskyddsförordningen avsedd personuppgiftsincident som ska anmälas, ska tillsynsmyndigheten anmäla upptäckten av incidenten till dataombudsmannen.

Om det i samband med en betydande incident på grundval av aktörens anmälan kan antas att det har begåtts ett brott för vilket det föreskrivna maximistraffet är fängelse i minst tre år, ska tillsynsmyndigheten underrätta polisen om upptäckten av den betydande incidenten.

Om en betydande incident påverkar andra medlemsstater i Europeiska unionen eller andra sektorer, ska tillsynsmyndigheten informera den i 18 § avsedda gemensamma kontaktpunkten om incidenten och sända anmälningar, rapporter och övriga uppgifter om den till kontaktpunkten.

Om en betydande incident påverkar en annan medlemsstat i Europeiska unionen ska den gemensamma kontaktpunkten utan onödigt dröjsmål underrätta Europeiska unionens cybersäkerhetsbyrå och de medlemsstater som berörs av incidenten. Den gemensamma kontaktpunkten ska på begäran också sända de anmälningar och rapporter som avses i 11—13 § till den gemensamma kontaktpunkten i den medlemsstat som berörs av incidenten. Den gemensamma kontaktpunkten får i detta syfte lämna ut information om betydande incidenter till Europeiska unionens cybersäkerhetsbyrå och till de gemensamma kontaktpunkterna i andra medlemsstater i Europeiska unionen.

18 §

Gemensam kontaktpunkt

Cybersäkerhetscentret vid Transport- och kommunikationsverket är den gemensamma kontaktpunkt som avses i artikel 8.3 i NIS 2-direktivet.

Den gemensamma kontaktpunkten har till uppgift att främja samarbetet och samordningen mellan tillsynsmyndigheterna vid fullgörandet av uppgifter enligt denna lag.

Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Europeiska unionens cybersäkerhetsbyrå med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilka det har underrättats med stöd av 11—13 och 15 §. Den gemensamma kontaktpunkten har rätt att för detta ändamål få anonymiserade och aggregerade uppgifter av tillsynsmyndigheten.

3 kap.

CSIRT-enheten

19 §

CSIRT-enheten

Vid Transport- och kommunikationsverket finns en i artikel 1.2 a i NIS 2-direktivet avsedd CSIRT-enhet för hantering av it-säkerhetsincidenter. Dess verksamhet ska ordnas separat från den tillsyn som utförs med stöd av 26 §.

CSIRT-enheten ska uppfylla följande krav:

1) den ska säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt,

2) dess lokaler och de informationssystem som den använder sig av ska vara belägna på säkra platser,

3) den ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden,
4) den ska säkerställa verksamhetens konfidentialitet och trovärdighet,
5) den ska ha tillräckligt med personal för att säkerställa att dess tjänster är ständigt tillgängliga och säkerställa att personalen har fått lämplig utbildning,
6) den ska ha beredskapsarrangemang för att säkerställa kontinuiteten i sina tjänster.
CSIRT-enheten ska tydligt ange de kommunikationskanaler som avses i 2 mom. 1 punkten och underrätta användargrupper och samarbetspartner om dessa.

20 §

CSIRT-enhetens uppgifter

CSIRT-enheten har till uppgift att
1) på nationell nivå övervaka och analysera cyberhot, sårbarheter och incidenter och samla in information och tillhandahålla tidiga varningar, larm, meddelanden och information om dem,
2) på begäran tillhandahålla stöd avseende realtidsövervakning eller nära realtidsövervakning av informationssäkerheten i kommunikationsnät och informationssystem,
3) reagera på incidentanmälningar och vid behov bistå den part som anmält incidenten i hanteringen av incidenten,
4) samla in och analysera information om hot och information om utredning av kränkningar av informationssäkerheten,
5) utarbeta risk- och incidentanalyser och stödja upprätthållandet av en lägesbild över cybersäkerheten,
6) delta i det CSIRT-nätverk som avses i artikel 15 i NIS 2-direktivet och bistå nätverkets medlemmar på deras begäran,
7) utse experter för sådana sakkunnigbedömningar som avses i artikel 19 i NIS 2-direktivet,
8) främja införandet av säkra verktyg för informationsutbyte,
9) ge anvisningar och rekommendationer om hantering av incidenter, krishantering inom cybersäkerheten och samordnad delgivning av information om sårbarheter.
CSIRT-enheten kan prioritera sina uppgifter på ett riskbaserat sätt i enlighet med tillgängliga resurser.
CSIRT-enheten samordnar de i 23 § avsedda frivilliga arrangemangen för informationsutbyte om cybersäkerhet mellan enheten själv, aktörer som omfattas av tillämpningsområdet för denna lag och andra sammanslutningar.
CSIRT-enheten kan producera i 1 mom. 2 punkten avsedda tjänster för realtidsövervakning eller nära realtidsövervakning av informationssäkerheten i kommunikationsnät och informationssystem för att säkerställa informationssäkerheten i kommunikationsnät och informationssystem, upptäcka och utreda incidenter samt förebygga cyberhot (*tjänst för upptäckande av kränkningar av informationssäkerheten*). CSIRT-enheten kan tillhandahålla tjänsten för upptäckande av kränkningar av informationssäkerheten direkt till de aktörer och andra sammanslutningar som begär den samt till sådana leverantörer av utlokaliserade säkerhetstjänster som tillhandahåller aktörer eller andra sammanslutningar en tjänst för upptäckande av kränkningar av informationssäkerheten (*servicecenter*).
För CSIRT-enhetens tjänster enligt 1 mom. 1 och 2 punkten samt 21 § 4 mom. kan en avgift tas ut av den som begär tjänsten. 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).

21 §

Nätbaserad kartläggning av sårbarheter i allmänna kommunikationsnät och informationssystem

CSIRT-enheten har rätt att på ett proaktivt, annat än inkräktande sätt observera och kartlägga information i kommunikationsnät och informationssystem som är anslutna till ett allmänt kommunikationsnät för att upptäcka sårbarheter, cyberhot och osäkert konfigurerade kommunikationsnät eller informationssystem (*kartläggning av sårbarheter*). Kartläggningen av sårbarheter görs för att upptäcka sårbara eller osäkert konfigurerade kommunikationsnät och informationssystem och för att informera de berörda parterna om iakttagelserna.

Vid genomförandet av kartläggningen av sårbarheter har CSIRT-enheten rätt att via ett allmänt kommunikationsnät inhämta information om identifieringsuppgifter om nätverksutrustning, teleterminalutrustning och andra informationssystem som är kopplade till det och om deras datakommunikationsarrangemang, de programvaror som används och deras funktion och tekniska genomförande och de tjänster som tillhandahållits med hjälp av dem. Kartläggningen av sårbarheter får inte medföra negativa effekter för funktionen hos det system eller den tjänst som är föremål för kartläggningen. Genom kartläggningen av sårbarheter får information inte inhämtas om kommunikation som förmedlas i ett allmänt kommunikationsnät eller i allmänt tillgängliga kommunikationstjänster.

Sådan information som upptäckts vid kartläggningen av sårbarheter och som kan kopplas till föremålet för kartläggningen får användas endast för att informera föremålet för kartläggningen om sårbarheter och risker som hänför sig till kommunikationsnätet eller informationssystemet. CSIRT-enheten kan dessutom använda information som inhämtats genom en kartläggning av sårbarheter för skötseln av de uppgifter som avses i 20 § 1 mom. 1, 4 och 5 punkten. Onödig information ska utplånas utan dröjsmål.

CSIRT-enheten har rätt att på begäran av den som är föremål för kartläggningen utföra kartläggningen av sårbarheter i kommunikationsnätet eller informationssystemet hos den som är föremål för kartläggningen på ett sätt som avviker från vad som föreskrivs i 1—3 mom. för att upptäcka en sådan sårbarhet, ett sådant cyberhot eller sådana osäkra konfigurationer som kan ha en betydande inverkan på kommunikationsnätet eller informationssystemet eller de tjänster som tillhandahålls med hjälp av dem (*riktad kartläggning av sårbarheter*).

I en kartläggning av sårbarheter och i en riktad kartläggning av sårbarheter får inte innehållet i eller förmedlingsuppgifter om elektroniska meddelanden behandlas. CSIRT-enheten ska utplåna den information som den fått vid en kartläggning av sårbarheter eller vid en riktad kartläggning av sårbarheter när informationen inte längre behövs för skötseln av de uppgifter som avses i denna paragraf.

22 §

Samordnad delgivning av information om sårbarheter

CSIRT-enheten är den samordnare för den samordnade delgivningen av informationen om sårbarheter som avses i artikel 12 i NIS 2-direktivet. I detta uppdrag tar CSIRT-enheten emot rapporter om sårbarheter och ser till att behövliga uppföljningsåtgärder vidtas med anledning av dem. Rapporter får lämnas anonymt.

I egenskap av samordnare kontaktar CSIRT-enheten den som rapporterar en sårbarhet och tillverkaren eller leverantören av IKT-produkten eller IKT-tjänsten och fungerar vid behov som mellanhand mellan dem, stödjer dem som rapporterar sårbarheter, förhandlar om tidsramar för delgivning av information om sårbarheter och samordnar hanteringen av sårbarheter som påverkar flera aktörer. Därtill ger CSIRT-enheten vägledning och råd om hur information rapporteras till och söks i den europeiska sårbarhetsdatabasen.

CSIRT-enheten har rätt att om sårbarheter till den europeiska sårbarhetsdatabasen rapportera information

1) som beskriver sårbarheten,
2) om den berörda IKT-produkten eller IKT-tjänsten och om hur allvarlig sårbarheten är med tanke på de omständigheter under vilka sårbarheten kan utnyttjas,
3) om tillgången till programfixar och, i avsaknad av tillgängliga programfixar, om tillsynsmyndighetens eller CSIRT-enhetens vägledning till användare av sårbara IKT-produkter eller IKT-tjänster om hur riskerna med meddelade sårbarheter kan begränsas.

Om CSIRT-enheten får kännedom om en sådan sårbarhet som kan ha en betydande påverkan på andra medlemsstater i Europeiska unionen ska den samarbeta med CSIRT-enheterna i dessa stater inom CSIRT-nätverket.

23 §

Frivilliga arrangemang för informationsutbyte om cybersäkerhet

Mellan CSIRT-enheten, aktörer och andra sammanslutningar än sådana som omfattas av tillämpningsområdet för denna lag kan frivilliga arrangemang för informationsutbyte om cybersäkerhet som samordnas av CSIRT-enheten upprättas, i syfte att förebygga och upptäcka cyberhot som riktas mot deltagande sammanslutningars och deras kunders kommunikationsnät, informationssystem eller tjänster samt i syfte att reagera på och återhämta sig från incidenter och begränsa deras inverkan.

Mellan dem som deltar i frivilliga arrangemang för informationsutbyte om cybersäkerhet kan lämnas ut information om
1) cyberhot,
2) incidenter och tillbud,
3) sårbarheter,
4) taktiker, tekniker och förfaranden,
5) angreppsindikatorer,
6) specifika fientliga aktörer,
7) cybersäkerhetsvarningar,
8) andra än i 1—7 punkten avsedda omständigheter som behövs för att avvärja cyberhot och incidenter.

Utöver vad som i 319 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om utlämnande av information får CSIRT-enheten till den som deltar i arrangemang för informationsutbyte lämna ut information om förmedlingsuppgifter som har samband med ett cyberhot eller en incident eller om ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando och som enheten fått vid utförandet uppgifter enligt denna lag.

En aktör eller annan sammanslutning som deltar i arrangemang för informationsutbyte får trots 136 § 4 mom. i lagen om tjänster inom elektronisk kommunikation på eget initiativ till CSIRT-enheten och någon annan som deltar i frivilliga arrangemang för informationsutbyte enligt denna lag lämna ut information om förmedlingsuppgifter som har samband med ett cyberhot eller en incident eller om ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando.

Den som deltar i arrangemang för informationsutbyte får behandla information om förmedlingsuppgifter som har samband med ett cyberhot eller en incident eller om ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando och som erhållits med stöd av denna paragraf endast för de ändamål som avses i 1 mom. CSIRT-enheten får dessutom behandla information som den fått med stöd av denna paragraf för skötseln av en uppgift som anges i 20 § 1 mom. Utlämnandet av information får inte begränsa skyddet för konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt för det syfte som anges i 1 mom.

24 §

Behandling av information i anslutning till tjänsten för upptäckande av kränkningar av informationssäkerheten

Aktörer och andra sammanslutningar som använder tjänsten för upptäckande av kränkningar av informationssäkerheten, servicecentret och CSIRT-enheten får till varandra lämna ut information som behövs för att övervaka informationssäkerheten i kommunikationsnät och informationssystem i syfte att förebygga och upptäcka cyberhot, reagera på och återhämta sig från incidenter samt begränsa deras inverkan. I den mån det är nödvändigt för genomförande av tjänsten för upptäckande av kränkningar av informationssäkerheten får den information som lämnas ut innehålla sådana elektroniska meddelanden eller förmedlingsuppgifter om dem som den aktör eller någon annan sammanslutning som använder tjänsten har begärt att ska behandlas i tjänsten och som den har rätt att behandla med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation.

På behandling av förmedlingsuppgifter och elektroniska meddelanden i tjänsten för upptäckande av kränkningar av informationssäkerheten vid CSIRT-enheten och i servicecentret tillämpas bestämmelserna i 136—138, 145 och 272 § i lagen om tjänster inom elektronisk kommunikation. CSIRT-enheten får dessutom använda förmedlingsuppgifter och andra uppgifter som den fått i samband med tillhandahållandet av tjänsten till stöd för upprätthållandet av en lägesbild över den nationella cybersäkerheten.

Vad som i 316 § 4 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om utplåning av uppgifter som gäller utredning av betydande kränkningar av eller hot mot informationssäkerheten och i 319 § 1 mom. i den lagen om sekretess gäller också meddelanden och förmedlingsuppgifter som lämnats ut till CSIRT-enheten för genomförande av tjänsten för upptäckande av kränkningar av informationssäkerheten.

25 §

Information som lämnats ut till CSIRT-enheten på frivillig basis

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 för skötseln av uppgifter enligt denna lag 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.

4 kap.

Tillsyn

26 §

Tillsynsmyndigheter

Tillsyn över efterlevnaden av denna lag, föreskrifter som utfärdats med stöd av den och bestämmelser som antagits med stöd av NIS 2-direktivet utövas av

1) Transport- och kommunikationsverket till den del det är fråga om aktörer som avses i 1—7 punkten i bilaga I och i 1—5 punkten i bilaga II,

2) Energimyndigheten till den del det är fråga aktörer som avses i 8 och 9 punkten samt 10 punkten underpunkterna a—c och 12 punkten underpunkt b i bilaga I,

3) Säkerhets- och kemikalieverket till den del det är fråga om aktörer som avses i 10 punkten underpunkterna d—g, 11 punkten och 12 punkten underpunkt a i bilaga I samt i 6 och 11—13 punkten i bilaga II,

4) Tillstånds- och tillsynsverket för social- och hälsovården till den det är fråga om aktörer som avses i 13 punkten underpunkterna a och b i bilaga I,

5) Närings-, trafik- och miljöcentralen i Södra Savolax till den del det är fråga om aktörer som avses i 14—15 punkten i bilaga I samt i 8 punkten i bilaga II,

6) Livsmedelsverket till den del det är fråga om aktörer som avses i 7 punkten i bilaga II,

7) Säkerhets- och utvecklingscentret för läkemedelsområdet till den del det är fråga om aktörer som avses i 13 punkten underpunkterna c—f i bilaga I och i 9 och 10 punkten i bilaga II.

Tillsynsmyndigheterna ska samarbeta vid genomförandet av tillsynen.

27 §

Inriktning av tillsynen

Tillsynen ska inriktas på de väsentliga aktörerna. Tillsynsmyndigheten kan dock inrikta tillsynen också gentemot andra än väsentliga aktörer om det finns grundad anledning att misstänka att aktören inte har iakttagit denna lag, föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet.

Med *väsentlig aktör* avses

1) en i bilaga I avsedd aktör som överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag,

2) kvalificerade tillhandahållare av betrodda tjänster, de som förvaltar ett toppdomänregister samt leverantörer av DNS-tjänster,

3) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster som uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag, samt

4) en aktör som avses i 3 § 3 mom.

Tillsynsmyndigheten kan ställa de uppgifter som föreskrivs för den i denna lag i prioritetsordning enligt en riskbaserad bedömning. Tillsynsmyndigheten ska vid inriktning av tillsynen och vid beslut om användning av åtgärder enligt 29—34 § beakta

1) arten och omfattningen av den verksamhet som avses i bilaga I eller II,

2) informationssystemets eller kommunikationsnätets betydelse för den verksamhet som avses i bilaga I eller II, och

3) de omständigheter som avses i 37 §.

28 §

Rätt att få information

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få information om hanteringen av cybersäkerhetsrisker, handlingsmodellen för riskhantering, hanteringsåtgärderna och betydande incidenter samt annan information som direkt anknyter till ovannämnda information och som är nödvändig för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker och över anmälan och rapporteringen av betydande incidenter.

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få förmedlingsuppgifter, lokaliseringsuppgifter och information om meddelanden som innehåller ett skadligt datorprogram eller ett skadligt

kommando, om det är nödvändigt för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapporteringen av betydande incidenter. Den information som tillsynsmyndigheten fått med stöd av detta moment är sekretessbelagd.

Tillsynsmyndigheten ska i begäran om information ange syftet med begäran och precisera den begärda informationen. Informationen ska lämnas ut utan dröjsmål, i den form som myndigheten begärt och avgiftsfritt.

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 samt en CSIRT-enhet, om det är nödvändigt för en uppgift som i denna lag föreskrivits för myndigheten. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än vad som är nödvändigt.

Tillsynsmyndighetens rätt att få information gäller inte tjänster eller information som CSIRT-enheten med stöd av denna lag producerat hos en aktör.

Rätten till information enligt denna paragraf gäller inte sekretessbelagd information om sådan tjänsteproduktion eller användning av tjänster i säkerhetsnätet som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) eller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

29 §

Inspektionsrätt

Tillsynsmyndigheten har rätt att förrätta inspektioner av aktörer. Inspektionen förrättas för tillsynen över att skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs, i den omfattning det behövs.

Om det är nödvändigt på grund av inspektionens art eller av tekniska orsaker som har samband med den, kan tillsynsmyndigheten begära att en annan tillsynsmyndighet förrättar inspektionen eller vid inspektionen anlita en annan tillsynsmyndighet, ett bedömningsorgan för informationssäkerhet och en utomstående expert i informationsteknik. Den som förrättar inspektionen och den som deltar i inspektionen ska ha sådan utbildning och erfarenhet som behövs för inspektionen. På utomstående experter tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Aktörer ska i den omfattning som inspektionen förutsätter ge den som förrättar inspektion tillträde till det kommunikationsnät eller informationssystem som inspektionen gäller och till andra utrymmen än sådana som är avsedda för boende av permanent natur. Tillsynsmyndigheten, andra myndigheter som förrättar inspektion, ett bedömningsorgan för informationssäkerhet och utomstående experter har för förrättande av inspektionen trots sekretessbestämmelserna eller andra begränsningar som gäller utlämnande av information rätt att få granska den information och de handlingar, maskinvaror och programvaror som är nödvändiga för tillsynsuppgiften, utföra behövliga tester och mätningar samt granska de säkerhetsarrangemang som aktören har genomfört. På inspektionsförrättarens rätt att förrätta inspektion och få information tillämpas vad som i 28 § 6 mom. föreskrivs om begränsningar i rätten att få information.

På förfarandet vid inspektionen tillämpas vad som i 39 § i förvaltningslagen (434/2003) föreskrivs om inspektion.

30 §

Säkerhetsrevision

Tillsynsmyndigheten har rätt att ålägga en aktör att låta utföra en säkerhetsrevision som gäller hanteringen av cybersäkerhetsrisker, om

1) aktören har drabbats av en betydande incident som har orsakat en allvarlig driftsstörning för tjänsterna eller orsakat betydande materiell eller immateriell skada, eller

2) aktören väsentligt och allvarligt har försummat att genomföra handlingsmodellen för hantering av cybersäkerhetsrisker enligt 8 § eller de hanteringsåtgärder som förutsätts i den eller annars väsentligt och allvarligt förfarit i strid med en skyldighet som föreskrivs i denna lag eller med stöd av den eller med stöd av NIS 2-direktivet.

Tillsynsmyndigheten har rätt att få information om resultaten av den utförda säkerhetsrevisionen samt att ålägga aktören att vidta sådana skäliga och proportionella åtgärder för att utveckla hanteringen av cybersäkerhetsrisker som säkerhetsrevisionen rekommenderar.

31 §

Tillsynsbeslut och varning

Tillsynsmyndigheten kan ålägga aktören att inom utsatt tid avhjälpa bristerna i fullgörandet av skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan genom ett beslut ålägga aktören att offentliggöra dessa brister eller andra omständigheter som har samband med överträdelser av denna lag, föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet.

Tillsynsmyndigheten kan ge en aktör en varning, om aktören inte har iakttagit denna lag, föreskrifter som utfärdats med stöd av den eller bestämmelser som antagits med stöd av NIS 2-direktivet. I varningen ska den brist eller försummelse som varningen gäller specificeras. Varningen ska ges skriftligen.

32 §

Begränsning av ledningens verksamhet

Tillsynsmyndigheten kan för viss tid förbjuda en person att vara ledamot eller ersättare i styrelsen, ledamot eller ersättare i förvaltningsrådet, verkställande direktör eller i annan därmed jämförbar ställning hos en väsentlig aktör, om denne upprepade gånger och allvarligt har brutit mot skyldigheterna i 10 §. Tillsynsmyndigheten ska innan den fattar ett beslut ge den väsentliga aktören en varning, i vilken den brist eller försummelse specificeras som, om den inte avhjälps, kan leda till ett beslut om begränsning av ledningens verksamhet samt reservera en skälig tid för aktören att avhjälpa bristen eller försummelsen. Beslutet får vara i kraft högst så länge som den brist eller försummelse som ligger till grund för beslutet inte har avhjälpts, dock högst fem år.

Med avvikelse från 1 mom. får ledningens verksamhet inte begränsas om det är fråga om en enskild näringsidkare, ett öppet bolag, ett kommanditbolag, en statlig myndighet, ett statligt affärsverk, ett välfärdsområde eller en välfärdssammanslutning, en kommunal myndighet, en självständig offentligrättslig inrättning, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland, ortodoxa kyrkan i Finland eller de två sistnämndas församlingar, kyrkliga samfälligheter och övriga organ.

33 §

Anmälan till dataombudsmannen

Om tillsynsmyndigheten i samband med skötseln av de uppgifter som anges i denna lag får kännedom om att en försummelse av skyldigheterna enligt 2 kap. kan leda till eller har lett till en sådan personuppgiftsincident som avses i den allmänna dataskyddsförordningen, som i enlighet med artikel 33 i förordningen ska anmälas till den tillsynsmyndighet som avses i den förordningen, ska tillsynsmyndigheten anmäla saken till dataombudsmannen.

Tillsynsmyndigheten ska göra en i 1 mom. avsedd anmälan till dataombudsmannen även om den tillsynsmyndighet som är behörig enligt den allmänna dataskyddsförordningen är etablerad i en annan medlemsstat.

34 §

Vite, hot om tvångsutförande och hot om avbrytande

Tillsynsmyndigheten kan förena ett beslut som den har fattat med stöd av denna lag med vite, hot om tvångsutförande eller hot om avbrytande.

5 kap.

Påföljdsavgift

35 §

Administrativ påföljdsavgift

En aktör kan påföras en administrativ påföljdsavgift om denne uppsåtligen eller av grov oaktsamhet försummar

1) att fullgöra riskhanteringsskyldigheten enligt 7 §, att utarbeta en handlingsmodell för hantering av cybersäkerhetsrisker enligt 8 § eller att beakta de delområden som avses i 9 § 1 mom. som en del av handlingsmodellen för hantering av cybersäkerhetsrisker,

2) att vidta de åtgärder som avses i 9 § 2 mom.,

3) att lämna en incidentanmälan enligt 11 §, delrapport enligt 12 § eller slutrapport enligt 13 § till tillsynsmyndigheten,

4) att lämna tillsynsmyndigheten de uppgifter som avses i 41 §.

Statliga myndigheter, statliga affärsverk, välfärdsområden eller välfärdssammanslutningar, kommunala myndigheter, självständiga offentligrättsliga inrättningar, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland, ortodoxa kyrkan i Finland och de två sistnämndas församlingar, kyrkliga samfälligheter och övriga organ får inte påföras påföljdsavgift.

36 §

Påföljdsavgiftsnämnd

I anslutning till Transport- och kommunikationsverket finns en påföljdsavgiftsnämnd. Nämnden påför en administrativ påföljdsavgift på framställning av tillsynsmyndigheten. Den administrativa påföljdsavgiften ska betalas till staten.

Transport- och kommunikationsverket utser nämndens ordförande och vice ordförande. Varje tillsynsmyndighet utser en ledamot i nämnden och en personlig ersättare för denne. Av nämndens ledamöter och ersättare förutsätts förtrogenhet med hantering av cybersäkerhetsrisker

och NIS 2-direktivet samt de skyldigheter som ställs i den reglering som genomför direktivet inom den utseende myndighetens tillsynsområde. Ordföranden och vice ordföranden för nämnden ska ha sådan tillräcklig juridisk sakkunskap som uppdraget förutsätter. Nämndens ledamöter utses för en period på tre år. Nämndens ledamöter ska agera oberoende och opartiskt i sitt uppdrag.

Påföljdsavgiftsnämnden ska fatta sitt beslut efter föredragning. Föredragande är en tjänsteman vid den tillsynsmyndighet vars tillsynsbehörighet det ärende som ska avgöras gäller. Nämnden är beslutför när ordföranden eller vice ordföranden och minst två andra ledamöter eller ersättare är närvarande. Som beslut gäller den mening som flertalet har understött. Vid lika röstetal gäller som beslut den mening som är lindrigare för den som påföljden riktas mot.

Påföljdsavgiftsnämnden har trots sekretessbestämmelserna rätt att avgiftsfritt få den i 28 § avsedda information som är nödvändig för påförande av påföljdsavgiften samt övrig information som är nödvändig för påförande av påföljdsavgiften eller för beräkning av dess belopp.

37 §

Påförande av påföljdsavgift

Den administrativa påföljdsavgiftens belopp ska basera sig på en helhetsbedömning där omständigheterna i fallet och åtminstone följande omständigheter beaktas:

1) hur allvarlig överträdelsen är och betydelsen av de bestämmelser som har överträtts så att allvaret i överträdelsen framgår av

a) upprepade oegentligheter,
b) underlåtenhet att underrätta om eller avhjälpa betydande incidenter,
c) underlåtenhet att avhjälpa upptäckta brister trots beslut av eller varningar från tillsynsmyndigheten,
d) förhindrande av tillsynsmyndighetens inspektion eller underlåtenhet att låta utföra en ålagd revision,
e) lämnande av felaktiga eller vilseledande uppgifter till myndigheten om riskhantering eller betydande incidenter,

2) överträdelsens varaktighet,
3) aktörens eventuella motsvarande tidigare överträdelser,
4) den skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs av överträdelsen,
5) graden av uppsåt,
6) åtgärder som aktören vidtagit för att förhindra eller begränsa skadan,
7) efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer,
8) aktörens vilja att samarbeta med tillsynsmyndigheten.

38 §

Påföljdsavgiftens maximibelopp

En administrativ påföljdsavgift som påförs en väsentlig aktör är högst 10 000 000 euro eller två procent av aktörens totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilken siffra som är högst.

En administrativ påföljdsavgift som påförs andra än väsentliga aktörer är högst 7 000 000 euro eller 1,4 procent av aktörens totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilken siffra som är högst.

39 §

Avstående från 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.

Påföljdsavgift får inte påföras den som för samma gärning har påförts en påföljdsavgift enligt artikel 83 i den allmänna dataskyddsförordningen.

40 §

Verkställighet av påföljdsavgift

Bestämmelser om verkställighet av påföljdsavgifter finns i lagen om verkställighet av böter (672/2002). En påföljdsavgift preskriberas när fem år har förflutit från den dag då ett lagakraftvunnet beslut om avgift meddelades. Påföljdsavgiften avskrivs när den betalningsskyldiga fysiska personen avlider.

6 kap.

Övriga bestämmelser

41 §

Förteckning över aktörer

Tillsynsmyndigheten för i fråga om sitt tillsynsområde en förteckning över aktörerna.

Aktörer ska lämna tillsynsmyndigheten följande uppgifter:

1) aktörens namn,

2) sin adress, sin e-postadress, sitt telefonnummer och andra aktuella kontaktuppgifter,

3) sina IP-adresser,

4) sin relevanta sektor och delsektor som avses i bilaga I eller II till NIS 2-direktivet,

5) huruvida aktören är en väsentlig aktör,

6) en förteckning över de medlemsstater i Europeiska unionen där den tillhandahåller tjänster som omfattas av NIS 2-direktivet, och

7) uppgift om deltagande i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 23 §.

Leverantörer av DNS-tjänster, de som förvaltar ett toppdomänregister, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av

innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster ska utöver de uppgifter som anges i 2 mom. lämna tillsynsmyndigheten följande uppgifter:

1) sin aktörstyp enligt bilaga I eller II till NIS 2-direktivet,

2) adress till sitt huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i medlemsstater i Europeiska unionen eller, om aktören inte är etablerad i Europeiska unionen, adress, e-postadress, telefonnummer och andra aktuella kontaktuppgifter till aktörens utsedda företrädare i Europeiska unionen, och

3) en förteckning över de medlemsstater i Europeiska unionen där aktören tillhandahåller tjänster.

Aktörerna ska utan dröjsmål underrätta om ändringar av de uppgifter som avses i denna paragraf. Tillsynsmyndigheten ska underrättas om ändringar av de uppgifter som avses i 2 mom. inom två veckor och av de uppgifter som avses i 3 mom. inom tre månader från tidpunkten för ändringen. Tillsynsmyndigheten kan meddela närmare tekniska föreskrifter om hur uppgifterna ska lämnas.

Tillsynsmyndigheten ska till den gemensamma kontaktpunkten lämna de uppgifter ur förteckningen över aktörer som behövs för att göra de anmälningar som avses i artiklarna 3.5 och 27.4 i NIS 2-direktivet. Den gemensamma kontaktpunkten svarar för att de anmälningar som avses i artiklarna 3.5 och 27.4 görs till Europeiska kommissionen, NIS-samarbetsgruppen och Europeiska unionens cybersäkerhetsbyrå. CSIRT-enheten har rätt att få uppgifter ur förteckningen över aktörer av tillsynsmyndigheten.

42 §

Nationell strategi för cybersäkerhet

Statsrådet antar en nationell strategi för cybersäkerhet och svarar för att den uppdateras regelbundet minst vart femte år.

Den nationella strategin för cybersäkerhet ska åtminstone omfatta de delområden som avses i artikel 7.1 och de riktlinjer som avses i artikel 7.2 i NIS 2-direktivet.

Statsrådet delger Europeiska kommissionen den nationella strategin för cybersäkerhet inom tre månader från det att den har antagits. Sådan information om strategin för cybersäkerhet kan undantas, vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

43 §

Plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser

För att specificera vilka kapaciteter, tillgångar och förfaranden som står till förfogande i händelse av en kris som avser cybersäkerhet utarbetas en plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser. Transport- och kommunikationsverket svarar för utarbetandet av planen i samarbete med de tillsynsmyndigheter som avses i 26 §, polisen, skyddspolisen, Försvarsmakten och Försörjningsberedskapscentralen.

Planen ska med avseende på hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser innehålla behövliga uppgifter om

1) målen för nationella beredskapsåtgärder och beredskapsverksamheter,

2) myndigheternas uppgifter och ansvarsområden,

3) krishanteringsförfaranden och deras integrering i den allmänna nationella ramen för krishantering samt kanaler för informationsutbyte mellan myndigheter,

4) nationella beredskapsåtgärder, vilka även omfattar övningar och utbildningsverksamhet,

5) centrala offentliga och privata intressenter och central infrastruktur,

6) förfaranden mellan myndigheter vid deltagande i en på EU-nivå samordnad hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser.

De uppgifter som avses i 2 mom. ska delges Europeiska kommissionen och det europeiska kontaktnätverk för cyberkriser som avses i artikel 16 i NIS 2-direktivet inom tre månader från det att planen antagits. Uppgifter kan undantas till den del som utlämnandet av dem skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

44 §

Cyberkrishanteringsmyndighet

Var och en av de myndigheter som avses i 43 § 1 mom. är i enlighet med sina lagstadgade uppgifter en sådan cyberkrishanteringsmyndighet som avses i artikel 9.1 i NIS 2-direktivet. Cybersäkerhetscentret vid Transport- och kommunikationsverket är samordnare vid hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser.

45 §

Myndighetssamarbete

Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska samarbeta för skötseln av de uppgifter som föreskrivs i denna lag och med stöd NIS 2-direktivet.

Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska vid behov samarbeta med polisen eller någon annan förundersökningsmyndighet, dataombudsmannen, Transport- och kommunikationsverket i fråga om de uppgifter verket har enligt luftfartslagen (864/2014), lagen om tjänster inom elektronisk kommunikation och eIDAS-förordningen samt med Finansinspektionen.

Tillsynsmyndigheterna ska informera det tillsynsforum som inrättats med stöd av artikel 32.1 i DORA-förordningen när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en aktör som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i DORA-förordningen.

Tillsynsmyndigheterna, Transport- och kommunikationsverket och Finansinspektionen ska regelbundet utbyta information om betydande incidenter och cyberhot.

46 §

Sökande av ändring

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

Tillsynsmyndighetens beslut ska iakttas trots ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat. 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).

47 §

Ikraftträdande

Denna lag träder i kraft den 8 april 2025.

Den anmälan som avses i 41 § ska göras senast inom en månad från det att denna lag trätt i kraft eller det att de kriterier som i 3 § anges för en aktör uppfylls.

Den handlingsmodell för hantering av cybersäkerhetsrisker som avses i 8 § ska upprättas senast inom tre månader från det att denna lag trätt i kraft eller det att de kriterier som i 3 § fastställts för en aktör uppfylls.

Helsingfors den 4 april 2025

Republikens President

Alexander Stubb

Kommunikationsminister Lulu Ranne

Bilaga I

Aktörer som bedriver följande verksamhet eller är av följande aktörstyp:

1. Lufttransport
a) Lufttrafikföretag enligt definitionen i artikel 3.4 i Europaparlamentets och rådets förordning (EG) nr 300/2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002, vilka bedriver kommersiell verksamhet
b) Flygplatsoperatörer som avses i 3 § 1 mom. 2 punkten i lagen om flygplatsnät och flygplatsavgifter (210/2011)
c) Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 om ramen för inrättande av det gemensamma europeiska luftrummet

2. Spårtrafik
a) Bannätsförvaltare som avses i 4 § 1 mom. 29 punkten i spårtrafiklagen (1302/2018) och bolag som tillhandahåller trafikledningstjänster
b) Järnvägsföretag som avses i 4 § 1 mom. 34 punkten i spårtrafiklagen
c) Tjänsteleverantörer som avses i 4 § 1 mom. 23 punkten i spårtrafiklagen

3. Sjöfart
a) Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar, exklusive de enskilda fartyg som drivs av dessa företag
b) Hamninnehavare som avses i 2 § 2 punkten i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) och aktörer som sköter anläggningar och utrustning i hamnar
c) VTS-tjänsteleverantörer som avses i 2 § 1 mom. 5 punkten i lagen om fartygstrafikservice (623/2005)

4. Vägtransport
a) Leverantörer av vägtrafikstyrnings- och vägtrafikledningstjänster som avses i 15 kap. i lagen om transportservice (320/2017)
b) De som tillhandahåller intelligenta transportsystem som avses i 160 § i lagen om transportservice

5. Verksamhetsutövare som avses i 2 § 1 mom. 5 punkten i lagen om markstationer och vissa radaranläggningar (96/2023) eller andra operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät

6. Digital infrastruktur
a) Leverantörer av internetknutpunkter, det vill säga en nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik, som tillhandahåller sammankoppling enbart för autonoma system och som varken kräver att den internettrafik som passerar mellan två deltagande autonoma system

ska passera genom ett tredje autonomt system eller ändrar trafiken eller påverkar den på något annat sätt
b) Leverantörer av DNS-tjänster
c) Registreringsenheter för toppdomäner
d) Leverantörer av molntjänster
e) Leverantörer av datacentraltjänster
f) Leverantörer av nätverk för leverans av innehåll
g) Tillhandahållare av betrodda tjänster
h) Tillhandahållare av allmänna elektroniska kommunikationsnät
i) Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster

7. Förvaltning av IKT-tjänster
a) Leverantörer av hanterade tjänster
b) Leverantörer av hanterade säkerhetstjänster

8. Elektricitet
a) Elföretag som avses i 3 § 1 mom. 21 punkten i elmarknadslagen (588/2013) och som bedriver elleverans enligt 11 punkten i det momentet
b) Distributionsnätsinnehavare som avses i 3 § 1 mom. 10 punkten i elmarknadslagen
c) Stamnätsinnehavare enligt 7 § i elmarknadslagen
d) Producenter som avses i 3 § 1 mom. 15 punkten i elmarknadslagen
e) Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943 om den inre marknaden för el
f) De parter på elmarknaden som avses i 3 § 1 mom. 37 punkten i elmarknadslagen och som tillhandahåller aggregering enligt 3 § 1 mom. 21 a punkten i elmarknadslagen, efterfrågeflexibilitet enligt 30 a punkten eller energilagring enligt 21 c punkten
g) Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn

9. Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 om främjande av användningen av energi från förnybara energikällor

10. Gas
a) Distributionsnätsinnehavare som avses i 3 § 1 mom. 10 punkten i naturgasmarknadslagen (587/2017)
b) Överföringsnätsinnehavare som avses i 3 § 1 mom. 9 punkten i naturgasmarknadslagen
c) Naturgasleverantörer som avses i 3 § 1 mom. 14 punkten i naturgasmarknadslagen
d) Innehavare av en lagringsanläggning som avses i 3 § 1 mom. 20 punkten i naturgasmarknadslagen
e) Innehavare av en behandlingsanläggning för kondenserad naturgas som avses i 3 § 1 mom. 22 punkten i naturgasmarknadslagen
f) Naturgasföretag som avses i 3 § 1 mom. 18 punkten i naturgasmarknadslagen
g) Operatörer av raffinaderier och bearbetningsanläggningar för naturgas

11 Olja
a) Operatörer av oljeledningar
b) Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
c) Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter

12. Vätgas
a) Operatörer för anläggningar för produktion och lagring av vätgas
b) Operatörer för anläggningar för överföring av vätgas

13. Hälso- och sjukvård
a) Tjänsteproducenter som avses i 4 § 2 punkten i lagen om tillsynen över social- och hälsovården (741/2023) och som producerar hälso- och sjukvårdstjänster som avses i 4 punkten i den paragrafen
b) EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 2022/2371 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU
c) Aktörer som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG om upprättande av gemenskapsregler för humanläkemedel
d) Aktörer som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2
e) Aktörer som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter
f) Inrättningar för blodtjänst enligt blodtjänstlagen (197/2005), apotek och aktörer som avses i Europaparlamentets och rådets direktiv 2011/24/EU om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård och som lämnar ut och tillhandahåller läkemedel och medicintekniska produkter

14. Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i Europaparlamentets och rådets direktiv (EU) 2020/2184 om kvaliteten på dricksvatten undantaget distributörer för vilka distribution av dricksvatten utgör en icke väsentlig del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor

15. Företag som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten enligt definitionen i artikel 2.1—2.3 i rådets direktiv 91/271/EEG om rening av avloppsvatten från tätbebyggelse, undantaget företag som samlar ihop, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten som en icke väsentlig del av sin allmänna verksamhet

Bilaga II

Aktörer som bedriver följande verksamhet eller är av följande aktörstyp:

1. Tillhandahållare av budtjänster och sådana tillhandahållare av posttjänster som avses i artikel 2.1 a i Europaparlamentets och rådets direktiv 97/67/EG om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna

2. Digitala leverantörer
a) Tillhandahållare av internetbaserade marknadsplatser
b) Leverantörer av sökmotorer
c) Leverantörer av plattformar för sociala nätverkstjänster

3. Aktörer som bedriver tillverkning av motorfordon, släpfordon och påhängsvagnar enligt avsnitt C huvudgrupp 29 i Nace Rev. 2

4. Aktörer som bedriver tillverkning av andra transportmedel som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2

5. Forskningsorganisationer vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte är högskolor eller andra utbildningsinstitutioner

6. Företag som tillverkar ämnen och distribuerar ämnen eller blandningar som avses i artikel 3.9 och 3.14 i Europaparlamentets och rådets förordning (EG) nr 1907/2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG och upphävande av rådets förordning (EEG) nr 793/93 och kommissionens förordning (EG) nr 1488/94 samt rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG samt företag som producerar varor enligt definitionen i artikel 3.3 i den förordningen genom att använda ämnen och blandningar, i det fall att ämnet måste registreras och verksamheten förutsätter tillstånd enligt 23 § eller anmälan enligt 24 § i lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (390/2005)

7. Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet, som bedriver grossisthandel, industriell produktion eller bearbetning

8. Verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG om avfall och om upphävande av vissa direktiv, dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är avfallshantering

9. Aktörer som tillverkar medicintekniska produkter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2017/745 om medicintekniska produkter, om

ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG

10. Aktörer som tillverkar medicintekniska produkter för in vitro-diagnostik enligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2017/746 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU, med undantag av aktörer som avses i 13 punkten underpunkt e i bilaga I till denna lag

11. Företag som bedriver tillverkning av datorer, elektronikvaror och optik enligt avsnitt C huvudgrupp 26 i Nace Rev. 2

12. Företag som bedriver tillverkning av elapparatur enligt avsnitt C huvudgrupp 27 i Nace Rev. 2

13. Företag som bedriver tillverkning av övriga maskiner enligt avsnitt C huvudgrupp 28 i Nace Rev. 2