Betänkande KoUB 1/2025 rd– RP 57/2024 rd

Kommunikationsutskottet

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet)

INLEDNING

Remiss

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) (RP 57/2024 rd): Ärendet har remitterats till kommunikationsutskottet för betänkande och till grundlagsutskottet och förvaltningsutskottet för utlåtande.

Utlåtanden

Följande utlåtanden har lämnats i ärendet:
- förvaltningsutskottet FvUU 15/2024 rd
- grundlagsutskottet GrUU 62/2024 rd

Sakkunniga

Utskottet har hört
- regeringssekreterare Veikko Vauhkonen, kommunikationsministeriet
- lagstiftningsråd Virpi Koivu, justitieministeriet
- lagstiftningsråd Eeva Lantto, finansministeriet
- enhetschef Olli Lehtilä, Transport- och kommunikationsverket, Cybersäkerhetscentret
- NIS-koordinator, specialsakkunnig Kalle Varjola, Transport- och kommunikationsverket, Cybersäkerhetscentret
- överinspektör Heli Heikkola, skyddspolisen
- ledande sakkunnig Taito von Konow, Skatteförvaltningen
- jurist Minna Koivula, Energimyndigheten
- gruppchef Ilkka Juva, Närings-, trafik- och miljöcentralen i Södra Savolax
- beredskapsexpert Juha Ilkka, Försörjningsberedskapscentralen
- direktör Kirsi Levä, Säkerhets- och kemikalieverket (Tukes)
- säkerhetsdirektör Matti Koskinen, Folkpensionsanstalten
- utvecklingschef Johanna Linnolahti, Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea
- jurist Jukka Räisänen, Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea
- ledande expert Arttu Malava, Tillstånds- och tillsynsverket för social- och hälsovården (Valvira)
- säkerhetschef Janne Rintamaa, Institutet för hälsa och välfärd (THL)

Godkänts
3.3

- Chief Compliance Officer Päivi Rokkanen, Posti Ab
- Chief Information Security Officer Iikka Salmela, Posti Ab
- säkerhetschef Jyrki Guttorm, Rundradion
- datasäkerhetschef Kim Johansson, Rundradion
- ansvarig jurist Outi Piirainen, Rundradion
- specialsakkunnig Martti Setälä, Finlands Kommunförbund
- chef för tillsynsfrågor Elina Thorström, DNA Ab
- Head of Privacy Antti-Pekka Manninen, Elisa Abp
- Senior Legal Counsel Irina Kitinprami, Telia Finland Oyj
- ledande konsult Antti Laatikainen, WithSecure Oyj
- ledande expert Markku Rajamäki, Finlands näringsliv rf
- direktör för samhällskontakter Jukka Ihanus, Livsmedelsindustriförbundet rf
- expert Tuukka Heikkilä, Finsk Energiindustri rf
- jurist Asko Metsola, FiCom rf
- ledande expert Mika Linna, Finanssiala ry
- expert Risto Rajala, Finnish Information Security Cluster - Kyberala ry, företräder även Teknologiindustrin rf
- ledande säkerhetsexpert Mirva Ojala, Kemiindustrin KI rf
- expert Merja Söderström, Finlands Dagligvaruhandel rf
- biträdande direktör Kirsti Tarnanen-Sariola, Finlands Hamnar rf.

Skriftligt yttrande har lämnats av
- Ålands landskapsregering
- inrikesministeriet
- försvarsministeriet
- undervisnings- och kulturministeriet
- jord- och skogsbruksministeriet
- arbets- och näringsministeriet
- social- och hälsovårdsministeriet
- miljöministeriet
- Finansinspektionen
- Rättsregistercentralen
- dataombudsmannens byrå
- Livsmedelsverket
- MTV Ab
- Sanoma Media Finland Oy
- Medieförbundet rf
- Upphovsrättens informations- och övervakningscentral rf.

Inget yttrande av
- utrikesministeriet
- Närings-, trafik- och miljöcentralen i Nyland.

PROPOSITIONEN

Regeringen föreslår att det stiftas en cybersäkerhetslag. I propositionen föreslås dessutom ändringar i lagen om informationshantering inom den offentliga förvaltningen, lagen om tjänster inom elektronisk kommunikation, luftfartslagen, spårtrafiklagen, lagen om transportservice, lagen om fartygstrafikservice, lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, lagen om behandling av kunduppgifter inom social- och hälsovården, elmarknadslagen, naturgasmarknadslagen, lagen om Energimyndigheten, lagen om tillsyn över el- och naturgasmarknaden, lagen om vattentjänster, lagen om verkställighet av böter, lagen om markstationer och vissa radaranläggningar och lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor.

Genom de föreslagna lagarna genomförs Europaparlamentets och rådets direktiv om cybersäkerhet. Syftet med direktivet är att stärka både EU:s gemensamma cybersäkerhetsnivå och medlemsstaternas nationella cybersäkerhetsnivå i fråga om sektorer och aktörer som anses vara kritiska med tanke på samhällets funktion genom att ålägga medlemsstaterna att fastställa förpliktande riskhanteringsåtgärder med avseende på cybersäkerhetsincidenter för aktörer som omfattas av direktivets tillämpningsområde.

Det föreslås att direktivet ska genomföras genom att det i en ny cybersäkerhetslag på ett samlat sätt föreskrivs om de skyldigheter som direktivet förutsätter. I fråga om den offentliga sektorn föreslås att det ska föreskrivas om skyldigheterna även i lagen om informationshantering inom den offentliga förvaltningen. Samtidigt upphävs i flera sektorspecifika lagar genomförandebestämmelserna för det upphävda direktivet om nät- och informationssäkerhet. När det gäller ordnandet av tillsynen fortsätter den sektorsvis uppdelade modellen. I propositionen föreslås bestämmelser också om en enhet för hantering av it-säkerhetsincidenter, som enligt förslaget ska vara placerad vid Transport- och kommunikationsverket, samt om en nationell strategi för cybersäkerhet och en ram för hantering av cyberkriser. Enligt förslaget ska direktivet genomföras enligt miniminivån och så att det nationella handlingsutrymmet utnyttjas fullt ut.

Enligt regeringsprogrammet för Petteri Orpos regering stärks samarbetet kring cybersäkerhet mellan myndigheterna och näringslivet, förbättrar regeringen informationssäkerheten inom kritiska sektorer och i undviks ytterligare nationell reglering samband med genomförandet av EU-lagstiftningen.

Lagarna avses träda i kraft den 18 oktober 2024.

UTSKOTTETS ÖVERVÄGANDEN

Allmänt

(1) Utskottet välkomnar att propositionen genomför EU:s cybersäkerhetsdirektiv ([1]),nedan NIS 2-direktivet. Det är nödvändigt att stärka EU:s gemensamma och medlemsstaternas nationella cybersäkerhetsnivå för att målen i direktivet ska kunna nås. I och med digitaliseringsutvecklingen är

cybersäkerheten allt viktigare i strävan att trygga samhällets kritiska funktioner och den övergripande säkerheten.

(2) Utskottet förordar det tillvägagångssätt som valts i propositionen, där det nationella handlingsutrymmet har använts så att genomförandet av direktivet sker på det sätt som miniminivån förutsätter i fråga om både tillämpningsområde och skyldigheter. Det är bra att man i detta sammanhang fokuserar på de krav som genomförandet av direktivet förutsätter samt på den nationella övergripande säkerheten och samverkan mellan myndigheterna. Utskottet betonar också betydelsen av konfidentiell samverkan mellan myndigheterna och privata aktörer och anser att detta kräver satsningar.

Anmälningsskyldighet

(3) Förvaltningsutskottet påpekar i sitt utlåtande FvUU 15/2024 rd att samma incident kan utlösa flera anmälningsskyldigheter samtidigt och att praxis och metoder för anmälan varierar för närvarande. Förvaltningsutskottet lyfter dessutom fram att anmälningar om olika nya tekniker, säkerhet och dataskydd kunde centraliseras till en enda datasäker rapporteringskanal. Då minskar de rapporteringsskyldiga aktörernas administrativa börda och kostnaderna för att ha flera parallella datasäkra rapporteringskanaler.

(4) Med stöd av inkommen utredning understöder utskottet i likhet med kommunikationsministeriet målet om en gemensam informationssäker rapporteringskanal. Ministeriet har konstaterat att en gemensam rapporteringskanal framför allt är en resursfråga, eftersom utvecklingen och underhållet av den medför systemkostnader. Dessutom har ministeriet konstaterat att man vid beredningen av den aktuella regleringen har strävat efter att undvika de framtida hinder eller begränsningar som regleringen medför för utvecklandet eller sammanslagningen av anmälningsförfarandet.

Skydd av personuppgifter och upphovsrätt

(5) Lagförslag 3 i den nu aktuella propositionen innehåller ändringsförslag som genomför artiklarna 27 och 28 i NIS 2-direktivet, vilka gäller databaser över domännamnsregistreringsuppgifter, och de omständigheter som artiklarna förutsätter i fråga om dem som förvaltar ett toppdomänregister och registrarer. De föreslagna bestämmelserna gäller bland annat införande och publicering av uppgifter i domännamnsregistret och besvarande av begäranden om uppgifter.

(6) Utskottet konstaterar att propositionen inte innehåller några särskilda bestämmelser om tillämpning eller undantag från tillämpning av lagstiftningen om skydd av personuppgifter vid behandlingen av utlämnande av uppgifter ur domännamnsregistret. Bestämmelser om åtkomst till domännamnsregistreringsuppgifter finns i artikel 28 i NIS 2-direktivet och om domännamnsregistrets förhållande till skyddet av personuppgifter och skyddet av immateriella rättigheter behandlas bland annat i skäl 109—112 i direktivet. Avvikande från offentlighetslagen ska Trans-

1 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

port- och kommunikationsverket besvara en begäran om åtkomst till registeruppgifter om domännamn utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av begäran.

(7) Kommunikationsministeriet har konstaterat att propositionen inte är avsedd att innehålla förslag som med stöd av bestämmelserna om dataskydd för personuppgifter syftar till att, avvikande från artikel 28.5 i NIS 2-direktivet, förhindra åtkomst till domännamnsregistreringsuppgifter. Dessutom bestäms frågorna om en ändamålsenlig grund för behandling av personuppgifter till skydd för immateriella rättigheter utifrån annan lagstiftning än den som nu föreslås.

(8) Enligt undervisnings- och kulturministeriets yttrande kan hänvisningen till dataskyddslagstiftningen inte inverka på den skyldighet att behandla och lämna ut uppgifter som grundar sig på lag eller EU:s direktiv om säkerställande av skyddet för immateriella rättigheter. Utskottet betonar att den aktuella propositionen eller det nationella genomförandet av NIS 2-direktivet inte påverkar tillämpningen av sådan nationell lagstiftning eller EU-lagstiftning om skydd av immateriella rättigheter.

Resurser

(9) Utskottet oroar sig för hur myndigheternas resurser ska räcka till. Utskottet anser att det i nuläget är viktigt att myndighetsfunktionerna prioriteras. Utskottet oroar sig dock särskilt för huruvida myndigheternas resurser är tillräckliga för att de lagstadgade uppgifterna ska kunna skötas på behörigt sätt och i synnerhet för att den nationellt viktiga cybersäkerheten ska kunna tryggas. Utskottet betonar att Transport- och kommunikationsverket i lagstiftningen har anvisats många nya lagstadgade uppgifter utan att verkets anslag har höjts. Verket har redan därför tvingats strömlinjeforma sin verksamhet och sätta upp sina uppgifter i prioritetsordning. Utskottet betonar därför vikten av att anvisa tillräckliga resurser för att trygga de uppgifter som är centrala med tanke på den nationella övergripande säkerheten. Utskottet anser att det i det rådande ekonomiska läget är viktigt att myndighetsfunktionerna prioriteras. Utskottet anser dock att det är viktigt att bevaka om myndighetsresurserna räcker till.

(10) Det är också viktigt att företagen har tillräckliga resurser för en tillräcklig cybersäkerhet.

Uppföljning av hur lagen fungerar

Rådgivning och anvisningar. (11) Kommunikationsministeriet anser att tillsynsmyndigheternas rådgivning och anvisningar är viktiga när lagen börjar tillämpas samt i situationer där småföretag och mikroföretag funderar på om de omfattas av något av kriterierna. Utskottet konstaterar dock att företaget självt i princip har de bästa förutsättningarna att bedöma om dess verksamhet omfattas av tillämpningsområdet för bilaga I eller II samt om företaget uppfyller storlekskriteriet eller om det berörs av en sådan grund för undantag som avses i 3 § 3 mom. i cybersäkerhetslagen. Vid eventuell osäkerhet ska företaget begära råd av tillsynsmyndigheten. Även om det inte finns någon uttrycklig bestämmelse om skyldighet att ta kontakt, sätter lagen inga hinder för att tillsynsmyndigheten på eget initiativ kontakta aktörer som myndigheten bedömer höra till tillämpningsområdet, men som inte har meddelat uppgifter till förteckningen över aktörer.

Samband med lagstiftningen om kritisk infrastruktur. (12) Utskottet konstaterar att cybersäkerhetslagen har samband med regeringens proposition till riksdagen med förslag till lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft och till vissa andra lagar (RP 205/2024 rd), genom vilken det så kallade CER-direktivet om kritiska entiteters motståndskraft genomförs (Europaparlamentets och rådets direktiv [2] av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av direktiv 2008/114/EG). I den propositionen föreskrivs det om en nationell strategi och en nationell riskbedömning som gäller kritisk infrastruktur och kritiska aktörers motståndskraft, om den allmänna styrningen och samordningen av verksamheten, om en samlad utvärderingsram för kritiska aktörer och om ett samstämmigt ramverk för bedömning av kritiska aktörer och om en enhetlig ram för att stärka kritiska aktörers motståndskraft mot hot av olika slag.

(13) I förslaget till cybersäkerhetslag är lagens tillämpningsområde bundet till begreppet kritisk aktör, som i sin tur bestäms enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Med anledning av grundlagsutskottets utlåtande (GrUU 62/2024 rd) har utskottet dock strukit den villkorliga bestämningen av tillämpningsområdet och föreskrivit en entydig definition av tillämpningsområdet som baserar sig enbart på cybersäkerhetslagen.

(14) Enligt erhållen utredning finns det dock anledning att samordna propositionerna och ändra cybersäkerhetslagen när den allmänna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har trätt i kraft.

Uppföljning. (15) På grund av lagens centrala betydelse anser utskottet det nödvändigt att kommunikationsministeriet noga följer hur lagens syften uppnås och tillämpas samt vid behov vidtar åtgärder för att avhjälpa observerade missförhållanden. Utskottet föreslår därför att riksdagen godkänner ett uttalande där

> *riksdagen förutsätter att statsrådet noga följer hur lagens syften uppnås och hur lagen tillämpas och vid behov vidtar åtgärder för att avhjälpa observerade missförhållanden.*

(16) Utskottet föreslår också att riksdagen godkänner ett uttalande där

> *riksdagen förutsätter att kommunikationsministeriet lämnar kommunikationsutskottet en utredning om hur lagens syften har nåtts och hur lagen har tillämpats senast den 31 augusti 2026.*

2 (EU) 2022/2557

DETALJMOTIVERING

Tekniska och lagtekniska ändringar

Utskottet har gjort tekniska och lagtekniska ändringar i 2, 5, 19, 32, 37 och 45 § i lagförslag 1 samt i dess bilagor I och II, i ingressen i lagförslag 2, i 318 § i lagförslag 3, i 9 § i lagförslag 13 och dessutom i 109 a § i lagförslag 17.

1. Cybersäkerhetslagen

11 §. Incidentanmälningar till myndigheten. Enligt erhållen utredning är ordalydelsen i 2 mom. ägnad att skapa tolkningsproblem i situationer där en incident har upptäckts men det först senare under behandlingen framgår att incidenten är betydande. Formuleringen bör preciseras så att de tidsgränser för första anmälan och uppföljande anmälan som avses i momentet börjar när det har upptäckts att incidenten är betydande, det vill säga när den betydande incidenten har kommit till aktörens kännedom. Det har enligt uppgift varit syftet med bestämmelsen och motsvarar ordalydelsen i artikel 23 i NIS 2-direktivet. Utskottet har preciserat momentets formulering så att den gäller en betydande incident.

17 §. Hantering av incidentanmälningar. Förvaltningsutskottet välkomnar i sitt utlåtande den i 17 § 3 mom. i cybersäkerhetslagen föreslagna skyldigheten att underrätta polisen om upptäckten av en betydande incident och anser att tröskelnivån är lämplig. Enligt förvaltningsutskottet bör det övervägas om formuleringen ”skäl att misstänka ett brott”, som ligger till grund för anmälningsskyldigheten, kan strykas, så att det inte krävs att den som handlägger anmälan ska göra en rättslig prövning av om tröskeln för ”skäl att misstänka ett brott” överskrids eller inte.

Kommunikationsministeriet anser att det är ändamålsenligt att ändra formuleringen om tröskeln för anmälan på det sätt som förvaltningsutskottet föreslår. Utskottet har därför ändrat formuleringen så att den inte kräver rättslig prövning.

Utskottet har preciserat anmälningsskyldigheten i 5 mom. så att den gäller en betydande incident.

23 §. Frivilliga arrangemang för informationsutbyte om cybersäkerhet. Utskottet har ersatt skyddet för privatlivet med integritetsskyddet.

40 §. Verkställighet av påföljdsavgift. Rättsregistercentralen föreslog i sitt utlåtande att paragrafen behöver kompletteras med en bestämmelse om hur en fysisk persons död inverkar på verkställigheten av påföljdsavgiften. Utskottet har därför kompletterat paragrafen med en bestämmelse om att påföljdsavgift som påförts en fysisk person avskrivs när personen avlider.

47 §. Ikraftträdande. Under sakkunnigutfrågningen föreslogs det övergångstider för anmälan till förteckningen över aktörer och för utarbetande av en sådan handlingsmodell för hantering av cybersäkerhetsrisker som avses i 8 § i cybersäkerhetslagen.

Utskottet anser att en månad efter lagens ikraftträdande är en lämplig övergångstid för bestämmelsen om anmälan till förteckningen över aktörer. Det är motiverat att en motsvarande över-

gångsperiod gäller också när en aktör efter lagens ikraftträdande börjar omfattas av lagens tillämpningsområde som ny aktör.

För utarbetande av en sådan handlingsmodell för hantering av cybersäkerhetsrisker som avses i 8 § i cybersäkerhetslagen anser utskottet att en lämplig övergångstid är tre månader efter lagens ikraftträdande. Det är motiverat att en motsvarande övergångsperiod gäller också när en aktör efter lagens ikraftträdande börjar omfattas av lagens tillämpningsområde som ny aktör.

Bilaga II. I fråga om punkt 6 i bilagan påpekar Säkerhets- och kemikalieverket Tukes att definitionerna i fråga om kemikaliebranschen är inexakta. Enligt uppgift från kommunikationsministeriet hänför sig hänvisningen i bilagans punkt 6 till definitionerna av ämnen och beredningar i REACH-förordningen [3]. Dessa definitioner är så öppna att tillämpningen av en hänvisning utan precisering kan medföra tolkningsproblem och i värsta fall en helt olämplig extensiv tolkning (tillverkning av vilket som helst föremål eller ämne).

Under riksdagsbehandlingen av propositionen har man enligt kommunikationsministeriet fått inofficiella tolkningsanvisningar från kommissionen om preciseringen av tillämpningsområdet i fråga om kemikaliebranschen. Med beaktande av kommissionens tolkningsanvisningar är en precisering av tillämpningsområdet möjlig och förenlig med hur kommissionen tolkar tillämpningsområdet, även om preciseringen begränsar tillämpningen jämfört med direktivets ordalydelse. Därför har utskottet preciserat 6 punkten så att den gäller ämnen som ska registreras eller som är tillståndspliktiga eller anmälningspliktiga enligt kemikaliesäkerhetslagen (390/2005).

2. Lagen om ändring av lagen om informationshantering inom den offentliga förvaltningen

2 §. Definitioner. Till följd av de ändringar som av nedan angivna orsaker görs i 3 § behövs det enligt kommunikationsministeriet inte någon definition av kritisk aktör. Utskottet stryker därför definitionen.

3 §. Lagens tillämpningsområde och avgränsningar av det.

Grundlagsutskottet förutsätter i sitt utlåtande att lagförslag 2 i propositionen ändras så att 4 a kap. i informationshanteringslagen inte tillämpas på riksdagens ämbetsverk. Det är ett villkor för att lagförslaget ska kunna behandlas i vanlig lagstiftningsordning.

Bestämmelser om avgränsning av tillämpningsområdet för det föreslagna nya 4 a kap. i informationshanteringslagen finns i 3 §. Genom den föreslagna ändringen fogas riksdagens ämbetsverk till förteckningen i 3 § 3 mom. över de myndigheter på vilka det nya 4 a kap. inte tillämpas. Samtidigt föreslås det att villkoret att avgränsningen av tillämpningsområdet ska tillämpas endast om myndigheten är en kritisk aktör stryks i momentets inledande stycke. I samband med strykningen av villkoret att myndigheten är en kritisk aktör föreslås det att också den nya definitionen av kri-

3 Europaparlamentets och rådets förordning (EG) N:o 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (REACH), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG samt upphävande av rådets förordning (EEG) N:o 793/93, kommissionens förordning (EG) N:o 1488/94, rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG

tisk aktör i 2 § 26 punkten stryks och att vissa strykningar görs i 3 § 4 och 5 mom. Enligt uppgift från kommunikationsministeriet har de föreslagna ändringarna bedömts i samråd med finansministeriet.

Också inom den offentliga förvaltningen kommer de eventuella kritiska aktörer som avses i CER-direktivet och som det hänvisas till i NIS 2-direktivet att bestämmas utifrån lagförslag 1 i regeringens proposition RP 205/2024 rd om genomförande av CER-direktivet (lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft), som är under behandling i riksdagen. Tillämpningen av CER-direktivet inom den offentliga förvaltningens verksamhetsområde, inklusive de undantag från tillämpningen som tillåts enligt CER-direktivet, bestäms närmare utifrån det nämnda lagförslaget. Därför kan man först efter att beredningen av den propositionen har framskridit och när innehållet i den föreslagna lagen om genomförande av CER-direktivet fastslagits med säkerhet beakta vilka aktörer inom den offentliga förvaltningen som kan definieras som kritiska aktörer, hur de kritiska aktörerna inom den offentliga förvaltningen ska definieras och i vilken omfattning tillämpningsområdet för det föreslagna 4 a kap. i informationshanteringslagen ska omfatta kritiska aktörer inom den offentliga sektorn utan förbehåll.

I princip omfattar tillämpningsområdet för det föreslagna 4 a kap. många myndigheter oberoende av om de i framtiden bedöms vara kritiska i enlighet med CER-direktivet. Genom ändringen preciseras dessutom att det föreslagna 4 a kap. inte tillämpas på vissa myndigheter, såsom ämbetsverk som lyder under riksdagen, oberoende av om de senare definieras som kritiska utifrån annan lagstiftning.

Kommunikationsministeriet bereder för närvarande en separat proposition med förslag till tekniska lagstiftningsändringar som behövs för att skyldigheterna enligt den föreslagna cybersäkerhetslagen (RP 57/2024 rd) ska kunna tillämpas på kritiska aktörer på det sätt som förutsätts i NIS 2- och CER-direktiven, om förpliktelserna enligt NIS 2 inte annars skulle vara tillämpliga på kritiska aktörer på det sätt som direktiven förutsätter. Ministeriet konstaterar att beredningen av propositionen pågår och att avsikten är att de behövliga ändringarna ska föreläggas riksdagen så snart som möjligt. I samband med den propositionen kan man närmare bedöma om det över huvud taget finns behov av en specialbestämmelse i informationshanteringslagen om tillämpningen av bestämmelserna på kritiska aktörer. Den slutliga formuleringen av behovet av denna specialbestämmelse i 3 § och av tillämpningen av 4 a kap. i informationshanteringslagen är beroende av hur den i regeringens proposition RP 205/2024 rd föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft i princip ska tillämpas inom den offentliga förvaltningen och med vilka undantag.

I den paragraf som bestämmer tillämpningsområdet och avgränsningen av tillämpningsområdet har utskottet därför strukit avgränsningen av tillämpningsområdet för kritiska aktörer inom den offentliga förvaltningen.

Undervisnings- och kulturministeriet anser att det inte finns några särskilda grunder för att kräva strängare cybersäkerhetsskyldigheter av statliga läroanstalter än av kommunala läroanstalter. Utskottet har därför preciserat 3 mom. 6 punkten så att statliga läroanstalter inte omfattas av tillämp-

ningsområdet för det nya 4 a kap. som föreslås i lagen om informationshantering inom den offentliga förvaltningen.

18 d §. Skyldighet att anmäla betydande incidenter. Enligt erhållen utredning är ordalydelsen i 1 och 2 mom. ägnad att skapa tolkningsproblem i situationer där en incident har upptäckts men det först senare under behandlingen framgår att incidenten är betydande. Formuleringen bör preciseras så att de tidsgränser för första anmälan och uppföljande anmälan som avses i momentet börjar när det har upptäckts att incidenten är betydande, det vill säga när den betydande incidenten har kommit till aktörens kännedom. Det har enligt uppgift varit syftet med bestämmelsen och motsvarar ordalydelsen i artikel 23 i NIS 2-direktivet. Utskottet har preciserat momentets formulering så att den gäller en betydande incident.

Ikraftträdandebestämmelsen. Utskottet har korrigerat tidsfristen för anmälan enligt 18 a § 2 mom. så att anmälan ska göras senast en månad efter lagens ikraftträdande.

3. Lagen om ändring av lagen om tjänster inom elektronisk kommunikation

Ikraftträdandebestämmelsen. Enligt propositionsmotiven berörs föreskrifter som meddelats med stöd av gällande 275 § 4 mom. av en övergångsbestämmelse. En sådan övergångsbestämmelse saknas dock, och därför har utskottet fogat den till lagens ikraftträdandebestämmelse.

15. Lagen om ändring av 1 § i lagen om verkställighet av böter

Ingressen. På grund av de ändringar som gjorts i paragrafen under behandlingen av propositionen är det nödvändigt att ändra ingressen och 1 § i ändringslagen.

1 §. Lagens tillämpningsområde. Av de skäl som nämns ovan har utskottet korrigerat formuleringarna i paragrafen.

FÖRSLAG TILL BESLUT

Kommunikationsutskottets förslag till beslut:

Riksdagen godkänner lagförslag 4—12, 14 och 16 i proposition RP 57/2024 rd utan ändringar.

Riksdagen godkänner lagförslag 1—3, 13, 15 och 17 i proposition RP 57/2024 rd med ändringar. ***(Utskottets ändringsförslag)***

Riksdagen godkänner två uttalanden. ***(Utskottets förslag till uttalanden)***

Utskottets ändringsförslag

1.

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 cyberincident,

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* ,

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,

4) en leverantör av DNS-tjänster, eller

5) en kritisk aktör som identifierats med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (/) inom någon annan sektor än sektorn för offentlig förvaltning som avses i punkt 10 i bilaga I till NIS 2-direktivet.

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 skyldighe-

ter 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 på återkallande av tillstånd 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).

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 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. Inn-

an 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 och förhindra eller minimera skadliga verkningar.

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

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

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 tillgängliga tekniska medel för att avvärja hot med beaktande av den aktuella utvecklingen.

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 dessutom iakttas Europeiska kommissionens genomförandeakter som antas med stöd av artikel 21.5 i NIS 2-direktivet.

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.

Den första anmälan ska göras inom 24 timmar från det att den betydande incidenten upptäcktes och den 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 Europeiska kommissionens genomförandeakt som antagits med stöd av artikel 23.11 i NIS 2-direktivet och där 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 ~~finns skäl att misstänka~~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 sår-

barheter 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 sådan 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 upprättas frivilliga arrangemang för informationsutbyte om

cybersäkerhet som samordnas av CSIRT-enheten, 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 förtroliga meddelanden och ~~privatlivet~~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 hante-

ring 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 förtroliga 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

Beloppet av den administrativa påföljdsavgiften baserar sig på en helhetsbedömning där omständigheterna i fallet och åtminstone följande omständigheter beaktas:

1) överträdelsens allvar och betydelsen av de bestämmelser som har överträtts så att överträdelsens allvar framgår av

a) upprepade oegentligheter,

b) underlåtenhet att underrätta om eller avhjälpa betydande incidenter,

c) underlåtenhet att avhjälpa upptäckta brister trots beslut eller varningar av 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 det lagakraft-

vunna beslutet om avgiften 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 de nämnda artiklarna görs till Europeiska kommissionen, NIS-samarbetsgruppen och Europeiska

unionens cybersäkerhetsbyrå. CSIRT-enheten har rätt att av tillsynsmyndigheten få uppgifter ur förteckningen över aktörer.

42 §

Nationell strategi för cybersäkerhet

Statsrådet antar den nationella strategin 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 underrättar Europeiska kommissionen om 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. Cyber-

säkerhetscentret 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 20 .

Den anmälan som avses i 41 § ska göras senast ~~den 31 december 2024~~en månad efter det att denna lag trätt i kraft eller senast när de kriterier som i 3 § anges för en aktör uppfylls.

Den handlingsmodell för hantering av cybersäkerhetsrisker som avses i 8 § ska göras upp senast tre månader efter det att denna lag trätt i kraft eller senast när de kriterier som i 3 § fastställts för en aktör uppfylls. (Nytt)

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 sjukvårdaktörer 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 en högskola eller någon annan utbildningsinstitution

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

2.

Lag

om ändring av lagen om informationshantering inom den offentliga förvaltningen

I enlighet med riksdagens beslut

ändras i lagen om informationshantering inom den offentliga förvaltningen (906/2019) 2 § 16 punkten, 3 § och 10 § 1 mom. 2 punkten, av dem 2 § 16 punkten sådan den lyder i lag 488/2023 och 3 § sådan den lyder delvis ändrad i lagarna 653/2021 och 488/2023, samt

fogas till 1 § ett nytt 2 mom., i stället för det 2 mom. som upphävts genom lag 710/2021, och till 2 § nya 17–25 punkter samt till lagen ett nytt 4 a kap. som följer:

1 §

Lagens syfte

— —

Genom denna lag genomförs bestämmelserna om skyldigheter för aktörer, om tillsynen över fullgörandet av dem och om påföljder i 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) inom sektorn för offentlig förvaltning som avses i punkt 10 i bilaga I till NIS 2-direktivet (*den offentliga förvaltningen*). Bestämmelser om genomförande av NIS 2-direktivet till övriga delar finns i cybersäkerhetslagen (/).

2 §

Definitioner

I denna lag avses med

— —

16) *behandlingsregler* av en fysisk person på förhand utarbetade regler avsedda att styra automatisk databehandling,

17) *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,

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,

18) *säkerhet i kommunikationsnät och informationssystem* kommunikationsnäts och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva 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,

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

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

21) *betydande cyberhot* ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en myndighets nätverks- och informationssystem eller användarna av dess tjänster genom att orsaka betydande materiell eller immateriell skada,

22) *cyberrisk* 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,

23) *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,

24) *betydande incident* en incident som

a) har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för en myndighet, eller

b) har påverkat eller kan påverka fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada,

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

~~26) *kritisk aktör* en myndighet eller någon annan som sköter en offentlig förvaltningsuppgift och som är en i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG avsedd kritisk aktör inom den offentliga förvaltningen.~~

3 §

Lagens tillämpningsområde och avgränsningar av det

Denna lag ska tillämpas på informationshantering och på användning av informationssystem, då myndigheter behandlar informationsmaterial, om inte något annat föreskrivs någon annanstans i lag. Bestämmelserna i 6 a kap. i denna lag ska tillämpas på införande och användning av *automatiserat beslutsförfarande*. Vad som i denna lag föreskrivs om myndigheter ska också tillämpas på universitet som avses i universitetslagen (558/2009) och på yrkeshögskolor som avses i yrkeshögskolelagen (932/2014).

Det föreskrivs särskilt om förfaranden som ska iakttas vid ärendehantering och tjänsteproduktion, om sekretessbeläggning och om rätten till information om myndighetshandlingar samt om arkivering av handlingar. I kyrkolagen (652/2023) föreskrivs om informationshantering och användning av informationssystem inom Finlands evangelisk-lutherska kyrka.

Bestämmelserna i 4 a kap. tillämpas inte på följande myndigheter och myndighetsverksamheter ~~endast om myndigheten är en kritisk aktör~~:

1) republikens presidents kansli, riksdagens ämbetsverk, Försvarsmakten, polisenheter som avses i polisförvaltningslagen (110/1992), Gränsbevakningsväsendet, Åklagarmyndigheten och Tullens brottsbekämpning,

2) domstolar och nämnder som har inrättats för att behandla besvärsärenden,

3) Försvarsfastigheter,

4) kommunala myndigheter med undantag för Helsingfors stad på vilken 4 a kap. tillämpas när staden sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar, ~~även om den inte är en kritisk aktör,~~

5) Finlands Bank,

6) universitet som avses i universitetslagen, yrkeshögskolor som avses i yrkeshögskolelagen, Räddningsinstitutet och övriga statliga utbildningsinstitutioner,

7) sådan tjänsteproduktion i säkerhetsnätet och användning av dess tjänster som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015),

8) myndigheter som har inrättats tillsammans med ett land som inte hör till Europeiska ekonomiska samarbetsområdet i enlighet med en internationell överenskommelse och diplomatiska el-

ler konsulära beskickningar i dessa länder och deras nät- och informationssystem, till den del dessa system finns i beskickningens lokaler eller upprätthålls för användare i ett dessa länder.

Bestämmelserna i 19, 20, 26 och 27 § ska inte tillämpas på rättskipningen vid domstolar eller nämnder som har inrättats för att behandla besvärsärenden. Bestämmelserna i 3 kap. ska inte tillämpas på riksdagens justitieombudsmans, justitiekanslerns i statsrådet eller domstolarnas verksamhet eller verksamheten vid nämnder som har inrättats för att behandla besvärsärenden och inte heller på republikens presidents kansli, riksdagens ämbetsverk, Folkpensionsanstalten, Finlands Bank, övriga självständiga offentligrättsliga inrättningar, universitet som avses i universitetslagen eller på yrkeshögskolor som avses i yrkeshögskolelagen. Bestämmelserna i 3 kap. ska tillämpas på välfärdsområden, välfärdssammanslutningar, kommuner och samkommuner då de sköter lagstadgade uppgifter. ~~Bestämmelserna i 18 g § 3 mom. och 18 h–18 l § ska inte tillämpas på riksdagens justitieombudsmans eller justitiekanslerns i statsrådet verksamhet. Bestämmelserna i 18 g § 3 mom. och 18 h–18 l § ska också inte tillämpas på republikens presidents kansli eller på rättskipningen vid domstolar eller nämnder som har inrättats för att behandla besvärsärenden, även om 4 a kap. i övrigt tillämpas på dem när de är kritiska aktörer.~~

Vad som i 4 kap., 22–24 och 25–27 § samt 6 a kap. föreskrivs om informationshanteringsenheter och myndigheter ska tillämpas på privatpersoner och privaträttsliga sammanslutningar samt sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter. På privatpersoner, privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter tillämpas dessutom vad som i 4 och 28 § föreskrivs om informationshanteringsenheter när de utövar offentlig makt på det sätt som avses i 4 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet eller när det särskilt föreskrivs att den lagen ska tillämpas på deras verksamhet. Vidare tillämpas vad som i 19 § 2 mom. samt i 24 a och 24 b § föreskrivs om myndigheter på privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter när de utövar offentlig makt på det sätt som avses i 4 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet. ~~Vad som i 4 a kap. föreskrivs om informationshanteringsenheter och myndigheter tillämpas på privatpersoner och privaträttsliga sammanslutningar samt sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter och är kritiska aktörer.~~

Denna lag ska inte tillämpas på statliga myndigheter i landskapet Åland. Lagens 13 a § och 6 a kap. ska dock tillämpas på statliga myndigheter på Åland när de sköter sådana myndighetsuppgifter som hör till rikets lagstiftningsbehörighet och som innebär automatiserat avgörande av ärenden enligt 53 e § i förvaltningslagen. Även 4 a kap. ska tillämpas på statliga myndigheter i landskapet Åland, om inte något annat följer av 3 mom.

10 §

Den offentliga förvaltningens informationshanteringsnämnd

I anslutning till finansministeriet finns en informationshanteringsnämnd för den offentliga förvaltningen (*informationshanteringsnämnden*) med uppgift att

— —

2) främja förfarandena i fråga om informationshantering och informationssäkerhet samt genomförandet av de krav som föreskrivs i denna lag, med undantag för vad som föreskrivs i 4 a kap.

— —

4 a kap.

Skyldigheter som gäller cybersäkerhet och tillsynen över att de fullgörs

18 a §

Aktörsindelning och anmälan om verksamhet

De informationshanteringsenheter som omfattas av tillämpningsområdet för detta kapitel är väsentliga aktörer inom den offentliga förvaltningen. Välfärdsområdena och välfärdssammanslutningarna samt Helsingfors stad är dock viktiga aktörer.

En informationshanteringsenhet ska till tillsynsmyndigheten anmäla

1) sitt namn,

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

3) sina IP-adressintervall,

4) uppgift om huruvida den är en väsentlig eller en viktig aktör inom den offentliga förvaltningen,

5) en förteckning över övriga medlemsstater i Europeiska unionen där enheten tillhandahåller sina tjänster,

6) sitt deltagande i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 23 § i cybersäkerhetslagen.

Informationshanteringsenheten ska utan dröjsmål, senast inom två veckor från en ändring, anmäla alla ändringar i de uppgifter som avses i 2 mom.

18 b §

Skyldighet att hantera cybersäkerhetsrisker och handlingsmodell för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska identifiera, utvärdera och hantera cyberrisker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sina funktioner eller för att tillhandahålla sina tjänster. Hanteringen av cybersäkerhetsrisker ska förhindra eller minimera incidenternas inverkan på verksamheten, driftskontinuiteten, tjänstemottagarna och andra tjänster. Informationshanteringsenheten ska vidta de åtgärder för hantering av cybersäkerhetsrisker som avses i 18 c §.

Informationshanteringsenheten 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 18 c § genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot cyberhot och incidenter fastställas och beskrivas.

Informationshanteringsenhetens ledning svarar för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av risker och

utövar tillsyn över genomförandet av den. Informationshanteringsenhetens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

18 c §

Åtgärder för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska vidta proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för hantering av cybersäkerhetsrisker för att hantera sådana cyberrisker hänför sig till säkerheten i de kommunikationsnät och informationssystem som enheten använder och för att förhindra eller minimera skadliga verkningar. I handlingsmodellen för hantering av cybersäkerhetsrisker och de åtgärder för hantering av cybersäkerhetsrisker som baserar sig på den ska åtminstone följande beaktas och uppdateras:

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

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 åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem och cybersäkerhetspraxis hos direkta leverantörer och tjänsteleverantörer samt resultatet av de samordnade riskbedömningar av kritiska leveranskedjor som avses i artikel 22.1 i NIS 2-direktivet,

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 upprätthålla och återställa säkerheten och driftssäkerheten,

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

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

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

Åtgärderna ska vara aktuella, lämpliga och proportionella i förhållande till riskexponeringen när det gäller de kommunikationsnät och informationssystem som informationshanteringsenheten använder, kommunikationsnätets eller informationssystemets betydelse för informationshanteringsenhetens verksamhet samt de direkta konsekvenser som en incident i dessa rimligtvis kan förutses ha. Vid dimensioneringen av åtgärderna ska dessutom beaktas informationshanteringsenhetens storlek, arten av dess verksamhet, sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, kostnaderna för åtgärderna samt tillgängliga tekniska medel för att avvärja cyberhot med beaktande av den aktuella utvecklingen.

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

18 d §

Skyldighet att anmäla betydande incidenter

Myndigheten ska utan dröjsmål, senast inom 24 timmar från upptäckten av en betydande incident lämna tillsynsmyndigheten en första anmälan om incidenten, i vilken det ska anges om incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar och om incidenten kan ha gränsöverskridande verkningar samt sannolikheten för sådana verkningar.

Myndigheten ska utan dröjsmål, senast inom 72 timmar från upptäckten av en betydande incident lämna tillsynsmyndigheten en uppföljande anmälan om incidenten, i vilken den information som avses i 1 mom. ska uppdateras och det ska anges en inledande bedömning av den betydande incidentens art, allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

Myndigheten ska inom en månad från det att den uppföljande anmälan lämnades in lämna tillsynsmyndigheten en slutrapport om den betydande incidenten. 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.

Om incidenten fortfarande fortgår när den slutrapport som avses i 3 mom. ska lämnas in, ska en delrapport om hur hanteringen av incidenten framskrider lämnas i stället för slutrapporten. Slutrapporten ska då lämnas in inom en månad från det att myndigheten har hanterat incidenten. När incidenten fortgår har tillsynsmyndigheten rätt att av myndigheten få ytterligare information eller en delrapport.

Vid anmälan av en betydande incident ska dessutom iakttas Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för anmälan samt en närmare definition av betydande incidenter.

18 e §

Mottagande av incidentanmälan

Tillsynsmyndigheten ska utan dröjsmål, om möjligt inom 24 timmar från mottagandet av den första anmälan som avses i 18 d § 1 mom., lämna ett svar till myndigheten. Svaret ska innehålla initial återkoppling om den betydande incidenten och, på myndighetens begäran, vägledning eller operativa råd om hanteringen av incidenten samt vägledning om hur den betydande incidenten ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet.

Tillsynsmyndigheten ska när den ger vägledning och operativa råd som avses i 1 mom. samarbeta med den CSIRT-enhet som avses i cybersäkerhetslagen. Vägledning och operativa råd kan ges av CSIRT-enheten i stället för av tillsynsmyndigheten.

18 f §

Frivillig underrättelse

En myndighet kan underrätta tillsynsmyndigheten också om andra än betydande incidenter samt om cyberhot och tillbud. Även de som avses i 3 §, på vilka detta kapitel inte tillämpas, kan göra en sådan underrättelse.

Tillsynsmyndigheten ska behandla frivilliga underrättelser som avses i 1 mom. med iakttagande av det förfarande som anges i 18 e §. Tillsynsmyndigheten får prioritera behandlingen av anmälningar som avses i 18 d § i förhållande till behandlingen av frivilliga underrättelser.

Myndigheter och andra som avses i 3 § kan i samband med en frivillig underrättelse lämna ut sådan information till tillsynsmyndigheten som tillsynsmyndigheten har rätt att få med stöd av 18 i §.

I samband med en frivillig underrättelse ska dessutom iakttas Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för underrättelser.

18 g §

Informationsskyldighet om betydande cyberhot och incidenter

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

En myndighet 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 myndigheten att informera om den betydande incidenten eller själv informera om saken.

I den information som avses i 1 och 2 mom. ska dessutom iakttas Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för underrättelser samt en närmare definition av betydande incidenter.

18 h §

Tillsynsmyndighet

Transport- och kommunikationsverket är den tillsynsmyndighet som avses i detta kapitel och den i artikel 8.1 i NIS 2-direktivet avsedda behöriga myndigheten inom den offentliga förvaltningen. Utöver vad som föreskrivs i detta kapitel ska tillsynsmyndigheten utöva tillsyn över att de

skyldigheter som föreskrivs i detta kapitel och i bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs inom den offentliga förvaltningen samt föra en förteckning över aktörerna inom den offentliga förvaltningen som innehåller de uppgifter som lämnats med stöd av 18 a §. Transport- och kommunikationsverket är självständigt och oberoende i sin verksamhet som tillsynsmyndighet.

Tillsynsmyndigheten kan ställa de tillsynsuppgifter som anges i denna lag i prioritetsordning enligt en riskbaserad bedömning. Tillsynsmyndigheten ska när den inriktar tillsynen och fattar ett tillsynsbeslut enligt 18 l § beakta de omständigheter som avses i 27 § 3 mom. och 37 § i cybersäkerhetslagen. Tillsynsmyndigheten kan inrikta tillsynen gentemot ett välfärdsområde, en välfärdssammanslutning eller Helsingfors stad endast om det finns en grundad anledning att misstänka att området, sammanslutningen eller staden inte har iakttagit bestämmelserna i detta kapitel eller i rättsakter som antagits med stöd av NIS 2-direktivet.

Om inte något annat föreskrivs i detta kapitel ska tillsynsmyndigheten vid behandlingen av sådana anmälningar om verksamhet som avses i 18 a §, av sådana anmälningar och underrättelser om incidenter som avses i 18 d och 18 f § och av annan information som erhållits i samband med tillsynsuppgiften och i samarbetet med andra myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan samt vid utlämnandet av information till dem iaktta vad som i 6 § 4 mom., 15 § 3 mom., 17 §, 18 § 3 mom., 26 § 2 mom., 28 § 4 och 5 mom., 33 §, 41 § 5 mom. och 45 § i cybersäkerhetslagen föreskrivs om behandling av information vid tillsynsmyndigheten, om tillsynsmyndighetens samarbete med andra myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan samt om utlämnandet av information till dem.

Bestämmelser om Transport- och kommunikationsverkets uppgifter som gemensam kontaktpunkt och CSIRT-enhet enligt NIS 2-direktivet finns i cybersäkerhetslagen.

18 i §

Tillsynsmyndighetens rätt att få information

Tillsynsmyndigheten har när den utför uppgifter enligt detta kapitel trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att 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. Myndigheten ska lämna ut informationen utan dröjsmål och avgiftsfritt.

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en myndighet 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.

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 eller information vars utlämnande skulle även-

tyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

Bestämmelser om de förpliktelser som gäller hantering av särskilt känsligt informationsmaterial finns i lagen om internationella förpliktelser som gäller informationssäkerhet.

18 j §

Tillsynsmyndighetens rätt att förrätta inspektioner

Tillsynsmyndigheten har rätt att i den omfattning som det behövs förrätta inspektion av en myndighet för tillsynen över att de skyldigheter som föreskrivs i detta kapitel eller i bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs.

Den som förrättar inspektionen ska ha tillräcklig utbildning och erfarenhet med hänsyn till inspektionens art och omfattning.

Myndigheten 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. För förrättande av inspektionen har den som förrättar 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 myndigheten har genomfört. På inspektionsförrättarens rätt att förrätta inspektion och få information tillämpas vad som i 18 i § 3 mom. föreskrivs om begränsningar i rätten att få information.

På förfarandet vid inspektionen tillämpas vad som i 39 § i förvaltningslagen föreskrivs om inspektion.

18 k §

Tilldelande av biträdande uppgift till bedömningsorgan för informationssäkerhet samt att låta utföra bedömning

Tillsynsmyndigheten kan tilldela ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011) en biträdande uppgift i anslutning till ett inspektionsuppdrag enligt 18 j §.

Tillsynsmyndigheten kan för tillsynen ålägga en myndighet att låta ett bedömningsorgan för informationssäkerhet utföra en bedömning av hanteringen av cybersäkerhetsrisker, om

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

2) myndigheten väsentligt och allvarligt har försummat att iaktta skyldigheterna att hantera cybersäkerhetsrisker enligt 18 b eller 18 c §.

På den som är anställd vid ett bedömningsorgan för informationssäkerhet och som bistår vid en inspektion och på en person som utför en bedömning tillämpas vad som i 18 j § 2–4 mom. föreskrivs om inspektionsförrättarens erfarenhet och utbildning samt inspektionsförrättarens rättigheter. Om inte något annat föreskrivs i detta kapitel, tillämpas lagen om bedömningsorgan för informationssäkerhet på bedömningsorganet för informationssäkerhet. På den som är anställd vid ett bedömningsorgan för informationssäkerhet tillämpas bestämmelserna om straffrättsligt tjäns-

teansvar för tjänstemän, med undantag för bestämmelserna om avsättningspåföljd, när han eller hon sköter uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

18 l §

Påföljder

Tillsynsmyndigheten kan ålägga en myndighet att inom utsatt tid avhjälpa bristerna i fullgörandet av skyldigheterna enligt detta kapitel eller bestämmelser som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan ålägga myndigheten att offentliggöra dessa brister eller andra omständigheter som har samband med överträdelser av de nämnda skyldigheterna.

Tillsynsmyndigheten kan ge myndigheten en varning, om den inte har fullgjort de skyldigheter som föreskrivs i detta kapitel eller i bestämmelser som antagits med stöd av NIS 2-direktivet. I varningen ska den brist eller försummelse som varningen gäller specificeras. Varningen ska ges skriftligen.

Tillsynsmyndigheten kan förena ett beslut som avses i 1 mom. med vite.

18 m §

Sökande av ändring

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

Bestämmelser om sökande av ändring i beslut som gäller föreläggande och utdömande av vite finns i viteslagen (1113/1990).

Denna lag träder i kraft den 20 .

Den anmälan som avses i 18 a § 2 mom. ska göras senast en månad efter det att denna lag trätt i kraft.

3.

Lag

om ändring av lagen om tjänster inom elektronisk kommunikation

I enlighet med riksdagens beslut

upphävs i lagen om tjänster inom elektronisk kommunikation (917/2014) 2 § 2 mom. och 247 a §, sådana de lyder, 2 § 2 mom. i lag 1207/2020 och 247 a § i lag 281/2018, och

ändras 165 § 1 mom., 167, 170 §, och 275 §, 308 § 3 mom., 313 § 2 mom. 2 punkten, 318 § 4 mom. och 342 § 2 mom.,

sådana de lyder, 165 § 1 mom., 170 §, 308 § 3 mom. samt 313 § 2 mom. 2 punkten i lag 1003/2018, 167 § i lagarna 1003/2018 och 1207/2020 samt 275 § och 318 § 4 mom. i lag 1207/2020 och 242 § 2 mom. i lag 1182/2023, samt

fogas till 165 §, sådan den lyder i lag 1003/2018, ett nytt 4 mom. och till 247 §, sådan den lyder i lag 1003/2018, ett nytt 5 mom.

som följer:

165 §

Registrarens anmälningsskyldighet

En registrar ska göra en anmälan till den myndighet som förvaltar domännamnsregistret innan den inleder sin verksamhet. Anmälan ska innehålla följande uppgifter:

1) registrarens namn, FO-nummer eller, om sådant saknas, annan identifieringsuppgift samt den e-postadress som ska användas för hörande och delgivning,

2) adress och aktuell kontaktinformation till registrarens huvudkontor och andra lagliga verksamhetsställen i Europeiska unionen eller, om registraren inte är etablerad i Europeiska unionen, adress, e-postadresser, telefonnummer och annan aktuell kontaktinformation till registrarens utsedda företrädare i Europeiska unionen,

3) registrarens IP-adressintervall,

4) en förteckning över de medlemsstater i Europeiska unionen där registraren tillhandahåller tjänster, och

5) andra än i 1-4 punkten avsedda uppgifter som behövs för tillsynen.

— —

Transport- och kommunikationsverket ska lämna den gemensamma kontaktpunkt som avses i 18 § i cybersäkerhetslagen (/) de uppgifter om registrarernas anmälningar som behövs för att göra en anmälan enligt artikel 27.4 i 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)* .

167 §

Anteckning av uppgifter i domännamnsregistret och offentliggörande av uppgifter

Ett domännamn ska registreras på domännamnsanvändaren. Domännamnsanvändaren ska lämna registraren korrekta och uppdaterade användar- och kontaktuppgifter som identifierar domännamnsanvändaren samt ändringar i dem. Registraren eller den som handlar på registrarens vägnar ska i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren och det registrerade domännamnet samt den e-postadress som ska användas för hörande och delgivning.

Transport- och kommunikationsverket kan förhindra registrering av ett domännamn i domännamnsregistret, om verket misstänker att de uppgifter som avses i 1 mom. är bristfälliga eller felaktiga och registraren trots uppmaning inte inom utsatt tid bevisar att uppgifterna är riktiga. Transport- och kommunikationsverket gör sina riktlinjer och förfaranden för säkerställande av att användaruppgifterna är korrekta offentligt tillgängliga.

Transport- och kommunikationsverket offentliggör uppgifterna i domännamnsregistret på sina webbsidor eller i någon annan elektronisk tjänst utan obefogat dröjsmål. Bestämmelser om skydd för personuppgifter finns i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och i dataskyddslagen, som kompletterar förordningen. Transport- och kommunikationsverket ska besvara en begäran om åtkomst till registeruppgifter om domännamn utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av begäran. I övrigt ska på utlämnande av uppgifter ur registret tillämpas 16 § i lagen om offentlighet i myndigheternas verksamhet. Transport- och kommunikationsverket gör sina riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.

Ett domännamn som har registrerats i domännamnsregistret gäller i högst fem år. Registraren kan förnya en domänregistrering för högst fem år i sänder.

Transport- och kommunikationsverket får utfärda närmare föreskrifter om hur registreringen tekniskt ska genomföras och om de uppgifter som ska lämnas i samband med registreringen samt om teknisk identifiering av domännamnsanvändaren och om verifiering av uppgifterna om domännamnsanvändaren.

170 §

Registrarens övriga skyldigheter

En registrar ska

1) innan ett domännamn registreras tillhandahålla behövlig information enligt denna lag om kraven på domännamnets innehåll och form,

2) uppdatera uppgifterna i domännamnsregistret,

3) kunna göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Transport- och kommunikationsverket har fastställt,

4) i tillräcklig omfattning och effektivt informera en domännamnsanvändare om att domännamnets giltighetstid löper ut,

5) på begäran av domännamnsanvändaren avregistrera ett domännamn innan dess giltighetstid har löpt ut,

6) sörja för informationssäkerheten i sin verksamhet,

7) utan dröjsmål meddela Transport- och kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den; samtidigt ska registraren också anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas,

8) göra sina riktlinjer och förfaranden för att säkerställa att uppgifterna i domännamnsregistret överensstämmer med bestämmelserna i 167 § 1 mom. offentligt tillgängliga,

9) utan obefogat dröjsmål göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga,

10) i enlighet med dataskyddslagstiftningen och avgiftsfritt ge åtkomst till registreringsuppgifter om domännamn samt svara den som legitimt begär åtkomst till registreringsuppgifter utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av en laglig och på tillbörligt sätt motiverad begäran,

11) göra riktlinjer och förfaranden för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga.

Transport- och kommunikationsverket får meddela närmare föreskrifter om information som ges till användare av domännamn, om information som ska göras offentligt tillgänglig, om givande av åtkomst till uppgifter, om de riktlinjer och förfaranden som avses i 8 och 11 punkten, om informationssäkerheten i registrarens verksamhet samt om när en störning som avses i 1 mom. 7 punkten ska anses vara betydande och om innehållet i anmälan samt anmälans utformning och hur den lämnas in.

Bestämmelser om skyldigheten för i 2 § 3 punkten i cybersäkerhetslagen en leverantör av DNS-tjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och för anmälan av avvikelser finns i cybersäkerhetslagen.

247 §

Skyldighet att sörja för informationssäkerheten vid kommunikationsförmedling och tillhandahållande av mervärdestjänster

— —

När det gäller att sörja för informationssäkerheten tillämpas dessutom vad som i cybersäkerhetslagen föreskrivs om sådana kommunikationsförmedlare och leverantörer av mervärdestjänster som omfattas av tillämpningsområdet för NIS 2-direktivet.

275 §

Störningsanmälningar till Transport- och kommunikationsverket

Ett teleföretag ska utan dröjsmål göra en anmälan till Transport- och kommunikationsverket om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. Teleföretaget ska också utan obefogat dröjsmål anmäla hur länge störningen eller hotet beräknas

pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas.

Om det ligger i allmänt intresse att det görs en anmälan om en störning kan Transport- och kommunikationsverket ålägga teleföretaget att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Transport- och kommunikationsverket får meddela närmare föreskrifter om när en störning som avses i 1 mom. är betydande samt föreskrifter om innehållet i de anmälningar som avses i 1 mom. samt anmälningarnas utformning och hur de lämnas in.

Transport- och kommunikationsverket ska bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna. En sådan störning som avses i 1 mom. ska också vid behov anmälas till Europeiska unionens cybersäkerhetsbyrå. På störningsanmälningar tillämpas dessutom vad som i cybersäkerhetslagen föreskrivs om incidentanmälningar.

308 §

Myndighetssamarbete

— —

Transport- och kommunikationsverket ska samarbeta med de myndigheter som utövar tillsyn över nät- och informationssäkerheten i övriga medlemsstater i Europeiska unionen, enheter för hantering av it-säkerhetsincidenter samt den samarbetsgrupp, det CSIRT-nätverk och det europeiska kontaktnätverk för cyberkriser som avses i artiklarna 14–16 i NIS 2-direktivet.

313 §

Behandling av tillsynsärenden vid Transport- och kommunikationsverket

— —

Transport- och kommunikationsverket kan ställa sina tillsynsuppgifter enligt denna lag i viktighetsordning. Transport- och kommunikationsverket får lämna ett ärende utan prövning om

— —

2) ärendet trots en misstanke om fel eller försummelser endast har en ringa betydelse med tanke på kommunikationsmarknadens funktion, kommunikationstjänsternas tillförlitlighet eller tryggandet av störningsfri elektronisk kommunikation och med tanke på deras intressen som använder tjänsterna, eller

— —

318 §

Utlämnande av information från myndigheter

— —

Kommunikationsministeriet och Transport- och kommunikationsverket har rätt att lämna ut sekretessbelagda dokument till och röja sekretessbelagd information för kommissionen, för Organet för europeiska regleringsmyndigheter för elektronisk kommunikation och för tillsynsmyn-

digheterna i andra EES-stater, om det är nödvändigt för tillsynen över kommunikationsmarknaden. Transport- och kommunikationsverket har rätt att lämna ut en sekretessbelagd handling som det har fått med stöd av 170 § 1 mom. 7 punkten, 171 § samt 275 § 1 mom., och att röja sekretessbelagd information för tillsynsmyndigheten i en annan EES-stat och för den samarbetsgrupp som avses i artikel 14 i NIS 2-direktivet och det CSIRT-nätverk som avses i artikel 15 i det direktivet, om det är nödvändigt med tanke på övervakningen av nät- och informationssäkerheten, och utlämnandet inte äventyrar intressen gällande säkerhet och företagshemligheter för de aktörer som avses i de paragrafer som nämns ovan eller konfidentialiteten i fråga om de uppgifter som lämnas ut.

— —

342 §

Omprövning

— —

Omprövning får begäras av beslut som Transport- och kommunikationsverket fattat om radiotillstånd enligt 39 §, reservering av radiofrekvenser enligt 44 §, numrering enligt 100 §, förhindrande av registrering av domännamn enligt 167 § 2 mom., avregistrering av domännamn enligt 169 § 1 mom., marknadsbaserad frekvensavgift enligt 288 §, informationssamhällsavgift enligt 289 §, tillsynsavgiften för televisions- och radioverksamhet enligt 293 § och registrering enligt artikel 19.5 i dataförvaltningsakten.

— —

_____

Denna lag träder i kraft den 20 .

De föreskrifter som meddelats med stöd av 275 § i dess lydelse vid ikraftträdandet av denna lag förblir i kraft.

_____

4.

Lag

om upphävande av 128 a och 128 b § i luftfartslagen

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs i luftfartslagen (864/2014) 128 a och 128 b §, sådana de lyder i lag 965/2018.

2 §

Denna lag träder i kraft den 20 .

5.

Lag

om upphävande av 169 § i spårtrafiklagen

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs i spårtrafiklagen (1302/2018) 169 §.

2 §

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av lagen om transportservice

I enlighet med riksdagens beslut
upphävs i lagen om transportservice (320/2017) 161 §, sådan den lyder i lag 1256/2020, samt
ändras 140 §, sådan den lyder i lagarna 579/2018, 984/2018 och 371/2019, som följer:

140 §

Informationssäkerhet inom vägtrafikstyrnings- och vägtrafikledningstjänster

Bestämmelser om skyldighet för en leverantör av vägtrafikstyrnings- och vägtrafikledningstjänster att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder och för anmälan av avvikelser finns i cybersäkerhetslagen (/).

Leverantören av vägtrafikstyrnings- och vägtrafikledningstjänster ska registrera och förvara lägesbilden av vägtrafiken så att upptagningarna är skyddade mot obehörig insyn. Dessa upptagningar ska förvaras i 14 dygn.

_____

Denna lag träder i kraft den 20 .

_____

7.

Lag

om upphävande av 18 a § i lagen om fartygstrafikservice

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs i lagen om fartygstrafikservice (623/2005) 18 a §, sådan den lyder i lag 947/2018.

2 §

Denna lag träder i kraft den 20 .

8.

Lag

om upphävande av 7 e och 7 f § i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) 7 e och 7 f §, sådana de lyder i lag 955/2018.

2 §

Denna lag träder i kraft den 20 .

9.

Lag

om ändring av 2 och 90 § i lagen om behandling av kunduppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

ändras i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) 2 § 3 mom. och 90 § som följer:

2 §

Tillämpningsområde och förhållande till annan lagstiftning

— —

Denna lag innehåller bestämmelser som kompletterar och preciserar 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*) och cybersäkerhetslagen (/) vid behandlingen av kunduppgifter inom social- och hälsovården och uppgifter som kunden själv producerar om sitt välbefinnande i samband med ordnandet och tillhandahållandet av social- och hälsovårdstjänster.

90 §

Underrättelse om avvikelser från de väsentliga kraven på ett informationssystem eller en välbefinnandeapplikation samt om störningar i informationssäkerheten avseende informationsnät

Om en tjänstetillhandahållare eller ett apotek konstaterar betydande avvikelser när det gäller uppfyllandet av de väsentliga kraven på ett informationssystem, ska denna underrätta producenten av informationssystemtjänsten om saken. Om avvikelsen i informationssystemet eller välbefinnandeapplikationen kan innebära en betydande risk för klient- eller patientsäkerheten eller informationssäkerheten, ska tjänstetillhandahållaren, apoteket, producenten av informationssystemtjänsten eller tillverkaren av informationssystemet, tillverkaren av välbefinnandeapplikationen, Folkpensionsanstalten eller Institutet för hälsa och välfärd underrätta Tillstånds- och tillsynsverket för social- och hälsovården om detta. Även andra aktörer kan underrätta Tillstånds- och tillsynsverket för social- och hälsovården om risker som de upptäcker. Om avvikelsen i informationssystemet kan innebära en betydande risk för apotekets verksamhet, ska apoteket dessutom underrätta Säkerhets- och utvecklingscentret för läkemedelsområdet om detta. Bestämmelser om rapportering av personuppgiftsincidenter till dataombudsmannen finns i artikel 33 i dataskyddsförordningen.

En tjänstetillhandahållare, ett apotek, Folkpensionsanstalten och en producent av en informationssystemtjänst eller en tillverkare av ett informationssystem eller en mellanhand ska utan dröjsmål underrätta Tillstånds- och tillsynsverket för social- och hälsovården om sådana betydande störningar i anslutning till informationssäkerheten i de driftsmiljöer och informationsnät som aktören använder och till följd av vilka användningen av informationssystem och tillhandahållandet av social- och hälsovårdstjänster kan äventyras avsevärt. Tillstånds- och tillsynsverket för social- och hälsovården får meddela närmare föreskrifter om när en störning är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

Ett apotek ska dessutom utan dröjsmål underrätta Säkerhets- och utvecklingscentret för läkemedelsområdet om sådana betydande störningar i anslutning till informationssäkerheten i de driftsmiljöer och informationsnät som apoteket använder och till följd av vilka apotekets verksamhet kan äventyras avsevärt. Säkerhets- och utvecklingscentret för läkemedelsområdet får meddela närmare föreskrifter om när en störning är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

Om det ligger i allmänt intresse att det görs en anmälan om en sådan avvikelse eller störning i anslutning till informationssäkerheten som avses i 1 och 2 mom., får Tillstånds- och tillsynsverket för social- och hälsovården ålägga tjänstetillhandahållaren, apoteket, Folkpensionsanstalten, producenten av informationssystemtjänsten eller tillverkaren av informationssystemet eller mellanhanden att informera allmänheten om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken. Dessutom kan Säkerhets- och utvecklingscentret för läkemedelsområdet ålägga apoteket att informera allmänheten om en i 3 mom. avsedd störning eller, efter att ha hört den anmälningspliktiga, själv informera om störningen.

_____

Denna lag träder i kraft den 20 .

_____

10.

Lag

om ändring av elmarknadslagen

I enlighet med riksdagens beslut

upphävs i elmarknadslagen (588/2013) 29 a § och 49 a § 5 mom., sådana de lyder, 29 a § i lag 287/2018 och 49 a § 5 mom. i lag 108/2019, samt

ändras 62 § 1 mom., sådant det lyder i lag 497/2023, som följer:

62 §

Specialbestämmelser som gäller slutna distributionsnät

På slutna distributionsnät och deras innehavare tillämpas inte 23, 23 a och 26 a §, 27 § 3 mom., 28, 29, 29 b, 50–52, 52 a, 53, 53 a, 54–56, 56 a, 58, 59 § och 61 a § 2 mom.

— —

_____

Denna lag träder i kraft den 20 .

_____

11.

Lag

om upphävande av 34 a § i naturgasmarknadslagen

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs i naturgasmarknadslagen (587/2017) 34 a §, sådan den lyder i lagarna 288/2018 och 327/2020.

2 §

Denna lag träder i kraft den 20 .

12.

Lag

om ändring av 1 § i lagen om Energimyndigheten

I enlighet med riksdagens beslut

ändras i lagen om Energimyndigheten (870/2013) 1 § 2 mom. 19 punkten, sådan den lyder i lag 418/2019, samt

fogas till 1 § 2 mom., sådant det lyder delvis ändrat i lagarna 634/2020, 804/2020, 606/2021 och 500/2023, en ny 20 punkt som följer:

1 §

Uppgifter

— —

Energimyndigheten sköter de uppgifter som myndigheten har enligt

— —

19) lagen om främjande av användningen av biobrännolja (418/2019),

20) cybersäkerhetslagen (/).

— —

Denna lag träder i kraft den 20 .

13.

Lag

om ändring av lagen om tillsyn över el- och naturgasmarknaden

I enlighet med riksdagens beslut

ändras i lagen om tillsyn över el- och naturgasmarknaden (590/2013) 9 §, 23 § 4 och 5 punkten och 28 § 1 mom. 1 punkten, av dem 23 § 4 och 5 punkten sådana de lyder i lag 589/2017 och 28 § 1 mom. 1 punkten sådan den lyder i lag 1002/2018, samt

fogas till 2 §, sådan den lyder i lagarna 633/2020 och 499/2023, ett nytt 2 moment och till 23 §, sådan den lyder i lag 589/2017, en ny 6 punkt som följer:

2 §

Tillämpningsområde

— —

Bestämmelserna i 23 och 24 § tillämpas dessutom på skötseln av de uppgifter som Energimyndigheten har enligt cybersäkerhetslagen (/).

9 §

Energimyndighetens behörighet i tillsynsärenden

Om någon bryter mot eller försummar de förpliktelser som föreskrivs i den nationella lagstiftning eller EU-lagstiftning som avses i 2 § 1 mom., ska Energimyndigheten förplikta vederbörande att rätta till sin överträdelse eller försummelse. I beslutet kan det bestämmas hur överträdelsen eller försummelsen ska rättas. I beslutet kan det också bestämmas att en avgift som tagits ut felaktigt ska betalas tillbaka till kunden, om inte återbäringsförfarandet enligt 14 § tillämpas.

23 §

Återkallande av ett elnätstillstånd eller naturgasnätstillstånd

Energimyndigheten kan återkalla ett elnätstillstånd, naturgasnätstillstånd eller en befrielse eller ett undantagslov som avses i 12 § i elmarknadslagen eller 11 § i naturgasmarknadslagen, om

— —

4) tillståndshavaren upprepade gånger och i väsentlig grad bryter mot naturgasnätsförordningen eller en förordning eller ett beslut om riktlinjer som kommissionen antagit med stöd av den, till de delar de ska tillämpas i Finland, och den varning som i förväg getts tillståndshavaren om att tillståndet kommer att återkallas inte har lett till att bristerna i verksamheten har rättats till,

5) tillståndshavaren upprepade gånger och i väsentlig grad bryter mot bestämmelserna i lagen om åtskillnad av innehavare av överföringsnät för naturgas, och den varning som i förväg getts tillståndshavaren om att tillståndet kommer att återkallas inte har lett till att bristerna i verksamheten har rättats till, eller

6) tillståndshavaren upprepade gånger och i väsentlig grad bryter mot cybersäkerhetslagen (/), och den varning som i förväg getts tillståndshavaren om att tillståndet kommer att återkallas inte har lett till att bristerna i verksamheten har rättats till.

28 §

Energimyndighetens rätt att lämna ut uppgifter till andra myndigheter

Utöver det som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Energimyndigheten rätt att trots bestämmelserna om sekretess lämna ut uppgifter till

1) Finansinspektionen, Konkurrens- och konsumentverket och konsumentombudsmannen för att de ska kunna sköta sina uppgifter,

— —

_____

Denna lag träder i kraft den 20 .

_____

14.

Lag

om ändring av 35 § i lagen om vattentjänster

I enlighet med riksdagens beslut

ändras i lagen om vattentjänster (119/2001) 35 § 2 mom., sådant det lyder i lag 1013/2018, som följer:

35 §

Tystnadsplikt

— —

Trots tystnadsplikten enligt lagen om offentlighet i myndigheternas verksamhet får uppgifter om enskildas och sammanslutningars ekonomiska ställning eller företagshemligheter och enskildas personliga förhållanden, som erhållits vid utförande av uppgifter enligt denna lag, lämnas ut till

1) tillsynsmyndigheten för utförande av uppgifter som avses i denna lag, och

2) åklagar- och polismyndigheter för utredande av brott.

_____

Denna lag träder i kraft den 20 .

_____

15.

Lag

om ändring av 1 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut

ändras i lagen om verkställighet av böter (672/2002) 1 § 2 mom. 33 punkten, sådan den lyder i lagarna 1183/2023, 23/2024, 36/2014, 545/2024, 651/2024, 845/2024, 952/2024 och 1122/2024, samt

fogas till 1 § 2 mom. ~~i lagen om verkställighet av böter (672/2002)~~, sådant det lyder i lagarna 1183/2023, 23/2024, 36/2014, 545/2024, 651/2024, 845/2024, 952/2024 och 1122/2024, en ny 34 punkt som följer:

1 §

Lagens tillämpningsområde

— —

På det sätt som föreskrivs i denna lag verkställs också

— —

33) en påföljdsavgift enligt 11, 11 a och 11 e § och en felavgift enligt 12 § i lagen om främjande av användningen av förnybara drivmedel för transport (446/2007),

34) en påföljdsavgift enligt 35 § i cybersäkerhetslagen (/).

_____

Denna lag träder i kraft den 20 .

_____

16.

Lag

om ändring av 8 § i lagen om markstationer och vissa radaranläggningar

I enlighet med riksdagens beslut

ändras i lagen om markstationer och vissa radaranläggningar (96/2023) 8 § 1 mom. 3 punkten som följer:

8 §

Ändring och återkallelse av tillstånd

Den myndighet som beviljat tillstånd får ändra eller återkalla ett tillstånd till bedrivande av markstations- eller radarverksamhet, om

— —

3) verksamhetsutövaren på ett väsentligt sätt har försummat eller brutit mot en skyldighet eller begränsning som anges i denna lag eller i cybersäkerhetslagen (/) eller mot tillståndsvillkoren,

— —

_____

Denna lag träder i kraft den 20 .

17.

Lag

om ändring av lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor

I enlighet med riksdagens beslut

fogas till 5 § i lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (390/2005), sådan paragrafen lyder i lagarna 358/2015 och 794/2020, ett nytt 10 mom. och till lagen en ny 109 a § som följer:

5 §

Förhållandet till annan lagstiftning

— —

Bestämmelser om skyldigheterna att hantera och rapportera cybersäkerhetsrisker och om myndigheternas samarbete för att hantera cybersäkerhetsincidenter och cybersäkerhetsrisker finns i cybersäkerhetslagen (/).

109 a §

Återkallande av tillstånd till följd av försummelse av skyldigheter som gäller cybersäkerhet

Om verksamhetsutövaren väsentligt och allvarligt försummar skyldigheterna enligt cybersäkerhetslagen, ska tillsynsmyndigheten sätta ut en tillräcklig tidsfrist för verksamhetsutövaren för korrigering av saken. Om verksamhetsutövaren inte har korrigerat bristerna inom den utsatta tiden, kan tillsynsmyndigheten helt eller delvis återkalla det tillstånd att bedriva verksamhet som den beviljat.

Denna paragraf gäller verksamhet för vilken Säkerhets- och kemikalieverket är tillsynsmyndighet i enlighet med 115 §.

Denna lag träder i kraft den 20 .

Betänkande KoUB 1/2025 rd

Utskottets förslag till uttalande

Riksdagen förutsätter

1) att statsrådet noga följer hur lagens syften uppnås och hur lagen tillämpas och vid behov vidtar åtgärder för att avhjälpa observerade missförhållanden, och

2) att kommunikationsministeriet senast den 31 augusti 2026 lämnar kommunikationsutskottet en utredning om hur lagens syften har nåtts och hur lagen har tillämpats.

Helsingfors 27.2.2025

I den avgörande behandlingen deltog

ordförande Jouni Ovaska cent
vice ordförande Timo Furuholm vänst
medlem Pekka Aittakumpu saf
medlem Marko Asell sd
medlem Heikki Autto saml
medlem Seppo Eskelinen sd
medlem Atte Harjanne gröna
medlem Petri Huru saf
medlem Aleksi Jäntti saml (delvis)
medlem Marko Kilpi saml
medlem Sheikki Laakso saf
medlem Mats Löfström sv
medlem Anna-Kristiina Mikkonen sd
medlem Jani Mäkelä saf (delvis)
medlem Martin Paasi saml (delvis).

Sekreterare var

utskottsråd Mika Boedeker.