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

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att det stiftas en lag om hantering av cybersäkerhetsrisker. 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 och lagen om vattentjänster.

Genom propositionen 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 (*NIS2-direktivet*). Syftet med NIS 2-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 NIS 2-direktivet ska genomföras genom att det i en ny lag om hantering av cybersäkerhetsrisker 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 tidigare direktivet om nät- och informationssäkerhet som nu ska upphävas. När det gäller ordnandet av tillsynen fortsätter den sektorsvis uppdelade modellen. I propositionen föreslås för genomförande av NIS 2-direktivet 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 NIS 2-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. Regeringen förbättrar informationssäkerheten inom kritiska sektorer och genomför programmet för utveckling av cybersäkerheten (6.4). Regeringen ser över den nationella cybersäkerhetsstrategin så att den motsvarar vår förändrade omvärld (8.5). Dessutom ska cybersäkerheten stärkas i nära samarbete med företag, näringslivet och civilsamhället, med beaktande av att en stor del av den kritiska infrastrukturen är i privat ägo (8.5). I samband med genomförandet av EU-lagstiftningen undviks ytterligare nationell reglering (6.1).

Lagarna avses huvudsakligen träda i kraft den 18 oktober 2024.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL..... **VIRHE. KIRJANMERKKIÄ EI OLE MÄÄRITETTY.**
MOTIVERING 5
1 BAKGRUND OCH BEREDNING 5
1.1 Bakgrund 5
1.2 Beredning 5
1.2.1 Beredningen av EU-rättsakten 5
1.2.2 Beredningen av propositionen 6
2 EU-RÄTTSAKTENS MÅLSÄTTNING OCH HUVUDSAKLIGA INNEHÅLL 7
2.1 Målsättning 7
2.2 Tillämpningsområde 8
2.3 Väsentliga och viktiga entiteter 9
2.4 Register över entiteter 10
2.5 Riskhanteringsskyldigheter 10
2.6 Rapporteringsskyldigheter 11
2.7 Tillsyn och administrativa sanktioner 12
2.8 Samarbete mellan myndigheter 13
2.8.1 CSIRT-enheterna 13
2.8.2 Samordnad delgivning av information om sårbarheter och en sårbarhetsdatabas 13
2.8.3 CSIRT-nätverk, NIS-samarbetsgrupp och EU-CyCLONe 14
2.9 Strategi för cybersäkerhet och nationella ramar för hantering av cybersäkerhetskriser 14
2.10 Nationellt handlingsutrymme 14
3 NULÄGE OCH BEDÖMNING AV NULÄGET 15
3.1 Genomförandet av NIS 1-direktivet 15
3.2 Energi 16
3.2.1 Elektricitet 16
3.2.2 Olja 17
3.2.3 Naturgas 17
3.2.4 Fjärrvärme och fjärrkyla 17
3.2.5 Vätgas 18
3.3 Transporter 18
3.3.1 Lufttransport 18
3.3.2 Järnvägstransport 19
3.3.3 Vägtransport 20
3.3.4 Sjöfart 21
3.4 Bankverksamhet och finansmarknadsinfrastruktur 21
3.4.1 Nationella bestämmelser 21
3.4.2 DORA-förordningen 23
3.5 Hälso- och sjukvårdssektorn 24
3.5.1 Vårdgivare 24
3.5.2 EU-referenslaboratorier 25
3.5.3 Entiteter som bedriver forskning och utveckling avseende läkemedel och tillverkar läkemedel 25
3.5.4 Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan 26
3.6 Dricksvatten och avloppsvatten 26

3.7 Digital infrastruktur och digitala leverantörer 27
3.7.1 Digitala leverantörer 28
3.7.2 Domännamn 28
3.7.3 Kommunikationsnät och kommunikationstjänster 28
3.7.4 Betrodda elektroniska tjänster 29
3.8 Förvaltning av tjänster inom informations- och kommunikationsteknik (IKT-tjänster) 29
3.9 Rymden 30
3.10 Post- och budtjänster 30
3.11 Avfallshantering 31
3.12 Produktion, bearbetning och distribution av kemikalier 32
3.12.1 Kemikalier och explosiva varor 32
3.12.2 Bestämmelser om tryckbärande anordningar 34
3.13 Produktion, bearbetning och distribution av livsmedel 34
3.14 Tillverkningssektorn 36
3.14.1 Tillverkning av medicintekniska produkter 37
3.14.2 Tillverkning av datorer, elektronikvaror och optik 37
3.14.3 Tillverkning av elapparatur 38
3.14.4 Tillverkning av övriga maskiner 39
3.14.5 Tillverkning av motorfordon och släpfordon 41
3.14.6 Tillverkning av andra transportmedel 41
7 SPECIALMOTIVERING 108
7.1 Lagen om hantering av cybersäkerhetsrisker 108
7.2 Lag om ändring av lagen om informationshantering inom den offentliga förvaltningen 159
7.3 Lag om ändring av lagen om tjänster inom elektronisk kommunikation 183
7.4 Lag om upphävande av 128 a § och 128 b § i luftfartslagen 186
7.5 Lag om upphävande av 169 § i spårtrafiklagen 187
7.6 Lag om ändring av lagen om transportservice 187
7.7 Lag om upphävande av 18 a § i lagen om fartygstrafikservice. 188
7.8 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 188
7.9 Lag om ändring av lagen om behandling av kunduppgifter inom social- och hälsovården 188
7.10 Lag om ändring av elmarknadslagen 189
7.11 Lag om upphävande av 34 a § i naturgasmarknadslagen 190
7.12 Lag om ändring av 1 § i lagen om Energimyndigheten 190
7.13 Lag om ändring av 28 § i lagen om tillsyn över el- och naturgasmarknaden 190
7.14 Lag om ändring av 35 § i lagen om vattentjänster 190
LAGFÖRSLAG 214
Lag om hantering av cybersäkerhetsrisker 214
BILAGA I 237
BILAGA II 239
Lag om ändring av lagen om informationshantering inom den offentliga förvaltningen 240
Lag om ändring av lagen om tjänster inom elektronisk kommunikation 250
Lag om upphävande av 128 a och 128 b § i luftfartslagen 254
Lag om upphävande av 169 § i spårtrafiklagen 254
Lag om ändring av lagen om transportservice 255
Lag om upphävande av 18 a § i lagen om fartygstrafikservice 255
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 256
Lag om ändring av lagen om behandling av kunduppgifter inom social- och hälsovården 256

Lag om ändring av elmarknadslagen 257
Lag om upphävande av 34 a § i naturgasmarknadslagen 258
Lag om ändring av 1 § i lagen om Energimyndigheten 258
Lag om ändring av 28 § i lagen om tillsyn över el- och naturgasmarknaden 259
Lag om ändring av 35 § i lagen om vattentjänster 259

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Beredningen av propositionen har föranletts av Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (nedan *NIS 2-direktivet*). De lagstiftningsändringar som krävs för det nationella genomförandet av NIS 2-direktivet som ingår i denna proposition har beretts under ett förvaltningsövergripande beredningsprojekt som inrättats av kommunikationsministeriet.

NIS 2-direktivet ersätter EU:s direktiv om nät- och informationssäkerhet, Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan NIS 1-direktivet). Vid en översyn av NIS 1-direktivet framkom de aspekter som presenteras nedan och med anledning av dem har man kommit fram till att ersätta direktivet med det nya NIS 2-direktivet. NIS 1-direktivet genomfördes nationellt i huvudsak genom lagändringar (RP 192/2017 rd, KoUB 6/2018 rd och RSv 25/2018 rd) som trädde i kraft den 9 maj 2018. Dessutom har tillämpningsområdet för skyldigheterna utökats nationellt genom ändringar (RP 34/2018 rd, GrUU 16/2018 rd, KoUB 14/2018 rd och RSv 68/2018 rd) som trädde i kraft den 1 januari 2019.

NIS 2-direktivet ska genomföras nationellt senast den 17 oktober 2024 och de nationella bestämmelserna ska tillämpas från och med den 18 oktober 2024.

1.2 Beredning

1.2.1 Beredningen av EU-rättsakten

År 2020 såg Europeiska kommissionen (nedan *kommissionen*) över NIS 1-direktivet och hurdana erfarenheter medlemsstaterna hade av dess tillämpning. Kommissionen ordnade också ett offentligt samråd om NIS 1-direktivet under 2020. Finland svarade för sin del på det offentliga samrådet utifrån riktlinjerna för föregripande inflytande (E 107/2020 rd).

Kommissionen ansåg att den digitala utvecklingen i samhället, som påskyndats av covid-19-pandemin, på ett väsentligt sätt förändrat den nuvarande omvärlden och medfört nya utmaningar som kräver innovativa lösningar. Antalet cyberkränkningar har ökat och de har blivit allt mer avancerade. Cybersäkerhetsstörningar hindrar utövandet av verksamhet på den inre marknaden, genererar ekonomisk förlust, undergräver användarnas förtroende för unionens ekonomi och samhälle. Enligt kommissionen reformerar förslaget till nytt direktiv den befintliga lagstiftningsramen med beaktande av förändringarna på den inre marknaden. Förslaget är också ett led i EU:s strategi för cybersäkerhet (JOIN(2020) 18 final) och dess målsättningar.

Kommissionen lade den 16 december 2020 fram ett förslag till NIS 2-direktiv (COM(2020) 823 final). Samtidigt publicerade kommissionen en konsekvensbedömning i anslutning till direktivförslaget (SWD(2020) 345 final, på engelska). Direktivförslaget behandlades i den övergripande arbetsgruppen för cyberfrågor inom rådet och i parlamentets utskott för industrifrågor, forskning och energi.

Statsrådets U-skrivelse (U 9/2021 rd) om förslaget till direktiv lämnades till riksdagen den 11 februari 2021. Finland ansåg att förslaget till direktiv i huvudsak motsvarade det nationella föregripande påverkansarbetet och stödde målet med förslaget om att bättre svara mot den förändrade cybermiljön och vidareutveckla EU:s gemensamma cybersäkerhetsnivå. Enligt Finland är det viktigt att de nya skyldigheterna och kraven är proportionella och riskbaserade och att särdragen i de olika sektorerna beaktas. Dessutom är det enligt Finland viktigt att medlemsstaterna trots förslaget fortfarande har ett tillräckligt nationellt handlingsutrymme så att de också kan införa sådana nationella åtgärder som säkerställer en hög cybersäkerhetsnivå. Riksdagen omfattade statsrådets ståndpunkt med särskild tonvikt på bestämmelsernas noggrannhet och samordning med den övriga EU-lagstiftningen (KoUU 8/2021 rd, StoURS 15/2021 rd).

Om framskridandet och den fortsatta behandlingen av kommissionens direktivförslag lämnades en kompletterande skrivelse (UJ 23/2021 rd) till riksdagen den 20 december 2021. I den kompletterande skrivelsen ansågs att förslaget i sin helhet framskridit till stor del i linje med Finlands ståndpunkt. Riksdagen hade inga anmärkningar om statsrådets riktlinjer för verksamheten.

1.2.2 Beredningen av propositionen

Kommunikationsministeriet inrättade en arbetsgrupp till stöd för det nationella genomförandet av NIS 2-direktivet i januari 2023 (nedan *huvudarbetsgruppen*). Huvudarbetsgruppen hade till uppgift att bedöma vilka lagstiftningsändringar som behövs för genomförandet av direktivet och att gemensamt utarbeta en regeringsproposition om de behövliga lagstiftningsändringarna. Huvudarbetsgruppens presidium kom från kommunikationsministeriet och medlemmarna från justitieministeriet, finansministeriet, miljöministeriet, jord- och skogsbruksministeriet, arbets- och näringsministeriet, social- och hälsovårdsministeriet, inrikesministeriet, försvarsministeriet och utrikesministeriet. Undervisnings- och kulturministeriet och statsrådets kansli utnämnde ingen medlem till huvudarbetsgruppen. Huvudarbetsgruppens sekretariat bestod av representanter från kommunikationsministeriet och Transport- och kommunikationsverkets Cybersäkerhetscenter. Huvudarbetsgruppen sammankom x gånger.

Kommunikationsministeriet inrättade också en underarbetsgrupp till huvudarbetsgruppen och den inriktade sig på offentlig förvaltning (nedan *underarbetsgruppen*). Underarbetsgruppen hade till uppgift att bedöma och bereda genomförandet av skyldigheterna i NIS 2-direktivet med avseende på sektorn offentlig förvaltning som omfattas av direktivets tillämpningsområde (NIS 2-direktivet bilaga I punkt 10). Underarbetsgruppens presidium och sekretariat kom från finansministeriet och medlemmarna från kommunikationsministeriet, justitieministeriet, Skatteförvaltningen, arbets- och näringsministeriet, miljöministeriet, jord- och skogsbruksministeriet, social- och hälsovårdsministeriet, inrikesministeriet, försvarsministeriet, utrikesministeriet, statsrådets kansli, undervisnings- och kulturministeriet och Kommunförbundet. Underarbetsgruppen sammankom x gånger.

I början av 2023 bjöd huvudarbetsgruppen också in olika intresseorganisationer till arbetsgruppens möten. Under huvudarbetsgruppens möten hördes bland annat Finanssiala ry, Finlands näringsliv rf, FiCom ry, Finnish Information Security Cluster - Kyberala ry, Livsmedelsindustriförbundet rf, Finsk Energiindustri rf, Finlands Dagligvaruhandel rf och Kemiindustrin KI rf. Kommunikationsministeriet ordnade den 30 mars 2023 tillsammans med Transport- och kommunikationsverkets Cybersäkerhetscenter ett evenemang för intressentgrupper om det nationella genomförandet av NIS 2-direktivet och det var öppet för alla. Dessutom ordnade finansministeriet den 4 maj 2023 ett webbinarium särskilt för aktörer inom offentlig förvaltning och där berättades om bestämmelserna i NIS 2-direktivet och hur det ska genomföras nationellt inom sektorn för offentlig förvaltning. Material från de båda evenemangen finns i projektfönstret för

projektet för det nationella genomförandet (https://valtioneuvosto.fi/sv/projektet?tunnus=LVM044:00/2022)

Utöver arbetet i arbetsgrupper har det under beredningen ordnats tvåpartssamtal bland annat med beredarna av andra nationella projekt som rör det nationella genomförandet av NIS 2-direktivet för att samordna projekten. Sekretariaten för huvud- och underarbetsgrupperna har också diskuterat med kommissionen om vissa detaljer när det gäller det nationella genomförandet. Kommunikationsministeriet har dessutom varit i kontakt med andra EU-medlemsstater för sammanställandet av den internationella jämförelsen.

Under beredningen av regeringspropositionen lät kommunikationsministeriet utreda[1] vilka ekonomiska konsekvenser riskhanteringsskyldigheterna i NIS 2-direktivet får särskilt för livsmedels- och tillverkningssektorerna. Utredningen genomfördes utifrån de svar man fått med hjälp av intervjuer och en elektronisk enkät. I utredningen deltog sammanlagt 20 företag, av vilka 10 kom från livsmedelssektorn och 10 från tillverkningssektorn. Utredningen och resultaten av den har varit till nytta i konsekvensbedömningarna i propositionen. Med tanke på beredningen av det nationella genomförandet av NIS 2-direktivet utredde dessutom finansministeriet i februari och mars 2023 med hjälp av intervjuer den offentliga förvaltningens synpunkter bland annat på direktivets tillämpningsområde och den behöriga myndigheten inom offentlig förvaltning.

2 EU-rättsaktens målsättning och huvudsakliga innehåll

2.1 Målsättning

Målet med NIS 2-direktivet är att stärka EU:s gemensamma och medlemsstaternas nationella cybersäkerhetsnivå med avseende på kritiska sektorer och entiteter genom att ålägga medlemsstaterna att införa skyldigheter för de entiteter som omfattas av direktivets tillämpningsområde gällande riskhanteringsåtgärder vid cybersäkerhetsstörningar.

Genom NIS 2-direktivet försöker man undanröja de skillnader i genomförandet av NIS 1-direktivet som observerats mellan medlemsstaterna särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk, genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs.

I NIS 2-direktivet fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå i Europeiska unionens medlemsstater. Direktivet innehåller skyldigheter som ålägger medlemsstaterna att anta nationella strategier för cybersäkerhet och att inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser, gemensamma kontaktpunkter för cybersäkerhet och enheter för hantering av it-säkerhetsincidenter (Computer security incident response teams, nedan *CSIRT-enheter*). Dessutom innehåller direktivet regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet.

[1] Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille, Insta Advance Oy (2023).

2.2 Tillämpningsområde

Det allmänna tillämpningsområdet för NIS 2-direktivet anges i artikel 2 i direktivet. Rapporterings- och riskhanteringsskyldigheterna i NIS 2-direktivet gäller de väsentliga och viktiga entiteter som anges i artikel 3 i direktivet.

Med stöd av artikel 2 är direktivet tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga I eller II som tillhandahåller sina tjänster eller bedriver sin verksamhet i Europeiska unionen. Dessutom är en förutsättning att entiteten betecknas som medelstort företag enligt kommissionens rekommendation 2003/361/EG eller överstiger trösklarna för medelstora företag. I bilaga I listas närmare de typer av entiteter som omfattas av direktivets tillämpningsområde och bedriver verksamhet inom följande sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster, offentlig förvaltning och rymden. I bilaga II listas närmare de typer av entiteter som hör till direktivets tillämpningsområde och bedriver verksamhet inom följande sektorer: post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning, digitala leverantörer och forskning.

Med stöd av artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG är medelstora företag, det vill säga andra än mikro- och småföretag, företag som sysselsätter minst 50 personer eller vars årsomsättning och vars balansomslutning överstiger 10 miljoner euro per år. Företag som överstiger trösklarna i definitionen av ett medelstort företag är företag som sysselsätter minst 250 personer eller vars årsomsättning överstiger 50 miljoner euro och vars balansomslutning överstiger 43 miljoner euro per år. Artikel 3.4 i bilagan till kommissionens rekommendation om ett offentligt organs kontroll över entitetens kapital eller röstandel är inte tillämplig vid bedömningen av om en entitet omfattas av NIS 2-direktivets tillämpningsområde.

Små- och mikroföretag faller i princip utanför direktivets tillämpningsområde, om de inte berörs av ett undantag som gör att de hör till NIS 2-direktivets tillämpningsområde oavsett storlek. Oavsett entiteternas storlek är NIS 2-direktivet också tillämpligt på entiteter av en typ som avses i bilaga I eller II, om tjänster tillhandahålls av

a) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,
b) tillhandahållare av betrodda tjänster, eller
c) registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.

NIS 2-direktivet är dessutom tillämpligt oavsett entiteternas storlek på entiteter som definieras som kritiska entiteter enligt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (nedan *CER-direktivet*) och på entiteter som tillhandahåller domännamnsregistreringstjänster.

Oavsett entiteternas storlek är NIS 2-direktivet dessutom tillämpligt på entiteter av en typ som avses i bilaga I eller II, om

a) entiteten är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
b) en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa,

c) en störning av den tjänst som entiteten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser,
d) entiteten 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 medlemsstaten som är beroende av denna entitet.

I NIS 2-direktivet finns skyldigheter för den offentliga förvaltningens entiteter främst inom central- och regionförvaltningen oavsett deras storlek. För offentliga förvaltningsentiteter på regional nivå är en ytterligare förutsättning för att höra till NIS 2-direktivets minimitillämpningsområde att entiteten enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet. Direktivet gäller dock inte offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Direktivet gäller inte heller rättsväsendet, parlamenten eller centralbankerna. Det finns nationellt handlingsutrymme när det gäller huruvida bestämmelserna i direktivet ska vara tillämpliga på offentliga förvaltningsentiteter på lokal nivå och utbildningsinstitut.

Dessutom har medlemsstaterna nationellt handlingsutrymme att från riskhanterings- och rapporteringsskyldigheterna undanta entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Undantaget gäller nämnda verksamheter eller tjänster. Om den särskilda entiteten bedriver en sådan verksamhet eller tillhandahåller sådana tjänster som nämns ovan, omfattar det nationella handlingsutrymmet att också de registreringsskyldiga som avses i avsnitt 2.4 får undantas. Som ett undantag till detta ska bestämmelserna i direktivet tillämpas på både särskilda entiteter och offentliga förvaltningsentiteter, om entiteten är en tillhandahållare av betrodda tjänster.

NIS 2-direktivet är inte tillämpligt på entiteter som medlemsstaterna har undantagit från tillämpningsområdet för förordning (EU) 2022/2554 (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) i enlighet med artikel 2.4 i den förordningen.

2.3 Väsentliga och viktiga entiteter

Skyldigheterna i NIS 2-direktivet gäller de väsentliga och viktiga entiteter som definieras i artikel 3. Den viktigaste skillnaden mellan väsentliga och viktiga entiteter är beroende av vilka tillsynsbefogenheter som inriktas på dem i direktivet. I fråga om väsentliga entiteter ska tillsynen omfatta förhandstillsyn och efterhandstillsyn, medan det för viktiga entiteter enligt direktivet räcker med endast efterhandstillsyn.

Väsentliga entiteter är de entiteter som avses i bilaga I till direktivet och som överstiger de trösklar för medelstora företag som anges i definitionen (artikel 2.1 i bilagan till rekommendation 2003/361/EG). De övriga entiteter som uppfyller definitionen av väsentlig entitet listas i artikel 3.1 b–g. Exempelvis ska entiteter som med stöd av CER-direktivet definieras som kritiska entiteter betraktas som väsentliga entiteter. I fråga om sektorn offentlig förvaltning ska

offentliga förvaltningsentiteter på statlig nivå betraktas som väsentliga entiteter. Väsentliga entiteter är främst sådana entiteter som hört till tillämpningsområdet för NIS 1-direktivet.

Som viktiga entiteter betraktas de entiteter som inte uppfyller definitionen av en väsentlig entitet, men som är av en typ som avses i bilaga I eller II.

2.4 Register över entiteter

Enligt artikel 3 i NIS 2-direktivet ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. För upprättandet av förteckningen ska de väsentliga och viktiga entiteterna lämna viss minimiinformation till de behöriga myndigheterna. Förteckningen ska ses över och uppdateras regelbundet och minst vartannat år. Med stöd av förteckningen ska kommissionen och NIS-samarbetsgruppen underrättas om de uppgifter som anges i artikel 3.5.

Dessutom ska Europeiska unionens cybersäkerhetsbyrå Enisa med stöd av artikel 27 skapa ett register över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, internetbaserade sökmotorer och plattformar för sociala nätverkstjänster. Den nationella gemensamma kontaktpunkten ska lämna de uppgifter som behövs för att skapa och upprätthålla registret till Enisa.

2.5 Riskhanteringsskyldigheter

Riskhanteringsskyldigheterna i NIS 2-direktivet är skyldigheter på miniminivå och avsikten har varit att formulera dem så teknologineutralt som möjligt, för att de ska hålla under tid och vara tillämpliga på en stor grupp olika entiteter. Entiteterna kan om de vill ta i bruk mer långtgående riskhanteringsåtgärder och på nationell nivå är det i fortsättningen också möjligt att införa bestämmelser om strängare riskhanteringsskyldigheter. Riskhanteringsskyldigheterna finns i artikel 20 och 21.

Enligt artikel 20 ska väsentliga och viktiga entiteters ledningsorgan godkänna de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21 och övervaka genomförandet av dem. Ledningsorganen ska kunna ställas till svars för entiteternas överträdelser av artikel 21. Medlemmarna i ledningsorganen är skyldiga att genomgå utbildning och medlemsländerna ska uppmuntra dem att erbjuda utbildning också till sina anställda.

I artikel 21 anges de delområden som entiteterna ska beakta inom riskhanteringen och riskhanteringsåtgärderna. Dessa är

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering,

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,

e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation,

f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,
i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,
j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Enligt direktivet ska entiteterna genomföra riskhanteringsåtgärderna så att nivån på säkerheten är lämplig i förhållande till den föreliggande risken. Vid bedömningen ska hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. Medlemsstaterna ska säkerställa att entiteter, när de överväger lämpliga åtgärder, beaktar de sårbarheter som är specifika för den verksamhet som entiteten bedriver.

2.6 Rapporteringsskyldigheter

Det föreskrivs om rapporteringsskyldigheter i artikel 23 i NIS 2-direktivet. Väsentliga och viktiga entiteter underrättar sin CSIRT-enhet eller sin behöriga tillsynsmyndighet om betydande incidenter. En incident ska anses vara betydande om den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. Rapporteringsskyldigheten består av tre faser.

En tidig varning ska lämnas utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att man fått kännedom om den betydande incidenten. Varningen ska i tillämpliga fall ange om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar. När en incident har gränsöverskridande verkningar ska den rapporteras till de övriga medlemsstaterna som påverkas av incidenten och till Enisa.

Incidentanmälan ska lämnas utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att man har fått kännedom om den betydande incidenten. I anmälan ska i tillämpliga fall informationen i den tidiga varningen uppdateras och en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer anges.

En slutrapport ska utarbetas senast en månad efter inlämningen av incidentanmälan och den ska innehålla en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst incidenten, tillämpade och pågående begränsande åtgärder samt i tillämpliga fall, incidentens gränsöverskridande verkningar. I händelse av en pågående incident vid tidpunkten för inlämnandet av slutrapporten, ska entiteten tillhandahålla en lägesrapport. Slutrapporten ska lämnas in en månad efter det att hanteringen av incidenten avslutats.

En delrapport ska lämnas på begäran av en CSIRT-enhet eller av den behöriga myndigheten. CSIRT-enheten eller den behöriga myndigheten ska utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varningen lämna ett svar till den underrättande entiteten. I svaret ingår initial återkoppling om den betydande incidenten och på entitetens begäran vägledning och råd om hanteringen av konsekvenserna.

I artikel 30 i direktivet föreskrivs det om frivillig underrättelse av CSIRT-enheterna eller tillsynsmyndigheterna. Frivillig underrättelse betyder andra underrättelser än de om betydande incidenter som hör till underrättelseskyldigheten för de entiteter som omfattas av tillämpningsområdet. Med stöd av artikel 30 ska tillsynsmyndigheten inom sitt ansvarsområde ta emot underrättelser om incidenter, cyberhot och tillbud både från entiteter som omfattas av tillämpningsområdet för direktivet och från andra entiteter. De frivilliga underrättelserna ska behandlas på samma sätt som de underrättelser som bygger på rapporteringsskyldighet och tillsynsmyndigheten har rätt att vid behov ge behandling av obligatoriska underrättelser företräde. I Finland har de myndigheter som är behöriga enligt NIS 1-direktivet samt Transport- och kommunikationsverkets Cybersäkerhetscenter tagit emot också andra underrättelser än de som de är förpliktade till enligt direktivet, även om det inte funnits några separata bestämmelser om frivilliga underrättelser. Utöver underrättelsen till myndigheten ska entiteten utan onödigt dröjsmål underrätta de mottagare av deras tjänster som kan påverkas av cyberhotet om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta. När så är lämpligt ska mottagarna informeras också om själva cyberhotet. Om allmänhetens medvetenhet om en betydande incident är nödvändig, får en CSIRT-enhet eller den behöriga myndigheten informera allmänheten om den betydande incidenten eller ålägga entiteten att göra detta.

2.7 Tillsyn och administrativa sanktioner

I NIS 2-direktivet föreskrivs det om de minimikrav för tillsynsåtgärderna och tillsynsmedlen som tillsynsmyndigheterna ska kunna rikta in på väsentliga och viktiga entiteter. I artikel 31 i NIS 2-direktivet föreskrivs det om allmänna aspekter på tillsyn och efterlevnadskontroll, i artikel 32 om minimiåtgärder i fråga om väsentliga entiteter och i artikel 33 om minimiåtgärder i fråga om viktiga entiteter. I artikel 31 får medlemsstaterna möjlighet att tillåta att tillsynsåtgärderna prioriteras enligt en riskbaserad metod. I artikeln förutsätts dessutom att medlemsstaterna ska säkerställa att de behöriga myndigheterna är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas.

Syftet med NIS 2-direktivet är enligt skäl 122 i ingressen att fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för dessa entiteter och de behöriga myndigheterna. Väsentliga entiteter bör omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Med stöd av NIS 2-direktivet krävs det inte att viktiga entiteter rapporterar systematiskt till tillsynsmyndigheten om att de handlar i enlighet med riskhanteringsåtgärderna för cybersäkerhet, utan i fråga om de viktiga entiteterna ska tillsynsmyndigheten utöva efterhandstillsyn i stället för allmän tillsyn.

I fråga om de väsentliga entiteterna ska medlemsstaterna säkerställa att myndigheterna har befogenheter att utföra de åtgärder som listas i artikel 32.2 a–g. I de här åtgärderna ingår bland annat att utföra olika inspektioner och revisioner samt begäranden om tillgång till uppgifter, handlingar och information som behövs för att myndigheterna ska kunna utföra sina tillsynsuppgifter. Enligt artikel 32.4 ska dessutom medlemsstaterna säkerställa att tillsynsmyndigheten har de befogenheter som anges i led a–i, såsom att utfärda varningar, anta bindande instruktioner eller ålägga entiteter att upphöra med beteenden som utgör en överträdelse av direktivet. Dessutom bör tillsynsmyndigheten ha möjlighet att påföra eller begära att relevanta organ eller domstolar påför administrativa sanktionsavgifter. I artikel 34 finns minimivillkor för det högsta beloppet av administrativa sanktionsavgifter. Det högsta beloppet för en administrativ sanktionsavgift som väsentliga entiteter kan påföras är minst 10 000 000 euro eller 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst. Det högsta beloppet för en administrativ

sanktionsavgift som viktiga entiteter kan påföras är minst 7 000 000 euro eller 1,4 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst. Enligt artikel 34.7 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter.

Dessutom ska tillsynsmyndigheterna ha de befogenheter som avses i artikel 32.5 a–b i NIS 2-direktivet, om de andra efterlevnadskontrollerna är ineffektiva. Medlemsstaterna ska säkerställa att om entiteten oavsett uppmaning inte avhjälper de brister som upptäckts i verksamheten inom den fastställda tidsfristen, får den behöriga myndigheten bland annat tillfälligt upphäva en certifiering eller auktorisation för tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten samt begära att relevanta organ eller domstolar inför ett tillfälligt förbud för en fysisk person att utöva ledningsfunktioner i den entiteten. Enligt artikel 32.5 tredje stycket är följderna i punkt 5 inte tillämpliga på sådana offentliga förvaltningsentiteter som omfattas av direktivet.

Enligt artikel 33 ska medlemsstaterna föreskriva för tillsynsmyndigheterna om nästan motsvarande befogenheter att rikta in olika tillsynsåtgärder på de viktiga entiteterna. Tillsynsåtgärder får emellertid inriktas på viktiga entiteter endast, när medlemsstaterna får bevis, indikationer på eller information om att en viktig entitet påstås underlåta att fullgöra direktivet, särskilt artiklarna 21 och 23.

2.8 Samarbete mellan myndigheter

2.8.1 CSIRT-enheterna

Artikel 10 i NIS 2-direktivet ålägger varje medlemsstat att utse en eller flera CSIRT-enheter som har till uppgift att hantera it-säkerhetsincidenter. CSIRT-enheternas uppgifter har preciserats i artikel 11 enligt vilken en CSIRT-enhet bland annat ska övervaka och analysera cyberhot, sårbarheter och incidenter, tillhandahålla tidiga varningar, larm, meddelanden och spridning av information, stödja de entiteter som omfattas av direktivets tillämpningsområde, vidta åtgärder till följd av incidenter, samla in och analysera uppgifter om incidenter, vara situationsmedveten när det gäller cybersäkerhet och delta i CSIRT-nätverket. En noggrannare förteckning över CSIRT-enheternas uppgifter finns i artikel 11.3. Kraven som CSIRT-enheterna ska uppfylla finns i artikel 11.1. Dessutom ska CSIRT-enheterna ha teknisk kapacitet för att utföra sina uppgifter.

2.8.2 Samordnad delgivning av information om sårbarheter och en sårbarhetsdatabas

Enligt artikel 12 ska varje medlemsstat utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av informationen om sårbarheter. Samordnarens uppgift är att kontakta de berörda entiteterna, stödja dem som rapporterat och förhandla om tidsramar för delgivning av information. Dessutom ska samordnaren försöka hantera sårbarheter som påverkar flera entiteter. Enligt direktivet ska det gå att rapportera om sårbarheter anonymt.

Enisa ska utveckla och underhålla en europeisk sårbarhetsdatabas som ska innehålla information som beskriver sårbarheten, en lista över de IKT-produkter eller IKT-tjänster som påverkas av sårbarheten samt tillgången till programfixar eller vägledning om hur riskerna med sårbarheter kan begränsas.

2.8.3 CSIRT-nätverk, NIS-samarbetsgrupp och EU-CyCLONe

Mellan medlemsländerna skapar NIS 2-direktivet flera olika nätverk med avsikt att möjliggöra cybersäkerhetssamarbete inom EU. EU-nätverk som skapades redan under NIS 1-direktivet är NIS-samarbetsgruppen (artikel 14) och CSIRT-nätverket (artikel 15). Målet med NIS-samarbetsgruppen är att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit mellan länderna och den består av företrädare för medlemsstaterna, kommissionen och Enisa. CSIRT-nätverket består av företrädare för CSIRT-enheterna samt företrädare för incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU). Avsikten med nätverket är att bidra till förtroende och tillit och att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna.

Utöver de här nätverken skapas i NIS 2-direktivet ett nytt nätverk, Europeiska kontaktnätverket för cyberkriser (nedan *EU-CyCLONe*). EU-CyCLONe har till uppgift att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. EU-CyCLONe består av företrädare för medlemsstaternas myndigheter för hantering av cyberkriser samt, i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande påverkan på tjänster och verksamhet som omfattas av direktivet, kommissionen. I andra fall deltar kommissionen som observatör i arbetet inom nätverket.

2.9 Strategi för cybersäkerhet och nationella ramar för hantering av cybersäkerhetskriser

I artikel 7 i NIS 2-direktivet åläggs medlemsstaterna att anta en nationell strategi för cybersäkerhet i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. I artikeln föreskrivs också om minimiinnehållet i de nationella strategierna för cybersäkerhet. Kommissionen ska meddelas om nationella strategier för cybersäkerhet inom tre månader från det att de antagits. Medlemsstaterna ska regelbundet och minst vart femte år bedöma sina strategier för cybersäkerhet.

Den nationella ramen för hantering av cybersäkerhetskriser enligt NIS 2-direktivet består av en cyberkrishanteringsmyndighet och en plan för hanteringen av cyberkriser och dessa finns det bestämmelser om i artikel 9. Varje medlemsstat ska utse eller inrätta en eller flera cyberkrishanteringsmyndigheter som har till uppgift att hantera storskaliga cybersäkerhetsincidenter och kriser. I en plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Vissa uppgifter om cyberkrishanteringsmyndigheten och om krishanteringsplanen ska rapporteras också till kommissionen.

2.10 Nationellt handlingsutrymme

NIS 2-direktivet är minimiharmoniserande till sin karaktär. I regel finns inget nationellt handlingsutrymme när det gäller miniminivån på innehållet och de åtgärder som förutsätts i NIS 2-direktivet. Det viktigaste nationella handlingsutrymmet har dock att göra med att NIS 2-direktivet inte hindrar medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten (artikel 5).

Det handlingsutrymme som finns i fråga om direktivets minimitillämpningsområde beskrivs i avsnitt 2.2. Dessutom får det nationellt föreskrivas att skyldigheterna i NIS 2-direktivet också

inriktas på sådana entiteter som inte i övrigt omfattas av direktivet, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

I fråga om definitionen av väsentliga entiteter förekommer nationellt handlingsutrymme på så sätt att en medlemsstat till definitionen av väsentliga entiteter i NIS 2-direktivet också kan foga sådana entiteter som före den 16 januari 2023 har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med NIS 1-direktivet eller nationell rätt (artikel 3.1 g).

I artikel 9 som gäller nationella ramar för hantering av cybersäkerhetskriser lämnar direktivet nationellt handlingsutrymme på så sätt att en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, så kallade cyberkrishanteringsmyndigheter, kan utses eller inrättas. Om fler än en myndighet utses eller inrättas, ska medlemsstaten utse en av dessa till att samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

I NIS 2-direktivet krävs inte att de entiteter som omfattas av dess tillämpningsområde använder certifierade IKT-produkter, IKT-tjänster och IKT-processer, men medlemsstaterna får enligt artikel 24.1 kräva att väsentliga eller viktiga entiteter använder sådana certifierade IKT-produkter, IKT-tjänster och IKT-processer som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 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 (nedan *cybersäkerhetsakten*). Med stöd av artikel 24.2 har kommissionen befogenhet att anta delegerade akter för att komplettera vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt artikel 49 i cybersäkerhetsakten.

När det gäller tillsynen finns det i NIS 2-direktivet bestämmelser om miniminivån för de behöriga myndigheternas åtgärder för tillsyn och efterlevnadskontroll och där finns inget nationellt handlingsutrymme. Enligt NIS 2-direktivet får medlemsstaterna dock tillåta sina behöriga myndigheter att prioritera tillsyn (artikel 31.2). Denna prioritering ska baseras på en riskbaserad metod.

NIS 2-direktivet förutsätter möjligheten till påförande av administrativa sanktionsavgifter för väsentliga och viktiga entiteter. Nationellt handlingsutrymme finns dock i fråga om huruvida administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter och huruvida väsentliga och viktiga entiteter kan föreläggas viten (artikel 34.6 och 34.7).

3 Nuläge och bedömning av nuläget

3.1 Genomförandet av NIS 1-direktivet

NIS 1-direktivet genomfördes nationellt i huvudsak genom lagändringar (RP 192/2017 rd) som trädde i kraft den 9 maj 2018. Målet med NIS 1-direktivet var att förbättra cybersäkerhetsberedskapen på unionens territorium och införa rapporteringsskyldighet för väsentliga entiteter i fråga om informationssäkerhetsincidenter. Det har inte stiftats någon nationell, horisontell allmän lag om informations- och nätverkssäkerheten, utan NIS 1-direktivet har genomförts genom att skyldigheterna införlivats i den sektorsspecifika speciallagstiftningen. Övervakningen av att skyldigheterna kring informationssäkerheten fullgörs har splittrats mellan flera sektorsspecifika myndigheter.

Bestämmelser för att genomföra NIS 1-direktivet finns i lagen om tjänster inom elektronisk kommunikation (917/2014), luftfartslagen (864/2014), spårtrafiklagen (1302/2018), lagen om fartygstrafikservice (623/2005), lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004, nedan *lagen om sjöfartsskydd*), lagen om transportservice (320/2017), elmarknadslagen (588/2013), naturgasmarknadslagen (587/2017) och lagen om vattentjänster (119/2001). I den sektorsspecifika lagstiftningen finns bestämmelser om de viktigaste tjänsteleverantörernas skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och att anmäla informationssäkerhetsincidenter till tillsynsmyndigheten och allmänheten.

Tillsynen i enlighet med NIS 1-direktivet har ordnats sektorsspecifikt, det vill säga sektorsspecifika tillsynsmyndigheter övervakar enheterna inom sin egen sektor. Energimyndigheten, Transport- och kommunikationsverket, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården Valvira samt Närings-, trafik- och miljöcentralen i Södra Savolax har varit tillsynsmyndigheter.

Eftersom NIS 2-direktivet upphäver skyldigheterna i NIS 1-direktivet och det föreskrivs om nya skyldigheter för att nå ett motsvarande mål även för de entiteter som hört till NIS 1-direktivets tillämpningsområde, behöver den nationella lagstiftningen granskas i samband med genomförandet av NIS 2-direktivet.

3.2 Energi

I fråga om energisektorn hör sektorerna el, olja, gas, fjärrvärme och fjärrkylning samt vätgas till NIS 2-direktivets tillämpningsområde. Av dessa sektorer har el, olja och gas redan tidigare ingått i NIS 1-direktivet och enligt den nationella bedömningen hörde elnätsinnehavare och innehavare av överföringsnät för naturgas till leverantörerna av samhällsviktiga tjänster. Tillämpningsområdet för NIS 2-direktivet är betydligt större än tillämpningsområdet för NIS 1-direktivet. Hittills har Energimyndigheten varit tillsynsmyndighet för energisektorn.

3.2.1 Elektricitet

I elmarknadslagen finns bestämmelser om elmarknadens säkerhet. I samband med det nationella genomförandet av NIS 1-direktivet infördes nätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten (29 a §) i elmarknadslagen. Med anledning av genomförandet av NIS 2-direktivet behöver 29 a § i elmarknadslagen upphävas för att undvika överlappande bestämmelser. I elmarknadslagen finns också andra bestämmelser om säkerheten på elmarknaden, såsom skyldighet att utveckla nätet (19 §), ansvar för säker, tillförlitlig och effektiv drift av elnätet (21 c §), nätinnehavarens beredskapsplanering (28 §), nätinnehavarens samarbetsskyldighet vid störningar (29 §), kvalitetskrav i fråga om stamnätets funktion (40 §), kvalitetskrav i fråga om högspänningsdistributionsnätets funktion (50 §), kvalitetskrav i fråga om distributionsnätets funktion (51 §) samt distributionsnätsinnehavarens information till nätanvändarna vid störningar (59 §). Dessutom har Strålsäkerhetscentralen utfärdat ett Kärnsäkerhetsdirektiv (YVL-direktiv) om hantering av kärnkraftverkets informationssäkerhet med stöd av 7 r § i kärnenergilagen (990/1987). På EU-nivå finns bestämmelser om förebyggande och beredskap inför elkriser i Europaparlamentets och rådets förordning (EU) 2019/941 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG. I skäl 7 i ingressen beskrivs förordningens förhållande till NIS-bestämmelserna: ”Denna förordning kompletterar direktiv (EU) 2016/1148 genom att säkerställa att cyberincidenter, på rätt sätt identifieras som en risk och att de åtgärder

som vidtas mot dem återspeglas korrekt i riskberedskapsplanerna". Särskilda regler för cybersäkerhet inom elsektorn får utfärdas genom en nätföreskrift i enlighet med Europaparlamentets och rådets förordning (EU) 2019/943 om den inre marknaden för el.

3.2.2 Olja

I lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (390/2005, nedan *kemikaliesäkerhetslagen*) och i författningar som utfärdats med stöd av den finns bestämmelser om vissa säkerhetsförpliktelser för dem som hanterar, upplagrar, överför och förvarar olja. Lagstiftningen är i första hand inriktad på att avvärja fysiska hot som uppstår vid oljehanteringen, och informations- och cybersäkerheten har inte beaktats i lagstiftningen. I kemikaliesäkerhetslagen, lagen om tryckbärande anordningar (1144/2016) och Europaparlamentets och rådets förordning (EU) nr 305/2011 om fastställande av harmoniserade villkor för saluföring av byggprodukter och om upphävande av rådets direktiv 89/106/EG finns bestämmelser om säkerhetskrav på de cisterner och rörsystem som används vid oljeupplagring. Regleringen av kemikaliesäkerheten och tryckbärande anordningar beskrivs närmare i avsnitt 3.12 Tillverkning, produktion och distribution av kemikalier. I samband med genomförandet av NIS 1-direktivet gjordes inga ändringar i den nationella lagstiftningen för oljesektorns del, eftersom det i den sektorn inte kunde identifieras någon sådan väsentlig entitet eller tjänst som skulle ha uppfyllt kriterierna i direktivet på nationell nivå.

3.2.3 Naturgas

Kemikaliesäkerhetslagen är allmän lag även för säkerheten i fråga om naturgas. I kemikaliesäkerhetslagen finns bestämmelser om vissa skyldigheter för sektorns aktörer när det gäller riskhantering och rapportering. Dessa skyldigheter är främst inriktade på att avvärja materiella hot, och informations- och cybersäkerheten har inte beaktats i bestämmelserna. I förordningar som utfärdats av statsrådet med stöd av kemikaliesäkerhetslagen finns också bestämmelser om säkerheten vid hanteringen av naturgas. Bestämmelser om naturgasnätens säkerhet finns i naturgasmarknadslagen. I samband med det nationella genomförandet av NIS 1-direktivet fogades 34 a § om överföringsnätsinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten till naturgasmarknadslagen. Med anledning av genomförandet av NIS 2-direktivet behöver 34 a § i naturgasmarknadslagen ändras. Dessutom finns bestämmelser om säkerheten i naturgasnät i 14 § om skyldighet att utveckla nätet, 27 § om nätinnehavarens beredskapsplanering och 28 § om nätinnehavarens samarbetsskyldighet vid störningar. Enligt artikel 8.6 i Europaparlamentets och rådets förordning (EG) nr 715/2009 om villkor för tillträde till naturgasöverföringsnäten och om upphävande av förordning (EG) nr 1775/2005 kan man med hjälp av nätföreskrifter stärka bland annat reglerna för nätets driftsäkerhet och tillförlitlighet och rutiner och procedurer för störningssituationer. Naturgas lagras och hanteras också på andra ställen än i naturgasnät (bl.a. LNG-terminaler). Naturgas lagras, hanteras och överförs i trycksatt form. Regleringen av tryckbärande anordningar beskrivs närmare i avsnitt 3.12 Tillverkning, produktion och distribution av kemikalier.

3.2.4 Fjärrvärme och fjärrkyla

Operatörer av fjärrvärme eller fjärrkyla är nya inom tillämpningsområdet för cybersäkerhetsskyldigheterna i NIS 2-direktivet. Ingen informations- eller cybersäkerhetsreglering har identifierats vad gäller operatörer av fjärrvärme eller fjärrkyla. Fjärrvärme produceras i huvudsak i pannanläggningar som det finns säkerhetsbestämmelser om i lagen om tryckbärande anord-

ningar (1144/2016). Även andra trycksatta rörsystem lyder under lagen om tryckbärande anordningar. Regleringen av tryckbärande anordningar beskrivs närmare i avsnitt 3.12 Tillverkning, produktion och distribution av kemikalier.

3.2.5 Vätgas

Produktion, upplagring och överföring av vätgas har inte omfattats av tillämpningsområdet för NIS 1-direktivet. På motsvarande sätt som naturgas lagras och hanteras vätgas i trycksatt form, och lagen om tryckbärande anordningar är också tillämplig på hanteringen av vätgas. Kemikaliesäkerhetslagen är allmän lag för säkerheten också när det gäller vätgas. I kemikaliesäkerhetslagen finns bestämmelser om vissa skyldigheter för sektorns aktörer när det gäller riskhantering och rapportering. Dessa skyldigheter är främst inriktade på att avvärja materiella hot, och informations- och cybersäkerheten har inte beaktats i bestämmelserna. Någon allmän reglering av vätgasmarknaden finns inte i Finland för närvarande.

3.3 Transporter

Till tillämpningsområdet för NIS 2-direktivet hör vissa entiteter inom sektorerna lufttransport, järnvägstransport, vägtransport och sjöfart. I samband med det nationella genomförandet av NIS 1-direktivet infördes nätverks- och informationssäkerhetsskyldigheter för den som tillhandahåller trafikledningstjänster, flygtrafiktjänster, fartygstrafikservice och intelligenta trafiksystem, förvaltare av statens bannät samt innehavare av samhällsviktiga flygplatser och hamnar. Det finns väldigt få nationella bestämmelser om informations- och cybersäkerhet inom transportsektorn utöver det nationella genomförandet av NIS 1-direktivet. Inom transportsektorn har Transport- och kommunikationsverket varit tillsynsmyndighet för alla undersektorer. I spårtrafiklagen finns ingen separat bestämmelse om tillsynsansvar med tanke på spårtrafiksektorn.

3.3.1 Lufttransport

Luftfarten är en internationell verksamhet och lagstiftningen om den civila luftfarten bygger till största delen på internationella överenskommelser och EU-lagstiftning. EU har nyligen antagit flera rättsakter som gäller cybersäkerheten inom luftfarten. Rättsakter om cybersäkerhet som gäller säkerhetsåtgärder inom luftfarten är redan i kraft, men till vissa delar börjar rättsakterna om cybersäkerhet tillämpas först i oktober 2025 och februari 2026, det vill säga minst ett år senare än regleringen i NIS 2-direktivet. Bestämmelser om informationssäkerhet inom luftfarten finns i följande EU-rättsakter som är direkt tillämpliga:

Kommissionens genomförandeförordning (EU) 2015/1998 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd.	Tillämpas på flygplatsoperatörer, lufttrafikföretag och verksamhetsutövare enligt det nationella säkerhetsprogrammet för civil luftfart.
Kommissionens genomförandeförordning (EU) 2023/203 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340, kommissionens genomförandeförordningar (EU)	Tillämpas från och med den 22 februari 2026 på vissa underhållsorganisationer, organisationer som svarar för fortsatt luftvärdighet, luftfartygsoperatörer, utbildningsorganisationer, flygmedicinska centrum, leverantörer av

2017/373 och (EU) 2021/664, och för behöriga myndigheter som omfattas av kommissionens förordningar (EU) nr 748/2012, (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340 och (EU) nr 139/2014, kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664 och om ändring av kommissionens förordningar (EU) nr 1178/2011, (EU) nr 748/2012, (EU) nr 965/2012, (EU) nr 139/2014, (EU) nr 1321/2014, (EU) 2015/340, och kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664.	flygtrafik- och flyginformationstjänster, operatörer av utbildningshjälpmedel för flygsimulering (FSTD), leverantörer av U-space-tjänster och leverantörer av gemensamma informationstjänster för U-space-luftrum och myndigheter. Tillämpas från och med den 1 januari 2026 på leverantörer av flygtrafiktjänster för Egnos.
Kommissionens delegerade förordning (EU) 2022/1645 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014.	Tillämpas från och med den 16 oktober 2025 på vissa tillverkningsorganisationer och konstruktionsorganisationer, flygplatsoperatörer och leverantörer av ledningstjänster för trafik på plattan.

EU-regleringen av informationssäkerheten inom luftfarten är tillämplig på en större grupp entiteter än NIS 2-direktivet och de skyldigheter som entiteterna åläggs motsvarar i stor utsträckning NIS 2-kraven. Denna speciallagstiftning om luftfarten kan betraktas som en sådan sektorsspecifik unionsrättsakt som avses i artikel 4 i NIS 2-direktivet.

När det gäller luftfarten har NIS 1-direktivet genomförts genom att det till luftfartslagen fogats 128 a och 128 b § om riskhanteringen i fråga om kommunikationsnät och informationssystem och rapportering av informationssäkerhetshändelser. Med stöd av 128 a § i luftfartslagen har också statsrådets förordning om samhällsviktiga flygplatser och hamnar (361/2018) utfärdats och i den anges de samhällsviktiga flygplatserna och hamnarna. Enligt förordningen är Helsingfors-Vanda flygplats och Åbo flygplats sådana flygplatser.

Med anledning av genomförandet av NIS 2-direktivet behöver 128 a och 128 b § i luftfartslagen upphävas för att undvika överlappande bestämmelser. Samtidigt upphävs statsrådets förordning om samhällsviktiga flygplatser och hamnar som utfärdats med stöd av 128 a § i luftfartslagen och 7 e § i lagen om sjöfartsskydd. NIS 2-direktivets tillämpningsområde förutsätter inte att de samhällsviktiga flygplatserna och hamnarna fastställs i en förordning av statsrådet.

3.3.2 Järnvägstransport

Nationella bestämmelser om järnvägarnas säkerhet finns i spårtrafiklagen och i 2 kap. finns de viktigaste bestämmelserna om järnvägssäkerheten. Genom spårtrafiklagen har Europaparlamentets och rådets direktiv (EU) 2016/798 om järnvägssäkerhet och Europaparlamentets och rådets direktiv (EU) 2016/797 om driftskompatibiliteten hos järnvägssystemet inom Europeiska unionen genomförts. Med stöd av dessa direktiv har också flera direkt tillämpliga delegerade

akter och genomförandeakter antagits. I spårtrafiklagen har NIS 1-direktivet till stora delar genomförts genom 169 § som ålägger förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder och att anmäla om informationssäkerhetsrelaterade störningar. Dessutom ger 169 § Transport- och kommunikationsverket befogenhet att informera om störningar, underrätta de övriga EES-staterna om störningar samt meddela närmare föreskrifter om när en sådan störning är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

Med anledning av genomförandet av NIS 2-direktivet behöver 169 § i spårtrafiklagen upphävas för att undvika överlappande bestämmelser. Det finns inga gällande informations- eller cybersäkerhetsbestämmelser om järnvägsföretag eller tjänsteleverantörer.

Den nationella lagstiftning som bygger på NIS 1-direktivet gäller inte förvaltare av privata spåranläggningar. I hamnområdena hos innehavare av samhällsviktiga hamnar finns också privata spåranläggningar, men i lagen om sjöfartsskydd har det inte tolkats som att riskhanteringsskyldigheten i fråga om kommunikationsnät och informationssystem för hamninnehavare gäller dessa privata spåranläggningar i havshamnar.

I 171 § i spårtrafiklagen finns bestämmelser om beredskapsskyldighet för bannätsförvaltare, tillhandahållare av trafikledningstjänster för järnvägar och tillhandahållare av trafikledningstjänster på metrobannät och spårvägsnät under undantagsförhållanden och vid störningar under normala förhållanden. Dessutom finns det i lagen om transportservice bestämmelser om skyldighet för järnvägsoperatörer (58 §) och för utövare av spårbunden stadstrafik (66 §) att förbereda sig för störningar under normala förhållanden och för undantagsförhållanden. Transport- och kommunikationsverket har utfärdat föreskriften Ordnande av beredskapsplanering i transportsystemet, som innehåller små krav på cybersäkerhet för bannätsförvaltare, tillhandahållare av trafikledningstjänster och i tillämpliga delar inom spårbunden stadstrafik. Entiteter inom den spårbundna stadstrafiken hör inte till tillämpningsområdet för NIS 2-direktivet. Föreskriften gäller också vissa aktörer inom luftfart och vägtrafik, men för deras del innehåller föreskriften inga krav på cybersäkerhet.

3.3.3 Vägtransport

Bestämmelser om riskhanterings- och rapporteringsskyldigheterna i NIS 1-direktivet finns i lagen om transportservice i fråga om aktörer som tillhandahåller trafikstyrnings- och trafikledningstjänster inom vägtrafiken. Skyldigheterna i NIS 1-direktivet genomfördes nationellt genom att till lagen foga 140 § om informationssäkerhet inom vägtrafikstyrnings- och vägtrafikledningstjänster och 141 § om skyldigheten att göra avvikelseanmälningar inom vägtrafikstyrnings- och vägtrafikledningstjänster. Med anledning av det nationella genomförandet av NIS 2-direktivet behöver 140 § i lagen om transportservice ändras.

Bestämmelser om införandet av intelligenta transportsystem finns i Europaparlamentets och rådets direktiv 2010/40/EU om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (nedan ITS-direktivet). ITS-direktivet har genomförts nationellt genom lagen om transportservice. I samband med genomförandet av NIS 1-direktivet fogades 161 § till lagen om transportservice och den gäller skyldigheten för den som tillhandahåller intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och anmäla om störning i informationssäkerheten. Med anledning av genomförandet av NIS 2-direktivet behöver 161 § i lagen om transportservice upphävas för att undvika överlappande bestämmelser.

3.3.4 Sjöfart

Bestämmelser om de operatörer av sjötrafikinformationstjänster som omfattas av NIS 2-direktivets tillämpningsområde finns i lagen om fartygstrafikservice. Enligt 16 § 5 mom. i lagen om fartygstrafikservice ska leverantören av fartygstrafikservice, det vill säga VTS-tjänsteleverantören, sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. Med fartygstrafikservice avses enligt definitionen i 2 § 1 mom. sådan övervakning och ledning av fartygstrafiken som har beredskap att samverka med trafiken och reagera på föränderliga trafiksituationer. Dessutom finns det i 18 a § bestämmelser om anmälan om störningar i anslutning till informationssäkerheten och i 28 § 4 mom. om tillsynen över informationssäkerhetsskyldigheterna. Med anledning av genomförandet av NIS 2-direktivet behöver 18 a § i lagen om fartygstrafikservice upphävas för att undvika överlappande bestämmelser.

NIS 2-direktivet är också tillämpligt på ledningsenheter för hamnar samt de enheter som sköter anläggningar och utrustning i hamnar. Säkerhetsåtgärderna i hamnar och hamnanläggningar bygger på bestämmelserna i den internationella SOLAS-konventionen och på den tillhörande ISPS-koden. Koden har genomförts genom Europaparlamentets och rådets förordning (EG) nr 725/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (nedan *EU:s förordning om sjöfartsskydd*).

De nationella bestämmelser som kompletterar EU:s förordning om sjöfartsskydd finns i lagen om sjöfartsskydd, genom vilken även Europaparlamentets och rådets direktiv 2005/65/EG om ökat hamnskydd har genomförts. I samband med genomförandet av NIS 1-direktivet fogades 7 e och 7 f § till lagen om sjöfartsskydd och de ålägger innehavare av samhällsviktiga hamnar att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder och att anmäla om störningar i informationssäkerheten. Med stöd av 7 e § har dessutom statsrådets förordning om samhällsviktiga flygplatser och hamnar (361/2018) utfärdats, och i den anges de flygplatser och hamnar som är samhällsviktiga. Dessa hamnar är Fredrikshamn, Kotka, Helsingfors, Åbo och Nådendal. Den nationella definitionen av en hamninnehavare i förhållande till den typ av entitet som anges i bilagan till NIS 2-direktivet kan kräva precisering.

Med anledning av genomförandet av NIS 2-direktivet behöver 7 e och 7 f § i lagen om sjöfartsskydd upphävas för att undvika överlappande bestämmelser. Samtidigt upphävs statsrådets förordning om samhällsviktiga flygplatser och hamnar som utfärdats med stöd av 7 e § i lagen om sjöfartsskydd och 128 a § i luftfartslagen. NIS 2-direktivets tillämpningsområde förutsätter inte att de samhällsviktiga flygplatserna och hamnarna fastställs i en förordning av statsrådet.

För sjöfartens del är NIS 2-direktivet också tillämpligt på transportföretag som bedriver persontrafik och godstrafik, exklusive de enskilda fartyg som drivs av dessa företag, och på enheter som sköter anläggningar och utrustning i hamnar. De här entiteterna har också hört till sektorerna i NIS 1-direktivet. I samband med det nationella genomförandet av NIS 1-direktivet gjordes inga ändringar i den nationella lagstiftningen i fråga om dessa entiteter, eftersom det i dessa sektorer på nationell nivå inte kunde identifieras någon sådan väsentlig entitet eller tjänst som skulle ha uppfyllt kriterierna i direktivet.

3.4 Bankverksamhet och finansmarknadsinfrastruktur

3.4.1 Nationella bestämmelser

Av finanssektorns entitetstyper omfattas kreditinstitut, operatörer av handelsplatser och centrala motparter av tillämpningsområdet för NIS 2-direktivet. Samma entiteter har också omfattats av

NIS 1-direktivets tillämpningsområde. I samband med genomförandet av NIS 1-direktivet bedömdes att sådan kreditinstitutsverksamhet som avses i kreditinstitutslagen (610/2014) och bedrivandet av sådan börsverksamhet som avses i lagen om handel med finansiella instrument (1070/2017) omfattas av regleringen.

Allmänna krav som ska ställas på kreditinstituts riskhanteringssystem finns i 9 kap. 2 § i kreditinstitutslagen. I 9 kap. 16 § 2 mom. i kreditinstitutslagen bestäms att kreditinstitut ska ha adekvata, trygga och funktionssäkra datasystem och i 16 § 3 mom. krävs att kreditinstitut ska upprätta beredskaps- och kontinuitetsplaner så att det är möjligt att bereda sig för störningar, säkerställa förmågan att fortlöpande bedriva verksamhet och begränsa förlusterna i störningssituationer. I 5 kap. 10 och 11 § finns bestämmelser om utläggande på entreprenad och förutsättningarna för detta och i kapitlets 16 § om skyldighet att vidta förberedelser för störningar. I fråga om kreditinstituten har Finansinspektionen varit den myndighet som övervakat att de här åläggandena har iakttagits.

I lagen om handel med finansiella instrument finns riskhanterings- och rapporteringsskyldigheter i fråga om aktörer som bedriver börsverksamhet. I 3 kap. 1 § finns krav som gäller organisering av verksamheten på en reglerad marknad, vilket ålägger aktörerna att säkerställa systemens motståndskraft och den verksamhetsrelaterade riskhanteringen. Enligt 3 kap. 2 § 2 mom. är börsen dessutom skyldig att underrätta Finansinspektionen, som är tillsynsmyndighet för börsverksamheten, om vissa störningar.

Finansinspektionens föreskrifter och anvisningar om hantering av operativa risker i företag under tillsyn inom finanssektorn (8/2014, uppdaterad 16.2.2022) preciserar skyldigheterna kring den operativa riskhanteringen inom kreditinstitut och börsverksamhet. I 6 kap. i föreskriften finns skyldigheter som gäller informationssystem och informationssäkerhet och 9 kap. behandlar rapporteringen till Finansinspektionen. Enligt 9.1 (2) ska en första anmälan till Finansinspektionen om betydande störningar och fel i tjänster som tillhandahålls för kunderna och i betalnings- och it-systemen göras omedelbart när de yppat sig. Enligt 9.1 (4) ska tillsynsobjektet lämna in en kompletterande anmälan till Finansinspektionen om de närmare detaljerna i störningen så snabbt som möjligt efter den första anmälan och en slutrapport efter att den egentliga orsaken till störningen har utretts. Finansinspektionen har också gett en föreskrift om utläggning av verksamhet (Föreskrifter och anvisningar 1/2012, ändrad 23.1.2018).

De här nationella skyldigheterna har ansetts uppfylla de krav på riskhantering och rapportering som har förutsatts i NIS 1-direktivet av de leverantörer av samhällsviktiga tjänster som hört till dess tillämpningsområde. Därför förutsatte genomförandet av NIS 1-direktivet inga ändringar i den nationella lagstiftningen om bank- och finanssektorn.

I NIS 2-direktivet har bankverksamhet och finansmarknadsinfrastruktur i bilaga I, som omfattar samma typ av entiteter, definierats som högkritiska sektorer och de betraktas således som väsentliga entiteter när trösklarna överskrids. I NIS 2-direktivet åläggs entiteterna mer detaljerade och omfattande riskhanterings- och rapporteringsskyldigheter än i NIS 1-direktivet. I samband med detta är det skäl att notera 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*).

3.4.2 DORA-förordningen

DORA-förordningen publicerades samtidigt som NIS 2-direktivet och den ska tillämpas 24 månader efter att den trätt i kraft. Syftet med DORA-förordningen är att stärka säkerheten i nätverks- och informationssystem som stöder finansmarknadens affärsprocesser. Bestämmelserna gäller riskhantering inom informations- och kommunikationsteknik (IKT), rapportering av allvarliga IKT-relaterade incidenter och underrättande om, på frivillig grund, betydande cyberhot till de behöriga myndigheterna, vissa finansiella entiteters rapportering av allvarliga betalningsrelaterade incidenter, testning av digital operativ motståndskraft, utbyte av information och underrättelser i samband med cyberhot och cybersårbarheter samt åtgärder för hantering av tredjepartsrelaterad IKT-risk. I förordningen finns dessutom bestämmelser om de krav i samband med de kontraktsmässiga arrangemang som har ingåtts mellan tredjepartsleverantörer av IKT-tjänster och finansiella entiteter och om den tillsynsram som tillämpas på för finansiella entiteter kritiska tredjepartsleverantörer av IKT-tjänster.

I skäl 16 i ingressen till DORA-förordningen och skäl 28 i ingressen till NIS 2-direktivet anges att förordningen utgör speciallagstiftning (lex specialis) i förhållande till NIS 2-direktivet. I DORA-förordningen åläggs finanssektorns entiteter mera långtgående skyldigheter att förbereda sig inför cyberhot än vad som krävs i NIS 2-direktivet. Enligt ingresserna ska bestämmelserna i NIS 2-direktivet om hanteringen av cybersäkerhetsrisker, rapporteringsskyldigheter, tillsyn och efterlevnadskontroll inte tillämpas på finansiella entiteter, utan på dem tillämpas DORA-förordningen. Samtidigt har man också identifierat ett behov att bevara starka förbindelser mellan finanssektorn och de myndigheter som avses i NIS 2-direktivet samt att garantera att informationsutbytet med finanssektorn fungerar. Dessutom ska medlemsstaterna fortsättningsvis inkludera finanssektorn i sina strategier för cybersäkerhet och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet. De behöriga myndigheter som inrättas enligt DORA-förordningen ska kunna samråda med de nationella CSIRT-enheterna och samarbeta med dem. DORA-förordningens tillämpningsområde är stort och omfattar nästan alla entiteter som nämns i EU:s finansmarknadslagstiftning. Närmare bestämmelser om tillämpningsområdet finns i artikel 2 i förordningen.

I förhållandet mellan DORA-förordningen och NIS 2-direktivet är det viktigaste att informationen om IKT-händelser måste löpa mellan både myndigheterna och de finansiella entiteterna. Den behöriga myndigheten enligt DORA-förordningen ska dela information om betydande händelser också till övriga myndigheter. De behöriga myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna enligt NIS 2-direktivet ska utföra ett lämpligt samarbete med medlemsstaternas brottsbekämpande myndigheter, dataskyddsmyndigheter och behöriga myndigheter enligt DORA-förordningen.

DORA-förordningen ålägger finansiella entiteter att genomföra en process för hantering av IKT-relaterade incidenter (artikel 17) och klassificera incidenter (artikel 18). Finansiella entiteter ska dessutom enligt artikel 19 rapportera allvarliga incidenter till den behöriga myndigheten. Cyberhot får också rapporteras på frivillig basis, om det inte finns någon skyldighet att rapportera incidenten, men entiteten anser att incidenten är relevant. De behöriga myndigheter som utsetts i EU:s gällande sektorsspecifika finansmarknadslagstiftning kommer i regel också att vara behöriga myndigheter enligt DORA-förordningen, och de ska ha den befogenhet som förutsätts i rättsakterna. I Finland kommer denna myndighet att vara Finansinspektionen. Enligt artikel 47 får de behöriga myndigheterna när så är lämpligt samråda och utbyta information med den gemensamma kontaktpunkten och de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS 2-direktivet samt när så är lämpligt av dem begära teknisk rådgivning och tekniskt stöd och ingå samarbetsarrangemang som gör det möjligt att inrätta effektiva och snabba samordningsmekanismer.

3.5 Hälso- och sjukvårdssektorn

Till tillämpningsområdet för NIS 2-direktivet hör vårdgivare, EU-referenslaboratorier, entiteter som bedriver forskning och utveckling avseende läkemedel, entiteter som tillverkar vissa farmaceutiska basprodukter och läkemedel och entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan. Tillämpningsområdet är betydligt större än i NIS 1-direktivet, till vilket endast hörde hälso- och sjukvårdsmiljöer för hälso- och sjukvårdssektorns del. I samband med att NIS 1-direktivet genomfördes ansågs den gällande lagstiftningen uppfylla kraven i direktivet, varför det inte gjordes några ändringar i den nationella lagstiftningen.

3.5.1 Vårdgivare

Till tillämpningsområdet för NIS 2-direktivet hör vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård. Enligt artikel 3 g i det direktivet avses med ’vårdgivare’ varje fysisk eller juridisk person eller varje annan entitet som lagligen bedriver hälso- och sjukvård på en medlemsstats territorium.

I lagen om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021, nedan *kunduppgiftslagen*) finns bestämmelser om social- och hälsovårdens informationssystem och deras säkerhetskrav. Enligt 7 § är tjänstetillhandahållarna skyldiga att ansluta sig som användare av de riksomfattande informationssystemtjänsterna (Kanta-tjänsterna). Bestämmelsen gäller såväl offentliga tillhandahållare som privata aktörer om de använder ett informationssystem som är avsett för behandling av klient- och patientuppgifter. I 14 § i kunduppgiftslagen förutsätts att en arkiveringstjänst ska skyddas i enlighet med de skyldigheter som gäller statliga myndigheters informationssäkerhet. Det finns bestämmelser om de här skyldigheterna i lagen om informationshantering inom den offentliga förvaltningen (906/2019). I 4 kap. i den lagen finns bestämmelser om informationssäkerhet, i synnerhet om informationssäkerhet i fråga om informationsmaterial och informationssystem i 13 § och information om och beredskap för störningssituationer i 13 a §.

I 27 § i kunduppgiftslagen åläggs en tjänstetillhandahållare, en mellanhand och Folkpensionsanstalten att utarbeta en informationssäkerhetsplan med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen. Enligt 39 § svarar Institutet för hälsa och välfärd för planeringen, styrningen och uppföljningen av de riksomfattande informationssystemtjänsterna. Institutet för hälsa och välfärd får dessutom befogenhet att meddela närmare säkerhetsföreskrifter. Enligt lagen ska en aktör underrätta Tillstånds- och tillsynsverket för social- och hälsovården om en betydande avvikelse i informationssystemet, om en avvikelse kan innebära en betydande risk för kundsäkerheten eller informationssäkerheten (41 §).

Kunduppgiftslagen har nyligen uppdaterats (RP 246/2022 rd, lag 703/2023) och i samband med detta fogades till lagen en ny 77 § enligt vilken tjänstetillhandahållare, apotek, mellanhänder och Folkpensionsanstalten ska utarbeta en informationssäkerhetsplan med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen. Dessutom fogades till lagen en ny 90 § enligt vilken aktörerna ska underrätta om avvikelser när det gäller uppfyllandet av de väsentliga kraven på ett informationssystem eller en välbefinnandeapplikation samt om störningar i anslutning till informationssäkerheten i informationsnät. Ändringarna träder i kraft den 1 januari 2024. Med anledning av genomförandet av NIS 2-direktivet behöver 90 § i kunduppgiftslagen ändras.

3.5.2 EU-referenslaboratorier

Bestämmelser om EU-referenslaboratorier finns 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. Enligt artikel 15.1 i förordningen får kommissionen på folkhälsoområdet eller för specifika områden inom folkhälsa som är relevanta för genomförandet av förordningen eller av de nationella planerna för förebyggande åtgärder, beredskap och insatser genom genomförandeakter utse EU-referenslaboratorier som ska ge stöd till nationella referenslaboratorier för att främja god praxis och medlemsstaternas frivilliga harmonisering av diagnostik, testmetoder och användning av vissa tester för medlemsstaternas enhetliga övervakning, anmälan och rapportering av sjukdomar.

Enligt artikel 15.2 i förordningen ska EU-referenslaboratorierna ansvara för samordningen av nätverket av nationella referenslaboratorier. Enligt artikel 15.3 ska European Centre for Disease Prevention and Control (ECDC) i samarbete med WHO:s referenslaboratorier svara för driften och samordningen av nätverket av EU-referenslaboratorier. Enligt artikel 15.5 ska EU-referenslaboratorierna vara opartiska, fria från intressekonflikter och i synnerhet inte befinna sig i en situation som direkt eller indirekt kan påverka deras yrkesetiska opartiskhet när de utför sina uppgifter som EU-referenslaboratorier, ha, eller ha avtalsenlig tillgång till, lämpligt kvalificerad personal med adekvat utbildning inom sitt kompetensområde, förfoga över, eller ha tillgång till, den infrastruktur, den utrustning och de produkter som krävs för att utföra de uppgifter som de ålagts, säkerställa att deras personal och eventuell kontraktsanställd personal har god kännedom om internationella standarder och internationell praxis, och att den senaste forskningen på nationell nivå, unionsnivå och internationell nivå beaktas i deras arbete, vara utrustade med, eller ha tillgång till, den utrustning som krävs för att de ska kunna utföra sina uppgifter i krissituationer samt när så är relevant vara utrustade för att följa relevanta standarder för bioskydd.

Det finns ingen nationell lagstiftning som kompletterar EU-bestämmelserna om EU-referenslaboratorierna. Behovet av nationell lagstiftning övervägs när det på EU-nivå finns anvisningar som kompletterar förordningen.

3.5.3 Entiteter som bedriver forskning och utveckling avseende läkemedel och tillverkar läkemedel

Till tillämpningsområdet för NIS 2-direktivet hör de entiteter som bedriver forskning och utveckling avseende de läkemedel som definieras i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG om upprättande av gemenskapsregler för humanläkemedel. Med läkemedel avses enligt artikel 1.2 i direktiv 2001/83/EG varje substans eller kombination av substanser som tillhandahålls med uppgift om att den har egenskaper för att behandla eller förebygga sjukdom hos människor, eller varje substans eller kombination av substanser som kan användas på eller administreras till människor i syfte antingen att återställa, korrigera eller modifiera fysiologiska funktioner genom farmakologisk, immunologisk eller metabolisk verkan eller att ställa diagnos. Till tillämpningsområdet för NIS 2-direktivet hör dessutom entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2.

I läkemedelslagen (395/1987) regleras i enlighet med 2 § tillverkning, import och distribution av läkemedel samt förmedling, försäljning och annan överlåtelse till förbrukning av läkemedel. Den gäller också läkemedelsfabriker, läkemedelspartiaffärer, förmedlare av läkemedel och apotek som bedriver ovan nämnd verksamhet, laboratorier som utför prekliniska säkerhetsprövningar av läkemedel samt tillverkning och distribution av läkemedel på sjukhus och hälsovårds-

centraler. Bestämmelserna inom läkemedelsbranschen bygger i stor utsträckning på bestämmelser på EU-nivå, i huvudsak på Europaparlamentets och rådets direktiv 2001/83/EG om upprättande av gemenskapsregler för humanläkemedel (nedan *läkemedelsdirektivet*). I läkemedelslagen och läkemedelsdirektivet finns inga bestämmelser om cybersäkerhet.

Bestämmelser om klinisk prövning av läkemedel finns i lagen om klinisk prövning av läkemedel (983/2021, nedan *prövningslagen*). Prövningslagen tillämpas enligt 1 § på förhandsgranskning, genomförande och tillsyn i fråga om kliniska prövningar av humanläkemedel på det sätt som kliniska prövningar definieras i Europaparlamentets och rådets förordning (EU) nr 536/2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (nedan *prövningsförordningen*). Den nationella lagen innehåller kompletterande bestämmelser till prövningsförordningen. I prövningsförordningen och den nationella prövningslagen finns inga bestämmelser om cybersäkerhet.

3.5.4 Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan

Till tillämpningsområdet för NIS 2-direktivet hör entiteter 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. Omedelbart efter det att ett hot mot folkhälsan har erkänts ska styrgruppen för brister på medicintekniska produkter samråda med den arbetsgrupp som avses i artikel 21.5. enligt artikel 22 i förordning (EU) 2022/123. Omedelbart efter det samrådet ska styrgruppen för brister på medicintekniska produkter anta en förteckning över kategorier av kritiska medicintekniska produkter som den betraktar som kritiska under hotet mot folkhälsan (förteckningen över kritiska medicintekniska produkter vid ett hot mot folkhälsan). Relevant information om kritiska medicintekniska produkter och därmed relaterade tillverkare ska i möjligaste mån samlas in från Eudamed när den är fullt fungerande. Informationen ska även samlas in från importörer och distributörer, beroende på vad som är lämpligt. Fram till dess att Eudamed är fullt fungerande får tillgänglig information även samlas in från nationella databaser eller andra tillgängliga källor. Styrgruppen för brister på medicintekniska produkter ska vid behov uppdatera förteckningen över kritiska medicintekniska produkter vid ett hot mot folkhälsan till dess att erkännandet av hotet mot folkhälsan har upphävts. För tillämpningen av artikel 25.2 ska styrgruppen för brister på medicintekniska produkter anta, och göra allmänt tillgänglig, den uppsättning information som avses i artikel 25.2 c och d som är nödvändig för att övervaka tillgång och efterfrågan på medicintekniska produkter som ingår i förteckningen över kritiska medicintekniska produkter vid hot mot folkhälsan och underrätta den arbetsgrupp som avses i artikel 21.5 om denna uppsättning information. Läkemedelsmyndigheten ska på en särskild sida på sin webbportal offentliggöra förteckningen över kritiska medicintekniska produkter vid hot mot folkhälsan, samt eventuella uppdateringar av den förteckningen, och information om faktiska brister på kritiska medicintekniska produkter som ingår i förteckningen över kritiska medicintekniska produkter vid hot mot folkhälsan.

Det finns ingen sådan nationell lagstiftning om entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid allvarliga hot mot folkhälsan som kompletterar EU-lagstiftningen.

3.6 Dricksvatten och avloppsvatten

Både dricksvatten och avloppsvatten har hört till det nationella tillämpningsområdet för NIS 1-direktivet vars krav i Finland genomfördes genom en ändring av lagen om vattentjänster. Lagen

om vattentjänster tillämpas både på hanteringen av dricksvatten och på hanteringen av avloppsvatten. Inom vattenförsörjningssektorn finns ingen annan sektorsspecifik cybersäkerhetsreglering, men av ett vattentjänstverk som levererar hushållsvatten krävs redan nu riskbedömning och riskhantering i fråga om vattenkvaliteten i samarbete med den som utövar verksamheten, myndigheterna och övriga intressentgrupper.

Enligt 15 b § i lagen om vattentjänster ska ett vattentjänstverk som levererar eller tar emot avloppsvatten till en volym om minst 5 000 kubikmeter vatten per dygn anmäla betydande störningar till närings-, trafik- och miljöcentralen. I 35 § 2 mom. finns bestämmelser om rätten att lämna ut informationssäkerhetsrelaterade uppgifter till Transport- och kommunikationsverket trots tystnadsplikten enligt lagen om offentlighet i myndigheternas verksamhet. I lagen om vattentjänster finns också bestämmelser om vattentjänstverks skyldighet att trygga sina tjänster i störningssituationer (15 a §) och om att utan dröjsmål anmäla betydande störningar i vattentjänsterna till närings-, trafik- och miljöcentralen (15 b §).

I 5 kap. i hälsoskyddslagen (763/1994) finns bestämmelser om riskhanteringsskyldigheter för anläggningar som levererar hushållsvatten. Genom lagen har riskhanteringsskyldigheterna i Europaparlamentets och rådets direktiv (EU) 2020/2184 om kvaliteten på dricksvatten genomförts. Enligt lagen ska anläggningen utöva riskbedömning och riskhantering i anslutning till egenkontrollen i samarbete med den som utövar verksamheten, myndigheterna och övriga intressentgrupper. Enligt 19 a § ska en aktör utarbeta en riskhanteringsplan för att hantera och förebygga risker. Med riskbedömning avses i huvudsak risker som påverkar vattenkvaliteten. De här skyldigheterna har preciserats i statsrådets förordning om riskhantering och egenkontroll inom produktionskedjan för hushållsvatten (7/2023). Förordningen har utfärdats med stöd av 19 a § 5 mom. i hälsoskyddslagen och 15 § 5 mom. i lagen om vattentjänster.

I fråga om vattenförsörjningen kräver NIS 2-direktivets tillämpningsområde att den nationella definitionen på 5000 kubikmeter slopas. I fortsättningen ska tillämpningsområdet bestämmas enligt typen av entitet och storleken på entiteten. Dessutom ska NIS 2-direktivet tillämpas oavsett entitetens storlek när en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på den allmänna ordningen, den allmänna säkerheten eller folkhälsan. Detta kan utöka tillämpningsområdet för vattenförsörjningens del. När det gäller skyldigheten att anmäla störningar i 15 b § i lagen om vattentjänster bedöms det inte som nödvändigt att införa ändringar med anledning av genomförandet av NIS 2-direktivet, eftersom bestämmelsen kommer att tillämpas också på andra störningar än sådana som är inriktade på kommunikationsnät och informationssystem. De ändringar som behöver göras i 15 b § bedöms i samband med genomförandet av CER-direktivet. Det föreslås att 35 § 2 mom. 3 punkten upphävs med anledning av genomförandet av NIS 2-direktivet för att undvika överlappande bestämmelser.

3.7 Digital infrastruktur och digitala leverantörer

Digitala leverantörer har i huvudsak omfattats av tillämpningsområdet i NIS 1-direktivet, men särskilt den digitala infrastrukturens entiteter blir nya entiteter att omfattas av tillämpningsområdet i NIS 2-direktivet. Nya entiteter att omfattas av NIS 2-direktivet är tillhandahållare av kommunikationsnät och kommunikationstjänster, tillhandahållare av betrodda elektroniska tjänster, leverantörer av nätverk för leverans av innehåll samt leverantörer av datacentraltjänster. Transport- och kommunikationsverkets Cybersäkerhetscenter har varit tillsynsmyndighet för sektorn under NIS 1-direktivet. Transport- och kommunikationsverkets Cybersäkerhetscenter övervakar redan nu tillhandahållandet av kommunikationsnät och kommunikationstjänster samt betrodda elektroniska tjänster. I den gällande lagstiftningen finns inga uttryckliga bestäm-

melser om leverantörer av nätverk för leverans av innehåll och leverantörer av datacentraltjänster, såvida inte verksamheten utifrån en bedömning från fall till fall uppfyller definitio nen av förmedling av kommunikation.

3.7.1 Digitala leverantörer

I lagen om tjänster inom elektronisk kommunikation finns bestämmelser om informationssäkerhetsskyldigheter för vissa digitala leverantörer, såsom leverantörer av internetbaserade marknadsplatser, sökmotortjänster och molntjänster. Bestämmelserna har fogats till den lagen i samband med genomförandet av NIS 1-direktivet. I 247 a § i lagen om tjänster inom elektronisk kommunikation föreskrivs att digitala leverantörer är skyldiga att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem. I 275 § 2 mom. finns dessutom bestämmelser om störningsanmälan till Transport- och kommunikationsverket. Det föreslås att 247 a § och 275 § 2 mom. upphävs med anledning av genomförandet av NIS 2-direktivet för att undvika överlappande bestämmelser.

3.7.2 Domännamn

I 21 kap. i lagen om tjänster inom elektronisk kommunikation finns bestämmelser om toppdomänen fi samt om domännamnsverksamhet och förmedling av domännamn i anslutning till den. En del av fi-registrarerna är samtidigt både tillhandahållare av domännamnsregistreringstjänster och leverantörer av domännamnssystemtjänster. Informationssäkerhetsskyldigheter för fi-domännamnsverksamhet och fi-registrarer infördes i lagen redan 2015 och sedan september 2016 har bestämmelserna tillämpats på domännamnsverksamhet och registrarer. I samband med att NIS 1-direktivet genomfördes nationellt ansågs att de befintliga informationssäkerhets- och rapporteringsskyldigheterna var tillräckliga och det gjordes inga separata ändringar i lagstiftningen.

I 170 och 171 § i lagen om tjänster inom elektronisk kommunikation finns bestämmelser om registrarers och Transport- och kommunikationsverkets skyldighet att sörja för informationssäkerheten inom sin verksamhet. I 170 § finns bestämmelser om en registrars skyldighet att göra en störningsanmälan till Transport- och kommunikationsverket. Transport- och kommunikationsverket har dessutom utfärdat en domännamnsföreskrift, 68/2016 M, med närmare bestämmelser om vilka skyldigheter en registrar har vid hanteringen av informationssäkerheten och om skyldigheten att anmäla störningar. Transport- och kommunikationsverket övervakar redan nu fi-registrarverksamheten i enlighet med 171 §. Artikel 27 och 28 i NIS 2-direktivet kräver att 21 kap. kompletteras.

3.7.3 Kommunikationsnät och kommunikationstjänster

Det finns bestämmelser om kommunikationsnät och kommunikationstjänster i lagen om tjänster inom elektronisk kommunikation. I 247 § föreskrivs det att den som förmedlar kommunikation och den som tillhandahåller mervärdestjänster är skyldiga att sörja för informationssäkerheten i fråga om sina tjänster och i 243 och 244 a § finns allmänna förpliktelser om hur informationssäkerheten för kommunikationsnät och kommunikationstjänster ska skötas. I avd. X finns dessutom bestämmelser om tryggande av kommunikationens och tjänsternas kontinuitet, vilket innefattar bland annat åtgärder för informationssäkerheten, skyldighet att avhjälpa betydande olägenheter eller störningar orsakade av kommunikationsnät, kommunikationstjänster eller utrustning, skyldighet att anmäla störningar till Transport- och kommunikationsverket och till abonnenter och användare. Skyldigheten för teleföretag att anmäla störningar innefattar inte enbart störningar i tjänstens funktionalitet utan också störningar i informationssäkerheten samt skyldigheten enligt direktivet om integritet och elektronisk kommunikation att anmäla kränkningar

av informationssäkerheten som gäller personuppgifter. I avd. X finns dessutom bestämmelser om teleföretags beredskapsplanering och skyldighet att ha beredskap för störningssituationer under normala förhållanden och för undantagsförhållanden. Transport- och kommunikationsverket har dessutom meddelat föreskrifter om televerksamhetens informationssäkerhet, störningar i televerksamheten, kommunikationsnätets kritiska delar, säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät samt domännamn.

3.7.4 Betrodda elektroniska tjänster

Betrodda elektroniska tjänster regleras 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*) och i den kompletterande lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan *autentiseringslagen*). Bestämmelser om säkerhetskrav på tillhandahållare av betrodda elektroniska tjänster finns i artikel 19 i eIDAS-förordningen, som i enlighet med artikel 42 i NIS 2-direktivet upphävs den 18 oktober 2024. De betrodda elektroniska tjänsterna kan vara antingen kvalificerade eller icke kvalificerade. Tillhandahållande av en kvalificerad betrodd tjänst förutsätter att ett ackrediterat organ för bedömning av överensstämmelse har bedömt tjänstens överensstämmelse med krav samt godkännande av Transport- och kommunikationsverket. I 32 § i autentiseringslagen finns närmare bestämmelser om fastställande av överensstämmelse hos kvalificerade betrodda tjänster. I föreskriften M72 av Transport- och kommunikationsverket finns närmare föreskrifter om kriterierna för bedömning av överenstämmelse med kraven på kvalificerade betrodda tjänster och kriterierna om kompetens för bedömning av tjänsternas överensstämmelse med kraven. Inget behov att införa ändringar i autentiseringslagen med anledning av NIS 2-direktivet har identifierats.

3.8 Förvaltning av tjänster inom informations- och kommunikationsteknik (IKT-tjänster)

Leverantörerna av tjänster inom informations- och kommunikationsteknik, alltså leverantörer av IKT-tjänster, har inte hört till NIS 1-direktivets tillämpningsområde, utan blir en ny sektor inom tillämpningsområdet för NIS 2-direktivet. De leverantörer av IKT-tjänster som omfattas av NIS 2-direktivet är leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster mellan företag, som är medelstora eller stora företag. I NIS 2-direktivet avses med leverantörer av hanterade tjänster, så kallad driftsentreprenad, en entitet som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans. Med leverantör av hanterade säkerhetstjänster avses en leverantör av hanterade tjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker. Med IKT-tjänst avses enligt artikel 2.13 i cybersäkerhetsakten en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem.

Tillhandahållandet av IKT-tjänster är för närvarande inte tillräckligt reglerat i lagstiftningen. Sett till lagen om tjänster inom elektronisk kommunikation kan det handla om en underleverantör till en kommunikationsförmedlare och denne har inga direkta egna skyldigheter enligt lagen. I vissa fall kan en leverantör av en hanterad säkerhetstjänst vara en sådan leverantör av mervärdestjänster som avses i den lagen och då omfattas denne av skyldigheten att sörja för informationssäkerheten för sina tjänster i 247 § 2 mom. i den lagen.

3.9 Rymden

Rymdsektorn har inte hört till tillämpningsområdet för NIS 1-direktivet, utan den fogas som ny sektor till tillämpningsområdet för NIS 2-direktivet. I Finland regleras rymdverksamheten nationellt i lagen om markstationer och vissa radaranläggningar (96/2023) och i lagen om rymdverksamhet (63/2018). Till tillämpningsområdet för NIS 2-direktivet hör operatörer av markbaserad infrastruktur som stöder tillhandahållandet av rymdbaserade tjänster.

I lagen om markstationer och vissa radaranläggningar finns bestämmelser om anläggande av markstationer och radaranläggningar och om tillståndsplikt och tillsyn i fråga om markstations- och radarverksamhet. Anläggande av markstationer och radaranläggningar är tillståndspliktig verksamhet med undantag av sedvanlig användning av satellittjänster. Tillstånds- och tillsynsmyndighet för fullgörandet av skyldigheterna i lagen är Transport- och kommunikationsverket.

Enligt 2 § 5 punkten i lagen om markstationer och vissa radaranläggningar avses med verksamhetsutövare i fråga om markstationer och radaranläggningar fysiska eller juridiska personer som bedriver eller har för avsikt att bedriva markstations- eller radarverksamhet eller som faktiskt ansvarar för sådan verksamhet. Ovannämnda operatörer av markbaserad infrastruktur som stöder tillhandahållandet av rymdbaserade tjänster är sådana verksamhetsutövare som avses i lagen om markstationer och vissa radaranläggningar. Alla nuvarande verksamhetsutövare omfattas dock inte av tillämpningsområdet för NIS 2-direktivet.

Verksamheten och verksamhetsutövarna måste uppfylla vissa krav på riskhantering, inklusive skyddande av verksamheten mot yttre störningar och hot mot informationssäkerheten, säkerställande av informationssäkerheten och den fysiska säkerheten, förmåga att upptäcka kränkningar av och hot mot informationssäkerheten, hantering av kontinuiteten i verksamheten och krissituationer, säkerheten i leveranskedjorna, dokumentering av praxis som gäller riskhanteringsförfarandet och säkerställandet av säkerheten i informationssystemen (6 §). Transport- och kommunikationsverket har rätt att få uppgifter för utredning av kränkningar av informationssäkerheten (14 §) och rätt att utföra inspektioner av verksamheten (13 §). En verksamhetsutövare är skyldig att anmäla om informationssäkerhetsrelaterade störningar till Transport- och kommunikationsverket (11 §).

Under beredningen av lagen om markstationer och vissa radaranläggningar (RP 113/2022 rd) försökte man beakta en del av kraven i de dåvarande förslagen till NIS 2-direktivet och CER-direktivet som var under beredning. Då lagen om markstationer och vissa radaranläggningar bereddes fanns det ingen information om hur NIS 2-direktivet skulle genomföras nationellt. Under beredningen av lagen strävade man efter att förslaget inte skulle stå i strid med det dåvarande förslaget till NIS 2-direktiv och man försökte beakta i synnerhet skyldigheterna kring hanteringen av informationssäkerhetsrisker och anmälningar om störningssituationer för att minimera senare ändringsbehov i lagstiftningen. Dessa skyldigheter i fråga om riskhantering, informationssäkerhet och störningsanmälningar gäller alla verksamhetsutövare när det gäller markstationer och radaranläggningar oavsett storlek förutom vissa undantag som gäller myndigheter. Det förutsätts att dessa skyldigheter uppfylls för att tillstånd ska beviljas och verksamheten få bedrivas.

3.10 Post- och budtjänster

Post- och budtjänsterna är en ny sektor som fogats till NIS 2-direktivets tillämpningsområde. På nationell nivå regleras posttjänsterna genom postlagen (415/2011). Den nationella regleringen av posttjänsterna har dock traditionellt fokuserat på att öppna postmarknaden och på

öppna data och inte på säkerhetsaspekter. Dessutom regleras posttjänsterna 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 (nedan *postdirektivet*) och Europaparlamentets och rådets förordning (EU) 2018/644 om gränsöverskridande paketleveranstjänster. Regleringen i postdirektivet är föråldrad och medlemsländerna har önskat att det ska uppdateras snarast. För närvarande finns det få bestämmelser om cybersäkerhet i fråga om posttjänsterna. I 64–66 § i postlagen finns bestämmelser om beredskapsskyldighet för postföretag när det gäller undantagsförhållanden. I Finland finns det ingen speciallagstiftning om tillhandahållande av budtjänster och verksamheten faller under de allmänna civilrättsliga bestämmelserna.

När det gäller postlagen eller annan speciallagstiftning om post- och budtjänster har man inte fastställt något behov av att införa ändringar med anledning av genomförandet av NIS 2-direktivet.

3.11 Avfallshantering

Avfallshanteringen har inte hört till NIS 1-direktivets tillämpningsområde, utan den har införts som ny sektor först i och med NIS 2-direktivet. Avfallshanteringssektorn är bred och i den ingår ett stort antal olika entiteter i olika storleksklasser, men i praktiken hör endast något tiotal entiteter till NIS 2-direktivet på grund av antalet anställda eller omsättningen. På nationell nivå regleras avfallshanteringen och beredskapsbestämmelserna om den i avfallslagen (646/2011), statsrådets förordning om avfall (978/2021), miljöskyddslagen (527/2014) och statsrådets förordning om miljöskydd (713/2014).

I 6 § 16 punkten i avfallslagen definieras avfallshantering som insamling, transport, återvinning och bortskaffande av avfall, inbegripet kontroll och uppföljning av sådan verksamhet och efterbehandling av platser för bortskaffande av avfall samt verksamhet som mäklare. I 120 § åläggs verksamhetsutövarna att följa och kontrollera den avfallshantering som de ordnar för att säkerställa att verksamheten uppfyller de krav som anges i lagar och förordningar. Enligt 120 § 2 mom. i avfallslagen ska den som bedriver miljötillståndspliktig avfallsbehandlingsverksamhet utarbeta en plan för uppföljningen och kontrollen av avfallsbehandlingen och den ska läggas fram för tillståndsmyndigheten. I 41 § i statsrådets förordning om avfall preciseras de uppgifter som ska ingå i planen.

Miljöskyddslagens 15 § ålägger den som utövar tillståndspliktig eller anmälningspliktig verksamhet att ha beredskap att hindra olyckor eller andra exceptionella situationer och att begränsa de skadliga konsekvenserna av dem. I 6 kap. som gäller tillståndsprövning och tillståndsvillkor anges dessutom till exempel förutsättningarna för beviljande av tillstånd (49 §), tillståndsvillkor om hindrande av förorening (52 §) och uppföljnings- och kontrollvillkor (62 §). I 3, 6 och 16 § i statsrådets förordning om miljöskydd preciseras innehållet i tillståndsansökan och anmälan.

I fråga om avfallshanteringsskyldigheterna behandlar den nationella regleringen inte särskilt frågor kring informations- och cybersäkerhet, och det finns ingen nationell reglering som följer kraven i NIS 2-direktivet.

3.12 Produktion, bearbetning och distribution av kemikalier

Produktion, bearbetning och distribution av kemikalier hörde inte till tillämpningsområdet för NIS 1-direktivet. Nationellt finns de centrala bestämmelserna om kemikaliers säkerhet i kemikaliesäkerhetslagen och de förordningar som utfärdats med stöd av den. Kemikaliesektorn regleras dessutom nationellt i kemikalielagen, vars syfte är att skydda människor och miljö mot faror och olägenheter orsakade av kemikalier. EU-lagstiftning om kemikaliesäkerhet finns 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 (nedan *Reach-förordningen*) och Europaparlamentets och rådets förordning (EG) nr 1272/2008 om klassificering, märkning och förpackning av ämnen och blandningar, ändring och upphävande av direktiven 67/548/EEG och 1999/45/EG samt ändring av förordning (EG) nr 1907/2006 (nedan *CLP-förordningen*). Syftet med Reach-förordningen är att garantera en hög skyddsnivå för människors hälsa och miljön, inbegripet främjande av alternativa metoder för att bedöma hur farliga ämnen är, samt att ämnen fritt kan cirkulera på den inre marknaden samtidigt som konkurrenskraft och innovation förbättras. Syftet med CLP-förordningen är att harmonisera kriterierna för klassificering av ämnen och blandningar samt märknings- och förpackningsregler.

3.12.1 Kemikalier och explosiva varor

Syftet med kemikaliesäkerhetslagen är att förebygga och avvärja skador som förorsakas av hantering av kemikalier och att främja den allmänna säkerheten (1 §). Kemikaliesäkerhetslagen har ett omfattande tillämpningsområde och gäller såväl enstaka människor som stora verksamhetsutövare. Tillämpningsområdet bygger inte heller på NIS 2-direktivets sektorindelning. I 4 § avgränsas tillämpningsområdet.

I de förordningar av statsrådet som utfärdats med stöd av kemikaliesäkerhetslagen har säkerhetskraven i lagen preciserats. När det gäller farliga kemikalier är centrala förordningar statsrådets förordning om övervakning av hanteringen och upplagringen av farliga kemikalier (685/2015), statsrådets förordning om säkerhetskraven vid industriell hantering och upplagring av farliga kemikalier (856/2012), statsrådets förordning om säkerhetskraven för flytgasanläggningar (858/2012) och statsrådets förordning om säkerhet vid hantering av naturgas (551/2009). I fråga om tillverkningen och upplagringen av explosiva varor är förordningarna statsrådets förordning om övervakning av tillverkningen och upplagringen av explosiva varor (819/2015) och statsrådets förordning om säkerhetskraven vid tillverkning, hantering och upplagring av explosiva varor (1101/2015) centrala.

Genom kemikaliesäkerhetslagen och de förordningar som utfärdats med stöd av den har man genomfört EU-skyldigheter nationellt, såsom Europaparlamentets och rådets direktiv 2012/18/EU om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och om ändring och senare upphävande av rådets direktiv 96/82/EG (nedan *Seveso III–direktivet*). När det gäller kemikaliesäkerhetslagen svarar Säkerhets- och kemikalieverket (Tukes) för tillsynen över produktionsanläggningar som kan orsaka storolyckor.

I 3 kap. i kemikaliesäkerhetslagen finns bestämmelser om förebyggande av storolyckor orsakade av farliga kemikalier (särskilt 30 §) och det bygger på skyldigheterna i Seveso III-direktivet. I 30 § föreskrivs att en verksamhetsutövare är skyldig att utarbeta en säkerhetsrapport eller

ett annat dokument där verksamhetsutövaren redogör för sina verksamhetsprinciper för förebyggande och begränsning av olyckor. I lagen finns dessutom bestämmelser om framläggande av säkerhetsrapporten (32 §) och verksamhetsutövares informationsskyldighet (31 §). I lagen bestäms att Säkerhets- och kemikalieverket Tukes ska utarbeta en tillsynsplan och ett tillsynsprogram (27 §) och i övrigt övervaka verksamhetsutövarna (26 a §). För omfattande industriell hantering och upplagring av farliga kemikalier krävs ett tillstånd enligt 23 § i kemikaliesäkerhetslagen och för tillverkning och upplagring av explosiva varor ett tillstånd enligt 58 § i samma lag.

Man har identifierat ett behov av en totalreform av kemikaliesäkerhetslagen. Förändringsbehovet föranleds i synnerhet av att regelverket ändrats och av skäl som hänför sig till grundlagen. Det har emellertid bedömts vara motiverat att genomföra beredskapen inför säkerhetshot som en separat helhet. Vid arbets- och näringsministeriet bereds regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor och av 21 § i säkerhetsutredningslagen (726/2014) (Projektfönster: TEM063:00/2018). I den propositionen föreslås det att lagens tillämpningsområde utvidgas till att omfatta skyddet av verksamheter mot hot mot säkerheten. Avsikten med propositionen är att föreskriva om beredskap inför säkerhetshot och de allmänna grunderna för säkerhetsarrangemang på ett sätt som förpliktar alla verksamhetsutövare.

I samband med det projektet föreslås det att en ny 12 a § fogas till kemikaliesäkerhetslagen och avsikten med den är att ålägga verksamhetsutövarna att planera, konstruera och underhålla datasystem så att processtyrningen, processövervakningen och sådana anordningar som är kritiska ur säkerhetssynpunkt inte kan hamna i ett sådant läge där processen inte längre är under kontroll och äventyrar säkerheten. Enligt 12 a § 2 mom. ska verksamhetsutövaren kunna upptäcka datasäkerhetsincidenter och hot mot datasäkerheten och begränsa följderna av dem. Det föreslås att myndighetsuppgifterna för tillstånd och tillsyn när det gäller beredskap inför säkerhetshot ska ges till lagens nuvarande tillstånds- och tillsynsmyndigheter som är Säkerhets- och kemikalieverket och räddningsmyndigheten. Åtgärdsskyldigheterna i utkastet motsvarar till stor del skyldigheterna i NIS 2-direktivet.

Enligt 3 § 1 mom. i kemikaliesäkerhetslagen tillämpas den på verksamheten inom försvarsmakten, om inte något annat föreskrivs särskilt i den lagen. Försvarsministeriet har utfärdat förordningar om säkerhetskrav vid (712/2017) och övervakning av (713/2017) industriell hantering och upplagring av farliga kemikalier inom försvarsförvaltningen. Dessutom finns det bestämmelser om militära explosiva varor i försvarsministeriets förordning (772/2009). Det är meningen att lagstiftningen om militära explosiva varor ska ses över (Projektfönster: PLM010:00/2020). Dessa säkerhetsbestämmelser fokuserar i första hand på att garantera den fysiska säkerheten, och cybersäkerheten har inte beaktats särskilt i bestämmelserna.

Förutom i den gällande lagstiftningen finns anvisningar om beredskap inför informationssäkerhets- och cyberattacker och bedömningen av cyberhot i Säkerhets- och kemikalieverkets guide Turvauhkiin varautumisesta vaarallisten kemikaalien käsittelyssä ja varastoinnissa. Den innehåller också en checklista för beredskap inför cyberhot. Den kemiska industrins europeiska takorganisation Cefic driver programmet Responsible Care, som även omfattar förberedelser inför cyberhot. I Finland har cirka hundra företag anslutit sig till Cefics program och de står för omkring 80 % av den kemiska industrins produktion.

3.12.2 Bestämmelser om tryckbärande anordningar

Bestämmelser om tryckbärande anordningar kan också tillämpas på entiteter som deltar i produktion, bearbetning och distribution av kemikalier. Genom lagen om tryckbärande anordningar (1144/2016) har Europaparlamentets och rådets direktiv 2014/68/EU om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av tryckbärande anordningar (omarbetning) och Europaparlamentets och rådets direktiv 2014/29/EU om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av enkla tryckkärl genomförts. I lagen finns dessutom nationella bestämmelser om säkerhet under drift. I den finns till exempel bestämmelser om säkerhetskrav för tryckbärande anordningar, förebyggande av olyckor och anmälan om olyckor och tillbud till myndigheter. Den myndighet som övervakar att skyldigheterna i lagen fullgörs är Säkerhets- och kemikalieverket Tukes. Tillämpningsområdet för lagen om tryckbärande anordningar överensstämmer inte med sektorindelningen i NIS 2-direktivet, utan till tillämpningsområdet hör aktörer från olika sektorer. Till tillämpningsområdet för bestämmelserna om tryckbärande anordningar hör också manöver- och säkerhetsutrustning för tryckbärande anordningar som under de förutsättningar som nämns i lagen om tryckbärande anordningar och i statsrådets förordning om tryckbärande anordningar (1548/2016) som utfärdats med stöd av den får användas via säkrad förbindelse för fjärrstyrning av sådana anordningar. Säkerhetsbestämmelserna i lagstiftningen om tryckbärande anordningar bygger på förebyggande av olyckor och det finns inga bestämmelser om cyberattacker. I samband med projektet att införa ändringar i kemikaliesäkerhetslagen i fråga om säkerhetshot har man inte för avsikt att ändra bestämmelserna om tryckbärande anordningar.

Utgångspunkten i både kemikaliesäkerhetslagen och lagen om tryckbärande anordningar är beredskap inför olyckor. De bestämmelser om beredskap inför säkerhetshot som föreslås i kemikaliesäkerhetslagen är också tillämpliga på tryckbärande anordningar, om dessa finns i ett objekt som omfattas att tillämpningsområdet för kemikaliesäkerhetslagen. På grund av förändringar i verksamhetsmiljön kommer också behovet av bestämmelser om säkerhetshot i lagstiftningen om tryckbärande anordningar att bedömas på nytt inom en nära framtid.

3.13 Produktion, bearbetning och distribution av livsmedel

Produktion, bearbetning och distribution av livsmedel har inte hört till tillämpningsområdet för NIS 1-direktivet. Nationellt regleras livsmedelssektorn i livsmedelslagen (297/2021) genom vilken 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 (nedan *allmänna livsmedelsförordningen*) har genomförts. Nationella sektorsspecifika bestämmelser finns dessutom i foderlagen (1263/2020), lagen om djursjukdomar (76/2021), beredskapslagen (1522/2011) och växtskyddslagen (1110/2019).

Livsmedelslagstiftningen omfattar utöver livsmedel också material som kommer i kontakt med livsmedel. Det finns nationella bestämmelser om kraven och skyldigheterna i fråga om dessa material i livsmedelslagen. I foderlagen finns dessutom bestämmelser om allmänna principer för fodersäkerhet och om skyldigheter för foderföretagare och tillsynsmyndigheter inom foderbranschen. Det primära ansvaret för livsmedels- och fodersäkerheten innehas av livsmedels- och foderföretagarna enligt den allmänna livsmedelsförordningen. Myndigheterna är skyldiga att genom sin egen verksamhet säkerställa att livsmedels- och foderföretagarna uppfyller de krav som gäller dem. I livsmedelslagstiftningen finns dock inga bestämmelser som gäller företagarnas informations- och cybersäkerhet, utan de ålägganden som gäller riskhantering och beredskap rör andra risker, såsom förhindrande av matförgiftningar, zoonoser och djursjukdomar.

Syftet med livsmedelslagen är att skydda konsumentens hälsa och ekonomiska intressen genom att garantera livsmedlens och livsmedelskontaktmaterialens säkerhet, trygga en god hälsomässig livsmedelskvalitet och övrig kvalitet enligt livsmedelsbestämmelserna och säkerställa att informationen om livsmedlen och livsmedelskontaktmaterialen är tillräcklig och korrekt. Lagens tillämpningsområde innefattar livsmedel, djur som används för livsmedelsproduktion, livsmedelskontaktmaterial, livsmedels- och kontaktmaterialverksamhet, livsmedels- och kontaktmaterialföretagare samt livsmedelstillsynen i alla stadier av produktions-, bearbetnings- och distributionskedjan för livsmedel och livsmedelskontaktmaterial (2 §).

Enligt 14 § i livsmedelslagen ska den spårbarhetsinformation som krävs enligt livsmedelsbestämmelserna lämnas till mottagaren i fråga om livsmedel, djur som används för livsmedelsproduktion och livsmedelskontaktmaterial. De djur som används för livsmedelsproduktion och andra eventuella ämnen som är avsedda för eller kan antas tillsättas till livsmedel måste gå att spåra. För detta ska företagaren ha ett system genom vilket de behöriga myndigheterna får tillgång till uppgifterna. I 15 § som gäller egenkontroll åläggs företagare att förvalta ett system för att identifiera och hantera faror i samband med sin verksamhet och säkerställa att verksamheten uppfyller de krav som ställs i livsmedelsbestämmelserna. I 15 § 2 mom. föreskrivs att företagaren ska göra upp en plan för provtagning och undersökning med tanke på eventuell upptäckt av salmonella, om denne för in livsmedel som omfattas av särskilda salmonellagarantier från en medlemsstat till en annan. Resultaten av egenkontrollen ska dokumenteras med tillräcklig precision och företagarna ska visa att de iakttar kraven på det sätt som myndigheten förutsätter.

Enligt 17 § ska företagare omedelbart underrätta den behöriga tillsynsmyndigheten om sådana allvarliga faror för människors hälsa som uppdagats i egenkontrollen eller på annat sätt samt om åtgärder som vidtagits för att rätta till dessa missförhållanden. I 17 § 2 mom. finns dessutom bestämmelser om företagares skyldighet att underrätta tillsynsmyndigheten om ett livsmedel har orsakat matförgiftning eller det finns misstanke om matförgiftning. Tillsynsmyndigheten kan förelägga att en produkt ska dras tillbaka från marknaden, om företagaren inte självmant vidtar åtgärder och den information som ges väsentligen strider mot bestämmelserna (57 §). Paragrafen ger också tillsynsmyndigheten en allmän rätt att informera om saken.

Bestämmelser om myndigheternas skyldigheter inom livsmedelssektorn finns bland annat i 24, 47, 48, och 82 § i livsmedelslagen. Livsmedelsverkets uppgifter anges i 24 § och enligt den ska Livsmedelsverket planera, styra och utveckla livsmedelstillsynen och utföra livsmedelstillsyn på riksnivå. Dessutom är Livsmedelsverket nationell myndighet eller nationell kontaktpunkt för livsmedelstillsyn enligt Europeiska unionens lagstiftning och internationella avtal (t.ex. den nationella kontaktpunkt för systemet för snabb varning (RASFF) som avses i artikel 50 i allmänna livsmedelsförordningen, kontaktpunkt EFSA Focal Point samt kontaktpunkt i informationsförmedlingsnätverket i anslutning till livsmedelsbedrägerier). Livsmedelsverket utarbetar också en nationell beredskapsplan för livsmedel med specificerade åtgärder som vidtas om livsmedlen har konstaterats utgöra en allvarlig risk för människors hälsa.

Enligt 48 § i livsmedelslagen ska Livsmedelsverket göra upp de provtagningsplaner som behövs för uppföljning och kontroll av zoonoser och göra behövliga anmälningar om resultaten av zoonosundersökningarna till livsmedelsföretagare och myndigheter. Även kommunen åläggs skyldighet att vidta åtgärder, om det på en anläggning för djur återkommande förekommer zoonoser eller om anläggningen misstänks vara smittkälla för en zoonos som konstaterats hos en människa. Enligt 47 § är kommunen skyldig att göra utredningar kring matförgiftningar. I 82 § föreskrivs om sekretess för uppgifter som erhållits vid tillsynen.

Också lagen om djursjukdomar (76/2021) behandlar livsmedelssäkerheten och den har som syfte att bekämpa djursjukdomar. Enligt 18 § ska ett slakteri enligt livsmedelslagen, en djurpark enligt djurskyddslagen (247/1996) samt en anläggning för avelsmaterial som förutsätter godkännande enligt EU:s djurhälsoförordning eller lagen om djursjukdomar utarbeta en beredskapsplan med tanke på sjukdomar i kategori a, om där hanteras djur som tillhör förtecknade arter. Genom förordning av jord- och skogsbruksministeriet bestäms vilka djursjukdomar som kräver en beredskapsplan och innehållet i beredskapsplanen preciseras. Enligt lagen om djursjukdomar är aktörer (19 §) och veterinärer samt laboratorier (20 §) skyldiga att anmäla om djursjukdomar till kommunalveterinären eller regionförvaltningsverket. Med stöd av 22 § är kommunalveterinären skyldig att anmäla till regionförvaltningsverket om en djursjukdom som anmälts till veterinären i enlighet med 19 och 20 §.

Bestämmelser om beredskapsplanering finns också i Europaparlamentets och rådets förordning (EU) 2016/429 om överförbara djursjukdomar och om ändring och upphävande av vissa akter med avseende på djurhälsa och i Europaparlamentets och rådets förordning (EU) 2017/625 om offentlig kontroll och annan offentlig verksamhet för att säkerställa tillämpningen av livsmedels- och foderlagstiftningen och av bestämmelser om djurs hälsa och djurskydd, växtskydd och växtskyddsmedel samt om ändring av Europaparlamentets och rådets förordningar (EG) nr 999/2001, (EG) nr 396/2005, (EG) nr 1069/2009, (EG) nr 1107/2009, (EU) nr 1151/2012, (EU) nr 652/2014, (EU) 2016/429 och (EU) 2016/2031, rådets förordningar (EG) nr 1/2005 och (EG) nr 1099/2009 och rådets direktiv 98/58/EG, 1999/74/EG, 2007/43/EG, 2008/119/EG och 2008/120/EG och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 854/2004 och (EG) nr 882/2004, rådets direktiv 89/608/EEG, 89/662/EEG, 90/425/EEG, 91/496/EEG, 96/23/EG, 96/93/EG och 97/78/EG samt rådets beslut 92/438/EEG.

Bestämmelser om beredskaps- och riskhanteringsskyldigheter för livsmedelssektorn finns också i växtskyddslagen och delvis i författningar som gäller produktionsinsatser, såsom foder, gödselmedel och växtskyddsmedel. Dessutom bedöms det nationella genomförandet av CER-direktivet kräva förändringar och preciseringar i lagstiftningen om livsmedelssektorn.

Anvisningar och planer för livsmedelstillsynen utgörs till exempel av anvisningen Riskklassificering av en livsmedelslokal och kontaktmaterialverksamhet och fastställande av tillsynbehov, Fleråriga nationella tillsynsplanen för livsmedelskedjan 2021–2024 och fleråriga nationella tillsynsplanen (VASU).

I livsmedelslagen och de andra lagarna om livsmedelssektorn har man inte upptäckt överlappningar eller motstridigheter med NIS-regleringen och därför har man inte fastställt något ändringsbehov i den sektorsspecifika lagstiftningen.

3.14 Tillverkningssektorn

Tillverkningssektorn har inte hört till tillämpningsområdet för NIS 1-direktivet. De viktigaste säkerhetsskyldigheterna inom tillverkningssektorn ingår i lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (390/2005), elsäkerhetslagen (1135/2016) och lagen om medicintekniska produkter. I strålsäkerhetslagen (859/2018) finns bestämmelser om strålsäkerhet. I bilaga II till NIS 2-direktivet är tillverkningssektorn indelad i delsektorerna tillverkning av medicintekniska produkter, tillverkning av datorer, elektronikvaror och optik, tillverkning av elapparatur, tillverkning av övriga maskiner, tillverkning av motorfordon, släpfordon och påhängsvagnar samt tillverkning av andra transportmedel. Inom sektorn består bestäm-

melser som gäller normala förhållanden av säkerhetsbestämmelser som fokuserar på produkternas kvalitet eller säkerhet eller på hanteringen av maskiner, anläggningar eller kemikalier som används under tillverkningen.

3.14.1 Tillverkning av medicintekniska produkter

Delsektorn medicintekniska produkter omfattar de entiteter som tillverkar de medicintekniska produkter som definieras 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 (nedan *MD-förordningen*) samt de entiteter som tillverkar de medicintekniska produkter för in vitro-diagnostik som definieras 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 (nedan *IVD-förordningen*).

I MD- och IVD-förordningarna stärks de väsentliga kraven bland annat på medicintekniska produkter som fungerar via ett elektroniskt system eller som i sig är programvaror. Förordningarna innefattar också vissa icke-inbäddade programvaror och i dem bygger angreppssättet på hela livscykeln. I de väsentliga kraven förutsätts att tillverkarna när de utvecklar och förverkligar sina produkter tillämpar riskhanteringsprinciperna och uppfyller kraven på informationssäkerhetsåtgärder samt går igenom motsvarande förfaranden för bedömning av överensstämmelse. Samordningsgruppen för medicintekniska produkter (Medical Devices Coordination Group, MDCG) utfärdade i december 2019 en separat anvisning om hur de fastställda väsentliga kraven om cybersäkerhet i bilaga I till MD- och IVD-förordningarna kan uppfyllas (Guidance on Cybersecurity for Medical Devices, MDCG 2019-16).

MD- och IVD-förordningarna kompletteras av lagen om medicintekniska produkter (719/2021) och lagen om vissa medicintekniska produkter enligt EU-direktiv (629/2010). Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea är tillsynsmyndighet enligt lagarna. I dessa nationella lagar finns inga separata bestämmelser om cybersäkerhetskrav på medicintekniska produkter eller på tillverkningen av dem.

3.14.2 Tillverkning av datorer, elektronikvaror och optik

Delsektorn tillverkning av datorer, elektronikvaror och optik i NIS 2-direktivet omfattar de företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i NACE Rev. 2. När det gäller tillverkningen av produkterna har man inte funnit någon sektorsspecifik reglering.

NACE Rev. 2 avsnitt C huvudgrupp 26:

26			Tillverkning av datorer, elektronikvaror och optik
	26.1		Tillverkning av elektroniska komponenter och kretskort
		26.11	Tillverkning av elektroniska komponenter
		26.12	Tillverkning av kretskort

	26.2		Tillverkning av datorer och kringutrustning
		26.20	Tillverkning av datorer och kringutrustning
	26.3		Tillverkning av kommunikationsutrustning
		26.30	Tillverkning av kommunikationsutrustning
	26.4		Tillverkning av hemelektronik
		26.40	Tillverkning av hemelektronik
	26.5		Tillverkning av instrument och apparater för mätning, provning och navigering samt ur
		26.51	Tillverkning av instrument och apparater för mätning, provning och navigering
		26.52	Urtillverkning
	26.6		Tillverkning av strålningsutrustning samt elektromedicinsk och elektroterapeutisk utrustning
		26.60	Tillverkning av strålningsutrustning samt elektromedicinsk och elektroterapeutisk utrustning
	26.7		Tillverkning av optiska instrument och fotoutrustning
		26.70	Tillverkning av optiska instrument och fotoutrustning
	26.8		Tillverkning av magnetiska och optiska medier
		26.80	Tillverkning av magnetiska och optiska medier

3.14.3 Tillverkning av elapparatur

Delsektorn tillverkning av elapparatur omfattar de entiteter som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i NACE Rev. 2. I elsäkerhetslagstiftningen finns inga bestämmelser om entiteters informations- och cybersäkerhet, utan de centrala säkerhetsbestämmelserna bygger på förebyggande av olyckor och produktsäkerhet.

I elsäkerhetslagen finns bestämmelser om säkerheten för elektronisk utrustning och elanläggningar. Lagen är uppbyggd av nationella bestämmelser och genomförandet av vissa av EU:s produktdirektiv. Lagen tillämpas med de undantag som nämns i 3 § på elektronisk utrustning och elanläggningar som används vid produktion, överföring, distribution eller användning av el och vilkas elektriska eller elektromagnetiska egenskaper kan förorsaka risk för skada eller störningar. Lagen tillämpas också på radioutrustning och kommunikationsnät till den del som dessa kan orsaka fara för någons liv, hälsa eller egendom, eller skadliga störningar om vilka det inte föreskrivs i lagen om tjänster inom elektronisk kommunikation eller i bestämmelser som utfärdats med stöd av den. Säkerhets- och kemikalieverket Tukes är den centrala tillsynsmyndigheten

enligt lagen. Om elektrisk utrustning eller elanläggning orsakar skada, får myndigheten begränsa användningen av utrustningen eller anläggningen och vid behov avlägsna utrustningen eller anläggningen från nätet.

NACE Rev. 2 avsnitt C huvudgrupp 27:

27			Tillverkning av elapparatur
	27.1		Tillverkning av elmotorer, generatorer och transformatorer samt eldistributions- och elkontrollapparater
		27.11	Tillverkning av elmotorer, generatorer och transformatorer
		27.12	Tillverkning av eldistributions- och elkontrollapparater
	27.2		Batteri- och ackumulatortillverkning
		27.20	Batteri- och ackumulatortillverkning
	27.3		Tillverkning av ledningar och kablar och kabeltillbehör
		27.31	Tillverkning av optiska fiberkablar
		27.32	Tillverkning av andra elektroniska och elektriska ledningar och kablar
		27.33	Tillverkning av kabeltillbehör
	27.4		Tillverkning av belysningsarmatur
		27.40	Tillverkning av belysningsarmatur
	27.5		Tillverkning av hushållsmaskiner och hushållsapparater
		27.51	Tillverkning av elektriska hushållsmaskiner och hushållsapparater
		27.52	Tillverkning av icke-elektriska hushållsmaskiner och hushållsapparater
	27.9		Tillverkning av annan elapparatur
		27.90	Tillverkning av annan elapparatur

3.14.4 Tillverkning av övriga maskiner

Delsektorn tillverkning av övriga maskiner i NIS 2-direktivet omfattar de företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i NACE Rev. 2. När det gäller tillverkningen av produkterna har man inte funnit något sektorsspecifik reglering.

NACE Rev. 2 avsnitt C huvudgrupp 28:

28			Tillverkning av övriga maskiner
	28.1		Tillverkning av maskiner för allmänt ändamål
		28.11	Tillverkning av motorer och turbiner utom för luftfartyg och fordon
		28.12	Tillverkning av fluidteknisk utrustning
		28.13	Tillverkning av andra pumpar och kompressorer
		28.14	Tillverkning av andra kranar och ventiler
		28.15	Tillverkning av lager, kugghjul och andra delar för kraftöverföring
	28.2		Tillverkning av andra maskiner för allmänt ändamål
		28.21	Tillverkning av ugnar och brännare
		28.22	Tillverkning av lyft- och godshanteringsanordningar
		28.23	Tillverkning av kontorsmaskiner och kontorsutrustning (utom datorer och kring-utrustning)
		28.24	Tillverkning av motordrivna handverktyg
		28.25	Tillverkning av maskiner och apparater för kyla och ventilation utom för hushåll
		28.29	Övrig tillverkning av maskiner för allmänt ändamål
	28.3		Tillverkning av jord- och skogsbruksmaskiner
		28.30	Tillverkning av jord- och skogsbruksmaskiner
	28.4		Tillverkning av maskiner för metallbearbetning och verktygsmaskiner
		28.41	Tillverkning av maskiner för metallbearbetning
		28.49	Tillverkning av övriga verktygsmaskiner
	28.9		Tillverkning av andra specialmaskiner
		28.91	Tillverkning av maskiner för metallurgi
		28.92	Tillverkning av gruv-, bergbrytnings- och byggmaskiner
		28.93	Tillverkning av maskiner för framställning av livsmedel, drycker och tobaksvaror
		28.94	Tillverkning av maskiner för produktion av textil-, beklädnads- och lädervaror
		28.95	Tillverkning av maskiner för produktion av massa, papper och papp
		28.96	Tillverkning av maskiner för gummi och plast

		28.99	Tillverkning av diverse övriga specialmaskiner

3.14.5 Tillverkning av motorfordon och släpfordon

Delsektorn tillverkning av motorfordon och släpvagnar i NIS 2-direktivet omfattar de företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i NACE Rev. 2. För fordonstillverkare och fordon finns enhetliga bestämmelser om godkännande av fordon med avseende på cybersäkerhet och ledningssystem för cybersäkerhet. De här kraven grundar sig på Europaparlamentets och rådets förordning (EU) 2018/858 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG och på FN-föreskrifter nr 155.

NACE Rev. 2 avsnitt C huvudgrupp 29:

29			Tillverkning av motorfordon, släpfordon och påhängsvagnar
	29.1		Motorfordonstillverkning
		29.10	Motorfordonstillverkning
	29.2		Tillverkning av karosserier för motorfordon; tillverkning av släpfordon och påhängsvagnar
		29.20	Tillverkning av karosserier för motorfordon; tillverkning av släpfordon och påhängsvagnar
	29.3		Tillverkning av delar och tillbehör till motorfordon
		29.31	Tillverkning av elektrisk och elektronisk utrustning för motorfordon
		29.32	Tillverkning av andra delar och tillbehör till motorfordon

3.14.6 Tillverkning av andra transportmedel

Delsektorn tillverkning av andra transportmedel i NIS 2-direktivet omfattar de företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i NACE Rev. 2. Till huvudgrupp 30 hör fartyg och båtar, flytande materiel, fritidsbåtar, rälsfordon, luftfartyg och rymdfarkoster o.d., militära stridsfordon, motorcyklar, cyklar och invalidfordon samt övrig transportmedelstillverkning. När det gäller delsektorn tillverkning av andra transportmedel har man inte funnit någon sektorsspecifik reglering av riskhanteringen av cybersäkerheten, förutom regleringen av cybersäkerheten inom luftfarten som presenteras i avsnitt 3.3.

NACE Rev. 2 avsnitt C huvudgrupp 30:

30			Tillverkning av andra transportmedel
	30.1		Skepps- och båtbyggeri
		30.11	Byggande av fartyg och flytande materiel
		30.12	Byggande av fritidsbåtar
	30.2		Tillverkning av rälsfordon
		30.20	Tillverkning av rälsfordon
	30.3		Tillverkning av luftfartyg, rymdfarkoster o.d.
		30.30	Tillverkning av luftfartyg, rymdfarkoster o.d.
	30.4		Tillverkning av militära stridsfordon
		30.40	Tillverkning av militära stridsfordon
	30.9		Övrig tillverkning av transportmedel
		30.91	Tillverkning av motorcyklar
		30.92	Tillverkning av cyklar och invalidfordon
		30.99	Övrig transportmedelstillverkning

3.15 Forskningsorganisationer

Forskningsorganisationer hörde inte till tillämpningsområdet för NIS 1-direktivet. Enligt artikel 6.41 i NIS 1-direktivet avses med forskningsorganisation en entitet 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 inbegriper utbildningsinstitutioner. Nationellt sett har Teknologiska Forskningscentralen VTT Ab (VTT) fastställts höra till tillämpningsområdet enligt definitionen.

Bestämmelser om Teknologiska Forskningscentralen VTT Ab finns i lagen om Teknologiska forskningscentralen VTT Ab (761/2014, nedan *VTT-lagen*). Enligt 2 § i den lagen är bolagets uppgift att i egenskap av oberoende och objektivt forskningsinstitut främja det att forskningen och teknologin tillgodogörs på ett mångsidigt sätt och kommersialiseras inom näringslivet och i samhället. I 6 § i lagen föreskrivs om skyldighet att vidta förberedelser och om bolagets skyldighet att säkerställa att dess uppgifter kan skötas så bra som möjligt också under exceptionella förhållanden med hjälp av en beredskapsplan och förberedelser för verksamhet under exceptionella förhållanden och genom andra åtgärder.

I VTT-lagen föreskrivs inte om krav på cybersäkerhet som ställs på bolaget3.16 Sektorn offentlig förvaltning

Sektorn offentlig förvaltning har inte hört till tillämpningsområdet för NIS 1-direktivet. Den har lagts till som högkritisk sektor först i NIS 2-direktivet. Reglering på nivån allmän lag som gäller nät- och informationssäkerhet inom sektorn offentlig förvaltning ingår i lagen om informationshantering inom den offentliga förvaltningen (906/2019, *informationshanteringslagen*). Offentliga aktörer har också omfattats av NIS 1-direktivet till exempel på sektorn hälso- och sjukvård.

3.16.1 Tillämpning av reglering i NIS 2-direktivet på sektorn offentlig förvaltning

I 4 kap. i informationshanteringslagen tillämpas reglering om informationssäkerhet i stor utsträckning inom den offentliga förvaltningen. Regleringen tillämpas på de myndigheter som avses i 4 § 1 mom. i informationshanteringslagen och också på privatpersoner, organisationer och på andra offentligrättsliga organisationer som inte är myndigheter till de delar de sköter offentliga förvaltningsuppgifter.

Nationellt föreslås det att reglering enligt NIS 2-direktivet som gäller enbart sektorn offentlig förvaltning som avses i bilaga 1.10 till direktivet – det vill säga skyldigheter som gäller cybersäkerhet och tillsyn över att de iakttas för en aktör inom offentlig förvaltning – fogas till informationshanteringslagen. Informationshanteringslagen ska vara en speciallag enligt NIS 2-direktivet i förhållande till den allmänna lag som föreslås, det vill säga lagen om hantering av cybersäkerhetsrisker. Det föreslås att reglering i informationshanteringslagen i enlighet med NIS 2-direktivet tillämpas på en mer begränsad grupp än de som regleringen om informationssäkerhet enligt 4 kap. i den lagen tillämpas på. Utgångspunkten är att direktivets miniminivå uppfylls. Det ska beaktas att om en offentlig aktör bedriver verksamhet inom någon av de andra sektorerna enligt direktivet kan den omfattas av regleringen i NIS 2 enligt den föreslagna lagen om hantering av cybersäkerhetsrisker. Genom lagen om hantering av cybersäkerhetsrisker sätts de skyldigheter som gäller alla andra sektorer som beskrivs i bilagorna till direktivet i kraft.

I direktivet förutsätts det att anmälningar om avvikelser ska kunna göras i bred utsträckning också av aktörer som inte hör till dem som fastställts i direktivet. Således ska också andra aktörer inom offentlig förvaltning än de som NIS 2-regleringen enligt förslaget ska tillämpas på kunna anmäla tillsynsmyndigheten om avvikelser och på så sätt utöka lägesbilden för cybersäkerheten. Dessa andra aktörer ska också kunna få stöd av tillsynsmyndigheten och CSIRT-enheten i behandlingen av avvikelsen.

3.16.2 Begrepp och definitioner

Med informationshantering avses enligt 2 § 9 punkten i informationshanteringslagen sådana åtgärder och informationssäkerhetsåtgärder baserade på behov som uppkommer i samband med en myndighets uppgifter eller övriga verksamhet, i syfte att hantera en myndighets informationsmaterial, informationen i olika behandlingsskeden och informationen i informationsmaterial, oberoende av på vilket sätt informationsmaterialen lagras och behandlas i övrigt. Med informationssystem avses enligt 2 § 3 punkten ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling. Med informationssäkerhetsåtgärder avses enligt 2 § 8 punkten säkerställande av informationsmaterials tillgänglighet, integritet och tillförlitlighet genom administrativa, funktionella och tekniska åtgärder.

I NIS 2-direktivet används i stället för informationssäkerhet till exempel följande begrepp:

- ”cybersäkerhet” med vilket avses all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot,

- ”cyberhot” med vilket avses en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer,
- ”nätverks- och informationssystem”, med vilket avses
  a) elektroniskt kommunikationsnät som definieras i artikel 2.1 i direktiv (EU) 2018/1972,
  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, eller
  c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas.

De begrepp som används i informationshanteringslagen avviker i någon mån från de som används i NIS 2-direktivet, och därför bör för genomförandet av direktivet de nödvändiga begrepp som används där fogas till informationshanteringslagen.

3.16.3 Riskhanteringsåtgärder för cybersäkerhet

Enligt artikel 21 i direktivet ska det föreskrivas att entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster. Dessutom ingår i artikel 21.2 i direktivet en detaljerad förteckning över åtgärder som åtminstone ska inbegripas i riskhanteringsåtgärderna för cybersäkerhet.

I 13 § i informationshanteringslagen föreskrivs om skyldighet att genomföra informationssäkerhetsåtgärder utifrån riskbedömning (1 mom.) och om myndigheters skyldighet att vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder (4 mom.). I 13 a § i lagen föreskrivs om informationshanteringens information om och beredskap för störningssituationer. Vad gäller tillförlitlighet hos anställda föreskrivs i 12 § om skyldighet att identifiera uppgifter som förutsätter särskild tillförlitlighet hos anställda eller personer som handlar för enhetens räkning. I 14 § 1 mom. föreläggs myndigheter skyldighet att om de överför sekretessbelagd information i det allmänna datanätet ska informationen överföras i ett krypterat eller på annat sätt skyddat format. Dessutom ska överföringen ordnas så att mottagaren verifieras eller identifieras på ett tillräckligt informationssäkert sätt, innan mottagaren kommer åt att behandla den överförda sekretessbelagda informationen. Lagens 16 § har samband med den åtkomsthantering som förutsätts i artikel 21. Enligt bestämmelsen ska den systemansvariga myndigheten definiera användarrättigheterna för informationssystem. Användarrättigheterna ska definieras utifrån användarens uppgiftsrelaterade användningsbehov och ska uppdateras.

De ovan beskrivna bestämmelserna i informationshanteringslagen täcker delvis skyldigheterna i artikel 21 i direktivet, men på grund av den delvis mer ingående regleringen och de begrepp som används i direktivet måste den reglering som gäller aktörers hantering av cybersäkerhetsrisker kompletteras.

3.16.4 Ledningens (ledningsorganets) ansvar

Enligt artikel 20.1 första stycket ska entiteters ledningsorgan godkänna de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21 och övervaka genomfö-

randet av dem. Dessutom ska ledningsorganen kunna ställas till svars för entiteternas överträdelser av den artikeln. Enligt artikel 20.1 andra stycket ”*påverkar tillämpningen av denna punkt inte nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner, samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner*”. Enligt artikel 20.2 ska entiteters ledningsorgan vara skyldiga att genomgå utbildning som gäller hantering av cybersäkerhetsrisker. Dessutom ska medlemsstaterna uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.

I 4 § 2 mom. i informationshanteringslagen föreskrivs delvis om ledningens ansvar och erbjudande av utbildning samt om ordnande av övervakning. Enligt bestämmelsen ska en informationshanteringsenhets ledning bland annat ombesörja att det vid enheten har definierats ansvaren för de uppgifter i anslutning till informationshanteringen, uppdaterade anvisningar om hantering av informationshanteringsansvar, kan erbjudas utbildning om författningar, föreskrifter och informationshanteringsenhetens anvisningar som gäller informationshanteringsenheten samt har ordnats tillräcklig övervakning när det gäller iakttagandet av författningarna, föreskrifterna och anvisningarna om informationshantering.

Såsom ovan har konstaterats avviker begreppen i någon mån från dem som används i NIS 2-direktivet, så de som formulerats i 4 § 2 mom. motsvarar som sådana inte helt det som föreskrivs i direktivet. I informationshanteringslagen föreskrivs inte heller om skyldighet för en informationshanteringsenhet eller ledningen för en myndighet att godkänna riskhanteringsåtgärder för cybersäkerhet, och inte heller någon uttrycklig skyldighet för ledningen att övervaka verkställigheten av dessa riskhanteringsåtgärder. Det finns inte heller bestämmelser om ledningens skyldighet att delta i utbildning. En bestämmelse om erbjudande av utbildning till de anställda finns (4 § 2 mom. 3 punkten). Vad gäller ledningens ansvar kan tjänsteansvar anses tillräckligt eftersom NIS 2-drektivet och den reglering som föreslås betonar ledningens uppgifter och ansvar i hanteringen av cybersäkerhetsrisker.

3.16.5 Anmälningsskyldigheter och tillsyn

I NIS 2-direktivet förutsätts det att det föreskrivs skyldighet för de aktörer som omfattas av tillämpningsområdet att anmäla vissa uppgifter som gäller deras verksamhet till en behörig myndighet. I direktivet förutsätts det också att det föreskrivs om skyldighet att anmäla till en behörig myndighet eller CSIRT-enheten om betydande cybersäkerhetsincidenter. Dessutom föresätter direktivet att det föreskrivs om övervakning av aktörerna.

I informationshanteringslagen ingår ingen reglering om skyldighet att anmäla om verksamhet, skyldighet att anmäla incidenter eller om någon egentlig tillsyn. I 10 § i lagen finns en bestämmelse om informationshanteringsnämndens bedömningsuppgift, men den gäller inte iakttagande av informationssäkerhet enligt 4 kap. i lagen. Dessutom har informationshanteringsnämnden i uppgift att främja genomförandet av förfarandena i fråga om informationshantering och informationssäkerhet samt genomförandet av de krav som föreskrivs i informationshanteringslagen. Regleringen i informationshanteringslagen ska alltså kompletteras i fråga om anmälningsskyldigheter och tillsyn.

3.16.6 Placering av bestämmelser som gäller sektorn offentlig förvaltning i informationshanteringslagen

Genom informationshanteringslagen styrs även manuell informationshantering som görs på papper, så det är inte möjligt att ersätta bestämmelserna om informationssäkerhet i informationshanteringslagen med bestämmelserna i NIS 2-direktivet. Bestämmelserna i informationshanteringslagen uppfyller inte heller helt till alla detaljer eller till de delar som gäller anmälningsskyldigheter och tillsyn det som krävs i NIS 2-direktivet.

Därför föreslås det att nya bestämmelser som uttryckligen gäller hantering av cybersäkerhetsrisker och andra skyldigheter enligt NIS 2-direktivet och tillsyn över att de iakttas fogas till informationshanteringslagen i ett eget kapitel. Detta är motiverat även för att det föreslås att NIS 2-reglering tillämpas på en mer begränsad grupp än regleringen om informationssäkerhet i informationshanteringslagen. Också den tillsyn som förutsätts i NIS 2-direktivet kan på så sätt riktas till iakttagande av de skyldigheter som det föreskrivs om i NIS 2-direktivet och som finns i ett eget kapitel.

3.16.7 Behov av ändring av informationshanteringslagen av nationella skäl

Skyldigheten att säkerhetsklassificera handlingar enligt 18 § i informationshanteringslagen gäller myndigheteter vid statliga ämbetsverk, inrättningar och affärsverk samt domstolar och nämnder som har inrättats för att behandla besvärsärenden. Behov av att utvidga skyldigheten att säkerhetklassificera har uppkommit under den tid informationshanteringslagen varit i kraft särskilt från Suomen Erillisverkot Oy som sköter uppgifter enligt lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015, nedan *säkerhetsnätslagen).* Det föreslås att skyldigheten att säkerhetsklassificera utvidgas till att gälla även Suomen Erillisverkot Oy och det dotterbolag som det äger helt när de sköter uppgifter som avses i säkerhetsnätslagen.

3.17 Strategi för cybersäkerheten

Den gällande nationella strategin för cybersäkerheten har godkänts genom principbeslut av statsrådet den 3 oktober 2019. Strategin grundar sig på de allmänna principer som fastställts i Strategi för cybersäkerheten i Finland 2013. Förnyandet och verkställandet av Strategin för cybersäkerheten 2019 uppgjordes utifrån en skrivning i regeringsprogrammet, och det var även en del av verkställandet av EU:s strategi för cybersäkerhet. Skäl för reformen 2019 var dessutom ändringar som skett i verksamhetsbetingelser samt utvecklingsobjekt som upptäckts nationellt.

Strategin för cybersäkerhet ställer upp centrala nationella mål genom vilka man strävar efter att utveckla cyberomgivningen och trygga funktioner som är viktiga för samhället. Dess tre strategiska riktlinjer är utveckling av internationellt samarbete, bättre koordinering av ledning, planering och beredskap som gäller cybersäkerheten, samt utveckling av kunnande som gäller cybersäkerhet.

Enligt cybersäkerhetsstrategin har en uppgift som statens cybersäkerhetsdirektör inrättats hos statsrådet 2020. Ett utvecklingsprogram för cybersäkerhet har utarbetats under ledning av statens cybersäkerhetsdirektör.

Statsrådets principbeslut för utvecklingsprogrammet av cybersäkerheten har likaså utarbetats utgående från strategin för cybersäkerhet2019 under ledning av statens cybersäkerhetsdirektör. Utvecklingsprogrammet är en konkret verkställighetsplan med målet att på lång sikt förbättra cybersäkerheten i hela samhället. Verkställigheten av Finlands strategi för cybersäkerheten följs av Säkerhetskommittén som finns i samband med försvarsministeriet.

Strategin för cybersäkerhet behöver uppdateras under den kommande regeringsperioden på grund av ändrade verksamhetsbetingelser och nya skyldigheter i fråga om lagstiftning. Den nuvarande cybersäkerhetsstrategin och utvecklingsprogrammet för cybersäkerhet uppfyller inte till innehållet de krav som NIS 2-direktivet ställer på en cybersäkerhetsstrategi.

Enligt regeringsprogrammet för statsminister Orpos regering revideras ledningsstrukturen för helhets- och cybersäkerheten under regeringsperioden under ledning av statsministern (8 kap.) och ”regeringen ser över den nationella cybersäkerhetsstrategin så att den motsvarar vår förändrade omvärld” (8.5 kap.).

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

I denna proposition föreslås det att det för genomförande av NIS 2-direktivet stiftas en ny lag om hantering av cybersäkerhetsrisker. Lagen innehåller de minimiskyldigheter som NIS 2-direktivet förutsätter för de aktörer som omfattas av dess tillämpningsområde. I lagen iakttas miniminivån enligt NIS 2-direktivet när det gäller tillämpningsområdet för skyldigheterna, deras omfattning och tillsynen över dem. I överensstämmelse med direktivet innehåller lagen också bestämmelser om tillsyn över att skyldigheterna fullgörs samt om en enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) och dess uppgifter. Den huvudsakliga metoden för genomförande av direktivet är omskrivning. Direktivets skyldigheter och krav skrivs om i den nationella lagstiftningen, särskilt till den del de gäller aktörerna. När det gäller vissa detaljerade bestämmelser av teknisk natur som gäller myndigheter används även hänvisningsmetoden för genomförandet. Genomförandet sker i enlighet med direktivets minimikrav.

I fråga om de skyldigheter som gäller enbart sektorn för offentlig förvaltning och tillsynen över att dessa fullgörs föreskrivs det separat i informationshanteringslagen. I förhållande till den föreslagna lagen om hantering av cybersäkerhetsrisker är informationshanteringslagen en speciallag. De bestämmelser i lagen om hantering av cybersäkerhetsrisker som gäller CSIRT-enheten samt bestämmelserna om informationsutbyte och myndighetssamarbete tillämpas också inom sektorn för offentlig förvaltning, till den del det inte föreskrivs om detta i informationshanteringslagen. Om en offentlig aktör är verksam inom någon annan sektor som omfattas av NIS 2-direktivet, kan den omfattas av NIS 2-bestämmelserna även eller enbart med stöd av lagen om hantering av cybersäkerhetsrisker. Detta gäller exempelvis välfärdsområden och välfärdssammanslutningar, Helsingfors stad och de kommuner som bedriver sådan verksamhet som beskrivs i de olika punkterna i bilaga I och II till NIS 2-direktivet, med undantag för punkt 10 i bilaga I. Även om det inte föreslås att de skyldigheter som följer av NIS 2-direktivet och som föreslås i informationshanteringslagen ska tillämpas på den verksamhet som bedrivs i några andra kommuner än Helsingfors stad (till den del staden sköter sådana uppgifter som enligt lag omfattas av välfärdsområdets organiseringsansvar), kan även andra kommuner med stöd av lagen om hantering av cybersäkerhetsrisker omfattas av NIS 2-bestämmelserna, om deras tjänster hör till de tjänster som definieras i bilagorna till NIS 2-direktivet och kommunen storleksmässigt motsvarar den definition av aktör som finns i lagen om hantering av cybersäkerhetsrisker.

Det föreslås inte att aktörer inom finansbranschen ska omfattas av tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker, eftersom dessa omfattas av DORA-förordningen och

de bestämmelser som verkställer den. I DORA-förordningen åläggs aktörerna inom finansbranschen sådana skyldigheter i fråga om beredskap inför cyberhot som är mera långtgående än de skyldigheter som ingår i NIS 2-direktivet.

Genom lagen om tjänster inom elektronisk kommunikation genomförs det som fordras enligt NIS 2-direktivets artikel 28 om en databas över domännamnsregistreringsuppgifter när det gäller registreringsenheter för toppdomäner och registrarer.

Skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem gäller privata eller offentliga aktörer som bedriver sådan verksamhet som avses i bilaga I eller II och som storleksmässigt är medelstora eller större enligt kommissionens definition av storleken på små och medelstora företag. Med vissa undantag kan skyldigheterna gälla även mindre företag än så. Lagen innehåller även en bestämmelse om att det genom förordning av statsrådet under vissa förutsättningar får föreskrivas att en aktör ska omfattas av lagens tillämpningsområde oavsett storlek. Lagen innehåller också bestämmelser om tillsyn över de riskhanterings- och rapporteringsskyldigheter som gäller dessa aktörer.

Tillsynsmyndigheterna utses sektorsvist utifrån den tillsynsmodell som följer NIS 1-direktivet. Tillsynsmyndigheten bestäms på basis av aktörens sektor. Tillsynsmyndigheterna är, enligt sektor, Transport- och kommunikationsverket, Energimyndigheten, Säkerhets- och kemikalieverket, Tillstånds- och tillsynsverket för social- och hälsovården, NTM-centralen i Södra Savolax, Livsmedelsverket, Säkerhets- och utvecklingscentret för läkemedelsområdet och Finansinspektionen. Tillsynsansvaret fördelar sig enligt sektor på följande sätt:

Tillsynsmyndighet	**Sektor enligt bilaga I eller II till NIS 2-direktivet**
Transport- och kommunikationsverket	Lufttransport, spårtrafik, sjöfart, vägtransport, rymden, digital infrastruktur, förvaltning av IKT-tjänster, tillhandahållare av budtjänster och posttjänster, digitala leverantörer, tillverkning (aktörer som bedriver tillverkning av motorfordon, släpfordon och påhängsvagnar, aktörer som bedriver tillverkning av andra transportmedel), forskningsorganisationer, offentlig förvaltning
Energimyndigheten	Elektricitet, operatörer av fjärrvärme eller fjärrkyla, gas (distributionsnätsinnehavare och överföringsnätsinnehavare)
Säkerhets- och kemikalieverket	Gas (naturgasleverantörer, innehavare av lagringsanläggningar, innehavare av behandlingsanläggningar för kondenserad naturgas, naturgasföretag och operatörer av raffinaderier och bearbetningsanläggningar för naturgas), olja, operatörer av anläggningar för produktion, lagring och överföring av vätgas, företag som tillverkar ämnen och distribuerar ämnen eller blandningar, företag som producerar varor genom att använda ämnen och blandningar samt tillverkning (aktörer som bedriver tillverkning av datorer, elektronikvaror och optik, aktörer som bedriver tillverkning av elapparatur och aktörer som bedriver tillverkning av övriga maskiner)

Tillstånds- och tillsynsverket för social- och hälsovården	Hälso- och sjukvård
NTM-centralen i Södra Savolax	Dricksvatten, avloppsvatten och avfallshantering
Livsmedelsverket	Livsmedelsföretag som bedriver grossisthandel, industriell produktion eller bearbetning
Säkerhets- och utvecklingscentret för läkemedelsområdet	Aktörer som tillverkar medicintekniska produkter och aktörer som tillverkar medicinsktekniska produkter för in vitro-diagnostik
Finansinspektionen	Bankverksamhet och finansmarknadsinfrastruktur

I propositionen föreslås det att man utnyttjar det nationella handlingsutrymme som innebär att tillsynsmyndigheten får rikta in tillsynen enligt en riskbaserad bedömning och i första hand på de väsentliga aktörerna.

Även framöver är det Cybersäkerhetscentret vid Transport- och kommunikationsverket som är CSIRT-enhet för hantering av it-säkerhetsincidenter samt gemensam kontaktpunkt.

Maximibeloppen av de administrativa sanktioner som NIS 2-direktivet kräver fastställs till den nivå som är det lägsta maximibeloppet som direktivet tillåter. Administrativa sanktioner påförs av påföljdsavgiftsnämnden på framställning av tillsynsmyndigheten. Påföljdsavgiftsnämnden är ett nytt organ, vars ledamöter har uppdraget som bisyssla, och den består av ledamöter som har utsetts av tillsynsmyndigheterna. Med stöd av det nationella handlingsutrymmet föreslås det en bestämmelse om att administrativa påföljdsavgifter enligt NIS 2-direktivet inte får påföras aktörer inom den offentliga förvaltningen.

Genom denna proposition åläggs statsrådet skyldighet att godkänna en cybersäkerhetsstrategi med det innehåll som är minimum enligt NIS 2-direktivet. Varje myndighet ska fungera som cyberkrishanteringsmyndighet enligt NIS 2-direktivet i enlighet med de uppgifter som föreskrivits för den i lagen. Cybersäkerhetscentret vid Transport- och kommunikationsverket fungerar som koordinator mellan cyberkrishanteringsmyndigheterna och svarar i samarbete med de andra myndigheterna även för upprättandet av den nationella ram för hantering av cybersäkerhetskriser som NIS 2-direktivet kräver för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Propositionen innehåller inget förslag om ändringar i säkerhetsmyndigheternas nuvarande befogenheter eller uppgiftsfördelning vad gäller hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

Genom denna proposition upphävs i den sektorsvisa lagstiftningen de bestämmelser som har utfärdats i syfte att genomföra NIS 1-direktivet, eftersom dessa i fortsättningen skulle vara överlappande i förhållande till den nya lag som utfärdas i syfte att genomföra NIS 2-direktivet. NIS 1-direktivet har för övrigt också upphävts genom NIS 2-direktivet. Det föreslås att bestämmelser upphävs eller ändras i följande lagar: 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 och lagen om tillsyn över el- och naturgasmarknaden. Dessutom görs det i lagen om Energimyndigheten vissa tekniska ändringar som följer av genomförandet av NIS 2-direktivet.

I förslaget utnyttjas inte det nationella handlingsutrymme som NIS 2-direktivet medger när det gäller en utvidgning av definitionen av väsentliga aktörer så att definitionen separat även skulle omfatta sådana väsentliga tjänsteleverantörer som har identifierats med stöd av NIS 1-direktivet i situationer där de annars inte skulle betraktas som väsentliga aktörer med stöd av NIS 2-direktivet.

I propositionen föreslås det inte heller att det nationella handlingsutrymmet utnyttjas i fråga om att tillämpa NIS 2-direktivet på aktörer inom sektorn offentlig förvaltning på lokal nivå eller inrättningar inom undervisnings- och utbildningssektorn. Som ett undantag tillämpas skyldigheterna på Helsingfors stad, till den del staden sköter sådana uppgifter som enligt lag omfattas av välfärdsområdets organiseringsansvar.

I överensstämmelse med det nationella handlingsutrymmet föreslås det i propositionen bestämmelser om undantag i fråga om tillämpningen av de skyldigheter som följer av NIS 2-direktivet på vissa aktörer som tillhandahåller tjänster till sådana aktörer inom den offentliga förvaltningen som bedriver verksamhet inom den nationella säkerheten, allmän säkerhet, försvaret eller brottsbekämpning, inbegripet förebyggande, utredning och avslöjande av brott samt lagföring av brott, eller som själva bedriver sådan verksamhet. Det nationella handlingsutrymmet utnyttjas fullt ut i överensstämmelse med NIS 2-direktivet när det gäller skyldigheterna för dessa aktörer.

I propositionen föreslås det inga ytterligare nationella krav för användningen av europeiska ordningar för cybersäkerhetscertifiering.

4.2 De huvudsakliga konsekvenserna

4.2.1 De huvudsakliga konsekvenserna av förslaget

Det som föreslås har konsekvenser för både den offentliga sektorn och privata aktörer. På ett allmänt plan förbättrar det som föreslås cybersäkerheten för vad som med tanke på verksamheten i samhället är kritiska aktörer och väsentliga tjänster, liksom förmågan att tolerera cyberstörningar och att återhämta sig från cyberattacker eller andra skadliga störningar i informationssystem och kommunikationsnät. Cyberattacker på infrastruktur som är kritisk för samhället och andra störningar i informationssystem och kommunikationsnät kan ha betydande och omfattande skadliga konsekvenser. Genom de åtgärder som föreslås strävar man efter att undvika att sådana realiseras.

Verkställandet av de skyldigheter som ingår i propositionen kommer att öka kostnaderna för de aktörer som är föremål för bestämmelserna när de ska fullgöra sina skyldigheter. Kostnader för att fullgöra skyldigheterna uppkommer särskilt i de sektorer som inte tidigare har omfattats av skyldigheterna enligt NIS 1-direktivet. För den offentliga sektorn och den offentliga ekonomin uppkommer det kostnader via de myndighetsuppgifter som genomförandet av NIS 2-direktivet förutsätter, särskilt från tillsynen över skyldigheter och CSIRT-enhetens verksamhet. Tillsynen över skyldigheter och CSIRT-enhetens verksamhet skapar ett behov av tilläggsresurser för de myndigheter som anvisas dessa uppgifter. Även för aktörerna inom den offentliga sektorn torde

det uppstå kostnader i någon mån när de ska följa direktivets krav i anslutning till cybersäkerhet. Å andra sidan uppnår man i och med dessa skyldigheter, genom bättre beredskap inför och reaktion på cyberattacker samt informationsutbyte, en högre nivå på cybersäkerheten i aktörernas verksamhet. På detta sätt kan man förebygga cyberattacker och de skadliga konsekvenserna av sådana, vilka annars kunde orsaka betydande skadliga konsekvenser och kostnader både för aktörerna och mera allmänt de aktörer i samhället som använder sig av aktörernas produkter eller tjänster.

Genom propositionen förenhetligas i lag de horisontella minimikrav på riskhanteringen inom informationssäkerheten som gäller för de aktörer som omfattas av tillämpningsområdet. En förändring jämfört med tidigare är att aktörerna blir skyldiga att själva identifiera om de omfattas av tillämpningsområdet för lagstiftningen och anmäla sig till tillsynsmyndighetens förteckning över aktörer, sköta riskhanteringen i överenstämmelse med lagen och rapportera om betydande incidenter till tillsynsmyndigheten och CSIRT-enheten. Jämfört med NIS 1-direktivets skyldigheter i fråga om riskhantering innehåller lagen mera detaljerade bestämmelser om de delområden som ska beaktas i riskhanteringen. Dessutom tillämpas riskhanterings- och rapporteringsskyldigheterna på en större grupp aktörer än de som omfattades av NIS 1-direktivet. Tillämpningsområdet kommer att omfatta alla aktörer som bedriver sådan verksamhet eller som är sådana typer av aktör som avses i bilagan till lagen och som storleksmässigt är medelstora eller större, dvs. som uppfyller storlekskriteriet för tillämpningsområdet. Tillämpningsområdet omfattar även aktörer som bedriver sådan verksamhet eller som är sådana typer av aktör som avses i bilagan till lagen och som inte uppfyller storlekskriteriet, men som omfattas av det undantag i överensstämmelse med NIS 2-direktivet som gäller tillämpning oberoende av aktörens storlek. Nya sektorer som omfattas av tillämpningsområdet är avloppsvatten och avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkningssektorn, vilken inbegriper bland annat medicintekniska produkter, datorer, elapparatur och motorfordon samt rymdsektorn, teletjänster och betrodda tjänster, leverantörer av CDN-tjänster, plattformar för sociala nätverkstjänster och den offentliga sektorn. Dessutom ska alla aktörer som identifieras som kritiska med stöd av CER-direktivet omfattas av lagen. Tillsammans med de sektorer som redan från tidigare omfattades av NIS-bestämmelserna är gruppen aktörer som omfattas av tillämpningsområdet storleksmässigt betydande. Konsekvenserna kan beräknas variera enligt sektor, särskilt på grund av den begränsning som gäller aktörens storlek, i och med att verksamheten inom många sektorer består av grupper av mindre aktörer. Då tillämpas skyldigheterna i princip inte på dessa aktörer.

Det som föreslås har konsekvenser för aktörerna inom den offentliga sektorn, både som övervakare av bestämmelserna och objekt för bestämmelserna. Kraven i överensstämmelse med NIS 2-direktivet vad gäller riskhantering och rapportering av incidenter gäller även aktörerna inom den offentliga sektorn, med undantag för lokal förvaltning. Myndighetsuppgifter som NIS 2-direktivet förutsätter är en tillsynsmyndighet för varje sektor, en CSIRT-enhet för hantering av it-säkerhetsincidenter samt internationellt samarbete med de andra EU-medlemsstaterna, kommissionen och Enisa i syfte att bekämpa de skadliga konsekvenserna av cyberstörningar. NIS 2-direktivet ålägger även en skyldighet att godkänna och upprätthålla en uppdaterad cybersäkerhetsstrategi, vilket statsrådet svarar för.

Som helhet betraktat kan man uppskatta att säkerheten i kommunikationsnät och informationssystem kommer att förbättras i och med genomförandet av NIS 2-direktivet, och detta gäller såväl offentliga som privata aktörer. Upprätthållandet av en hög nivå på cybersäkerheten har indirekt betydelse för samhället även ur ett bredare perspektiv. Inom den privata sektorn finns det viktiga tjänster och funktioner som är väsentliga för upprätthållandet av kritisk infrastruktur, och en förbättring av deras resiliens vid störningar förbättrar samhällets resiliens i kriser. Via

rapportering av incidenter och tillsyn över riskhanteringen är det möjligt att bilda sig en bättre och mera detaljerad lägesbild än nu av cybersäkerheten inom olika sektorer och, även på ett allmänt plan, i samhället. I och med de nya kraven och tillsynen över dem ökar medvetenheten och kunskapsnivån i fråga om cybersäkerhet inom både den privata och den offentliga sektorn.

Det som föreslås förenhetligar kriterierna för de aktörer som omfattas av tillämpningsområdet inom hela EU och minskar till denna del medlemsstaternas administrativa börda i fråga om att identifiera aktörer. Även de krav som ställs på aktörerna förenhetligas i EU-medlemsstaterna. De medelstora eller större aktörer som bedriver sådan verksamhet som avses i bilagorna till NIS 2-direktivet ska i princip omfattas av tillämpningsområdet på basis av verksamhetens art och aktörens storlek. Små företag och mikroföretag omfattas i princip inte av tillämpningsområdet, om de inte omfattas av det undantag som innebär att de omfattas av tillämpningsområdet för NIS 2-direktivet oberoende av storlek. En medlemsstat får under vissa förutsättningar fortsättningsvis identifiera även små aktörer och mikroaktörer som väsentliga och låta dem omfattas av tillämpningsområdet, om de tjänster som de producerar kan betraktas som väsentliga med tanke på kontinuiteten i samhällets verksamhet. Förslaget förenhetligar skyldigheterna i fråga om cybersäkerhet och rapportering och utvidgar tillämpningsområdet så att det gäller nya sektorer och aktörer. Tillsynsmyndigheterna får även, utöver de uppgifter de redan har, nya tillsynsuppgifter, såsom tillsyn över de aktörer som har tagits med i tillämpningsområdet.

Storlekskriteriet för aktörer som omfattas av tillämpningsområdet motsvarar storlekskriteriet för NIS 2-direktivets tillämpningsområde. Med stöd av artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG är medelstora företag, dvs. andra företag än mikroföretag och små företag, företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år. Som ett sådant företag som når över de tröskelvärden som används i definitionen av ett medelstort företag, och alltså som ett företag som storleksmässigt betraktas som ett sådant väsentligt företag som avses i lagen, betraktas ett företag som sysselsätter minst 250 personer eller vars årsomsättning överstiger 50 miljoner euro och vars balansomslutning överstiger 43 miljoner euro per år. Artikel 3.4 om ett offentligt organs kontroll över en aktörs kapital eller röstandel i bilagan till kommissionens rekommendation tillämpas inte när det ska avgöras om en aktör ska omfattas av tillämpningsområdet.

På aktörerna tillämpas samma riskhanterings- och rapporteringsskyldigheter oberoende av sektor och storlek. Sektorns särdrag bör beaktas när man definierar riskerna med verksamheten och de riskhanteringsåtgärder som är nödvändiga. Skyldigheten att rapportera om betydande incidenter ändras så att rapporteringen sker i två steg. Den första anmälan ska göras inom 24 timmar från det att den betydande incidenten upptäcktes. Anmälan ska, beroende på fallet, innehålla uppgifter om huruvida incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller om den kan ha gränsöverskridande verkningar. Om en incident har gränsöverskridande verkningar, ska den rapporteras till de andra medlemsstaterna som den påverkar, samt till Enisa.

Den uppföljande anmälan ska göras inom 72 timmar från det att den betydande incidenten upptäcktes. Anmälan ska, beroende på fallet, uppdatera uppgifterna i en tidig varning och innehålla en första bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. Den första och uppföljande anmälan kan också göras genom en enda anmälan, om aktören inom tidsfristen för den första anmälan har tillgång till även de uppgifter som krävs för den uppföljande anmälan. Genom den uppföljande anmälan kan man även komplettera uppgifterna i den första anmälan.

Vidare ska det upprättas en slutrapport om en betydande incident senast inom en månad från det att anmälan om incidenten lämnades in. Rapporten ska innehålla en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst incidenten, begränsande åtgärder som har vidtagits eller som planeras samt, beroende på fallet, gränsöverskridande konsekvenser av incidenten. En delrapport eller ytterligare information om behandlingen av ärendet ska lämnas på begäran av tillsynsmyndigheten samt, när det gäller en långvarig incident, inom en månad efter att den uppföljande anmälan lämnades.

4.2.2 Aktörer som omfattas av tillämpningsområdet för riskhanterings- och rapporteringsskyldigheterna

Förslaget ändrar tillämpningsområdet för skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem jämfört med hur NIS 1-direktivet genomfördes. Det tillämpningsområde för skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem som föreslås omfattar de aktörer som bedriver sådan verksamhet som avses i bilagan till lagen, eller som är en sådan typ av aktör som avses i bilagan och som uppfyller eller överskrider storlekskriteriet för tillämpningsområdet, eller som omfattas av det undantag som gäller tillämpning av skyldigheterna oberoende av storlek. Dessutom tillämpas skyldigheterna på sådana aktörer som med stöd av CER-direktivet har identifierats som kritiska, oberoende av storlek. En ändring jämfört med NIS 1-direktivet är att de aktörer som omfattas av tillämpningsområdet inte definieras i sektorer, utan alla aktörer som bedriver sådan verksamhet eller som är en sådan typ av aktör som avses i bilagan, och som uppfyller storlekskriteriet eller omfattas av undantaget i fråga om storlek, omfattas direkt av tillämpningsområdet. De NIS-skyldigheter som gäller för aktörerna upphävs även i de sektorsvisa lagarna och överförs till lagen om hantering av cybersäkerhetsrisker, förutom när det gäller aktörer inom den offentliga förvaltningen.

Storlekskriteriet för skyldigheternas tillämpningsområde baserar sig på definitionen av ett medelstort företag. Med stöd av artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG är medelstora företag, dvs. andra företag än mikroföretag och små företag, företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år. Artikel 3.4 om ett offentligt organs kontroll över en aktörs kapital eller röstandel i bilagan till kommissionens rekommendation tillämpas inte när det ska avgöras om en aktör ska omfattas av tillämpningsområdet för NIS 2-direktivet. Det allmänna storlekskriteriet för tillämpningsområdet är alltså att aktören ska sysselsätta minst 50 personer eller att aktörens omsättning eller balansomslutning överstiger 10 miljoner euro per år, dvs. att aktören motsvarar den definition av ett medelstort företag som finns i kommissionens rekommendation. De aktörer som överskrider det som enligt definitionen är en medelstor aktör är sådana väsentliga aktörer som avses i förslaget. I enlighet med kommissionens rekommendation är ett företag som når över de tröskelvärden som används i definitionen av ett medelstort företag ett företag som sysselsätter minst 250 personer eller vars årsomsättning överstiger 50 miljoner euro och vars balansomslutning överstiger 43 miljoner euro per år.

Tillämpningsområdet för skyldigheterna omfattar också, oberoende av storlek, aktörer inom den offentliga förvaltningen och sådana aktörer som är tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner eller leverantörer av DNS-tjänster.

Dessutom omfattar tillämpningsområdet för skyldigheterna sådana aktörer som med stöd av CER-direktivet ska definieras som kritiska aktörer, oberoende av storlek.

Vidare kan tillämpningsområdet för skyldigheterna genom förordning av statsrådet utvidgas till att omfatta aktörer som är en sådan typ av aktör som avses i bilaga I eller II, om a) aktören i medlemsstaten är den enda leverantören av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, b) en störning av den tjänst som aktören tillhandahåller kan ha en betydande påverkan på allmän ordning, allmän säkerhet eller folkhälsa, c) en störning av den tjänst som aktören tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser, eller d) 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 medlemsstaten som är beroende av denna aktör.

Skyldigheterna enligt lagen om hantering av cybersäkerhetsrisker tillämpas på de typer av aktör som definieras i bilagorna inom följande sektorer:

Sektorer som även omfattades av tillämpningsområdet för NIS 1-direktivet	**Sektorer inom vilka nya aktörer börjar omfattas av tillämpningsområdet för NIS-skyldigheterna**
Energi	Avfallshantering, avloppsvatten
Transporter	Tillverkning, produktion och distribution av kemikalier
Bankverksamhet och finansmarknadsinfrastruktur	Produktion, bearbetning och distribution av livsmedel
Hälso- och sjukvård	Tillverkning: tillverkning av medicintekniska produkter, tillverkning av datorer, elektronikvaror och optik, tillverkning av elapparatur, tillverkning av övriga maskiner, tillverkning av motorfordon, släpfordon och påhängsvagnar samt tillverkning av andra transportmedel.
Dricksvatten	Rymden
Digital infrastruktur	Förvaltning av IKT-tjänster
Digitala leverantörer	Post- och budtjänster
	Forskning
	Offentlig förvaltning

Av sektorerna och typerna av aktör har en del omfattats av tillämpningsområdet för riskhanterings- och rapporteringsskyldigheterna sedan genomförandet av NIS 1-direktivet och en del börjar omfattas först nu. Definitionerna av de typer av aktör som omfattas av tillämpningsområdet utvidgas delvis också inom de sektorer som har omfattats av NIS 1-direktivet. Härnäst behandlas sektorsvis de typer av aktör som omfattas av tillämpningsområdet samt antalet aktö-

rer som omfattas av riskhanterings- och rapporteringsskyldigheterna. Bestämmelser om skyldigheterna för den offentliga förvaltningen finns i lagen om informationshantering inom den offentliga förvaltningen. En närmare beskrivning av de typer av aktör som omfattas av tillämpningsområdet finns sektorsvis under tabellen.

Energisektorn

Energisektorn har omfattats av NIS 1-direktivet och skyldigheterna införlivades med den sektorsvisa lagstiftningen. När det gäller energisektorn betraktades i Finland elnätsinnehavare och innehavare av överföringsnät för naturgas som tillhandahållare av väsentliga tjänster. Skyldigheterna inbegriper aktörens skyldighet att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som aktören använder samt att lämna Energimyndigheten en anmälan (NIS-anmälan) om sådana betydande informationssäkerhetsrelaterade störningar som är riktade mot deras system. Inom energisektorn fanns det i början av 2023 totalt 88 företag som var sådana aktörer enligt NIS 1-direktivet som skulle övervakas. Energimyndigheten har varit tillsynsmyndighet.

I NIS 2-direktivet utvidgas bestämmelsernas omfång vad gäller energisektorn. Inom energisektorn omfattar direktivets tillämpningsområde följande typer av aktör:

Elektricitet	Elleverantörer och elproducenter, distributionsnätsinnehavare, stamnätsinnehavare, elmarknadsoperatörer, vissa parter på elmarknaden och laddningsoperatörer
Fjärrvärme och fjärrkyla	Operatörer av fjärrvärme eller fjärrkyla
Olja	Operatörer av oljeledningar, operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja samt centrala lagringsenheter
Gas	Distributionsnätsinnehavare, överföringsnätsinnehavare, naturgasleverantörer, innehavare av lagringsanläggningar, innehavare av behandlingsanläggningar för kondenserad naturgas, operatörer av raffinaderier och bearbetningsanläggningar för naturgas samt vissa företag inom naturgasbranschen
Väte	Operatörer av anläggningar för produktion, lagring och överföring av vätgas

Av de typer av aktör som hör till energisektorn omfattade NIS 1-direktivet delvis elektricitet, gas och olja. I och med de ändringar som föreslås i NIS 2-direktivet ökar antalet aktörer inom energisektorn som omfattas av tillämpningsområdet betydligt jämfört med de aktörer som i Finland har identifierats som väsentliga med stöd av NIS 1-direktivet. Direktivet berör många organisationer inom energisektorn som bedriver sådan verksamhet som beskrivis ovan. Inom energisektorn är Energimyndigheten även i fortsättningen tillsynsmyndighet, liksom delvis även Säkerhets- och kemikalieverket.

Transportsektorn

Transportsektorn har omfattats av NIS 1-direktivet och bestämmelser om de väsentliga tjänsteleverantörernas skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem införlivades med den sektorsvisa lagstiftningen. Knappt tio aktörer inom lufttransport, sjöfart, spårtrafik och vägtransport har omfattats av lagstiftningen. NIS 1-direktivet genomfördes så att det gällde trafikledning, flygtrafiktjänst, bannätsförvaltare samt hamnar och flygfält i TEN-T-kärnnätet, vilket täcker in en del av de typer av aktör inom transportsektorn som har definierats i NIS 1-direktivet. I och med NIS 2-direktivet utvidgas bestämmelserna till att gälla även andra typer av aktör, såsom kommersiella lufttrafikföretag, järnvägsföretag och vissa transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster. Transport- och kommunikationsverket har varit tillsynsmyndighet.

I och med NIS 2-direktivet utvidgas tillämpningsområdet för skyldigheterna även inom transportsektorn. Nya typer av aktör som börjar omfattas av tillämpningsområdet är bland annat lufttrafikföretag, järnvägsföretag samt vissa företag som bedriver person- eller godstrafik. När det gäller transportsektorn omfattar tillämpningsområdet följande typer av aktör:

Lufttransport	Kommersiella lufttrafikföretag, flygplatsoperatörer och leverantörer av flygkontrolltjänster
Spårtrafik	Bannätsförvaltare och bolag som tillhandahåller trafikledningstjänster, järnvägsföretag och tjänsteleverantörer enligt spårtrafiklagen
Sjöfart	Vissa transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, hamninnehavare och aktörer som sköter anläggningar och utrustning i hamnar samt VTS-tjänsteleverantörer
Vägtransport	Trafikstyrning och tillhandahållare av intelligenta transportsystem

Inom transportsektorn ökar antalet aktörer som omfattas av tillämpningsområdet både med nya typer av aktör och inom de sektorer som har omfattats av NIS 1-direktivet. Inom transportsektorn kommer uppskattningsvis ca 40–80 aktörer att omfattas av tillämpningsområdet och de flesta finns inom sektorerna lufttransport, spårtrafik och sjöfart. Transport- och kommunikationsverket kommer även framöver att vara tillsynsmyndighet.

När det gäller de nya typerna av aktör finns det få förpliktande bestämmelser om informations- eller cybersäkerhet. Lufttransport är dock ett undantag där de gemensamma europeiska transportformsspecifika bestämmelserna kraftigt ökar. Det finns redan delvis gällande lagstiftning om informationssäkerheten inom lufttransport och från och med år 2026 ska den tillämpas på ett heltäckande sätt inom nästan hela lufttransportsektorn. EU-regelverket i fråga ska tillämpas på en större grupp aktörer än NIS 2-direktivet, och de skyldigheter som åläggs aktörerna motsvarar till stor del NIS 2-kraven.

Bankverksamhet och finansmarknadsinfrastruktur

När det gäller de typer av aktör som definieras i NIS 2-direktivet har bankverksamhet och finansmarknadsinfrastruktur omfattats av NIS 1-direktivet. Tillämpningsområdet har omfattat

kreditinstitut, operatörer av handelsplatser och centrala motparter. Den bankverksamhet och finansmarknadsinfrastruktur som definieras i bilaga I till NIS 2-direktivet omfattar samma typer av aktör. Finansinspektionen har varit och kommer att fortsätta att vara tillsynsmyndighet.

I stället för skyldigheterna enligt NIS 2-direktivet omfattas aktörerna i praktiken av de särskilda sektorsspecifika bestämmelserna för finanssektorn vad gäller åtgärder som är väsentliga med tanke på hanteringen av cybersäkerhetsrisker, och särskilt av DORA-förordningen. I DORA-förordningen åläggs aktörerna inom bank- och finanssektorn en mera långtgående skyldighet än skyldigheterna enligt NIS 2-direktivet att ha beredskap inför cyberhot, och på dessa aktörer tillämpas inte NIS 2-direktivets bestämmelser om hantering av cybersäkerhetsrisker, rapporteringsskyldighet, tillsyn eller verkställighet, utan i stället DORA-förordningen. NIS 2-direktivet medför inga betydande sektorsspecifika konsekvenser för bank- och finanssektorn.

Hälso- och sjukvårdssektorn

Inom hälso- och sjukvårdssektorn är vårdgivarna en väsentlig typ av aktör som omfattas av tillämpningsområdet. Tjänsteleverantörer inom social- och hälsovården har omfattats av NIS 1-direktivet och NIS 2-direktivet medför inga betydande förändringar i tillämpningsområdet för dessa typer av aktör. Välfärdsområdena har sedan ingången av 2023 varit offentliga tjänsteproducenter inom social- och hälsovården och bestämmelser om deras riskhanterings- och rapporteringsskyldigheter enligt NIS 2-direktivet finns i informationshanteringslagen, som en del av skyldigheterna för den offentliga sektorn. Privata aktörer inom social- och hälsovården omfattas av tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker. När det gäller NIS 1-skyldigheterna har Valvira varit tillsynsmyndighet.

Nya aktörer som börjar omfattas av tillämpningsområdet i och med NIS 2-direktivet är EU-referenslaboratorier, forskning och utveckling avseende läkemedel samt tillverkning av läkemedel, farmaceutiska basprodukter och medicintekniska produkter. Inom hälso- och sjukvårdssektorn leder NIS 2-direktivets utvidgade tillämpningsområde till att nya typer av aktör börjar omfattas av skyldigheterna. Följaktligen ökar antalet aktörer som ska övervakas. Valvira är även i fortsättningen tillsynsmyndighet.

För närvarande är enheter inom den offentliga hälso- och sjukvården skyldiga att ansluta sig till Kanta-tjänsterna. Detta förutsätter att man använder informationssystem som uppfyller säkerhetskraven och som certifieras av en extern aktör. Organisationerna ska också upprätta en säkerhetsplan. I lagen om kunduppgifter föreskrivs det om anslutning till Kanta-tjänsterna och certifiering samt ges Institutet för hälsa och välfärd behörighet att meddela föreskrifter om de säkerhetsegenskaper som krävs samt om innehållet i säkerhetsplanen. Dessutom föreskrivs det om skyldighet att anmäla avvikelser till Valvira. NIS 2-direktivet medför inga betydande tilläggsåtgärder för tjänsteleverantörerna inom hälso- och sjukvården.

Det finns ca 150–160 företag som är sådana privata tjänsteproducenter inom hälso- och sjukvården som på basis av personalstyrkan omfattas av tillämpningsområdet, dvs. som har en personal på minst 50 personer. Eftersom tillämpningsområdet kommer att omfatta även offentliga tjänsteproducenter samt de nya typer av aktör som börjar omfattas av tillämpningsområdet, kommer antalet aktörer inom denna sektor som ska övervakas att vara större än så här.

Dricks- och avloppsvatten

Leverantörer och distributörer av dricksvatten samt företag som samlar ihop, släpper ut och renar avloppsvatten omfattas av NIS 2-direktivets tillämpningsområde. Leverans och distribution av dricksvatten har omfattats av NIS 1-direktivet. I Finland genomfördes NIS 1-bestämmelserna genom en ändring av lagen om vattentjänster år 2018 så att de i fråga om både drickvatten och avloppsvatten gällde sådana vattentjänstverk som levererar vatten eller tar emot avloppsvatten till en volym av minst 5 000 kubikmeter i dygnet, samt sådana vattentjänstverk som levererar vatten till dessa verk eller som renar deras avloppsvatten. Bestämmelserna gäller alltså för närvarande vattenverk, avloppsvattenverk och sådana vattentjänstverk som fungerar som grossister. Aktörerna är uppskattningsvis ca 70.

Avloppsvattensektorn är en ny sektor inom regelverket, men aktörernas antal ökar inte av att den börjar omfattas av bestämmelserna. De nuvarande NIS-bestämmelserna i lagen om vattentjänster gäller nämligen alla anläggningar som överstiger en viss storlek och som sörjer för bortledande och behandling av spillvatten. Majoriteten av de anläggningar som omfattas av NIS 1-direktivets bestämmelser har hand om både dricksvatten och avloppsvatten.

I och med det som föreslås slopas det kriterium på 5 000 kubikmeter som avgränsar det nationella tillämpningsområdet och framöver är det i fråga om dricksvatten och avloppsvatten, på samma sätt som inom de andra sektorerna, typen av aktör och aktörens storlek som avgör om aktören omfattas av tillämpningsområdet. NIS 2-direktivet förväntas inte i väsentlig grad öka antalet aktörer som omfattas av tillämpningsområdet inom sektorn för dricks- och avloppsvatten. De anläggningar med en volym som understiger 5 000 kubikmeter som i dag inte omfattas av tillämpningsområdet kan på basis av personalen och omsättningen vara mikroaktörer eller små aktörer och följaktligen delvis också falla utanför NIS 2-direktivets tillämpningsområde. Man räknar med att antalet aktörer som omfattas av tillämpningsområdet hålls kvar på samma nivå eller minskar. Det är vanligt att aktörerna inom sektorn för dricks- och avloppsvatten bedriver verksamhet som motsvarar bägge typerna av aktör. Det beräknas att inom denna sektor uppgår antalet aktörer som omfattas av tillämpningsområdet och som överskrider storlekskriteriet eller definieras som kritiska med stöd av CER-direktivet till totalt ca 20–40 aktörer. Det finns också några aktörer som överskrider storlekskriteriet för väsentliga aktörer.

När det gäller sektorn för dricks- och avloppsvatten har närings-, trafik- och miljöcentralen varit tillsynsmyndighet. I fråga om vattentjänster koncentreras framöver tillsynen över de skyldigheter som har ålagts med stöd av NIS 2-direktivet till närings-, trafik- och miljöcentralen i Södra Savolax, som är tillsynsmyndighet oberoende av vilket område aktören är etablerad i.

Digital infrastruktur och digitala leverantörer

Av dem som levererar digital infrastruktur och digitala tjänster har leverantörer av internetbaserade marknadsplatser, sökmotorer och molntjänster redan omfattats av tillämpningsområdet för NIS 1-direktivet. Det har uppskattats att antalet leverantörer av internetbaserade marknadsplatser, sökmotorer eller molntjänster som är verksamma i Finland uppgår till totalt ca 70–80 aktörer, av vilka visserligen endast en del har sitt huvudkontor i Finland. Transport- och kommunikationsverket har varit tillsynsmyndighet.

I och med NIS 2-direktivet ökar antalet typer av aktör som omfattas av bestämmelsernas tillämpningsområde betydligt inom sektorn för digital infrastruktur. Nya typer av aktör inom sektorn för digital infrastruktur som börjar omfattas av tillämpningsområdet är leverantörer av nätverk för leverans av innehåll (content delivery network providers), tillhandahållare av betrodda tjänster, tillhandahållare av allmänna kommunikationsnät och kommunikationstjänster (teleföretag) och leverantörer av datacentraltjänster. Utöver dem utvidgas tillsynen över DNS-tjänster

till att även omfatta auktoritativa namnservrar, förutom rekursiva namnservrar. Dessutom räknas leverantörer av plattformar för sociala nätverkstjänster, tillhandahållare av internetbaserade marknadsplatser och leverantörer av sökmotorer till de digitala leverantörerna. En del av de aktörer som tillhandahåller de aktuella tjänsterna kan emellertid redan från tidigare ha omfattats av NIS 1-direktivets tillämpningsområde. Exempelvis en del av leverantörerna av datacentraltjänster eller tjänster för leverans av innehåll är sannolikt också leverantörer av molntjänster enligt NIS 1-direktivet.

Av de olika typerna av aktör omfattar tillämpningsområdet, oberoende av storlek, tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster. I och med att storlekskriteriet inte tillämpas ökar antalet sådana här aktörer inom tillämpningsområdet. När det gäller andra typer av aktör tillämpas storlekskriteriet även inom sektorn för digital infrastruktur, om inte aktörerna omfattas av något annat undantag, såsom att de identifieras som väsentliga aktörer med stöd av CER-direktivet.

Inom sektorn för digital infrastruktur uppskattas antalet aktörer som omfattas av tillämpningsområdet öka betydligt till följd av att tillämpningsområdet utvidgas. I fråga om dessa typer av aktör förutsätter tillhandahållandet av tjänster att tjänsteleverantören redan i utgångsläget har en hög nivå på hanteringen av cybersäkerhetsrisker. När det gäller tillhandahållare av allmänna kommunikationsnät och kommunikationstjänster samt tillhandahållare av betrodda tjänster har aktörerna på det sätt som beskrivs i avsnitt 1.1.3 och 1.1.4 redan tidigare omfattats av informationssäkerhetskrav. NIS 2-direktivet beräknas inte medföra några betydande ytterligare skyldigheter för aktörerna. Det har uppskattats att det finns totalt ca 30 tillhandahållare av elektroniska betrodda tjänster som omfattas av tillämpningsområdet, och av dessa finns det en som tillhandahåller kvalificerade betrodda tjänster. Transport- och kommunikationsverket kommer även framöver att vara tillsynsmyndighet.

Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll samt tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster ska omfattas av jurisdiktionen i enbart den medlemsstat där de har sitt huvudsakliga etableringsställe. I fråga om sådana här aktörer har det uppskattats att det finns endast ett fåtal av dem som är etablerade i Finland, och i enlighet med bestämmelserna om internationell behörighet är det den medlemsstat där en aktör är etablerad som ansvarar för tillsynen över aktören. Det har uppskattats att det finns totalt ca 20–30 leverantörer av DNS-tjänster och några tiotal leverantörer av datacentraltjänster eller nätverk för leverans av innehåll som omfattas av tillämpningsområdet, dvs. som är etablerade i Finland.

Förvaltning av informations- och kommunikationstekniktjänster

Den sektor som gäller leverantörer av IKT-tjänster är en helt ny sektor jämfört med tillämpningsområdet för NIS 1-direktivet. De lagstadgade skyldigheter att hantera cybersäkerhetsrisker och rapportera om dem som följer av NIS 2-direktivet är nya för aktörerna inom denna sektor, vilka börjar omfattas av tillämpningsområdet för bestämmelserna som en ny typ av aktör.

Sektorn för leverantörer av IKT-tjänster (ICT service providers) består av leverantörer av hanterade tjänster och hanterade säkerhetstjänster mellan företag. Villkoret är att de uppfyller det allmänna storlekskriteriet, dvs. företagen ska vara medelstora eller större. Även leverantörerna av IKT-tjänster omfattas av jurisdiktionen i enbart den medlemsstat där de har sitt huvudsakliga

etableringsställe. Det har uppskattats att det finns totalt några tiotal aktörer som har sitt huvudsakliga etableringsställe i Finland och som omfattas av tillämpningsområdet för NIS 2-direktivet. För dessa aktörer är skyldigheterna enligt NIS 2-direktivet i huvudsak nya skyldigheter. I fråga om dessa typer av aktör förutsätter tillhandahållandet av tjänster att tjänsteleverantören redan i utgångsläget har en hög nivå på hanteringen av cybersäkerhetsrisker. Därför beräknas inte iakttagandet av riskhanterings- och rapporteringsskyldigheterna medföra några betydande kostnader för aktörerna. Transport- och kommunikationsverket är tillsynsmyndighet.

Rymden

Rymden är en ny sektor inom NIS-direktivets tillämpningsområde. Inom denna sektor gäller bestämmelserna aktörer som bedriver markstationsverksamhet och andra operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster. När det gäller markbaserad infrastruktur hör de medelstora och stora aktörerna till de väsentliga aktörerna, och de små aktörerna räknas som andra aktörer. Enligt bedömningen är majoriteten av företagen i Finland små.

När det gäller sådana verksamhetsutövare som avses i lagen om markstationer har aktörerna på det sätt som beskrivs i avsnitt 3.9 redan tidigare omfattats av informationssäkerhetskrav. Bedömningen är att NIS 2-direktivet inte kommer att medföra några betydande ytterligare skyldigheter för aktörerna. I förarbetena till lagen om markstationer och vissa radaranläggningar är bedömningen att den verksamhet inom rymdsektorn som omfattas av tillämpningsområdet för skyldigheterna är jämförelsevis liten i Finland (RP 113/2022 rd, s. 17–20).

Post- och budtjänster

Post- och budtjänster är ett nytt tillämpningsområde för NIS-direktivet. Det har inte tidigare ställts några cybersäkerhetskrav på post- och budtjänster, vilket betyder att de skyldigheter som nu föreslås är nya för aktörerna och att dessa är en ny grupp av aktörer inom tillämpningsområdet för NIS-skyldigheterna. Tillämpningsområdet ska omfatta tillhandahållare av posttjänster och tillhandahållare av budtjänster. Med posttjänster avses tjänster såsom insamling, sortering, transport och distribution av postförsändelser. Med postförsändelser avses uttryckligen sådana färdiga försändelser som den som tillhandahåller samhällsomfattande tjänster ska transportera och som har adresserats till en viss mottagare. Förutom brevförsändelser kan dessa försändelser även vara exempelvis böcker, kataloger, tidningar och periodiska publikationer samt postpaket som innehåller varor med eller utan kommersiellt värde.

När det gäller post- och budsektorn beräknas NIS 2-aktörerna utgöra en liten grupp i Finland. I sin utredning om postmarknaden 2020[2] konstaterade Transport- och kommunikationsverket att i fråga om volymen beräknas budbranschen vara ganska liten. Enligt uppgifterna från Transport- och kommunikationsverket kan antalet små aktörer som tillhandahåller budtjänster trots den lilla distributionsvolymen ändå vara rätt stort. Enligt Transport- och kommunikationsverkets bedömning kommer merparten av de bud- och distributionsföretag som är verksamma i Finland sannolikt ändå inte att omfattas av tillämpningsområdet för bestämmelserna i och med att tillämpningsområdet är avgränsat på basis av storlek. När det gäller posttjänster kommer i Finland åtminstone den som tillhandahåller samhällsomfattande tjänster och som fungerar som tillhandahållare av posttjänster enligt postdirektivet att omfattas av tillämpningsområdet. Denna aktör är för närvarande Posti Ab. Förutom Posti Ab beräknas tillämpningsområdet i Finland omfatta

[2] Utredning om postmarknaden, Transport- och kommunikationsverket (2020). (På finska)

endast enstaka aktörer inom sektorn för post- och budtjänster. Transport- och kommunikationsverket är tillsynsmyndighet.

Avfallshantering

Avfallshantering är ett nytt tillämpningsområde för NIS 2-direktivet. Skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem är nya för aktörerna inom avfallshanteringen och dessa aktörer är nya aktörer att övervaka. Det är närings-, trafik- och miljöcentralen i Södra Savolax som ska utöva tillsyn över aktörerna inom avfallshanteringen.

Ett stort antal aktörer av varierande slag och storlek är verksamma inom avfallshanteringssektorn. Med avfallshantering avses insamling, transport, återvinning och bortskaffande av avfall, inbegripet kontroll och uppföljning av sådan verksamhet och efterbehandling av platser för bortskaffande av avfall samt verksamhet som mäklare.

Majoriteten av de behandlingsanläggningar för avfall och avfallstransportföretag som är verksamma i Finland är små lokala eller regionala företag som på basis av sin storlek inte kommer att omfattas av de bestämmelser som nu föreslås. Det finns uppskattningsvis ca 400 behandlingsanläggningar för avfall som har tillstånd av regionförvaltningsverket eller som står under tillsyn av NTM-centralerna samt ca 2 000–3 000 avfallstransportföretag som är godkända för anteckning i det avfallshanteringsregister som avses i avfallslagen. Den största delen av dem är lokala eller regionala företag som inte kommer att omfattas av tillämpningsområdet, men bland dem finns det också aktörer som uppfyller eller överskrider storlekskriteriet för tillämpningsområdet. Med beaktande av storlekskriteriet beräknas det att ett tiotal aktörer kommer att omfattas av tillämpningsområdet inom avfallshanteringssektorn.

Skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem är nya för aktörerna inom avfallshanteringen. Det finns allmän beredskapslagstiftning om avfallshantering i 15 och 52 § i miljöskyddslagen och 3, 6 och 16 § i miljöskyddsförordningen (beredskapsskyldighet) samt i 120 § i avfallslagen och 41 § i avfallsförordningen (plan för uppföljning och kontroll av avfallsbehandlingen). Enligt bestämmelserna ska verksamhetsutövarna ha beredskap att hindra olyckor och andra exceptionella situationer och att begränsa de skadliga konsekvenserna av dem för hälsan och miljön. En verksamhetsutövare med tillstånd av regionförvaltningsmyndigheten ska utifrån en riskbedömning utarbeta en beredskapsplan, reservera behövliga anordningar och annan utrustning, utarbeta instruktioner, testa anordningarna och utrustningen samt öva åtgärder inför eventuella olyckor och andra exceptionella situationer. Bestämmelserna gäller emellertid inte särskilt nätverks- och informationssäkerhetsfrågor och uppfyller inte heller kraven i NIS 2-direktivet.

De aktörer som omfattas av NIS 2-direktivets tillämpningsområde är medelstora och större aktörer, vars huvudsakliga verksamhetsområde är avfallshantering. Enligt statistikcentralen och företags- och organisationsdatasystemet (FODS) finns det vad gäller personalstyrkan ca 30 sådana här företag i Finland. På basis av personalstyrkan kan man klassificera sex av dessa företag som stora företag och följaktligen som väsentliga aktörer. På basis av omsättning och balansomslutning kommer ca 30 företag att omfattas av tillämpningsområdet för bestämmelserna. Bland dessa finns det ett flertal företag som ägs av kommuner samt samkommuner. De största aktörerna ingår i företagskoncerner, vilka kan omfattas av tillämpningsområdet för bestämmelserna även vad gäller annan verksamhet än avfallshantering.

Tillverkning, produktion och distribution av kemikalier

Tillverkning, produktion och distribution av kemikalier är en ny sektor inom NIS-regelverket. Sådana företag som tillverkar och distribuerar kemikalier och som uppfyller storlekskriteriet omfattas av tillämpningsområdet. För aktörerna är de skyldigheter att hantera cybersäkerhetsrisker och rapportera om dem som åläggs i lag nya och för tillsynsmyndigheten är aktörerna en ny grupp av aktörer som ska övervakas. Gruppen nya aktörer som börjar omfattas av tillämpningsområdet är storleksmässigt betydande. Säkerhets- och kemikalieverket är tillsynsmyndighet.

Produktion, bearbetning och distribution av livsmedel

Produktion, bearbetning och distribution av livsmedel är en ny sektor inom NIS-regelverket. Tillämpningsområdet omfattar sådana livsmedelsföretag som bedriver industriell produktion eller bearbetning, distribution, parti- och detaljhandel. Inom livsmedelssektorn har de stora företagen en central roll i Finland, inom både tillverkningsindustrin och handeln. Sektorn är mycket beroende av import och det ömsesidiga beroendet av andra sektorer är stort. Ur ett cybersäkerhetsperspektiv utgör livsmedelssektorn en komplicerad helhet: det finns verksamhetsställen i alla landskap, men vissa företag inom sektorn (t.ex. de företag som producerar olja) är koncentrerade regionalt. I vårt land med dess långa avstånd tryggas å andra sidan matförsörjningen genom en utspridd produktion och direkta leveranser.

Skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem är nya för aktörerna inom livsmedelssektorn och dessa aktörer är nya aktörer att övervaka. När det gäller NIS 2-skyldigheterna är det Livsmedelsverket som utövar tillsyn över aktörerna inom livsmedelssektorn. Annan tillsyn över aktörerna inom livsmedelssektorn utövas av kommunerna.

Inom livsmedels- och dryckesindustrin har närmare 65 procent av verksamhetsställena under fem anställda (Lukes statistik). Över 90 procent av alla verksamhetsställen har färre än 20 anställda och det finns 32 verksamhetsställen med över 200 anställda (Livsmedelsindustriförbundet ETL, Faktagaffeln 2021). Utifrån dessa uppgifter kan man sluta sig till att NIS 2-direktivet kommer att gälla några tiotal industriföretag. Det finns ca 2 800 affärer inom dagligvaruhandeln (Finlands Dagligvaruhandel 2022). Antalet hypermarketar är 158, varuhus 88 och stora supermarketar 712. Omsättningen för vissa enskilda hypermarketar överstiger gränsen på 50 miljoner euro. Verksamheten inom livsmedelssektorn kännetecknas av att leverans- och partikedjan spelar en mycket viktig roll för kontinuiteten i verksamheten. Inom näthandeln finns det ett flertal aktörer och deras betydelse ökar.

Det finns sju centrala partiaktörer. Utöver dem finns det ett flertal små partiförsäljare inom branschen. Av de centrala partiaktörerna är fem verksamma inom foodservice, dvs. matservicesektorn. Livsmedelsindustrin levererar ca 30 procent av foodservice-aktörernas råvaror. De centrala partiaktörerna börjar omfattas av NIS 2-tillämpningsområdet på basis av sin storlek eller för att de är väsentliga aktörer enligt CER-direktivet.

Foodservice-sektorn betjänar yrkeskök på såväl den privata som den offentliga sidan. I Finland finns det över 16 000 yrkeskök, vilka tillreder ca 749 miljoner måltider om året. Sektorn kännetecknas av att det finns många aktörer av varierande storlek. Det finns några matserviceaktörer som är centrala med tanke på försörjningsberedskapen och i deras verksamhet är informations- och cybersäkerheten av väsentlig betydelse. Enligt Foodservice-partihandlarna gör ca 85–90 procent av de offentliga aktörerna sina livsmedelsbeställningar i maskinläsbar form. Foodservice är en verksamhet som bygger på nätverk, där var och en har sin egen roll. Därför kan verksamheten vara känslig för cyberstörningar.

Antalet aktörer med anknytning till servering är stort, men den största delen av dem är restauranger. I fråga om yrkeskök finns det cirka sex centrala aktörer, som baserar sig på foodservice-partihandeln. Utöver dem finns det ett flertal små partiförsäljare inom branschen. Livsmedelsindustrin levererar ca 30 procent av foodservice-aktörernas råvaror.

Strukturen av de företag inom livsmedelsbranschen som livsmedelstillsynsmyndigheten känner till och övervakar beskrivs i tabell x på basis av verksamhetsställena. Livsmedelstillsynsmyndighetens register grundar sig på den verksamhet som bedrivs på de olika verksamhetsställena och är därför inte helt inriktat på företag eller ägare. När det gäller produktion och bearbetning av livsmedel delas verksamhetsställena och funktionerna in i olika riskklasser i förhållande till de livsmedelssäkerhetsfaktorer som ansluter sig till funktionerna och omfattningen av verksamheten, dvs. produktionsvolymen. När det gäller den högsta riskklassen är produktionsvolymen vid anläggningarna inom mjölkbranschen två miljoner liter i fråga om den mjölk som mottas. På riksnivå är mängden två miljarder liter. I fråga om anläggningarna inom kött-, fisk- och äggbranschen är produktionsvolymen över tio miljoner kilogram hos objekten i den högsta riskklassen. När det gäller annan tillverkning ligger gränsen vid en miljon kilogram eller 100 miljoner liter. De viktigaste aktörerna när det gäller yrkeskök är de matserviceaktörer som producerar mat till sjukhus, äldreboenden och daghem och som börjar omfattas av NIS 2 i och med att de är kritiska aktörer enligt CER-direktivet.

När det gäller handeln finns det 483 objekt som hör till den högsta riskklassen (> 1 000 m2). Av dessa urskiljer sig sex partiaffärer och ett detaljhandelsobjekt med mycket hög risk. Livsmedelsförpackningar är av kritisk betydelse för produktionen, bearbetningen och distributionen av livsmedel. Enligt livsmedelstillsynsmyndighetens riskbedömning finns det i fråga om kontaktmaterial för livsmedel fem högriskaktörer.

Tillämpningsområdet för förslaget omfattar sådana företag som är medelstora eller större. På basis av de register som förs av livsmedelstillsynsmyndigheterna uppskattas dessa företag uppgå till över 300 inom livsmedelssektorn. Av dem är uppskattningsvis ca 70–100 aktörer väsentliga aktörer.

Tabell x. Uppskattning av antalet viktiga och väsentliga aktörer enligt NIS 2-direktivet på basis av de verksamhetsställen som var införda i livsmedelstillsynsmyndighetens register år 2022

Sektor	Uppskattning av antalet viktiga aktörer enligt NIS 2	Uppskattning av antalet väsentliga aktörer enligt NIS 2
Livsmedelstransporter	7	2
Lagring och djupfrysning av livsmedel	10	2
Tillverkning av livsmedel, med undantag för mjölk-, kött-, fisk- ägg- och spannmålsbranschen	19	8

Fiskbranschen	62	5
Köttbranschen	24	11
Mjölkbranschen	13	2
Äggbranschen	7	4
Export och import	6	2
Spannmåls- och växtbranschen	4	2
Försäljning	**-**	**7**
Matserviceaktörer	-	3
Tillverkning av livsmedelsförpackningar	-	5
Totalt	162	53

Tillverkningssektorn

Tillverkningssektorn är ett nytt tillämpningsområde i NIS 2-direktivet. Tillämpningsområdet omfattar de företag som tillverkar sådana produkter som avses i bilagan till lagen och som uppfyller storlekskriteriet. För aktörerna är de skyldigheter att hantera cybersäkerhetsrisker och rapportera om dem som åläggs i lag nya och för tillsynsmyndigheten är aktörerna en ny grupp av aktörer som ska övervakas. Gruppen nya aktörer som börjar omfattas av tillämpningsområdet är storleksmässigt betydande. Tillsynsmyndigheter är dels Fimea, dels Transport- och kommunikationsverket och dels Säkerhets- och kemikalieverket.

När det gäller tillverkningssektorn omfattar tillämpningsområdet medelstora eller större aktörer som bedriver följande verksamheter:

Medicintekniska produkter	Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
Tillverkning av datorer, elektronikvaror och optik	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2 Tillverkning av datorer, elektronikvaror och optik Tillverkning av elektroniska komponenter och kretskort Tillverkning av elektroniska komponenter Tillverkning av kretskort Tillverkning av datorer och kringutrustning Tillverkning av datorer och kringutrustning Tillverkning av kommunikationsutrustning Tillverkning av kommunikationsutrustning

	Tillverkning av hemelektronik Tillverkning av hemelektronik Tillverkning av instrument och apparater för mätning, provning och navigering samt ur Tillverkning av instrument och apparater för mätning, provning och navigering Urtillverkning Tillverkning av strålningsutrustning samt elektromedicinsk och elektroterapeutisk utrustning Tillverkning av strålningsutrustning samt elektromedicinsk och elektroterapeutisk utrustning Tillverkning av optiska instrument och fotoutrustning Tillverkning av optiska instrument och fotoutrustning Tillverkning av magnetiska och optiska medier Tillverkning av magnetiska och optiska medier
Tillverkning av elapparatur	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2 Tillverkning av elapparatur Tillverkning av elmotorer, generatorer och transformatorer samt eldistributions- och elkontrollapparater Tillverkning av elmotorer, generatorer och transformatorer Tillverkning av eldistributions- och elkontrollapparater Batteri- och ackumulatortillverkning Batteri- och ackumulatortillverkning Tillverkning av ledningar och kablar och kabeltillbehör Tillverkning av optiska fiberkablar Tillverkning av andra elektroniska och elektriska ledningar och kablar Tillverkning av kabeltillbehör Tillverkning av belysningsarmatur Tillverkning av belysningsarmatur Tillverkning av hushållsmaskiner och hushållsapparater Tillverkning av elektriska hushållsmaskiner och hushållsapparater Tillverkning av icke-elektriska hushållsmaskiner och hushållsapparater Tillverkning av annan elapparatur Tillverkning av annan elapparatur
Tillverkning av övriga maskiner	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2 Tillverkning av övriga maskiner Tillverkning av maskiner för allmänt ändamål Tillverkning av motorer och turbiner utom för luftfartyg och fordon Tillverkning av fluidteknisk utrustning Tillverkning av andra pumpar och kompressorer Tillverkning av andra kranar och ventiler Tillverkning av lager, kugghjul och andra delar för kraftöverföring Tillverkning av andra maskiner för allmänt ändamål Tillverkning av ugnar och brännare

	Tillverkning av lyft- och godshanteringsanordningar Tillverkning av kontorsmaskiner och kontorsutrustning (utom datorer och kringutrustning) Tillverkning av motordrivna handverktyg Tillverkning av maskiner och apparater för kyla och ventilation utom för hushåll Övrig tillverkning av maskiner för allmänt ändamål Tillverkning av jord- och skogsbruksmaskiner Tillverkning av jord- och skogsbruksmaskiner Tillverkning av maskiner för metallbearbetning och verktygsmaskiner Tillverkning av maskiner för metallbearbetning Tillverkning av övriga verktygsmaskiner Tillverkning av andra specialmaskiner Tillverkning av maskiner för metallurgi Tillverkning av gruv-, bergbrytnings- och byggmaskiner Tillverkning av maskiner för framställning av livsmedel, drycker och tobaksvaror Tillverkning av maskiner för produktion av textil-, beklädnads- och lädervaror Tillverkning av maskiner för produktion av massa, papper och papp Tillverkning av maskiner för gummi och plast Tillverkning av diverse övriga specialmaskiner
Tillverkning av motorfordon, släpfordon och påhängsvagnar	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2 Tillverkning av motorfordon, släpfordon och påhängsvagnar Motorfordonstillverkning Motorfordonstillverkning Tillverkning av karosserier för motorfordon; tillverkning av släpfordon och påhängsvagnar Tillverkning av karosserier för motorfordon; tillverkning av släpfordon och påhängsvagnar Tillverkning av delar och tillbehör till motorfordon Tillverkning av elektrisk och elektronisk utrustning för motorfordon Tillverkning av andra delar och tillbehör till motorfordon
Tillverkning av andra transportmedel	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2 Tillverkning av andra transportmedel Skepps- och båtbyggeri Byggande av fartyg och flytande materiel Byggande av fritidsbåtar Tillverkning av rälsfordon Tillverkning av rälsfordon Tillverkning av luftfartyg, rymdfarkoster o.d. Tillverkning av luftfartyg, rymdfarkoster o.d. Tillverkning av militära stridsfordon Tillverkning av militära stridsfordon Övrig tillverkning av transportmedel

	Tillverkning av motorcyklar Tillverkning av cyklar och invalidfordon Övrig transportmedelstillverkning

Det finns ett betydande antal företag som bedriver sådan verksamhet som hör till tillverkningssektorn. För de aktörer som omfattas av tillämpningsområdet är de lagstadgade skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem nya skyldigheter. Den kontinuerliga digitaliseringen av tillverkningssektorn har lett till en allt större yta för cyberangrepp och ett behov för aktörerna att på eget initiativ utveckla hanteringen av cybersäkerhetsrisker och beredskapen inför störningar. En betydande andel av de företag som bedriver tillverkningsverksamhet är storleksmässigt också små företag, vilket betyder att de inte uppfyller storlekskriteriet för tillämpningsområdet.

Forskningsorganisationer

Forskningsorganisationer omfattades inte av tillämpningsområdet för NIS 1-direktivet. Enligt NIS 2-direktivet avses med forskningsorganisation en entitet 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 inbegriper utbildningsinstitutioner. Endast några enstaka aktörer har identifierats nationellt som sådana aktörer som omfattas av tillämpningsområdet enligt denna definition. För aktörerna är de lagstadgade skyldigheterna att hantera cybersäkerhetsrisker och rapportera om dem nya skyldigheter. Transport- och kommunikationsverket är tillsynsmyndighet.

Offentlig förvaltning

Aktörerna inom den offentliga förvaltningen börjar omfattas av tillämpningsområdet för NIS-skyldigheterna som en ny typ av aktör, i och med att den offentliga förvaltningen inte har omfattats av tillämpningsområdet för NIS 1-direktivet. I fråga om aktörerna inom den offentliga förvaltningen tillämpas inte storlekskriteriet och tillämpningsområdet bestäms i enlighet med det som föreskrivs i lagen om informationshantering inom den offentliga förvaltningen. Skyldigheterna är nya för den offentliga förvaltningen och tillsynen över dem är en ny uppgift. Transport- och kommunikationsverket är tillsynsmyndighet.

Via tillämpningsområdet för informationshanteringslagen börjar sammanlagt ca 160 aktörer omfattas av NIS 2-skyldigheterna som aktörer inom den offentliga förvaltningen. Denna siffra inbegriper statens centralförvaltning, ämbetsverk och inrättningar, statens affärsverk och självständiga offentligrättsliga inrättningar samt välfärdsområdena och välfärdssammanslutningar, inbegripet Helsingfors stad. Om beskickningarna i utlandet räknas med som separata aktörer uppgår antalet aktörer inom sektorn för offentlig förvaltning till totalt ca 250 aktörer.

4.2.3 De huvudsakliga konsekvenserna för registrarer

Förmedling av domännamn omfattas inte av riskhanterings- och rapporteringsskyldigheterna enligt NIS 2-direktivet, om inte aktören tillhandahåller även någon annan tjänst som omfattas av tillämpningsområdet, såsom DNS-tjänster. Registrarer åläggs emellertid vissa andra skyldigheter som påverkar deras verksamhet. Den viktigaste av dem är skyldigheten att utarbeta och offentliggöra riktlinjer och förfaranden för säkerställande av att uppgifterna i domännamnsregistret är korrekta och för utlämnande av registreringsuppgifter om domännamn. Dessutom ska

en registrar göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga, samt svara den som begär åtkomst till registreringsuppgifter utan obefogat dröjsmål och senast inom 72 timmar efter det att registraren har tagit emot en laglig och vederbörligen motiverad begäran.

Skyldigheten att offentliggöra registreringsuppgifter om domännamn kan kräva att aktörerna utvecklar sina system för att rent tekniskt kunna offentliggöra registreringsuppgifterna. Bedömningen är att de förslag som gäller säkerställande av att uppgifterna i domännamnsregistret är korrekta inte har några betydande konsekvenser för registrarerna, i och med att dessa aktörer redan nu enligt lag är skyldiga att i domännamnsregistret anteckna korrekta och uppdaterade uppgifter om domännamnsanvändaren som identifierar användaren. Förslagen kan emellertid ha konsekvenser av särskilt engångsnatur när bestämmelserna börjar tillämpas.

4.3 Ekonomiska konsekvenser

Konsekvenser för företagen

Det som föreslås anses ha ekonomiska konsekvenser för de företag som omfattas av tillämpningsområdet, särskilt via riskhanterings- och rapporteringsskyldigheterna samt lämnandet av uppgifter till förteckningen över aktörer. Förslaget ökar kostnaderna och den administrativa bördan för de aktörer som omfattas av tillämpningsområdet, men förbättrad cybersäkerhet anses även ha positiva konsekvenser för såväl företagens förutsättningar att bedriva affärsverksamhet som samhällsekonomin och samhällets kristålighet. Investering i hanteringen av cybersäkerhetsrisker förbättrar driftssäkerheten för de företag som omfattas av tillämpningsområdet och främjar affärsverksamhet i ett allt mer digitaliserat samhälle. Färre cybersäkerhetsstörningar gör att aktörerna kan undvika sådana kostnader som beror på skadliga konsekvenser av störningar.

Det anses att förslaget har kostnadseffekter för företagen särskilt via den skyldighet som gäller riskhantering. Förutom de kostnader som beror på riskhanteringsskyldigheterna kommer skyldigheten att rapportera om betydande incidenter och skyldigheten att anmäla sig till den förteckning över aktörer som tillsynsmyndigheten för att medföra smärre kostnader för aktörerna. Kostnaderna för dessa skyldigheter bedöms som helhet vara små i förhållande till riskhanteringen och genomförandet av riskhanteringsåtgärder. Det kan också uppstå kostnader för företagen på grund av sådana tillsynsåtgärder som tillsynsmyndigheten riktar mot ett företag.

Kostnaderna för riskhantering och riskhanteringsåtgärder kan delas in i engångskostnader och löpande kostnader. Beloppet av de kostnader som förslaget ger upphov till påverkas av nivån på den hantering av cybersäkerhetsrisker som företaget har haft sedan tidigare, verksamhetens art och omfattning samt antalet och kvaliteten på de kommunikationsnät och informationssystem som används i verksamheten.

I allmänhet uppgår IT-kostnaderna till i genomsnitt ca 4–5 procent av ett företags omsättning. Beroende på aktörens storlek, cybermognad och sektorn är variationsintervallet 1,5–5 procent. Exempelvis inom livsmedelssektorn bedömdes kostnaderna för cybersäkerhet uppgå till i genomsnitt 0,28 procent av den årliga omsättningen och inom tillverkningssektorn till 0,69 procent av den årliga omsättningen.[3] Enligt kommissionens uppskattning beräknas kostnaderna för

[3] Insta (2023) Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille (utredning om de ekonomiska konsekvenserna av riskhanteringsskyldigheterna enligt cybersäkerhetsdirektivet, dvs. NIS 2-direktivet, för livsmedelssektorn och tillverkningssektorn)

cybersäkerhet uppgå till i genomsnitt 0,52 procent av den årliga omsättningen inom de olika sektorerna.

Enligt kommissionens uppskattning beräknas skyldigheterna enligt NIS 2-direktivet under de första åren efter genomförandet öka de nuvarande IT-kostnaderna för cybersäkerhet för en aktör som omfattas av tillämpningsområdet med i genomsnitt 12–22 procent, beroende på om den aktör som berörs av skyldigheterna har omfattats av tillämpningsområdet för NIS 1-direktivet.[4]

Kostnaderna för säkerställande av cybersäkerheten räknas oftast mera allmänt till aktörernas totala IKT-kostnader, vilket betyder att det är svårt att separera ut de kostnader som gäller enbart cybersäkerhet, och en sådan separation är ofta svårdefinierbar. Till kostnaderna för cybersäkerhet kan man allmänt räkna olika typer av utgifter såsom utrustning, programvara och datatrafikförbindelser. Andra kostnader som främjar cybersäkerhet kan vara administrativa utgifter, personalutgifter, olika kvalitetsrevisioner och utbildningar. Vidare bör man beakta skyldigheterna enligt direktivet att säkerställa nätverks- och informationssystemens fysiska säkerhet, vilket kan medföra utgifter för exempelvis installation och underhåll av olika typer av utrustning och kablar. Cyberattacker och cyberstörningar samt andra kränkningar av datasäkerhet och dataskydd kan ha betydande negativa ekonomiska konsekvenser för både de företag som tillhandahåller tjänster via ett informationssystem eller kommunikationsnät och dem som använder sig av tjänsterna. Kostnaderna för cyberstörningar kan uppskattas grovt utifrån vad verkliga cyberstörningar har kostat för aktörerna. Det är många olika faktorer som påverkar kostnaderna för störningar, såsom störningens art och omfattning, dess konsekvenser för kontinuiteten i aktörens och sektorns verksamhet samt hur snabbt aktören återhämtar sig från störningen. Störningar kan orsaka både direkta utrednings- och reparationskostnader och indirekta kostnader på grund av exempelvis avbrott i verksamheten eller ett skadat anseende. I och med att cyberstörningarna ökar exponentiellt har kostnaderna för dem också ökat totalt sett. De direkta kostnaderna för exempelvis den cyberattack som riktades mot staden Lahtis år 2019 uppgick till 685 670 euro.[5] År 2020 spred sig ett sabotageprogram som var inriktat på företaget SolarWinds övervakningsverktyg Orion Platform till tusentals organisationer. Konsekvenserna av cyberattacken uppgick till i genomsnitt 11 procent av den årliga omsättningen eller ca 12 miljoner dollar per företag. [6] För företaget SolarWinds orsakade händelsen kostnader som uppgick till åtminstone 40 miljoner dollar år 2021. Förutom detta bedömdes det att företagets anseende orsakades betydande skada, vilket innebär att kostnaderna kan uppskattas vara mycket större.[7] Man kan grovt konstatera att kostnaderna för olika cyberstörningar i allmänhet är betydligt större än kostnaderna för sådan hantering av cybersäkerhetsrisker som sker i ren överensstämmelse med skyldigheterna enligt förslaget. Om ett företag genom hanteringen av cybersäkerhetsrisker kan avvärja de skadliga konsekvenserna av störningar i cybersäkerheten har detta positiva ekonomiska konsekvenser för företaget. Kommissionen har bedömt att kostnaderna för cybersäkerhetsstörningar och -kriser kan uppgå till totalt 118 miljarder euro på tio år på EU-nivå.

---

[4] Summering av kommissionens konsekvensbedömning i samband med antagandet av NIS 2-direktivet: SWD(2020) 344 final https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0344:FIN:EN:PDF

[5] YLE (2019) ”En cyberattack har kostat staden Lahtis närmare 690 000 euro” (på finska) https://yle.fi/a/3-10914550

[6] Cybersecurity Impact Report 2021 https://www.ironnet.com/resource-library/2021-cybersecurity-impact-report

[7] Cybersecurity Dive (2021) One year later: has SolarWinds changed how industry builds software? https://www.cybersecuritydive.com/news/solarwinds-1-year-later-cyber-attack-orion/610990/

Det som föreslås kan anses ha konsekvenser som främjar företagens konkurrenskraft på ett positivt sätt, i och med att det ålägger de företag som omfattas av direktivet att upprätthålla en hög nivå på cybersäkerheten. Genom förslaget åläggs företagen även att beakta cybersäkerheten i leveranskedjorna, vilket betyder att ett företag som ser till att dess cybersäkerhet är på en tillräckligt hög nivå med större sannolikhet är en samarbetspartner och konsumentens val. Till exempel det sabotageprogram som drabbade företaget SolarWinds påverkade även andra aktörer i företagets leveranskedja, vilka också orsakades kostnader på grund av reparationsåtgärder.

I samband med beredningen av denna proposition lät kommunikationsministeriet göra en utredning om de kostnader som riskhanteringsskyldigheten enligt artikel 21 i NIS 2-direktivet kommer att orsaka de finländska företagen. Målet med utredningen var att bedöma kostnaderna av riskhanteringsskyldigheten enligt direktivet inom sektorerna för livsmedel och tillverkning, eftersom företagen inom dessa sektorer inte har omfattats av tillämpningsområdet för NIS 1-direktivet och det finns ett betydande antal företag inom dessa sektorer som i och med denna proposition kommer att börja omfattas av tillämpningsområdet som nya aktörer. Utredningen genomfördes av Insta Advance Oy (nedan Insta). Utredningen är tillgänglig i statsrådets tjänst för projektinformation (Hankeikkuna) under projektnummer LVM0044:00/2022 (länk: https://valtioneuvosto.fi/sv/projektet?tunnus=LVM044:00/2022).

Utredningen genomfördes med utgångspunkt i artikel 21 i NIS 2-direktivet om de delområden som ska beaktas i riskhantering och riskhanteringsåtgärder. Med stöd av de föreslagna 7–9 § i lagen om hantering av cybersäkerhetsrisker motsvarar de delområden som ska beaktas i riskhanteringen artikel 21 i NIS 2-direktivet.

Enligt utredningen orsakar riskhanteringsskyldigheten företagen inom livsmedels- och tillverkningssektorn en engångskostnad på i genomsnitt ca 320 000 euro per företag, av vilket 27 procent utgör arbetskostnader och 73 procent övriga kostnader. De kostnader som är av löpande karaktär uppgår till i genomsnitt ca 214 000 euro, av vilket 26 procent är arbetskostnader och 74 procent övriga kostnader. Inom livsmedelssektorn uppskattades genomsnittskostnaderna vara lägre än inom tillverkningssektorn. Inom livsmedelssektorn uppskattades engångskostnaderna uppgå till 274 000 euro och de löpande kostnaderna till 148 000 euro. Inom tillverkningssektorn uppskattades engångskostnaderna uppgå till 367 000 euro och de löpande kostnaderna till 279 000 euro.

Av de delområden som ska beaktas i riskhanteringen var bedömningen att kostnader är förenade med de delområden som gäller strategier för riskanalys och informationssystemens säkerhet, incidenthantering, säkerställande av säkerheten i leveranskedjan och säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem. Varje delområde som ska beaktas i riskhanteringen uppskattades orsaka engångskostnader till mellan 12 100 och 52 900 euro och de löpande kostnaderna till mellan 4 500 och 39 500 euro.

I utredningen försökte man också bedöma vilken kostnadsnytta riskhanteringsskyldigheterna medförde för företagen. Enligt utredningen är en bedömning av en eventuell kostnadsnytta i euro förenad med så stor osäkerhet att företagen i regel inte kunde presentera någon bedömning av den. I företagens svar upprepades emellertid uppfattningen att en förbättring av nivån på cybersäkerheten ofrånkomligen har betydande positiva företagsekonomiska konsekvenser, och kraven i anslutning till cybersäkerhet syns enligt företagen på många sätt i affärsverksamheten. Kostnadsnytta ansågs vara förenad med i synnerhet ett ökat förtroende hos kunderna och att cyberattacker försvåras samt att de skadliga konsekvenserna av cyberattacker minskar.

Enligt förslaget ska aktörerna i enlighet med ett tillvägagångssätt som beaktar alla riskfaktorer identifiera de risker som riktas mot kommunikationsnät och informationssystem och deras fysiska miljö samt vidta uppdaterade, proportionerliga och tillräckliga riskhanteringsåtgärder. Aktörerna ska ha en handlingsmodell för riskhantering och i handlingsmodellen och de hanteringsåtgärder som grundar sig på den ska åtminstone de delområden som avses i artikel 21 i NIS 2-direktivet beaktas och hållas uppdaterade. Vad som är tillräckliga åtgärder bör bedömas i relation till de risker som verksamheten är förenad med, aktörens storlek och allmänna utsatthet vad gäller cybersäkerhetsrisker, dvs. sannolikheten för att det inträffar incidenter och deras allvarlighetsgrad, med beaktande av deras samhälleliga och ekonomiska konsekvenser. I riskhanteringen krävs det inte likadana åtgärder av alla aktörer, utan åtgärderna ska bedömas riskbaserat.

Härnäst följer en beskrivning av de kostnader som har uppskattats för riskhanteringen för aktörerna inom sektorerna för livsmedel och tillverkning, uppdelat enligt de delområden inom riskhanteringen som avses i artikel 21 i NIS 2-direktivet.

1. Riskanalys och informationssystemens säkerhet

Enligt artikel 21.2 a i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa strategier för riskanalys och informationssystemens säkerhet. I direktivet finns det ingen närmare definition av hurdana strategier företagen minst ska upprätta.

Inom livsmedelssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten skulle uppgå till 30 001–50 000 euro. Andra kostnader av löpande karaktär uppskattades till högst 5 000–15 000 euro, men många företag uppskattade också att fullgörandet av skyldigheten inte skulle leda till några andra kostnader av löpande karaktär. Enligt den uppskattning som har gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 32 000 euro under det första året och därefter 11 400 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 21–50 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten skulle uppgå till 5 000–30 000 euro. Andra kostnader av löpande karaktär uppskattades till högst 5 000–30 000 euro. Enligt den uppskattning som har gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 52 900 euro under det första året och därefter 36 900 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

De siffror som presenteras baserar sig på företagens egen uppskattning av omfattningen av den dokumentation som behövs. Det kan finnas betydande skillnader mellan olika företag i uppskattningarna av den arbetsinsats som behövs samt kostnaderna beroende på sektorn, affärsverksamhetsmiljön och den nuvarande dokumentationen.

2. Incidenthantering

Enligt artikel 21.2 b i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa incidenthantering för att identifiera eventuella incidentrisker, för att förebygga, upptäcka, hantera och återhämta sig från incidenter och för att begränsa deras inverkan. Med incident avses 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 nätverks- och informationssystem.

Enligt experternas bedömning kan man, när målet ska nås, i enlighet med riskanalysen från den aktör som bestämmelserna gäller beakta olika tekniska lösningar för förbättring av observationsförmågan, såsom centraliserad logghantering, SIEM-system (Security Information and Event Management) för identifiering av incidenter och lösningar för skydd av terminaler, såsom EDR (Endpoint Detection and Response). Dessutom ska ett företag identifiera de nätverk som det använder, de IKT-tjänster, -produkter och -enheter som är kopplade till dem samt den trafik som sker via dem. Ett företag ska med tanke på incidenter och störningar ha processer som omfattar identifiering av sådana här situationer och hur man ska agera medan de pågår samt tillvägagångssätt för hur man ska informera om incidenter internt, till kunder och till myndigheter (Insta 2023).

Inom livsmedelssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten skulle uppgå till 30 001–50 000 euro. Andra kostnader av löpande karaktär uppskattades till högst 5 000–15 000 euro.

Enligt den uppskattning som har gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 47 200 euro under det första året och därefter 19 700 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 21–50 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten skulle uppgå till 5 000–15 000 euro. Andra kostnader av löpande karaktär uppskattades till högst 15 001–30 000 euro. Enligt den uppskattning som har gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 43 200 euro under det första året och därefter 39 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

3. *Driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering*

Enligt artikel 21.2 c i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering.

Enligt experternas bedömning kan bland annat kontinuitets- och återhämtningsplaner som gäller IKT-produkter och IKT-tjänster, fastställande av återställningstestning av IKT-produkter och

IKT-tjänster som en del av dessa planer samt regelbunden övning i återställning av IKT-produkter och IKT-tjänster och i verksamhet under cybersäkerhetsincidenter ingå i hanteringsåtgärderna för driftskontinuiteten och krishanteringen.

Inom livsmedelssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 15 001–30 000 euro. Andra kostnader av löpande karaktär uppskattades uppgå till högst 5 000–15 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för bedömning av regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 31 200 euro under det första året och därefter 19 400 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–15 000 euro. Andra kostnader av löpande karaktär uppskattades uppgå till högst 15 001–30 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 32 100 euro under det första året och därefter 29 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

4. *Säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje aktör och dess direkta leverantörer eller tjänsteleverantörer*

Enligt artikel 21.2 d i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer.

Enligt skäl 85 i ingressen till NIS 2-direktivet bör företagen bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos sina leverantörer och tjänsteleverantörer, inbegripet deras förfaranden för säker utveckling. Väsentliga och viktiga entiteter bör framför allt uppmuntras att införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer. Dessa entiteter kan beakta risker som härrör från leverantörer och tjänsteleverantörer på andra nivåer.

För att fullgöra skyldigheten som gäller säkerhet i leveranskedjorna bör företagen enligt experternas bedömning med beaktande av företagets verksamhetsmiljö fastställa roller, ansvar och befogenheter i fråga om cybersäkerheten både inom företaget och i hela leveranskedjan. Dessutom bör företagen upprätta en beskrivning av leveranskedjorna och den ska innehålla beroenden, sårbarheter, hot och riskeffekter. Beskrivningen bör även omfatta tjänsteleverantörernas och leverantörernas viktigaste underleverantörer. Företagen bör också övervaka cybersäkerheten i fråga om IKT-produkterna och IKT-tjänsterna under hela deras livstid och samarbeta med interna och externa intressentgrupper genom att dela information och bästa praxis. (Insta 2023).

Inom livsmedelssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–15 000 euro. Det uppskattades att inga andra kostnader av löpande karaktär uppstår till följd av skyldigheten.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 39 100 euro under det första året och därefter 23 200 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–100 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–15 000 euro. Andra kostnader av löpande karaktär uppskattades uppgå till högst 5 000–15 000 euro, men lika många uppskattade att det inte uppstår några kostnader av löpande karaktär eller att summan av dem blir mindre än 5 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för bedömning av regleringsbördan medför anpassningen till skyldigheten en kostnad av engångskaraktär på i snitt 46 500 euro under det första året och därefter 31 700 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

5. *Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation*

Enligt artikel 21.2 e i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.

Enligt skäl 80 i ingressen till NIS 2-direktivet bör medlemsstaterna främja användningen av relevanta europeiska och internationella standarder bland väsentliga och viktiga entiteter, eller så får de ålägga entiteter att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer. Enligt skäl 78 i ingressen bör säkerheten i nätverks- och informationssystem dessutom omfatta lagrade, överförda och behandlade uppgifters säkerhet. Riskhanteringsåtgärder för cybersäkerhet bör föreskriva systemanalys, med beaktande av den mänskliga faktorn, för att få en fullständig bild av nätverks- och informationssystemets säkerhet.

Enlig expertbedömningen bör företagen beakta om de använder sig av specificerade krav för upphandlingarna och om de följer upp leverantörernas överensstämmelse med kraven regelbundet. Företagen bör beakta leverantörernas certifikat samt referensramarna för dataskyddet i fråga om IKT-produkterna och IKT-tjänsterna, när de bedömer leverantörer och IKT-produkter och IKT-tjänster.

Enligt bedömningen av Instas experter bör mänskliga hotfaktorer också beaktas vid bedömningen av säkerheten i nätverks- och informationssystem, till exempel genom användbarhetstestning, beskrivning av användningsfall och differentiering av uppgifter. På fullgörandet av

skyldigheten inverkar också om man får och följer upp rapporter om informationssäkerhetsincidenter av leverantörer och när det gäller IKT-produkter och IKT-tjänster. Med tanke på utvecklingen av nätverks- och informationssystemen bör företagen använda en process för säker programutveckling och den bör övervakas.

Inom livsmedelssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att anpassningen till skyldigheten inte leder till några andra kostnader av engångskaraktär eller av löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 30 800 euro under det första året och därefter 21 900 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–30 000 euro. Det uppskattades att inga andra kostnader av löpande karaktär uppstår.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 34 200 euro under det första året och därefter 25 100 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

6. Strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet

Enligt artikel 21.2 f i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet.

Fullgörandet av denna skyldighet kräver enligt experternas bedömning beroende på företagets verksamhet både allmänna mätare och mätare som är specifika för hanteringsåtgärderna genom vilka man kan mäta hur effektiv informationssäkerheten är. Företaget måste också följa upp mätarna regelbundet. Dessutom bör mätresultaten utvärderas och rapporteras till ledningen. Till strategierna och förfarandena för att bedöma hanteringsåtgärdernas effektivitet hör också metoder för kontinuerlig förbättring, genom vilka man planerar och genomför utvecklingsåtgärder på basis av mätresultaten. Företagen bör också bedöma och beakta den risk som finns kvar i deras verksamhet efter att hanteringsåtgärderna genomförts. (Insta 2023).

Inom livsmedelssektorn var, enligt utredningen, färre än 10 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–15 000 euro. Det uppskattades att inga andra kostnader av löpande karaktär uppstår till följd av skyldigheten.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 12 100 euro under det första året och därefter 4 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–50 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader för anpassningen till skyldigheten uppgår till 5 000–50 000 euro, men många bedömde också att fullgörandet av skyldigheten inte medför några andra engångskostnader. Det uppskattades att inga andra kostnader av löpande karaktär uppstår.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 34 700 euro under det första året och därefter 27 600 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

7. Grundläggande praxis för cyberhygien och utbildning i cybersäkerhet

Enligt artikel 21.2 g i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa grundläggande praxis för cyberhygien och utbildning i cybersäkerhet. Enligt skäl 89 i ingressen till NIS 2-direktivet bör företagen anta ett brett spektrum av grundläggande cyberhygienrutiner, såsom nollförtroendeprinciper, programuppdateringar, enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användarmedvetenhet, anordna utbildning för sin personal och öka medvetenheten om cyberhot, nätfiske eller sociala manipuleringstekniker.

Vid de intervjuer som Insta genomförde upptäcktes att det i NIS 2-direktivet som exempel på grundläggande cyberhygienrutiner nämns några sådana förfaranden som kan vara svåra att genomföra särskilt för de mindre företag som omfattas av direktivets tillämpningsområde. Exempel på sådana förfaranden är särskilt nollförtroendeprincipen, det vill säga Zero Trust.

Inom livsmedelssektorn var, enligt utredningen, företagens uppskattning att anpassningen till skyldigheten inte medför några engångsdagsverken. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Utöver detta uppskattade företagen att beloppet av andra kostnader för anpassningen till skyldigheten uppgår till högst 30 001–50 000 euro. Dock bedömde flera också att fullgörandet av skyldigheten inte medför andra engångskostnader. Andra kostnader av löpande karaktär uppskattades uppgå till högst 15 001–30 000 euro, men många uppskattade också att kostnaderna blir mindre än 5 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 21 900 euro under det första året och därefter 19 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, färre än 10 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir 10–20. Utöver detta uppskattade företagen att beloppet av andra engångskostnader som används för anpassningen till skyldigheten uppgår till högst 5 000–15 000 euro, men många bedömde också att fullgörandet av skyldigheten inte medför några andra engångskostnader. Andra kostnader av löpande karaktär uppskattades uppgå till 5 000–15 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 37 100 euro under det första året och därefter 26 700 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

8. Strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering

Enligt artikel 21.2 h i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering.

Enligt experternas bedömning kan företagen, när de bedömer denna skyldighet, särskilt fästa vikt vid om de har dokumenterade strategier för kryptografi och kryptering som tar i beaktande aspekter som autenticitet, integritet och konfidentialitet. Dessutom kan företagen bedöma om valen av algoritmer, protokoll, nycklarnas längd och krypteringsprodukter har gjorts i enlighet med gällande rekommendationer och om hanteringen och skyddet av nycklarna och certifikaten är dokumenterade.

Enligt utredningen uppskattade företagen inom livsmedelssektorn att anpassningen till skyldigheten skulle medföra färre än 10 dagsverken och många bedömde att skyldigheten inte medför några engångsdagsverken. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Skyldigheten bedömdes inte medföra några andra kostnader av engångskaraktär eller löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 23 000 euro under det första året och därefter 10 200 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Skyldigheten bedömdes inte medföra några andra kostnader av engångskaraktär eller löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 30 900 euro under det första året och därefter 23 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

9. Personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning

Enligt artikel 21.2 i i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning. Enligt skäl 79 i ingressen till NIS 2-direktivet bör entiteter som ett led i sina riskhanteringsåtgärder för cybersäkerhet också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Dessa åtgärder bör vara förenliga med direktiv (EU) 2022/2557. Enligt artikel 13.1 e i direktiv 2022/2557 (CER-direktivet) ska kritiska entiteter vidta åtgärder som är nödvändiga för att säkerställa en ändamålsenlig hantering av personalsäkerhet, med vederbörlig hänsyn till åtgärder

såsom fastställande av kategorier av personal som utför kritiska funktioner, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14 och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer.

Utöver vad som tidigare nämnts bedömde experterna att inom strategierna för åtkomstkontroll bör man fästa vikt vid beviljande, ändring och slopande av rättigheter samt vederbörlig övervakning. Strategierna för åtkomstkontroll bör täcka företagets hela kritiska infrastruktur och lokaler samt känslig information. Tillgångsförvaltningen bör omfatta både fysiska och immateriella tillgångar. Dessutom bör företaget ha strategier för åtaganden om sekretess och tystnadsplikt.

I enkäten upptäcktes att kravet på tillgångsförvaltningen delvis lämnar rum för tolkning, eftersom termen tillgångsförvaltning inte definieras exakt i NIS 2-direktivet. Då företagen intervjuades framkom att vid tillgångsförvaltningen granskades ofta alla informationstillgångar i enlighet med standarden ISO 27001 och med beaktande av övriga typer av tillgångar som hör till dem. Enligt en snäv tolkning kan man med tillgångsförvaltning i detta sammanhang dock avse till exempel förvaltning av tillgångar som en person förfogar över, såsom arbetsredskap. En vid tolkning kan omfatta alla tillgångar som är av värde för företaget. Det bör noteras att arbetsmängden och summan av de övriga kostnaderna för att utveckla tillgångsförvaltningen varierar betydligt beroende på i vilken omfattning åtgärderna för tillgångsförvaltningen genomförs. I intervjuerna användes definitionen enligt standarden ISO 27001 för tillgångsförvaltningen.

Enligt utredningen uppskattade företagen inom livsmedelssektorn att anpassningen till skyldigheten medför färre än 10 dagsverken. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10, men många bedömde att fullgörandet av skyldigheten inte medför några dagsverken som upprepas årligen. Skyldigheten bedömdes inte medföra några andra kostnader av engångskaraktär eller löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 12 000 euro under det första året och därefter 8 500 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, högst 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten, men många bedömde att fullgörandet av skyldigheten medför färre än 10 dagsverken. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Skyldigheten bedömdes inte medföra några andra kostnader av engångskaraktär eller löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 18 000 euro under det första året och därefter 11 000 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

10. Användning inom aktören, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem

Enligt artikel 21.2 j i NIS 2-direktivet ska riskhanteringsåtgärder för cybersäkerhet inbegripa användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem. Ibruktagandet av multifaktorautentisering i stora företags alla system skulle kunna orsaka oskäligt stora kostnader. Ibruktagandet kan till exempel kräva att dyrare licenser tas i bruk i molntjänster och i gamla system kan det vara svårt att ta i bruk multifaktorautentisering. Ibruktagandet bygger dock på riskbedömning och användningen är inte obligatorisk i alla miljöer utan endast när så är lämpligt. Multifaktorautentisering anses också vara till nytta för ett företag särskilt som ibruktagandet bygger på riskbedömning.

Nivån på de ekonomiska konsekvenserna av fullgörandet av riskhanteringsskyldigheterna i propositionen påverkas bland annat av den allmänna nivån på cybermognaden hos sektorerna och aktörerna och på förmågor som för närvarande varierar såväl mellan olika sektorer som mellan olika aktörer. På bedömningen inverkar också sektors- och aktörsspecifika riskbedömningar. Ju skadligare och mer vittgående konsekvenser en cyberstörning kan få för en viss aktör, desto mer investeringar kan påvisandet av överensstämmelse med kraven i direktivet kräva, beroende av nivån på aktörens cybermognad. Eventuella kostnadseffekter bör också sättas i relation till aktörens storlek. Aktörer som omfattats av tillämpningsområdet för NIS 1-direktivet får i regel lägre kostnader som beror direkt på skyldigheter i den här propositionen, eftersom de redan har omfattats av cybersäkerhetsskyldigheterna och åtgärder som stärker cybersäkerheten redan har vidtagits.

Enligt utredningen uppskattade företagen inom livsmedelssektorn att anpassningen till skyldigheten medför högst 10–20 dagsverken. Många bedömde dock att anpassningen till skyldigheten inte medför några dagsverken. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10, men många bedömde att fullgörandet av skyldigheten inte medför några dagsverken som upprepas årligen. Skyldigheten bedömdes inte medföra några andra kostnader av engångskaraktär eller löpande karaktär.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 24 700 euro under det första året och därefter 10 100 euro per år för de företag inom livsmedelssektorn som deltog i enkäten.

Inom tillverkningssektorn var, enligt utredningen, 10–20 dagsverken företagens uppskattning av hur många engångsdagsverken som skulle användas till att anpassa sig till skyldigheten. Bedömningen var att antalet dagsverken som upprepas årligen blir färre än 10. Många bedömde att fullgörandet av skyldigheten inte medför några dagsverken som upprepas. Andra kostnader av engångskaraktär uppskattades uppgå till under 5 000 euro. Bedömningen var att de årliga kostnaderna av löpande karaktär uppgår till under 5 000 euro.

Enligt den uppskattning som gjorts med hjälp av räknaren för regleringsbördan medför anpassningen till skyldigheten en engångskostnad på i genomsnitt 37 300 euro under det första året och därefter 27 700 euro per år för de företag inom tillverkningssektorn som deltog i enkäten.

Delområdet för riskhantering	Livsmedelssektorn		Tillverkningssektorn	
	Engångs-kostnader	Årliga kostnader	Engångs-kostnader	Årliga kostnader
1. Riskanalys och informationssystemens säkerhet	32 200 €	11 400 €	52 900 €	36 900 €

2. Incidenthantering	47 200 €	19 700 €	43 200 €	39 500 €
3. Driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering	31 200 €	19 400 €	32 100 €	29 500 €
4. Säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje aktör och dess direkta leverantörer eller tjänsteleverantörer	39 100 €	23 200 €	46 500 €	31 700 €
5. Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation	30 800 €	21 900 €	34 200 €	25 100 €
6. Strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet	12 100 €	4 500 €	34 700 €	27 600 €
7. Grundläggande praxis för cyberhygien och utbildning i cybersäkerhet	21 900 €	19 500 €	37 100 €	26 700 €
8. Strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering	23 000 €	10 200 €	30 900 €	23 500 €
9. Personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning	12 000 €	8 500 €	18 000 €	11 000 €
10. Användning inom aktören, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem	24 700 €	10 100 €	37 300 €	27 700 €
Sammanlagt	274 000 €	148 000 €	367 000 €	279 000 €

Enligt utredningen orsakas de största kostnaderna av följande skyldigheter: riskanalys och informationssystemens säkerhet, incidenthantering samt säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje aktör och dess direkta leverantörer eller tjänsteleverantörer. Det bör noteras att de sektorer som valts för granskningen inte tidigare omfattats av NIS-bestämmelserna, varför siffrorna kan bedömas vara en form av maximum för de

kostnader som uppstår av bestämmelserna. Försörjningsberedskapscentralen har bedömt att cybermognaden inom både livsmedelsindustrin och industrin ligger under basnivån och att läget kräver en utveckling som svarar mot det nuvarande hot- och riskläget. Som en särskild svaghet för livsmedelsindustrin identifierades brister i hanteringsprocesserna för cyberrisker och deras inverkan på det riskbaserade beslutsfattandet samt brister i lägesbilden för cybersäkerheten till exempel när det gäller nyttan av logguppgifter. Som särskilda brister inom industrin upptäcktes utvecklingen av leverantörshanteringen och identifieringen av bindningar, riskhanteringen samt konsekvenser av brister i stödet och intresset från ledningen.

För andra sektorer än livsmedelssektorn och tillverkningssektorn går det inte att göra liknande uppskattningar i euro. Nivån på de ekonomiska konsekvenserna i propositionen påverkas bland annat av den allmänna nivån på cybermognaden hos sektorerna och aktörerna och på förmågor som för närvarande varierar såväl mellan olika sektorer som mellan olika aktörer. På bedömningen inverkar också sektors- och aktörsspecifika riskbedömningar. Ju skadligare och mer vittgående konsekvenser en cyberstörning kan få för en viss aktör, desto mer investeringar kan påvisandet av överensstämmelse med kraven i direktivet kräva, beroende av nivån på aktörens cybermognad. Eventuella kostnadseffekter bör också sättas i relation till aktörens storlek. I regel påverkas storleken på kostnaderna också av om aktören omfattats av tillämpningsområdet för skyldigheterna i NIS 1-direktivet. Eftersom livsmedels- och tillverkningssektorns aktörer i huvudsak inte omfattats av tillämpningsområdet för NIS 1-direktivet, kan kostnaderna för de delområden som ska beaktas i riskhanteringen rent allmänt uppskattas motsvara de presenterade kalkylerna inom de aktörsspecifika variationerna.

Sektorernas cybermognad har i Finland utretts på uppdrag av Försörjningsberedskapscentralen.[8] I utredningen fastställdes för varje sektor också en bedömning av hotnivåns inverkan på sektorn. År 2022 var nivån på cybermognaden högst inom telekommunikationssektorn, IKT- och it-sektorn samt finanssektorn, som traditionellt har varit föremål för cyberbrottslighet och därför redan länge varit reglerade sektorer, också inom NIS 1-direktivets tillämpningsområde. Sektorerna har lyckats utveckla sin cybersäkerhet utifrån affärsverksamheten och riskerna. Bedömningen är att de här sektorerna tack vare en stark mognadsnivå lyckas svara mot den nuvarande risk- och hotbilden. Därför bedöms sektorerna få lägre kostnader för att fullgöra skyldigheterna i NIS 2-direktivet, emedan de åtgärder som direktivet kräver redan i stor utsträckning utförs i enlighet med kraven.

Sektorerna för energi och hälso- och sjukvård överskrider också den basnivå som fastställts som ett medeltal för mognaden, men för sektorerna har hot- och risknivåns inverkan bedömts som betydande, det vill säga att det inom sektorerna finns många funktioner som kan bedömas som viktiga med tanke på riskerna. Inom energisektorn börjar många nya aktörer omfattas av NIS 2-direktivet. Dessa nya aktörer är elnätsinnehavare, elproducenter, elförsäljare, elbörser, innehavare av naturgasnät, operatörer av LNG-terminaler (de som endast är kopplade till ett nät eller också övriga), naturgasleverantörer, LNG-leverantörer, vätgasaktörer, aktörer för fjärrvärme och fjärrkyla, oljeraffinering och oljeupplagring. Bedömningen är att hotnivån blir mer betydande inom energisektorn. Mognadsnivån bedöms i allmänhet som god och man har förberett sig på olika hot. Sektorn delas dock in i aktörer med en hög och en låg mognadsnivå och informationssäkerhetskulturen varierar mellan de olika aktörerna. Dessutom har det konstaterats att organisationer som verkar inom ett större geografiskt område har investerat mer i cybersäkerhet än lokala aktörer. Fullgörandet av skyldigheterna i NIS 2-direktivet kan därmed leda till

[8] Huoltovarmuuskeskus (2022) Toimialojen kyberkypsyyden selvitys 2022.

större kostnadseffekter för vissa aktörer, i synnerhet de nya aktörer som börjar omfattas av lagstiftningen.

Inom sektorn för hälso- och sjukvården omfattas de offentliga välfärdsområdena av NIS 2-direktivets tillämpningsområde och nya inom direktivets tillämpningsområde är också vissa forskningsinstitut och laboratorier. Åtgärder för dataskydd är ombesörjda inom hälso- och sjukvården i och med den reglering som finns, men när det gäller cybersäkerheten har man bedömt att många aktörer behöver mer systematiska åtgärder. Särskilt skyddet av kritiska tjänster och de leveranskedjor där nivån på tjänsteleverantörernas cybersäkerhet följs upp och skyldigheterna i avtalen ställs upp bedömdes som svaga. Beredskap inför hybridhot som ett led i kontinuitetsplaneringen och regelbundna övningar ansågs vara en svaghet inom sektorn. Särskilt inom dessa delområden kan fullgörandet av skyldigheterna i NIS 2-direktivet antas medföra kostnader, även om förändringarna inte bedöms vara betydande för NIS 1-aktörernas del.

I utredningen underskred NIS 2-sektorerna logistik, livsmedelsindustri, industri, vattenförsörjning, handel och distribution samt hamnar och sjöfart basnivån för mognaden något. Sektorerna bedöms få kostnader för fullgörandet av skyldigheterna i NIS 2-direktivet.

Bedömningen är att hotnivån blir mer betydande inom vattenförsörjningen. Den totala mognaden underskrider en god basnivå, och sektorns centrala roll för att samhället ska fungera bedöms vara betydande. Av denna anledning anser man att det inom sektorn behöver investeras i cybersäkerheten för tillräcklig beredskap mot nuvarande hotbilder. Som en särskild svaghet identifierades bristerna i totalhanteringen av cybersäkerheten, svag insyn i partnernas verksamhet i utvecklingsarbetet och ett högt beroendeförhållande till it-tjänsteleverantörer. Vattenförsörjningen har dock omfattats av NIS-direktivet, varför cybersäkerhetsregleringen redan är inriktad på dess aktörer. Vattenförsörjningen är dock med tanke på samhällsfunktionen en kritisk tjänst och större incidenter kan eskalera till lokala katastrofer, varför riskerna är större och därmed kan det uppstå högre kostnader för genomförandet av NIS 2-direktivet för sektorn.

Bedömningen är att hotnivån blir mer betydande inom logistiksektorn. Sektorn utvecklas kontinuerligt och är utsatt för konkurrens samt förändringar i leveranskedjorna, vilket innebär att den övergripande hanteringen av cybersäkerheten bör uppmärksammas särskilt. Sektorns svaghet identifierades som brister i fastställandet och implementeringen av policyer och riktlinjer för logghantering och i omfattningen och säkerställandet av bevakningen av systemnivån och den operativa tekniken. Utöver detta bedömdes identifieringen av beroenden mellan tredjeparter och funktionerna som en svaghet.

För handeln och distributionen bedömdes betydelsen av hotnivån vara neutral. För sektorn handel och distribution ligger den totala cybermognaden under en god basnivå, vilket betyder att beredskapen inför cyberhot inte är heltäckande. I fråga om mognadsnivån fanns det stor variation mellan de olika aktörerna. Som svagheter inom sektorn identifierades bristen på riskhanteringskultur för cybersäkerheten och dess inverkan på utmaningarna med det riskbaserade beslutsfattandet och att cybersäkerhetsaspekten beaktas sämre i jämförelse med den operativa kontinuiteten, bland annat inom följande delområden: hanteringen av incidenter och störningar, hanteringen av sårbarheter, tillgångsförvaltningen och skyddet av kritiska tjänster.

För hamnarna och sjöfarten bedömdes betydelsen av hotnivån vara neutral. Sektorns mognad är dock låg och man ansåg att det krävs betydande åtgärder för att sektorn på ett bra sätt ska kunna svara mot den nuvarande hotnivån. Sektorn har en framträdande roll i upprätthållandet av den nationella försörjningsberedskapen under undantagsförhållanden. Sektorns svaghet upptäcktes

vara bristen på ledning, som hindrar genomförandet av utvecklingsbehoven, varför genomförandet av cybersäkerhetsinvesteringar hämmas. Dessutom upptäcktes brister i definitionen av den grundläggande cybersäkerhetshanteringen. På grund av detta är bedömningen att det uppstår mer kostnader för sektorn för fullgörandet av NIS 2-skyldigheterna. Det finns inga uppgifter om nivån på cybermognaden för de övriga aktörerna inom transportsektorn. Sektorn har dock tidigare omfattats av NIS-skyldigheter, varför det inom sektorn finns aktörer som inte får så stora kostnader då skyldigheterna ska fullgöras. Inom sektorn kommer dock många nya aktörer att omfattas av bestämmelserna och kostnaderna kommer sannolikt vara större för dessa aktörer.

I Finland har cybermognaden inte undersökts i fråga om de övriga NIS 2-sektorerna.

Konsekvenser för samhällsekonomin

Genom propositionen försöker man förbättra de kritiska sektorernas cybersäkerhet och på detta sätt förbättra förtroendet för marknaden samt samhällsekonomin. Propositionens konsekvenser för samhällsekonomin är indirekta.

Propositionen har konsekvenser för den offentliga ekonomin och de utgörs av nya myndighetsuppgifter och en utökad grupp aktörer som ska övervakas. Konsekvenserna för den offentliga ekonomin beskrivs i avsnitt 4.4.

Den tyngre regleringsbörda som propositionen medför innebär att aktörerna blir tvungna att lägga mer resurser på cybersäkerheten. Detta kan minska företagens vinst på kort sikt och det är också möjligt att de tilläggsresurser som inriktas på dataskyddet och informationssäkerheten tas från den övriga verksamheten. En omsköttgod nivå på informationssäkerheten och dataskyddet kan dock ge företagen ett gott rykte och således främja en framgångsrik affärsverksamhet. Antagligen minskar satsningar på cybersäkerheten informationssäkerhetsstörningar och då minskar risken för luckor i cybersäkerheten och kostnaderna som orsakas av sådana kan åtminstone delvis undvikas för hela samhällsekonomin.

De kritiska sektorernas informationssäkerhet och dataskydd har stor betydelse för samhällsekonomin. Störningar som orsakats av brister i informationssäkerheten och dataskyddet skulle direkt påverka löntagarna inom sektorerna och utvecklingen av bruttonationalprodukten. Brister i informationssäkerheten och dataskyddet inom de kritiska sektorerna påverkar också den samhällsekonomiska verksamheten och utvecklingen längs andra effektkedjor. Ömsesidigt beroende mellan sektorerna och indirekta kostnader hör till de viktigaste konsekvenserna. Kostnaderna för brister i informationssäkerheten och dataskyddet upprepas inom andra sektorer på grund av det ömsesidiga beroendet.

Brister i informationssäkerheten och dataskyddet kan ha omfattande inverkan på företagens verksamhetsförutsättningar och den samhällsekonomiska verksamheten, om till exempel informationsintrång påverkar folkets förtroende för ett fungerande samhälle eller deras förväntningar på företagen. För företagen kan avbrott i verksamheten på grund av en störningssituation i informationssäkerheten eller dataskyddet orsaka kostnader både på grund av avbrott i produktionen eller tillhandahållandet av tjänster och på grund av avlägsnandet av störningens skadliga effekter. Dessutom kan en bristande cybersäkerhet leda till indirekta kostnader, om kundernas förtroende för företaget rubbas, vilket i sin tur kan leda till minskat kundantal och minskad försäljning.

En lucka i informationssäkerheten kan ha följder för hushållens förtroende, vilket kan leda till rubbningar i det digitala ekonomisystemet. Misstron mot institutioner kan också öka om informationssäkerheten och dataskyddet anses vara dåligt skötta i samhället. Med tanke på hushållen orsakar brister i dataskyddet och informationssäkerheten direkta kostnader på en allmän nivå om man blir tvungen att skaffa nyttigheter på annat sätt då informationssäkerheten brister eller åtkomsten till nyttigheterna bryts. Till direkta kostnader hör också de tilläggsresurser som krävs av folket till exempel för att leta efter en ny tjänsteleverantör eller för bättra den egna informationssäkerheten eller det egna dataskyddet.

Harmoniserade bestämmelser förbättrar verksamheten på EU:s inre marknad och sänker kostnader för företag som utvidgar från ett land till ett annat. Enligt en uppskattning som kommissionen gjorde i samband med NIS 1-direktivet föranleder en utvidgning av företagsverksamheten till ett annat EU-land enskilda företag en tilläggskostnad på ca 9 000 euro. Att realisera den digitala inre marknaden fullt ut kan möjliggöra en tillväxt på 415 miljarder euro för EU:s bruttonationalprodukt, varför tillväxtpotentialen är betydande i och med gemensamma bestämmelser.

4.3 Konsekvenser för myndigheternas verksamhet

Konsekvenser för myndigheternas uppgifter och den offentliga ekonomin

Propositionens konsekvenser för myndigheterna utgörs av konsekvenser av att nya myndighetsuppgifter ska utföras och konsekvenser som uppstår för den offentliga förvaltningen när de nya bestämmelserna ska följas. I detta underavsnitt beskrivs propositionens konsekvenser för myndigheterna med avseende på myndigheternas verksamhet. I nästa underavsnitt behandlas de konsekvenser som uppstår för den offentliga förvaltningens aktörer när bestämmelserna ska följas.

Propositionen har ekonomiska konsekvenser för Transport- och kommunikationsverket på grund av skötseln av nya uppgifter. Transport- och kommunikationsverket ska enligt förslaget sköta om CSIRT-enhetens uppgifter, uppgiften som samordnare mellan de nationella cyberkrishanteringsmyndigheterna, tillsynsmyndighetens uppgifter inom olika sektorer, den nationella kontaktpunktens uppgifter i enlighet med NIS 2-direktivet samt vissa uppgifter som hör samman med påföljdsavgiftsnämnden. Eftersom antalet uppgifter ökar för Transport- och kommunikationsverket i och med genomförandet av NIS 2-direktivet, förutsätts att Transport- och kommunikationsverket får tilläggsresurser som täcker de kostnader som de nya uppgifterna orsakar.

Propositionen får på grund av skötseln av de nya tillsynsuppgifterna ekonomiska konsekvenser för Energimyndigheten, Säkerhets- och kemikalieverket, Tillstånds- och tillsynsverket för social- och hälsovården, Närings-, trafik- och miljöcentralen i Södra Savolax, Livsmedelsverket, Säkerhets- och utvecklingscentret för läkemedelsområdet och Finansinspektionen, som är sektorsspecifika tillsynsmyndigheter. Av tillsynssamarbetet med de ovannämnda myndigheterna följer också direkta ekonomiska konsekvenser för dataombudsmannen. Beloppet av kostnaderna för tillsynen är beroende av antalet och kvaliteten på de aktörer som omfattas av tillämpningsområdet inom varje sektor samt av antalet aktörer som inte har omfattats av tillämpningsområdet för bestämmelserna i NIS 1-direktivet. Uppdraget som tillsynsmyndighet är nytt för Säkerhets- och kemikalieverket, NTM-centralen i Södra Savolax, Livsmedelsverket och Säkerhets- och utvecklingscentret för läkemedelsområdet. I förhållande till genomförandet av NIS 1-direktivet i Finland utökas tillämpningsområdet i och med att NIS 2-direktivet träder i kraft

och av tillsynsmyndigheterna förutsätts bredare kompetens, vilket leder till tilläggskostnader för varje tillsynsmyndighet.

Å andra sidan slopas inriktningen som användes som kriterium i NIS 1-direktivet, från identifieringsprocessen av kritiska aktörer och tillämpningsområdet för skyldigheterna fastställs i fortsättningen utifrån aktörernas sektor och storlek. Vid insamlandet av en förteckning över aktörerna drar man nytta av aktörernas egna anmälningar samt befintliga registeruppgifter. De här faktorerna bedöms minska den administrativa bördan för myndigheterna jämfört med den tillsyn som skett med stöd av NIS 1-direktivet. Tillsynsmyndigheten kommer dessutom att ha möjlighet att rikta tillsynen enligt en riskbaserad metod och sätta sina uppgifter i prioritetsordning, vilket påverkar myndighetens tillsynskostnader. Jämfört med de sektorsbestämmelser som ska tillämpas generellt kan det att NIS 2-bestämmelserna koncentreras till en ny allmän lag emellertid öka behovet av rådgivning om tillämpningsområdet för skyldigheterna.

Tillsynsuppgiften förutsätter tilläggsresurser vid varje tillsynsmyndighet, eftersom antalet aktörer som ska övervakas ökar inom varje tillsynsmyndighets tillsynssektor och det av myndigheterna krävs kompetens i tillsynsverksamheten som sträcker sig längre än tillsynen i NIS 1-direktivet. De sektorer som inte omfattats av NIS 1-direktivet och de tillsynsmyndigheter som inte tidigare haft en tillsynsuppgift enligt NIS 1-direktivet, klarar inte av att genomföra tillsynen enligt NIS 2-direktivet utan nya resurser. I avsnitt 5.1 behandlas alternativet att ordna centraliserad tillsyn, vilket har bedömts orsaka en större kostnadseffekt för den offentliga ekonomin än modellen med uppdelad tillsyn.

I följande tabell presenteras det uppskattade behovet av tilläggsresurser för tillsynsuppgiften för varje tillsynsmyndighet.

Myndighet	Sektor som ska övervakas	Uppskattat behov av tilläggsresurser	Tillsynsmyndighet för NIS 1
Transport- och kommunikationsverket	Luftfart, spårtrafik, sjöfart, vägtransport, rymden, digital infrastruktur, förvaltning av IKT-tjänster, tillhandahållare av bud- och posttjänster, digitala leverantörer, tillverkning (företag som bedriver tillverkning av motorfordon, släpfordon och påhängsvagnar, företag som bedriver tillverkning av andra transportmedel), forskningsorganisationer, offentlig förvaltning.	8,5 årsverken och informationssystemsinvesteringar på 0,4 mn € för 2024 och 0,15 mn € fr.o.m. 2025.	Ja
Energimyndigheten	El, operatörer av fjärrvärme eller fjärrkyla, gas (distributions- och överföringsnätsinnehavare)	Kompletteras senare	Ja

Säkerhets- och kemikalieverket	Gas (naturgasleverantörer, innehavare av lagringsanläggningar, innehavare av en behandlingsanläggning för kondenserad naturgas, naturgasföretag samt operatörer av raffinaderier och bearbetningsanläggningar för naturgas), olja, operatörer av anläggningar för produktion, lagring och överföring av vätgas, företag som tillverkar ämnen och distribuerar ämnen eller blandningar och företag som producerar varor genom att använda ämnen och blandningar, tillverkning (företag som bedriver tillverkning av datorer, elektronikvaror och optik, företag som bedriver tillverkning av elapparatur och företag som bedriver tillverkning av övriga maskiner).	5 årsverken + informationssystemsinvesteringar på 0,2 mn € för 2024 och 0,06 mn € fr.o.m. 2025.	Nej
Tillstånds- och tillsynsverket för social- och hälsovården	Hälsa	2 årsverken samt informationssystemsinvesteringar av engångskaraktär på ca 0,15 mn € och 10 000–20 000 euro årligen fr.o.m. 2025.	Ja
NTM-centralen i Södra Savolax	Avfallshanteringen	2,5 årsverken och en engångskostnad på ca 40 000 samt informationssystemskostnader på 0,05 mn € fr.o.m. 2025.	Nej
NTM-centralen i Södra Savolax, enheten för vattentjänster	Dricksvatten och avloppsvatten	3 årsverken och ca 100 000 euro i anslag för köptjänster.	Ja
Livsmedelsverket	Livsmedelsföretag som bedriver grossisthandel och industriell produktion och bearbetning	5 årsverken och informationssystemskostnader på 0,54 mn €	Nej

		för 2024 och 0,05 mn € årligen fr.o.m. 2025.	
Säkerhets- och utvecklingscentret för läkemedelsområdet	Aktörer som tillverkar medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik	Kompletteras senare	Nej
Finansinspektionen	Bankverksamhet och finansmarknadsinfrastruktur	Inga konsekvenser.	Ja
Dataombudsmannen	-	2,5 årsverken	-
Sammanlagt			

Det råder brist på cybersäkerhetsexperter i Finland, varför rekryteringssvårigheter kan uppstå till följd av att både myndigheterna och de aktörer som är föremål för bestämmelserna behöver fler experter på området. I förslaget har man försökt skapa förutsättningar för ett nära samarbete mellan myndigheterna, med hjälp av vilket cybersäkerhetskompetensen kan utvecklas över sektorsgränserna.

Förslaget innehåller också vissa ytterligare förpliktelser för registrarer enligt lagen om tjänster inom elektronisk kommunikation. Transport- och kommunikationsverket övervakar registrarernas verksamhet och i och med de nya förpliktelserna utökas tillsynsuppgiften till att omfatta iakttagandet av de nu föreslagna förpliktelserna. De nya tillsynsuppgifterna som riktas mot registrarerna bedöms förutsätta en tilläggsresurs på 0,5 årsverken utöver den tabell som beskrivs ovan.

Transport- och kommunikationsverket

Utöver tillsynsuppgifterna föreslås Transport- och kommunikationsverket få andra myndighetsuppgifter för vilka det behövs tilläggsresurser. Transport- och kommunikationsverket har varit den CSIRT-enhet som nämns i NIS 1-direktivet redan tidigare, men i och med NIS 2-direktivet ökar enhetens uppgifter betydligt. De nya uppgifterna förutsätter att nya funktioner inrättas och att befintliga funktioner och informationssystemen utvecklas. Centrala uppgifter som föreslås för CSIRT-enheten är att reagera på kränkningar av informationssäkerheten och bistå aktörerna, delta i det internationella samarbetet, analysera uppgifter om sårbarheter samt samordna processen med att offentliggöra information om sårbarheter. De nya uppgifter som föreslås för CSIRT-enheten samt de tillsynsuppgifter som hänvisas Transport- och kommunikationsverket bedöms kräva tilläggsresurser på sammanlagt 8–17 årsverken samt för systemutveckling sammanlagt 400 000 euro år 2024 och därefter årligen 150 000 euro.

Transport- och kommunikationsverket utser också ordförande och vice ordförande i den påföljdsavgiftsnämnd som inrättas för påförande av påföljdsavgifter. Dessutom är Transport- och kommunikationsverket samordnare för hanteringen av storskaliga cybersäkerhetsincidenter och

cybersäkerhetskriser samt svarar för utarbetandet av en plan för hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser i samarbete med övriga myndigheter. Uppgifterna är nya för Transport- och kommunikationsverket och förutsätter en tilläggsresurs om sammanlagt 0,5 årsverken. Dessutom ska Transport- och kommunikationsverket fortsätta som den gemensamma kontaktpunkt som avses i NIS 1- och NIS 2-direktivet. Den gemensamma kontaktpunkten främjar bland annat samarbetet och samordningen mellan tillsynsmyndigheterna. Uppgiften kan enligt bedömningen genomföras med nuvarande resurser.

Transport- och kommunikationsverket behöver tilläggsresurser motsvarande sammanlagt minst 8,5 årsverken med anledning av de nya uppgifter som beskrivs ovan. Dessutom uppstår kostnader för Transport- och kommunikationsverket med anledning av de systeminvesteringar som behövs för genomförandet av uppgifterna på 0,4 miljoner euro för år 2024 och 0,15 miljoner euro från och med 2025. På den resursnivån kan Transport- och kommunikationsverket utföra de viktigaste uppgifterna som krävs för genomförandet av NIS 2-direktivet på miniminivå genom att dra nytta av möjligheterna att effektivisera nuvarande funktioner och rikta om befintliga resurser inom verket.

Med ovannämnda tilläggsresurser utför Transport- och kommunikationsverket på miniminivå sektortillsynsuppgifterna som hör till myndigheten, behandlingen av lagstadgade anmälningar, besvarande av anmälningar och det tekniska genomförandet av det nya anmälningsförfarandet, den tekniska skanningskompetens som krävs i bestämmelserna, sårbarhetssamordning och påföljdsavgiftsnämndens uppgifter. Bestämmelserna ställer upp nya uppgifter och krav också på registreringstjänster för domännamn, myndigheternas analys- och forensikkompetens, stödet till de kritiska sektorerna, det internationella samarbetet, uppgifter som gäller certifiering och standardisering samt utvecklingen av IKT-förmågorna och automatiseringen. Ovannämnda uppgiftshelheter och krav hör också till Transport- och kommunikationsverket. Transport- och kommunikationsverket kan dock inte bidra till dessa uppgiftshelheter på den föreslagna resursnivån och därför krävs tilläggsresurser.

I budgeten för 2024 har Transport- och kommunikationsverket för nya uppgifter som hänför sig till genomförandet av NIS 2-direktivet beviljats finansiering om 8,5 årsverken och informationssystemsinvesteringar på 0,4 miljoner euro för år 2024 och 0,15 miljoner euro från och med 2025. De tilläggskostnader för Transport- och kommunikationsverket som beskrivits ovan ska täckas ur moment 31.01.02 Transport- och kommunikationsverkets omkostnader inom ramen för anslagen från och med 2024.

Dataombudsmannen

Propositionen har ekonomiska konsekvenser för dataombudsmannen. Dataombudsmannen får mer arbete främst av skyldigheten i 46 § i lagförslag 1 enligt vilken tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten vid behov ska samarbeta bland annat med dataombudsmannen. För det andra följer mer arbete av behandlingen av anmälningar om hanteringen av personuppgiftsincidenter samt eventuella samtidiga tillsynsförfaranden. Dataombudsmannen behandlar anmälningar om personuppgiftsincidenter som lämnats på basis av EU:s allmänna dataskyddsförordning och lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). Alla aktörer som ska övervakas med stöd av lagförslag 1 som enligt dataskyddslagstiftningen betraktas som personuppgiftsansvariga eller personuppgiftsbiträden är redan nu skyldiga att lämna anmälningar. I enlighet med lagförslag 1 i propositionen är tillsynsmyndigheten skyldig att informera dataombudsmannen om det i samband med en anmäld incident har skett en personuppgiftsincident eller om

en försummelse av skyldigheterna i lagen kan leda till eller har lett till en sådan personuppgiftsincident som avses i den allmänna dataskyddsförordningen. Med beaktande av att tillämpningsområdet för direktivet utvidgas när NIS 2-direktivet genomförs och att också personuppgiftsansvariga och personuppgiftsbiträden har en motsvarande anmälningsskyldighet direkt med stöd av dataskyddslagstiftningen, kan man vänta sig att antalet anmälningar ökar och att det av lagstiftningen kan följa överlappande anmälningar om personuppgiftsincidenter.

De föreslagna bestämmelserna kan delvis överlappa övervakningen av iakttagandet av de informationssäkerhetsskyldigheter som hör samman med hanteringen av personuppgifter enligt dataskyddslagstiftningen. Detta betyder också att tillsynsåtgärder som inleds av dataombudsmannen kan vara anhängiga samtidigt om en enskild försummelse som konstaterats av en tillsynsmyndighet, vilket innebär extra arbete för dataombudsmannen. Till den del som de tillsynsåtgärder som avses i lagförslag 1 och dataombudsmannen tillsynsåtgärder är anhängiga samtidigt, måste myndighetssamarbetet särskilt säkerställas i enlighet med 41 § i lagförslag 1 om att påföljdsavgiften inte påförs för samma gärning vid båda tillsynsförfarandena.

Av regleringen följer konsekvenser för personalen och konsekvenser för informationshanteringen. De engångskostnader som föranleds av ändringen i informationssystemet ska täckas med anslag ur rambeslutet för statsfinanserna och statsbudgeten. För dataombudsmannens del uppgår det permanenta behovet av tilläggsfinansiering på grund av de föreslagna bestämmelserna till sammanlagt minst 2,5 årsverken som senast måste ingå i budgeten för 2025 (moment 25.01.03). Eftersom lagstiftningen börjar tillämpas i oktober 2024 och de nya bestämmelserna förutsätter att man förbereder sig inför tillsynssamarbetet, uppstår en del effekter senast i slutet av 2024. Effekterna av tilläggsarbetet realiseras fullt ut år 2025.

Energimyndigheten (Kompletteras senare)

Säkerhets- och kemikalieverket

Säkerhets- och kemikalieverket (Tukes) föreslås vara behörig myndighet till centrala och betydande delar vid genomförandet av NIS 2-direktivet. Säkerhets- och kemikalieverket är underställt sex olika ministeriers förvaltningsområden och till verket har tillstånds- och tillsynsärenden som gäller kemiska produkter och säkerheten och tillförlitligheten i fråga om produkter, apparatur och anläggningar centraliserats samt Finlands bedömnings- och ackrediteringsorgan (FINAS). För verket är uppgifterna som behörig myndighet enligt NIS 2-direktivet nya, och verket har ingen tidigare kompetens eller resurs inom uppgiftsområdet. Verksamhetsområdena och aktörsfältet är delvis bekanta för myndigheten. De föreslagna nya uppgifterna är betydande med tanke på näringslivet och verket och kräver att verket skaffar ny kompetens genom rekryteringar och omskolning. Det är motiverat att kompetensen om cybersäkerhetshot utvecklas vid och koncentreras till Säkerhets- och kemikalieverket, då verkets tillstånds- och tillsynsuppgifter till betydande del är inriktade på sektorer som är viktiga och kritiska för samhället och säkerheten, såsom produktion, industriell hantering och lagring av farliga kemikalier (anläggningar som kan medföra fara för en storolycka), elektriska produkter och elektrisk utrustning, tryckbärande anordningar och tillsynen under driften av tryckbärande anordningar, mätinstrument och mätningarnas tillförlitlighet, gruvdrift och energisektorn, såsom natur- och biogas samt vätgas. På lång sikt är det när det gäller säkerheten i samhället och inom de viktiga sektorerna

ändamålsenligt att uppgifter om cybersäkerheten sammanförs till Säkerhets- och kemikalieverket med tanke på både utvecklingen av kritisk kompetens och kostnadseffektivitet.

Det totala resursbehovet för de nya lagstadgade myndighetsuppgifterna bedöms under 2024–2026 uppgå till fem (5) årsverken i fråga om experter för att verkställa ändringarna i lagstiftningen och utveckla nya förfaranden för myndighetstillsynen. Anslagen ses över på nytt år 2026, när det finns erfarenheter av aktörsfältets omfattning och tillsynsfältets utmaningar.

Säkerhets- och kemikalieverket föreslås få tilläggsresurser om sammanlagt 510 000 euro (5 årsverken 450 000 och 60 000 för driftskostnader för Vallu-systemet) för år 2024 (32.01.08) och framåt. Dessutom föreslås för 2024 att Vallu-systemet förnyas till en engångskostnad på 200 000 euro.

Tabell (tusen euro)

	2024	2025	2026	2027
Personalkostnader (5 årsverken)	450	450	450 (+ ev. behov av extra årsverken)	450 (+ ev. behov av extra årsverken)
Investeringsutgifter (VALLU)	200 (av engångskaraktär)	0	0	0
Driftskostnader som hör till VALLU	0	60	60	60
Tillägg till budgetpropositionen sammanlagt	650	510	510 (+ behov av extra årsverken)	510 (+ behov av extra årsverken?)

NTM-centralen i Södra Savolax

I fråga om NTM-centralen i Södra Savolax utgörs de konsekvenser som orsakas av uppgiften som tillsynsmyndighet för vattenförsörjningen, det vill säga för dricksvatten- och avloppsvattenverken, av ett permanent tillsynsbehov, köptjänster som behövs för de inspektioner som anges i 29 § i lagförslag 1 och engångsinvesteringar. Myndighetstillsynen enligt NIS 2-direktivet integreras som en del av övervakningen av vattentjänsternas beredskapsplaner, som effektiviseras. Av de vattentjänstverk som omfattas av tillämpningsområdet för NIS 2-direktivet krävs en utredning av att kraven i lagen uppfylls och dessa saker bör ingå i den beredskapsplan enligt lagen om vattentjänster som ska lämnas till tillsynsmyndigheten med vissa intervall. Under inspektioner enligt 29 § används vid granskningen tjänster av utomstående experter på informationsteknik bland annat för att utföra de tester och mätningar som behövs. Engångsinvesteringarna består av ändringar i övervakningsfunktionerna som behöver göras i vattenförsörjningens informationssystem. Bedömningen är att tillämpningsområdet omfattar sammanlagt åtminstone ca 20–40 verk som ska övervakas. Den permanenta tilläggsresurs som behövs för tillsynsuppgifter vid NTM-centralen i Södra Savolax uppgår till 3 årsverken. På motsvarande sätt föreslås ett fast anslag på 100 000 euro per år för köp av experttjänster. Under momentet föreslås 100 000 euro för 2025 för utveckling av de behövliga informationssystemen.

Till de väsentliga aktörer som omfattas av NIS 2-direktivet och som ska omfattas av tillsynen hör enligt 3 § 1 mom. 1 punkten direkt två vattentjänstverk. Beroende på det kommande genomförandet av CER-direktivets tillämpningsområde bedömer man att antalet verk som ska övervakas enligt NIS 2-direktivet uppgår sammanlagt till åtminstone 20–40 stycken. Den permanenta tilläggsresurs som behövs för tillsynsuppgifter vid NTM-centralen i Södra Savolax uppgår till 3 årsverken. På motsvarande sätt föreslås ett fast anslag på 100 000 euro per år för köp av experttjänster. Under momentet föreslås 100 000 euro för 2025 för utveckling av de behövliga informationssystemen.

För NTM-centralen i Södra Savolax består tillsynen över avfallshanteringen av helt nya uppgifter. I den nuvarande situationen passar inte systemen på plattformen Y-alusta, såsom övervakningssystemet för miljötillstånd, avfallshanteringsregistret med flera, som används vid övervakningen av miljötillstånd och behandlingen av avfallshanteringsregisterärenden och rapporteringen om dem inte som sådana för genomförandet av NIS 2-direktivet eller för en framgallring av de aktörer som ska övervakas. I systemen behandlas inte företagens ekonomiska uppgifter eller uppgifter om företagens personalmängd, vilka behövs i gallringen av aktörerna. I plattformen kan man dessutom inte behandla säkerhetsklassificerade handlingar och handlingarna i anslutning till säkerhetsarrangemangen är sådana. Arkiveringen av plattformens handlingar sker i ärendehanteringssystemet USPA.

Enligt den bedömning som NTM-centralen i Södra Savolax gjort förutsätter genomförandet av skyldigheterna i direktivet för avfallshanteringens del att systemen uppdateras och vidareutvecklas samt ett behov av temporära och permanenta personalresurser. Utvecklandet av systemen förutsätter en engångskostnad på 0,2 miljoner euro. Systemens årliga driftskostnader bedöms uppgå till 0,05 miljoner euro från och med 2025, eftersom systemen endast delvis kommer att omfattas av de befintliga underhållsavtalen. Under beredningen och i början av genomförandet behövs 1 årsverke (80 000 euro) för en personalresurs av engångskaraktär och permanent 1,5 årsverken (120 000 euro) som tilläggsresurs. I början är alltså behovet av tilläggsresurser sammanlagt 2,5 årsverken (200 000 euro). I synnerhet när verksamheten inleds framhävs behovet av information, rådgivning och utbildning, vilket förutsätter ca 40 000 euro som en engångskostnad. Med ovannämnda tilläggsresurser klarar NTM-centralen i Södra Savolax de uppgifter som genomförandet av direktivet förutsätter på miniminivå. Behoven av tilläggsanslag placeras under arbets- och näringsministeriets huvudtitel under moment 32.01.02 Närings-, trafik- och miljöcentralernas omkostnader.

Livsmedelsverket

För Livsmedelsverket föranleder de nya uppgifterna ett behov av tilläggsresurser på sammanlagt 5 årsverken för de uppgifter som hör till verkställigheten i enlighet med regeringspropositionen. Dessutom uppstår kostnader för Livsmedelsverket med anledning av de informationssystemsinvesteringar som behövs för genomförandet av uppgifterna på 0,54 miljoner euro för år 2024 och 0,05 miljoner euro från och med 2025. På den resursnivån kan Livsmedelsverket utföra de uppgifter som krävs för genomförandet av NIS 2-direktivet på miniminivå genom att dra nytta av möjligheterna att effektivisera nuvarande funktioner och rikta om befintliga resurser inom verket. För 2024 är avsikten att göra en framställan om tilläggsanslag för moment 30.20.01 (Livsmedelsverkets omkostnader) i vårens tilläggsbudgetproposition och annars i samband med den normala ram- och budgetberedningen.

Tillstånds- och tillsynsverket för social- och hälsovården Valvira

För Tillstånds- och tillsynsverket för social- och hälsovården Valvira medför propositionen nya tillsynsuppgifter. För närvarande kommer man inte inom verket att anvisa personresurser för tillsynen enligt NIS 2-direktivet. Verket borde ha beredskap för uppskattningsvis minst tio NIS 2-inspektioner årligen, snabbare behandling av NIS-störningsanmälningar än för närvarande och förvaltning av NIS-organisationsregistret. Enligt verkets uppskattning kräver fullgörandet av skyldigheterna en tilläggsresurs på 2 årsverken för tillsyn och i fråga om informationssystemen en engångsinvestering på ca 0,15 miljoner euro och fortlöpande kostnader på ca 10 000–20 000 euro per år.

Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea (Kompletteras senare)

Övriga myndighetskostnader

Propositionen leder inte till nya resursbehov inom Finansinspektionen.

Utöver riskhanterings- och rapporteringsskyldigheterna föreslås också några nya skyldigheter för förvaltare av domännamnsregister. I Finland förvaltas registret över domännamn som slutar på toppdomänen fi av Transport- och kommunikationsverket. Transport- och kommunikationsverket åläggs skyldighet att offentliggöra uppgifter ur domännamnsregistret i en elektronisk tjänst samt besvara begäran om åtkomst till personuppgifter ur registret utan obefogat dröjsmål och senast inom 72 timmar efter mottagandet av begäran. Transport- och kommunikationsverket ska dessutom göra sina riktlinjer och förfaranden för säkerställande av användaruppgifternas riktighet och för utlämnande av registreringsuppgifter om domännamn offentligt tillgängliga. För Transport- och kommunikationsverket uppstår kostnader av de här uppgifterna.

Dessutom uppstår myndighetskostnader i någon mån när strategin för cybersäkerhet och planen för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser utarbetas och hålls uppdaterade. De beskrivna kostnaderna täcks inom ramen för de behöriga myndigheternas befintliga anslag.

Konsekvenser för aktörer inom offentlig förvaltning som föremål för riskhanterings- och rapporteringsskyldigheter

Riskhanterings- och rapporteringsskyldigheter ska tillämpas också hos aktörer inom offentlig förvaltning för att genomföra NIS 2-direktivet. Således får propositionen konsekvenser för de aktörer inom offentlig förvaltning som omfattas av tillämpningen också för att de fullgör skyldigheterna. Det föreslås att det ska föreskrivas om skyldigheterna och deras tillämpningsområde i informationshanteringslagen.

I propositionen föreslås ett nytt 4 a kap. i informationshanteringslagen med bestämmelser om de skyldigheter som gäller cybersäkerhet enligt NIS 2-direktivet som är tillämpliga på de statliga ämbetsverk och inrättningar, statliga affärsverk, självständiga offentligrättsliga inrättningar samt välfärdsområden, välfärdssammanslutningar och Helsingfors stad när de sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar.

I propositionen föreslås att en informationshanteringsenhet som omfattas av tillämpningsområdet ska anmäla sig som aktör enligt de bestämmelserna till Transport- och kommunikationsverket. I enlighet med bestämmelserna i direktivet ska en informationshanteringsenhet identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sin verksamhet, uppdatera en handlingsmodell för hantering av cybersäkerhetsrisker och vidta åtgärder för hanteringen av cybersäkerhetsrisker. Informationshanteringsenhetens ledning svarar för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av cybersäkerhetsrisker. Informationshanteringsenhetens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

I 4 kap. i informationshanteringslagen finns bestämmelser om skyldigheter och krav som gäller informationshanteringsenheter och myndigheter i fråga om informationssäkerhet. I 4 § 2 mom. finns dessutom bestämmelser om en informationsenhets lednings ansvar. Dessa bestämmelser tillämpas också på de myndigheter och informationshanteringsenheter som hör till tillämpningsområdet för de föreslagna bestämmelserna. Så som beskrivs i avsnitt 3.16 som behandlar nuläget, omfattar de gällande bestämmelserna i informationshanteringslagen delvis redan nu skyldigheterna enligt direktivet. Även om bestämmelserna i enlighet med direktivet förutsätter uttryckliga bestämmelser när det gäller cybersäkerheten, uppkommer inga sådana nya skyldigheter och krav för myndigheterna och informationshanteringsenheterna som ökar deras arbete på ett väsentligt sätt om sådant som de är förpliktade till redan i de gällande bestämmelserna i informationshanteringslagen. Det handlar främst om beaktande av riskerna med cybersäkerheten som en egen helhet, medan cybersäkerheten med stöd av den nuvarande lagstiftningen har beaktats som en del av informationssäkerheten. Inte heller de ansvar som innehas av informationshanteringsenhetens ledning kommer att öka på något betydande sätt.

En informationshanteringsenhet som omfattas av tillämpningsområdet för 4 a kap. i informationshanteringslagen är skyldig att anmäla betydande incidenter till Transport- och kommunikationsverket. Anmälningsskyldigheten delas in i en första anmälan som lämnas inom 24 timmar, en uppföljande anmälan som lämnas inom 72 timmar och en slutrapport som lämnas efter en månad. Om incidenten fortfarande pågår när slutrapporten ska lämnas in, ska en delrapport lämnas i stället för slutrapporten. Tidsfristerna enligt direktivet börjar räknas från det att informationshanteringsenheten fått kännedom om incidenten.

Den första anmälan och den uppföljande anmälan behöver inte vara omfattande till innehållet. I regel uppfylls anmälningsskyldigheten av en kort beskrivning av incidenten och en bedömning av om den misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar och om den kan ha gränsöverskridande verkningar. Uppgörandet av slutrapporten kräver mer arbete av myndigheten än de ovannämnda anmälningarna. Emellertid finns tid att arbeta med den i en månad från anmälningsskyldighetens början. Det är osannolikt att en myndighet blir tvungen att fortlöpande utarbeta sådana slutrapporter som avses i bestämmelsen, utan det handlar om ett arbete som kommer att ske då och då och som måste utföras med befintliga resurser. Bestämmelserna i direktivet kräver inte heller att fortlöpande övervakning eller andra motsvarande åtgärder ordnas för att upptäcka incidenter. Myndigheten/informationshanteringsenheten bör i enlighet med sin riskbedömning bedöma hur den med hjälp av sina befintliga resurser ordnar behövliga åtgärder för att upptäcka incidenter och göra anmälan om dem.

En myndighet som omfattas av tillämpningsområdet har möjlighet att få stöd för genomförandet av skyldigheter i enlighet med bestämmelserna av Transport- och kommunikationsverket som övervakar bestämmelserna och till vars uppgift hör en allmän skyldighet att ge anvisningar och

råd i enlighet med 4 a kap. i informationshanteringslagen. Transport- och kommunikationsverket ska också ge anvisningar och råd om hanteringen av incidenten. Genom riskhanteringen av cybersäkerheten förbättras också cybersäkerheten i informationshanteringsenheternas och myndigheternas verksamhet och detta förebygger sannolikt incidenter och deras skadliga verkningar. De myndigheter som omfattas av tillämpningsområdet har utvecklat sin cybersäkerhetsnivå som ett led i den nuvarande beredskapen och skötseln av de nuvarande uppgifterna förutsätter att man sörjer för riskhanteringen i fråga om cybersäkerheten. De föreslagna ändringarna i informationshanteringslagen för att genomföra NIS 2-direktivet anses därmed inte medföra alla myndigheter betydande behov av tilläggsresurser på grund av att myndigheterna är föremål för skyldigheterna i NIS 2-direktivet. För en del av myndigheterna kan de föreslagna bestämmelserna förutsätta höjd beredskapsnivå och ändringar i informationssystemen. Kostnaderna som uppstår när bestämmelserna iakttas ska täckas med anslag ur rambeslutet för statsfinanserna och statsbudgeten.

I propositionen föreslås dessutom att skyldigheten att säkerhetsklassificera handlingar i 18 § i informationshanteringslagen ska gälla Suomen Erillisverkot Oy och dess helägda dotterbolag när dessa sköter uppgifter som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät. Dessa aktörer har färdigheter i säkerhetsklassificering av handlingar och hantering av säkerhetsklassificerade handlingar och den föreslagna skyldigheten har således inga särskilda konsekvenser för deras verksamhet. I informationsutbyte och samarbete som sker i säkerhetsnätsverksamheten blir hanteringen av handlingar tillsammans med de säkerhetsklassificerande myndigheterna också tydligare, när det finns enhetliga lagstadgade krav om anteckning om säkerhetsklass för handlingar och om de förfaranden som ska följas vid hanteringen av dem.

4.5 Andra konsekvenser som gäller människor och samhället

Konsekvenser för säkerheten

Den digitala utvecklingen av samhällen, som bland annat covid-19-pandemin satt fart på, har väsentligt ändrat på den nuvarande verksamhetsmiljön och fört med sig nya utmaningar. Antalet kommunikationsnät och informationssystem och deras betydelse som en del av produktionen av de tjänster som samhällets verksamhet kräver och verksamheten i samhällets kritiska infrastruktur ökar fortsättningsvis. Antalet cyberhot och cyberattacker har ökat och cyberattackerna utvecklas kontinuerligt när teknologin utvecklas. Funktioner som är kritiska med tanke på samhället är allt mer beroende av informationssystem och kommunikationsnät där cyberstörningar som förekommer kan medföra betydande skadliga konsekvenser, utöver för den aktör som är föremål för störningen, även för samhället i större utsträckning. Också ändringar i utrikes- och säkerhetspolitiken har avspeglats i cyberomgivningen. Risken för överbelastningsangrepp, inbrott, skadliga datorprogram och statlig verksamhet har ökat och hotnivån stigit. Cyberattacker används som en del av den hybridpåverkan som riktas mot samhället.

Enligt förslaget stärks samhällets allmänna cybersäkerhetsnivå och resiliens. När den kunskap som gäller cybersäkerhet och riskhanteringsåtgärderna för cybersäkerhet förbättras blir det svårare och dyrare att orsaka skadliga konsekvenser för tjänster som är centrala för samhällets verksamhet. Genom de förslag till upprättande av en nationell cybersäkerhetsstrategi och en omfattande plan för hantering av cyberkriser som ingår i propositionen strävar man efter att utveckla hela samhällets cybersäkerhet som helhet och beredskap att svara på omfattande cyberincidenter som överskrider gränser mellan medlemsstater.

Genom förslaget förbättras verksamhetsförutsättningarna för aktörer som är viktiga med tanke på samhällets verksamhet i en förändrad verksamhetsmiljö. Förslaget förenhetligar riskhantering och krav på rapportering om risker som gäller cybersäkerhet på olika sektorer och utvidgar regleringen om cybersäkerhet till att täcka flera aktörer. I förslaget betonas beredskap och förebyggande åtgärder för att man mer förutseende än tidigare ska kunna svara på ändringar i cyberomgivningen, störningar och sårbarheter. Målet är att undvika avbrott som orsakas av cyberstörningar i kontinuiteten i tjänster och funktioner som är centrala med tanke på samhällets verksamhet, för en störning i tillhandahållandet av en kritisk tjänst kan medföra betydande skada för samhället. En störning som skett i en av samhällets kritiska funktioner (till exempel i energiproduktionen eller funktionen i kommunikationsnät) kan märkbart påverka även tillgången till andra kritiska tjänster och orsaka omfattade skadliga konsekvenser för samhället. Dessutom kan konsekvenserna för kontinuiteten i vissa kritiska tjänster, utöver ekonomiska förluster, även orsaka hot som riktas mot till exempel medborgares liv och hälsa. Vid riskhanteringen bör man också beakta att hot mot cybersäkerheten är sektorsövergripande samt betydelsen av leveranskedjor. Skyldigheterna i förslaget är investeringar i samhällets driftssäkerhet och cyberresiliens.

Rapportering om betydande incidenter särskilt beträffande slutrapporteringen förbättrar informationsöverföringen till centrala myndigheter och på så sätt utformandet av en gemensam lägesbild över betydande incidenter och orsakerna till dem i samhället. Kombinerat med motsvarande skyldigheter i andra EU-medlemsstater ökar genomförandet av NIS 2-direktivet den mängd information som myndigheterna får om cyberstörningar via Enisa. Dessutom innehåller propositionen flera förslag genom vilka man stärker samarbetet och informationsutbytet mellan myndigheter och de aktörer som omfattas av skyldigheterna.

Kommunikationsnät och informationssystem står i global förbindelse med varandra, och också en cyberattack eller en cyberstörning som riktas mot en annan medlemsstat kan få återverkningar i Finland. Genomförandet av NIS 2-direktivet i EU:s medlemsstater förbättrar den allmänna toleransen mot cyberstörningar och beredskapsnivån inför dem i hela EU genom att förenhetliga kraven på cybersäkerhet hos de kritiska sektorerna och förbättra medlemsländernas samarbete vid gränsöverskridande cyberstörningar. Förslaget minskar också på fragmenteringen i den inre marknaden och jämnar ut aktörernas verksamhetsförutsättningar. Störningar i cybersäkerheten försvårar verksamheten på den inre marknaden, medför ekonomiska förluster och försämrar användarnas förtroende för unionens ekonomiska liv och samhällsliv. Genom effektiv riskhantering som gäller cybersäkerhet kan man minska på antalet störningar i cybersäkerheten och de konsekvenser de medför.

Konsekvenser för informationssamhället och dataskyddet

Förslaget ger positiva effekter på informationssamhällets utveckling, för det främjar ibruktagandet av informationssäkra tjänster och förfaranden och skapar på så sätt efterfrågan på sådana tjänster och på professionella inom cybersäkerhet. En förbättring av cybersäkerhetsnivån minskar på de störningar som förekommer i användningen av tjänster och främjar ett allmänt förtroende för digitala tjänster.

De krav på utbildning som regleringen kräver bedöms även öka personalens kännedom om och förståelsen av informationssäkerheten särskilt i organisationer där sådan utbildning inte tidigare har tillhandahållits. En förbättring av den nationella cybersäkerheten kräver, utöver experter på

cybersäkerhet, även en allt bättre kännedom om informationssäkerhet i vardagen hos medborgare och företag. Förslaget höjer efterfrågan på kunskap om hantering av cybersäkerhetsrisker och ökar kunskapen om hanteringen av dem hos aktörer som omfattas av tillämpningsområdet.

Det har bedömts att förslaget förbättrar också myndigheternas kännedom om cybersäkerhet. Den föreslagna sektorsspecifika tillsynsmodellen främjar utvecklandet av kompetensen inom cybersäkerhet hos de sektorsspecifika tillsynsmyndigheterna. Dessutom utökar utvidgandet av rapporteringsskyldigheten till flera sektorer och aktörer även myndigheternas omdöme avseende cyberhot som riktas mot aktörer.

Dataskyddet för den information som behandlas i informationssystem och kommunikationsnät kräver utveckling av egenskaper inom informationssäkerhet. Åtgärderna för förbättring av cybersäkerheten i informationssystem och kommunikationsnät påverkar dataskyddet för den information som ska behandlas i dem så att det blir bättre.

Förslaget får konsekvenser för informationsmaterial och informationssystem som avses i 8 § 2 mom. i informationshanteringslagen. Förslaget kompletteras med en konsekvensbedömning av ändringarna inom informationshanteringen.

Miljökonsekvenser

Propositionen har inte konstaterats få några betydande miljökonsekvenser.

Förslaget främjar bättre utnyttjande av den senaste generationens IKT-infrastruktur och IKT-tjänster, vilka blir mer hållbara med tanke på miljön. Genom förslaget stärks cybersäkerheten inom sådana kritiska sektorer som är utsatta för cybersäkerhetsrisker och betydande incidenter kan, om de förverkligas, medföra såväl direkta som indirekta allvarliga miljökonsekvenser. Till den delen är energisektorn, avfallshanteringen och vattenförsörjningen särskilt viktiga sektorer. Förslaget främjar indirekt förhindrandet av skadliga miljökonsekvenser som orsakas av betydande incidenter genom att förbättra aktörernas hantering av cybersäkerhetsrisker inom sektorer som är betydande för miljön.

5 Övriga alternativ för genomförandet

5.1 Alternativen och deras konsekvenser

5.1.1 Nationellt utvidgande av riskhanterings- och rapporteringsskyldigheter

Det nationella genomförandet av NIS 2-direktivet kräver reglering av skyldigheterna enligt direktivet på lagnivå. Skyldigheterna enligt NIS 2-direktivet gäller huvudsakligen detaljerad och harmoniserande reglering på miniminivå. Det finns huvudsakligen ingen nationell rörelsefrihet vad gäller NIS 2-direktivets minimitillämpningsområde eller skyldigheternas innehåll. Den nationella rörelsefriheten beskrivs ovan i avsnitt 2.10.

Vid genomförandet av NIS 2-direktivet har alternativen bedömts enligt en miniminivå i förhållande till ett nationellt uppställande av riskhanterings- och rapporteringsskyldigheter på högre nivå eller utvidgande av tillämpningsområdet. Ur de företags perspektiv som agerar på den inre marknaden är en nationell reglering som genomför NIS 2-direktivet och som är jämförbar mellan Finland och 11 andra medlemsstater eftersträvansvärd, för att kraven i NIS 2-direktivet på

de aktörer som omfattas av tillämpningsområdet ska vara så jämförbara som möjligt i medlemsstaterna. På grund av jämförbarheten av den reglering som genomför NIS 2-direktivet i förhållande till andra medlemsstater har utgångspunkten valts till att vara en miniminivå för riskhanterings- och rapporteringsskyldigheterna på den nivå direktivet ställer.

5.1.2 Regleringsmodell på andra sektorer än offentlig förvaltning

I beredningen av propositionen har man bedömt genomförandet av regleringen antingen i den föreslagna formen, det vill säga genom att anta en lag om hantering av cybersäkerhetsrisker eller genom att ta in genomförandebestämmelserna i NIS 2-direktivet som en del av den sektorsspecifika lagstiftningen. Vid genomförandet av NIS 1-direktivet stannade man för att foga till direktivets genomförandebestämmelser som en del av sektorsspecifik lagstiftning. De riskhanterings- och rapporteringsskyldigheter som NIS 1-direktivet kräver är dock i märkbar utsträckning mer allmänna och öppna än de motsvarande skyldigheterna i NIS 2-direktivet. I samband med genomförandet av NIS 1-direktivet ansåg man också att skyldigheterna i fråga inte skilde sig från aktörers övriga riskhantering på ett sådant sätt att det skulle ha varit befogat att lagstifta om dem i olika lagar (RP 192/2017 rd). De riskhanterings- och rapporteringsskyldigheter som ställs i NIS 2-direktivet är dock betydligt mer detaljerade, och det kan inte till exempel längre anses att en allmän skyldighet för aktörer till beredskap eller riskhantering motsvarar skyldigheterna i NIS 2-direktivet. Det sätt att lagstifta som ska väljas påverkas kraftigt även av den ökade betydelse cybersäkerheten fått under de senaste fem åren. Finland var ett undantag i EU vid genomförandet av NIS 1-direktivet vad gäller sättet att dela upp lagstiftningen. En betydande del av de andra medlemsstaterna antog redan senast i samband med genomförandet av NIS 1-direktivet en så kallad cybersäkerhetslag.

En modell som innebär en lag är ett fördelaktigt alternativ också för att det bättre uppfyller NIS 2-direktivets syfte, det vill säga markerar miniminivån för skyldigheterna inom cybersäkerhet. Syftet med den lag som nu föreslås om hantering av cybersäkerhetsrisker är att, utöver reglering om cybersäkerhet för aktörer som är kritiska med tanke på samhällets funktioner, också vara ett allmänt exempel på regleringsramen för skyldigheter inom cybersäkerhet. På så sätt förtydligar modellen med en lag även den nationella regleringen om cybersäkerhet, som i Finland är uppdelad på många sektorsspecifika lagar och enskilda bestämmelser som gäller cybersäkerhet. Valet förordas även av att tillämpningsområdet för NIS 2-direktivet är betydligt mer omfattande än för NIS 1-direktivet, och det har inte reglerats tidigare om all verksamhet som omfattas av tillämpningsområdet vad gäller verksamhetstyper eller sektorer. En sektorsspecifikt uppdelad reglering om skyldigheterna kräver således tillägg i många sektorlagar och en helt ny lag eller någon annan lösning för de aktörers del för vilka det inte finns någon sektorsspecifik reglering. Det ska observeras att lite mer än det dubbla antalet sektorer omfattas av NIS 2-direktivets tillämpningsområde jämfört med NIS 1-direktivets. NIS 2-direktivets reglering beträffande skyldigheter för aktörer och tillsynen över dem är också noggrannare och mer detaljerad än regleringen i NIS 1-direktivet, vilket medför sektorsspecifik uppdelning på flera sektorlagar med ett betydande antal nya bestämmelser som motsvarar varandra och vilkas tillämpningsområde kan avvika från tillämpningsområdet för lagens övriga bestämmelser. Det kan inte anses eftersträvansvärt sett ur perspektivet för regleringens tydlighet och regleringsbördan. Man måste också beakta att modellen en lag, för att säkerställa en hög nivå på cybersäkerheten, sannolikt bör kompletteras med branschvis reglering på lägre nivå för olika sektorer där man vid behov på en mer detaljerad nivå kan föreskriva om säkerställandet av cybersäkerheten i verksamheten hos de aktörer som omfattas av tillämpningsområdet. Förverkligat på detta sätt har alla sektorer gemensamma skyldigheter och mål i en ny allmän lag, vars krav kan preciseras sektorsspecifikt.

5.1.3 NIS 2-speciallag för sektorn offentlig förvaltning och tillämpning på sektorn

För sektorn offentlig förvaltning när den utövar ren offentlig förvaltning finns det ny reglering i NIS 2-direktivet i förhållande till NIS 1-direktivet. Flera bestämmelser i direktivet gäller sektorn offentlig förvaltning, och i dem ingår nationellt övervägande och rörelsefrihet. Dessa bestämmelser gäller bland annat de aktörer och de uppgifter som behandlas och som omfattas av tillämpningsområdet, för vilkas del bland annat uppgifter som gäller nationell säkerhet, allmän säkerhet och försvaret inte berörs av direktivet. Dessutom finns det undantag i bestämmelser som gäller tillsyn över och påföljder för aktörer. Begränsningarna av informationsbehandling gäller också verksamhet som hör till andra sektorer, men speciellt gäller de sektorn offentlig förvaltning.

Informationssäkerheten inom offentlig förvaltning berörs av allmän lag, det vill säga informationshanteringslagen, vars reglering gäller NIS 2-direktivets reglering till de delar som beskrivs i avsnitt 3.16. Den reglering som krävs i NIS 2-direktivet är på grund av den nationella rörelsefriheten för offentlig förvaltning och dess särdrag ansetts vara ändamålsenlig att placera i informationshanteringslagen. Då finns de skyldigheter som gäller informationssäkerheten på nivån allmän lag som gäller aktörer inom sektorn offentlig förvaltning samlade i en lag. Genom bestämmelserna i NIS 2-direktivet blir det ett tillämpningsområde som avviker från övrig tilllämpning i informationshanteringslagen, och regleringen samlas därför i ett kapitel där skyldigheterna och tillsynen över dem organiseras för sektorn offentlig förvaltning. Vad gäller lägesmedvetenhet inom den sektorsspecifika tillsynen och den offentliga förvaltningen är det också ändamålsenligt att det föreskrivs särskilt om tillsyn och tillsynsmyndighet för aktörerna inom offentlig förvaltning i förhållande till andra sektorer där det också finns offentliga aktörer. En offentlig aktör kan beträffande den verksamhet den utövar omfattas av tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker (t.ex. välfärdsområdenas och välfärdssammanslutningarnas hälso- och sjukvård). En offentlig aktör kan även omfattas av enbart tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker, eftersom informationshanteringslagen inte ska tillämpas på till exempel kommuner eller samkommuner (med undantag för Helsingfors stad till vissa delar) och inte på andra än myndigheter som sköter offentliga förvaltningsuppgifter. Dessa offentliga aktörers ställning i förhållande till NIS 2-direktivet bestäms enligt lagen om hantering av cybersäkerhetsrisker om de utövar verksamhet på någon annan sektor som nämns i bilaga I och II ti NIS 2-direktivet. Som exempel på en sådan aktör kan nämnas samkommunen Helsingforsregionens miljötjänster HRM, som utövar verksamhet bland annat på sektorn vatten- och avfallshantering. För den sektorsspecifika tillsynen och för insamling av lägesinformation är det viktigt att en offentlig aktör på någon annan sektor i direktivet (annan än sektorn offentlig förvaltning) även omfattas av tillsynen på specialsektorn i fråga och att tillsyn och anmälningsskyldighet för specialområdet i fråga gäller aktören.

Inom sektorn offentlig förvaltning har det inte ansetts ändamålsenligt att tillämpa direktivets skyldigheter i bredare utsträckning nationellt än vad som är nödvändigt. Inom sektorn offentlig förvaltning gäller reglering om informationssäkerhet. Den reglering om informationssäkerhet som ingår i 4 kap. i informationshanteringslagen och som betonar riskhantering tillämpas på alla aktörer inom offentlig förvaltning inklusive enskilda personer eller organisationer som sköter offentliga förvaltningsuppgifter. Skyldigheter som gäller informationssäkerhet ingår även i den allmänna dataskyddsförordningen. Som en aspekt har det även beaktats att det med stöd av dataskyddsförordningen redan finns en tillsynsmyndighet vars uppgifter också omfattar tillsyn över sektorn offentlig förvaltning. För cybersäkerhetens del förutsätts det i NIS 2-direktivet att också den offentliga förvaltningens iakttagande av skyldigheterna ska övervakas. För att kanalisera tillsynsmyndighetens resurser är det ändamålsenligt att hänföra skyldigheter endast till dem som också i beredningen av direktivet har ansetts som kritiska aktörer. Dessutom betonas

det i den föreslagna regleringen att också andra aktörer inom offentlig förvaltning kan anmäla om cyberhot, incidenter och tillbud till tillsynsmyndigheten, vilket i och för sig är möjligt också i nuläget. Enligt den föreslagna regleringen ska Transport- och kommunikationsverket dock ha en tydligare roll än tidigare vid behandlingen av anmälningar från offentliga sektorn och sammanfattande av lägesbild samt vid informationsutbyte mellan myndigheter. Också de behörigheter som föreslås för CSIRT-enheten stöds i många fall också av en förbättring av den offentliga förvaltningens informations- och cybersäkerhet.

Enligt artikel 2.5 i direktivet får medlemsstaterna föreskriva att direktivet ska tillämpas på offentliga förvaltningsentiteter på lokal nivå och på utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet. Trots att direktivet i sig möjliggör att tillämpningsområdet utvidgas till kommuner och aktörer inom utbildningssektorn föreslås det inte att dessa ska omfattas av tillämpningsområdet för 4 a kap. i informationshanteringslagen, med undantag för Helsingfors stad när den sköter uppgifter som hör till organiseringsansvaret för välfärdsområden.

På grund av skäl som gäller nationell säkerhet, allmän säkerhet, försvaret eller myndigheter inom sektorn brottsbekämpning samt tjänsteproducenter av säkerhetsnät och användning av tjänsterna gäller, utom de ovannämnda skälen som gäller prövning av ändamålsenlighet och känslig information som ska behandlas, föreslås det inte att dessa aktörer ska omfattas av tillämpningsområdet för regleringen. De nämnda aktörerna är enligt skyldigheterna i informationshanteringslagen redan på grund av verksamhetens natur, internationella skyldigheter i fråga om informationssäkerhet samt enligt säkerhetsnätslagen och statsrådets förordning om verksamheten i den offentliga förvaltningens säkerhetsnät (1109/2015) som utfärdats med stöd av den samt enligt finansministeriets föreskrifter rätt heltäckande skyldiga att sörja för cybersäkerheten. Genom den lag som föreslås begränsas inte heller möjligheterna att iaktta regleringen i 4 a kap. även hos dessa myndigheter. Också de kan beakta skyldigheterna att hantera cybersäkerheten som en kontrollista för informationssäkerhet. Dessa aktörer kan också frivilligt och i den utsträckning de vill meddela Transport- och kommunikationsverket om incidenter samt samarbeta i övrigt som de gjort även hittills.

Gällande lagstiftning möjliggör i viss utsträckning inspektionsrätt för Transport- och kommunikationsverket också i fråga om tjänster som gäller säkerhetsnät (325 § 2 mom. i lagen om tjänster inom elektronisk kommunikation). Dessutom finns för Transport- och kommunikationsverket uppgifter i lagstiftningen som gäller bedömning och godkännande av myndigheters informationssystem och datakommunikation (t.ex. lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2022) och Lag om internationella förpliktelser som gäller informationssäkerhet 588/2004)). I flera lagar finns också bestämmelser om handräckning. I till exempel 23 § i nätsäkerhetslagen är Försvarsmakten, polisen, Gränsbevakningsväsendet och Transport- och kommunikationsverket skyldiga att på begäran av finansministeriet i den utsträckning det är möjligt ge de tillhandahållare av tjänster inom säkerhetsnätet handräckning för att säkerställa en störningsfri verksamhet inom säkerhetsnätets tjänsteproduktion. Även i denna regeringsproposition stöder de uppgifter som föreslås för CSIRT-enheten och samarbetet mellan myndigheter för sin del även hanteringen av cybersäkerhetsrisker hos myndigheter som inte omfattas av denna lag och som sköter uppgifter inom sektorerna nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning.

5.1.4 Ordnandet av tillsyn

I beredningen av förslaget har man, vad gäller ordnandet av tillsynen över aktörernas skyldigheter, som alternativ bedömt antingen en centraliserad eller en sektorsspecifikt decentraliserad modell för tillsynen. Tillsynsansvaret över den reglering som genomför NIS 1-direktivet har

anvisats de myndigheter som övervakar också andra skyldigheter inom hanteringen av säkerhetsrisker med stöd av sektorsspecifika specialbestämmelser, där skyldigheterna enligt NIS 1-direktivet har fogats till. I beredningen av förslaget har man således bedömt alternativet huruvida man ska fortsätta med den tillsynsmodell som genomfördes för NIS 1-direktivet, det vill säga att sektorsspecifikt dela ansvaret för tillsynen mellan de myndigheter som övervakar också andra säkerhets- och riskhanteringsskyldigheter, eller om det är motiverat att koncentrera tillsynen hos en behörig myndighet som övervakar skyldigheter enligt NIS 2-direktivet på alla sektorer.

I beredningen har man inte konstaterat någon existerande myndighet som enligt gällande lag har de tillsynsbehörigheter som krävs för den miniminivå enligt NIS 2-direktivet som gäller NIS 2-sektorn, eller någon myndighet i vars nuvarande tillsynsuppgifter övervakning över skyldigheterna enligt NIS 2-direktivet är en del som passar in naturligt. I beredningen har man konstaterat att uppgifter av samma slag som de föreslagna tillsynsuppgifterna har anvisats flera olika myndigheter, och av de nuvarande myndigheterna har ingen den övergripande expertis som den föreslagna regleringen kräver om olika sektorers särdrag och cybersäkerhet. Ur perspektivet centralisering av tillsynen har man som alternativ bedömt en koncentration av uppgifterna hos en ny tillsynsmyndighet eller hos Cybersäkerhetscentret på Transport- och kommunikationsverket, i vars särskilda uppgifter ingår uppgifter som gäller främjande av allmän informationssäkerhet, och som stöder, styr och övervakar informationssäkerheten och att integritetsskyddet tillgodoses i elektronisk kommunikation samt upprätthåller den nationella lägesbilden av cybersäkerheten. I beredningen har det bedömts att rollen för Cybersäkerhetscentret på Transport- och kommunikationsverket som samtidigt centraliserad tillsynsmyndighet för varje sektor och som styrande CSIRT-enhet som undersöker kränkningar av informationssäkerheten förenat med Cybersäkerhetscentrets nuvarande uppgifter skapar en omfattande uppgiftshelhet som blir oändamålsenlig både för de aktörer som omfattas av tillämpningsområdet och för myndigheten. Samtidigt medför uppgiftshelheten olägenheter för skötseln av Cybersäkerhetscentrets nuvarande uppgifter. Om tillsynen centraliseras måste det därför inrättas en ny myndighet som utövar tillsynen eller en självständig enhet i samband med den existerande myndigheten. Med beaktande av det antal aktörer som ska övervakas och tillämpningsområdets omfattning samt det behov av sektorsspecifik expertis som krävs för tillsynen medför inrättandet av en ny myndighet enligt vad som kan förutses högre utgifter än om tillsynen delas upp sektorsspecifikt.

Det finns existerande tillsynsmyndigheter på NIS 2-sektorerna som övervakar de helheter som fastställts för dem i sektorsspecifik lagstiftning eller delområden som gäller säkerhet och riskhantering vid sidan av annat. Om myndighetsuppgifterna i fortsättningen centraliseras på endast en myndighet kan detta medföra överlappande tillsynsbehörigheter och överlappande rapporteringsskyldigheter för aktörerna. Att tillsynen ordnas sektorsspecifikt förespråkas också av att cybersäkerheten inte är någon avskild del av verksamheten hos aktörer som ska övervakas, utan när samhället digitaliseras ses cybersäkerheten som ett delområde i helhetssäkerheten för verksamheten. Ur aktörens synvinkel uppfattas hanteringen av olika risker typiskt sett som en helhet, och det är i princip inte motiverat att avskilja eller granska hanteringen av cybersäkerhetsrisker eller tillsynen av den avskild från hantering av andra risker som en separat helhet. En störning som riktas mot en tjänst kan orsakas av störningar som riktas mot informationssystem eller av en störning som gäller annan säkerhet. Dessutom kan en störning utöver cybersäkerheten sannolikt påverka en aktörs övriga verksamhet och dess säkerhet med sektorsspecifika särdrag. Till exempel på trafiksektorn kan en cyberstörning märkbart påverka även trafiksäkerheten eller på hälso- och sjukvårdssektorn kund- eller patientsäkerheten. Därför är det också ur aktörens synvinkel en i princip klarare lösning som medför en mindre administrativ börda att tillsynen över hanteringen av olika risker och skyldigheter som gäller verksamhetens säkerhet och kontinuitet och rapporteringen av störningar inte är uppdelad på flera myndigheter, utan att aktören i princip

övervakas av en myndighet vad gäller säkerhets- och riskhanteringsskyldigheter som riktas mot verksamheten.

Genom ett sektorsspecifikt tillvägagångssätt och organisering av tillsynen kan man ta sektorsspecifika särdrag i beaktande och bättre beakta övrig sektorsspecifik reglering. Oberoende av vilken tillsynsmodell som väljs ska expertis som gäller cybersäkerheten i varje fall stärkas hos alla myndigheter för att genomföra deras nuvarande tillsynsuppgifter så att myndigheterna bättre än tidigare kan förstå cybersäkerhetens betydelse i den verksamhet de övervakar. Också ur tillsynsmyndighetens perspektiv har det bedömts ändamålsenligt att bedöma säkerheten i verksamheten hos den som ska övervakas som en helhet.

Nyttan med en centraliserad tillsynsmodell är modellens klarhet för aktörer som utövar verksamhet på flera olika sektorer som omfattas av tillämpningsområdet. En centraliserad tillsynsmodell koncentrerar även den expertis som gäller riskhanteringsskyldigheter i fråga om cybersäkerhet hos myndigheten. Å andra sidan kräver centralisering att en ny självständig tillsynsfunktion eller tillsynsmyndighet inrättas, eller att en existerande tillsynsfunktion utvidgas betydligt, eftersom man inte har konstaterat någon existerande myndighet till vars nuvarande uppgifter en tväradministrativ tillsynsfunktion på ett naturligt sätt kan fogas. I en centraliserad tillsynsmodell får tillsynsmyndigheten ett avsevärt antal aktörer som ska övervakas och en omfattande uppgift att observera och övervaka aktörer i olika sektorer som omfattas av tillämpningsområdet. Om tillsynsuppgiften koncentreras på en myndighet för varje sektor blir tillsynsfältet märkbart omfattande.

En centraliserad tillsynsmodell har ansetts vara det mest motiverade alternativet för övervakning enligt den allmänna dataskyddsförordningen och den reglering som utfärdats för genomförande av den. I motsats till regleringen om dataskydd omfattar tillämpningsområdet för NIS 2-direktivet endast de aktörer som uppfyller kriterierna försektorer som det föreskrivs om i direktivet. Aktörernas antal och art samt verksamhetens samhälleliga betydelse varierar sektorsspecifikt, vilket talar för en tillsynsmodell där sektorsspecifika särdrag samt annan sektorsspecifik reglering än den som gäller cybersäkerhet och riskhantering kan samordnas så väl som möjligt för tillsyn enligt NIS 2-direktivet. På flera sektorer har man konstaterat reglering om informationssäkerhet eller annan existerande reglering som gäller riskhantering, säkerhet eller verksamhetens kontinuitet som kompletterar NIS 2-direktivet. Då kan man genom att centralisera sådana tillsynsuppgifter hos samma myndighet uppnå synergifördelar och undvika överlappande tillsynsbehörigheter eller oklarheter i fråga om behörigheter.

Det ska också observeras att skyldigheten att hantera risker enligt NIS 2-direktivet till innehållet är sådan att tillsynen av den, oberoende av tillsynsmodell, kräver att tillsynsmyndigheten har både marknadskännedom om sektorn i fråga och kännedom om sektorsspecifika särdrag, såsom kännedom om annan relevant lagstiftning och bästa praxis. Tillsynsmyndigheten ska känna till den sektor och den marknad som ska övervakas väl, för hantering av cybersäkerhetsrisker, såsom även övrig riskhantering, är mycket organisations- och sektorsspecifik. Olika risker riktas mot olika organisationer, och även verkliga störningssituationer kan få mycket olika konsekvenser för samhället beroende på inom vilken sektor en aktör finns som störningen riktas mot. De skyldigheter som ställts upp i NIS 2-direktivet utgör till karaktären minimireglering, och i regleringen om informations- och cybersäkerheten finns också märkbara sektorsspecifika skillnader. En del av de sektorer som omfattas av tillämpningsområdet för NIS 2-direktivet har gällande reglering om informations- och cybersäkerhet som kompletterar NIS 2-direktivet, och

regleringen strävar efter en högre nivå för cybersäkerhet eller ställer upp mer detaljerade skyldigheter.

Med beaktande av de ovan anförda omständigheterna under beredningen har man som slutresultat för bedömningen av alternativ stannat för att det finns skäl för att tillsynen för varje sektor anvisas en sektorsspecifik myndighet för ändamålsenlig organisering av tillsynen och för undvikande av oklarheter som gäller behörighet. Samordning av tillsynen och på grund av effektiviteten är det motiverat att tillsynsuppgiften, som fortsättning på den nuvarande tillsynsmodellen anvisas den myndighet som redan enligt gällande lagar övervakar aktörer på en sektor och de skyldigheter i fråga om hantering av säkerhetsrisker som gäller dem. En sektorsspecifik myndighet har den bästa kännedomen om särdragen hos sektorn i fråga och om övrig reglering som gäller verksamheten. Då har tillsynsmyndigheten den bästa expertisen och omdömesförmågan i fråga om de omständigheter som gäller riskhantering för sektorn. Sektorsspecifika myndigheter har även den bästa marknadsförståelsen om sektorn i fråga, och därmed bättre möjligheter att bedöma aktörer som omfattas av regleringen och de risker som riktas mot dem samt incidenters betydelse och konsekvenser. Under beredningen har man dock observerat att utförandet av de tillsynsuppgifter som nu föreslås också kräver en ny slags specialkompetens av tillsynsmyndigheten. Det kan dock vara svårt att ordna sådan tillsyn, speciellt hos myndigheter som tidigare inte har haft de slag av tillsynsuppgifter som nu föreslås. Å andra sidan kräver samhället när det digitaliseras att myndigheterna utvecklar omdömesförmåga som gäller cybersäkerhet också för att övervaka andra säkerhetsförpliktelser än de som gäller cybersäkerhet enligt sina nuvarande uppgifter. Dessutom kräver koncentrationen av tillsynen på en myndighet på motsvarande sätt anskaffande av tillräcklig kompetens och resurser till den myndigheten som uppgiften anvisas, vilket medför kostnader särskilt vad gäller det omfattande tillämpningsområdet och kännedomen om sektorsspecifika särdrag. Ur perspektivet för resursering har det också ansetts ändamålsenligt att cybersäkerhetsskyldigheter övervakas sektorsspecifikt av samma myndigheter som övervakar aktörer som omfattas av reglering även till andra delar. Helhetskostnaderna för en ny centraliserad myndighet som utövar tillsyn bedöms bli cirka 20–50 procent högre än om tillsynen ordnas på samma nivå som i en decentraliserad modell.

Utöver det som framförs ovan har en sektorsspecifik tillsynsmodell som antagits i genomförandet av NIS 1-direktivet upplevts vara huvudsakligen funktionell, och tillförlitliga förbindelser och samarbete har bildats mellan de nuvarande tillsynsmyndigheterna och de aktörer som är föremål för tillsynen. Syftet med samarbetet är att förbättra nivån på cybersäkerheten, riskhanteringen och resiliensen. Samarbetet mellan de nationella existerande myndigheterna och mellan företag har under årens lopp utvecklats till att huvudsakligen fungera, och det är inte ändamålsenligt att kringskära detta samarbete i samband med genomförandet av NIS 2-direktivet.

Tillsynsmyndighet för den offentliga förvaltningen

I förslaget föreslås det att den behöriga tillsynsmyndigheten för den offentliga sektorn enligt direktivet blir Transport- och kommunikationsverket. Under beredningen har olika alternativ för behörig myndighet bedömts. Finansministeriet intervjuade vid sidan av annat för att utreda saken under februari–mars 2023 olika organisationer inom offentlig förvaltning samt representanter för tillsynsmyndigheterna enligt NIS 1-direktivet. Enligt intervjuer fick Cybersäkerhetscentret under Transport- och kommunikationsverket mest stöd som behörig myndighet. I intervjuer lyftes Cybersäkerhetscentrets redan existerande skicklighet och kompetens fram i fråga om tillsyn. Dessutom konstaterades det att en centraliserad tillsyn producerar synergieffekter i förhållande till att tillsynen över den offentliga förvaltningen delas upp på flera myndigheter. Även bristen på kompetens inom området cybersäkerhet togs upp, och på grund av den är det inte motiverat att inrätta en ny myndighet eller anvisa någon annan myndighet tillsynsuppgiften.

Dessutom konstaterades det i intervjuer att det inte heller lönar sig att göra för många steg i tillsynen för att undvika att den blir invecklad, och att det är åskådligt att en myndighet övervakar alla aktörer inom offentlig förvaltning som enligt direktivet omfattas av bestämmelserna i informationshanteringslagen. Justitieministeriet och kommunikationsministeriet lyfte upp frågan om en tillsynsmyndighets möjlighet att övervaka en myndighet som står över den i hierarkin. Därför bör myndigheten eventuellt vara en oberoende aktör på statsrådsnivå. Å andra sidan konstaterades i intervjuerna att Transport- och kommunikationsverket redan i nuläget har uppgifter som gäller genomförande av internationella skyldigheter inom informationssäkerhet vilka också gäller ministerienivån.

Andra möjliga behöriga myndigheter som togs upp var till exempel regionförvaltningsverken och dataombudsmannens byrå. Även Statens revisionsverk föreslogs i en intervju som behörig myndighet. I intervjuerna togs det ändå upp att de ovannämnda myndigheterna inte i nuläget har kompetens att sköta uppgiften utan tilläggsresursering. Som ett alternativ föreslogs även inrättandet av en ny, självständig och oberoende myndighet.

Utöver intervjuerna tillfrågades medlemmarna i en underarbetsgrupp, som koncentrerar sig på sektorn offentlig förvaltning, om deras syn på en behörig myndighet. Enligt kommunikationsministeriet bör uppgiften som tillsynsmyndighet för ministerierna i princip vara en myndighet på samma nivå som statsrådet och vara så centraliserad som möjligt. Enligt justitieministeriet bör centralisering utnyttjas i tillämpliga delar, men samtidigt bör riskerna med centraliseringen beaktas. Arbets- och näringsministeriet frågade om det borde finnas någon centraliserad ”mellannivå” i regionförvaltningen och lokalförvaltningen som samlar in information och samordnar ärenden på sitt område och centraliserat förmedlar informationen från området till Transport- och kommunikationsverket. Enligt miljöministeriet kan man, om myndighetsuppgifter centraliseras på regional eller lokal nivå, bedöma en modell där närings-, trafik- och miljöcentralerna sköter ärendet, eller där ärendena koncentreras hos en närings-, trafik- och miljöcentral, såsom det gjordes för vattenförsörjningens del vid genomförandet av NIS 1-direktivet. Enligt inrikesministeriet vore en modell med en myndighet bäst där anmälningar om incidenter slutligen alltid sänds (t.ex. till Transport- och kommunikationsverket), som får rätt eller skyldighet att överlämna information om en informationssäkerhetshändelse till myndigheterna för nationell säkerhet. Enligt utrikesministeriet bör den behöriga myndigheten vara antingen Transport- och kommunikationsverket eller Myndigheten för digitalisering och befolkningsdata. Enligt finansministeriet är det ändamålsenligt att koncentrera tillsynen hos en myndighet och inte dela upp den på flera olika myndigheter. Behörig myndighet på statsrådsnivå bör vara en organisation vars kompetens och uppgifter stöder uppfyllandet av skyldigheter som gäller cybersäkerhet.

Såsom det lagts fram i de ovannämnda intervjuerna och svaren har Cybersäkerhetscentret på Transport- och kommunikationsverket de bästa förutsättningarna och kompetensen att vara tillsynsmyndighet för sektorn offentlig förvaltning enligt direktivet. Det föreslås ändå att uppgiften i informationshanteringslagens reglering ges till Transport- och kommunikationsverket, eftersom där ingår sådan utövning av offentlig makt som myndigheten ska ansvara för. På Transport- och kommunikationsverket kan uppgiften dock anvisas personalen på Cybersäkerhetscentret. Trots att Cybersäkerhetscentret redan från tidigare har specialkompetens och sakkunskap som gäller tillsyn av cybersäkerhet kräver den uppgift som föreslås i propositionen också tilläggsresurser till centret. Behovet av tilläggsresurser är då ändå mindre jämfört med om uppgiften anvisas någon annan myndighet.

Det är inte heller ändamålsenligt att dela upp uppgiften på flera myndigheter. Trots att det i intervjuer och svar har konstaterats vara problematiskt att ministerier övervakas av ett ämbetsverk på hierarkiskt sett lägre nivå har det i beredningen bedömts att detta inte utgör hinder för utförandet av tillsynen på det sätt som föreslås i propositionen. Med beaktande av tillsynens karaktär och syfte enligt direktivet är en centralisering av tillsynsuppgiften hos Transport- och kommunikationsverket även för ministeriernas del det mest ändamålsenliga. Ämbetsverket har den bästa sakkunskapen och skickligheten att klara uppgiften, vilket ska anses som en mer vägande grund än det att tillsynen på grund av strukturella skäl i förvaltningen för ministeriernas del delas upp på någon aktör på statsrådsnivå. En sådan uppdelning ökar kostnaderna vilket dessutom äventyrar tillsynens kvalitet och att den genomförs enhetligt.

5.1.5 Påföljdsavgift

I propositionen föreslås det att en påföljdsavgift för verksamhet som strider mot skyldigheterna i NIS 2-direktivet påförs av en påföljdsavgiftsnämnd som finns i samband med Transport- och kommunikationsverket och som består av medlemmar som utses av tillsynsmyndigheterna.

Grundlagsutskottet har när det gäller de höga påföljdsavgifterna riktat uppmärksamhet mot rättskyddsrelaterade aspekter. Grundlagsutskottet har funnit det problematiskt att en enskild tjänsteman självständigt kan förordna en väldigt hög administrativ påföljdsavgift. I enlighet med grundlagsutskottet ståndpunkt borde det med anledning av de rättsskyddsrelaterade orsaker som omfattas av 21 § i grundlagen utfärdas bestämmelser om att ett kollegialt organ har till uppgift att besluta om avsevärt stora administrativa påföljdsavgifter (GrUU 14/2018 rd, s. 19). Artikel 34 i NIS 2-direktivet förutsätter att medlemsstaterna fastställer miniminivån på det högsta beloppet för administrativa sanktionsavgifter för väsentliga aktörer till 10 000 000 EUR eller 2 % av aktörens globala årsomsättning och för andra än väsentliga aktörer till 7 000 000 EUR eller 1,4 % av den totala globala årsomsättningen beroende på vilken siffra som är högst. Eftersom man för överträdelser eller försummelser av NIS 2-direktivet bör kunna påföra också höga påföljdsavgifter är det på grund av de synpunkter som gäller rättsskyddet enligt grundlagen inte motiverat att någon annan än ett organ med flera medlemmar får uppgiften att påföra administrativa påföljdsavgifter. Om varje tillsynsmyndighet påför administrativa påföljdsavgifter på sina egna sektorer kräver det en reglering om beslutsförfarandet som avviker från konventionellt förvaltningsbeslut, såsom kollegialt beslutsfattande.

Vad gäller behörigheten att påföra påföljdsavgift har som alternativ bedömts vara att avgiften påförs av domstol, att behörigheten att påföra påföljdsavgift centraliseras hos Transport- och kommunikationsverket eller av en påföljdsavgiftsnämnd som består av tillsynsmyndigheter. Något existerande kollegialt organ till vars uppgifter behörigheten att påföra påföljdsavgift lämpar sig naturligt har inte konstaterats, och därför har man stannat för de beskrivna alternativen.

Det är exceptionellt att en domstol som första instans påför en administrativ påföljdsavgift. Också grundlagsutskottet har förhållit sig reserverat till att uppgifter som gäller påförande av administrativa påföljdsavgifter ges till domstolar (GrUU 12/2019 rd). Eftersom ändringssökandet sker i ett steg kan det inte anses motiverat att anvisa behörigheten till förvaltningsdomstolarna. Skillnaden mellan en påföljdsavgiftsnämnd och centralisering av behörigheten som central processuell skillnad är, att en påföljdsavgiftsnämnd består av medlemmar som utses av varje tillsynsmyndighet, medan i en centraliserad modell endast Transport- och kommunikationsverket eller tjänstemän i den tillsynsmyndighet som föreslår att påföljdsavgift påförs deltar i beslutsfattandet om påföljdsavgifter. I den föreslagna modellen för tillsyn, där tillsynen över aktörerna sektorsspecifikt delas upp på olika tillsynsmyndigheter enligt en modell som utgör en fortsättning på genomförandet av NIS 1-direktivet, är nyttan med en påföljdsavgiftsnämnd i

förhållande till centralisering av behörigheten att sektorsspecifik sakkunskap utnyttjas och att en representant för varje tillsynsmyndighet deltar när påföljdsavgifter påförs, vilket leder till hög sektorsspecifik sakkunskap och att påföljdspraxis är förutsebar och enhetlig mellan olika aktörer. Att centralisera behörigheten i fråga om påföljder hos en tillsynsmyndighet är inte konsekvent när tillsynen annars är sektorsspecifikt uppdelad. En fördel med centralisering av behörigheten i fråga om påföljder i relation till en påföljdsavgiftsnämnd är den administrativt sett lättare strukturen. Organiserandet av verksamheten hos en påföljdsavgiftsnämnd medför dock inte några väsentligt högre administrativa kostnader, för den inrättas i samband med en existerande myndighet, det vill säga Transport- och kommunikationsverket och sammanträder endast vid behov. Det räknas med att behovet av att påföra påföljdsavgifter sker sällan, för tillsynsmyndigheten har flera befogenheter att styra aktörerna och förplikta dem att korrigera lagstridig verksamhet. Därför bedöms anvisandet av behörigheten att påföra påföljdsavgifter till en påföljdsavgiftsnämnd av de föreliggande alternativen vara det mest motiverade, när tillsynen har ordnats sektorsspecifikt och varje tillsynsmyndighet finns representerad i nämnden.

5.2 Metoder som planerats eller genomförts av andra medlemsstater

5.2.1 Sverige

Sveriges reglering om nationell nät- och informationssäkerhet ingår i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster 2018:1174 som grundar sig på skyldigheter i NIS 1-direktivet. Med stöd av lagen har dessutom en kompletterande förordning (2018:1175) utfärdats.

Utifrån NIS 2-direktivet bereds i Sverige en offentlig statlig utredning om nationellt sett viktiga frågor (statens offentliga utredningar) med syftet att utgöra ett beredningsunderlag innan ett lagförslag utarbetas. Utredningen avses bli klar senast den 23 februari 2024. Utgångspunkterna för statens offentliga utredning fastställs i en verkställighetspromemoria publicerad den 2 mars 2023 (Kommittédirektiv: Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft, nedan *verkställighetspromemorian*).

Enligt verkställighetspromemorian är utgångspunkten för regleringen i fråga om tillsyn över skyldigheter att fortsätta med de myndighetsenheter som anvisats utifrån NIS 1-direktivet. Tillsynen över skyldigheter som gäller informationssäkerhet har i Sverige decentraliserats på myndigheter för olika sektorer (Statens energimyndighet [energi], Transportstyrelsen [trafik], Finansinspektionen [banksektorn och finansmarknadens infrastruktur], Inspektionen för vård och omsorg [hälso- och sjukvård], Livsmedelsverket [leverans och distribution av vatten] samt Post- och telestyrelsen [digital infrastruktur och leverantörer av digitala tjänster]). Tillsynsmyndigheter ska inriktas på nya sektorer som i och med NIS 2-direktivet kommer att omfattas av nät- och informationssäkerheten.

Den nationella myndigheten MSB (Myndigheten För Samhällsskydd och Beredskap) som ansvarar för försörjningsberedskap har ansvarat för koordinering av tillsynen och har varit centraliserad kontaktpunkt för nät- och informationssäkerheten, representerat Sverige i en arbetsgrupp mellan medlemsstaterna och varit CSIRT-enhet. Enligt verkställighetspromemorian vill man att motsvarande uppgifter fortsättningsvis ligger på MSB :s ansvar när NIS 2-direktivet genomförs, och det anses ändamålsenligt att MSB företräder Sverige i Europas nätverk för de kontaktorganisationer som sköter cyberkriser.

Sveriges nationella strategi för informations- och cybersäkerhet (Nationell strategi för samhällets informations- och cybersäkerhet 2016/17:213) blev klar 2016. Syftet med strategin är att bidra till att skapa långsiktiga förutsättningar för aktörerna att förbättra sin informations- och cybersäkerhet samt att höja medvetenheten och kunskapen om informations- och cybersäkerhet i hela samhället. Strategin har uppdaterats 2018 genom en komplettering i form av en bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet.

5.2.2 Estland

I Estland genomfördes NIS 1-direktivet nationellt genom en allmän lag om cybersäkerhet (Küber-turvalisuse seadus). För beredningen av det nationella genomförandet av NIS 2-direktivet ansvarar ekonomi- och kommunikationsministeriet (Majandus- ja Kommunikatsiooniministeerium) med syftet att göra de ändringar i den nationella allmänna lagen om cybersäkerhet som det nya direktivet kräver. Estlands nationella lag om cybersäkerhet har ändrats 2022 genom lag om ändring av cybersäkerhetslagen och andra lagar (Küberturvalisuse seaduse ja teiste seaduste muutmiseseadus). Bakgrunden till ändringsprojektet är ett behov av att se över den nationella lagstiftningen utifrån EU-lagstiftningen, och dess centrala mål var stärka den offentliga sektorns standard för informationssäkerhet och utvidga standarden till att gälla alla nät- och informationssäkerhetssystem genom att ersätta ISKE (Infosüsteemide turvameetmete süsteem) med en ny EITS-standard (Eesti infoturbestandard).

Det huvudsakliga syftet med det andra ändringsprojektet för den allmänna lagen om cybersäkerhet är att delvis göra skyldigheterna i NIS 2-direktivet till en del av den nationella lagstiftningen.

Tillsyns- och samarbetsskyldigheterna enligt NIS 1-direktivet har ordnats centralt. Estlands ämbetsverk för informationssystem (Riigi Infosüsteemi Amet) har varit nationell kontaktpunkt, behörig myndighet och CSIRT-enhet. Den senaste nationella strategin som gäller cybersäkerhet (Küberturvalisuse strateegia) som publicerats i Estland gäller 2019–2020. Strategin fastställer nationellt de centrala mål för cybersäkerhet genom vilka Estlands cybersäkerhet kan utvecklas.

5.2.3 Danmark

I Danmark har skyldigheterna i NIS 1-direktivet genomförts genom lagen Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester, nedan NIS 1-lagen. Lagen ställer krav på informations- och nätsäkerhet på centrala tjänsteleverantörer och föreskriver om tillsyn över aktörer. Centraliserad kontaktpunkt och CSIRT-aktör i Danmark enligt NIS 1-lagen är Center for Cybersikkerhed, och myndighetstillsynen är koncentrerad till näringsverket (Erhvervsstyrelse). Aktörerna ska med stöd av skyldigheterna i lagen rapportera om kränkning av cybersäkerhet till Center for Cybersikkerhed och till näringsverket.

Danmarks National strategi for cyber- og informationssikkerhed 2022–2024 har publicerats i december 2021.

Danmarks försvarsministerium ansvarar för genomförandet av NIS 2-direktivet.

5.2.4 Tyskland

NIS 1-direktivet har genomförts nationellt genom en lag om genomförande av nät- och informationssäkerhetsdirektivet (Gesetz zur Umsetzung der NIS-Richtlinie). Utifrån skyldigheterna i

direktivet utvidgades BSI:s (Bundesamt für Sicherheit in der Informationstechnik) befogenheter för tillsyn och genomförande. BSI har fungerat som centraliserad kontaktpunkt och nationell CSIRT-enhet i Tyskland enligt NIS 1-direktivet. Även myndighetstillsynen har ordnats centraliserat. BSI är övervakande myndighet enligt NIS 1-direktivet. Genomförandet av NIS 1-direktivet krävde inte stora ändringar i den nationella regleringen, för den lag om informationssäkerhet som var i kraft från och med 2015 (IT-Sicherheitsgesetz) har krävt åtgärder för riskhantering och rapportering för förbättring av cybersäkerheten hos aktörerna inom kritisk infrastruktur (KRITIS).

I Tyskland planerar man att genomföra NIS 2-direktivet genom en informationssäkerhetslag 3.0 (IT-Sicherheitsgesetz 3.0). Avsikten med den nya lagen är att bearbeta den tidigare versionen av informationssäkerhetslagen (IT-Sicherheitsgesetz 2.0) som trädde i kraft 2021. Den grundar sig på KRITIS-aktörer som finns inom en sektor som definierats som kritisk. Aktörerna omfattas av regleringen när de tröskelvärden som lagen fastställer uppfylls. Tröskelvärdet är i regel 500 000 personer som omfattas av en tjänst som ska erbjudas. Gränsvärdena inom NIS 2-regleringen avviker från Tysklands reglering, för NIS 2 kräver 50 anställda och en omsättning på 10 000 000 euro. Eftersom tillämpningsområdet för den nationellt gällande regleringen avviker från tillämpningsområdet enligt NIS 2-direktivet måste det i samband med det nationella genomförandet av direktivet beslutas om hur tillämpningsområdet ska fastställas i fortsättningen.

NIS 2 går i sina skyldigheter längre än Tysklands nuvarande nationella reglering i fråga om skyddsåtgärder, rapporteringsskyldigheter, tillsynsåtgärder, administrativa påföljder och registreringsskyldigheter. Även internt informationsutbyte och samarbete mellan medlemsländer i EU kommer att öka i och med de nya NIS 2-skyldigheterna.

5.2.5 Frankrike

I Frankrike har NIS 1-direktivet genomförts som en del av en lag genom vilken man strävade efter att förenhetliga den nationella säkerhetsregleringen med Europeiska unionens reglering (LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le do-maine de la sécurité). I Frankrike är ANSSI (Agence nationale de la sécurité des systèmes d'information) centraliserad nationell kontaktpunkt, och lägescentral för informationssäkerhet är CERT-FR, som är placerad i samband med ANSSI, är CSIRT-enhet enligt NIS 1-direktivet.

Skyldigheter som gäller informationssäkerhet ingår nationellt i reglering som gäller kritisk infrastruktur genom en lagreform (CIIP, loi n° 2013–1168 du 18 décembre 2013). Syftet med lagen är att reglera skyldigheter i fråga om riskhantering och rapportering som gäller informationssäkerhet för nationella aktörer. Den rapportering som lagen kräver ska sändas till Frankrikes nationella cybersäkerhetsmyndighet ANSSI.

En strategi för digital säkerhet (Stratégie nationale pour la sécurité du numérique) har publicerats 2015, och syftet med den är att främja informationssystemens stabilitet, ekonomiska utveckling och medborgarnas tilltro till informationssystem.

6 Remissvar

[Kompletteras senare.]

7 Specialmotivering

7.1 Lagen om hantering av cybersäkerhetsrisker

1 §. *Tillämpningsområde*. Genom lagen genomförs NIS 2-direktivet. På det sätt som direktivets tillämpningsområde förutsätter föreskrivs det om vissa för samhället kritiska aktörers riskhanterings- och rapporteringsskyldigheter i fråga om cybersäkerheten samt om tillsynen över att skyldigheterna iakttas. De aktörer som omfattas av lagens tillämpningsområde definieras i 3 §.

För att genomföra NIS 2-direktivet föreskrivs det i lagen dessutom om den enhet för hantering av it-säkerhetsincidenter som avses i artikel 10 i NIS 2-direktivet, dvs. CSIRT-enheten (Computer Security Incident Response Team), dess uppgifter och de krav som ställs på dess verksamhet samt om vissa andra omständigheter i anslutning till myndighetssamarbetet för hantering av cybersäkerhetsincidenter och cyberrisker.

2 §. *Definitioner.* I paragrafen föreskrivs det om de definitioner som används i lagen. Definitionerna motsvarar i huvudsak definitionerna i NIS 2-direktivet.

I *1 punkten* definieras registreringsenhet för toppdomäner på motsvarande sätt som i artikel 6.21 i NIS 2-direktivet. Med registreringsenhet för toppdomäner eller TLD-registreringsenhet avses en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

Enligt *2 punkten* avses med CER-direktivet Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

I *3 punkten* definieras datacentraltjänst. Definitionen motsvarar till sitt innehåll artikel 6.31 i NIS 2-direktivet. Med datacentraltjänst avses 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. I skäl 35 i NIS 2-direktivet kompletteras definitionen i artikel 6.31. Enligt skälet omfattar begreppet sådana leverantörer av datacentraltjänster som inte ingår i en molninfrastruktur.

I *4 punkten* definieras leverantör av DNS-tjänster. Definitionen motsvarar till sitt innehåll artikel 6.20 i NIS 2-direktivet. Med leverantör av DNS-tjänster avses 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.

Enligt 5 *punkten* avses med DORA-förordningen 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.

Enligt *6 punkten* avses med eIDAS-förordningen 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.

I *7 punkten* definieras sårbarhet. Definitionen motsvarar till sitt innehåll artikel 6.15 i NIS 2-direktivet. Med sårbarhet avses en svaghet, känslighet eller brist hos en IKT-produkt enligt definitionen i artikel 2.12 i cybersäkerhetsförordningen (EU) 2019/881 eller en IKT-tjänst enligt definitionen i artikel 2.13 i cybersäkerhetsförordningen som kan utnyttjas genom ett cyberhot.

I *8 punkten* definieras leverantör av hanterade tjänster. Definitionen motsvarar till sitt innehåll artikel 6.39 i NIS 2-direktivet. Med leverantör av hanterade tjänster avses en aktör som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av 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.

I *9 punkten* definieras kvalificerad tillhandahållare av betrodda tjänster. Med kvalificerad tillhandahållare av betrodda tjänster avses en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i eIDAS-förordningen, dvs. en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

I *10 punkten* definieras medelstor aktör. En medelstor aktör kan vara antingen en offentlig eller en privat organisation som uppfyller villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG. Definitionen följer definitionen av medelstort företag i kommissionens rekommendation 2003/361/EG, men dock så att artikel 3.4 i bilagan till rekommendationen, dvs. begränsningarna av ägande- eller rösträtten för offentliga organ, inte tillämpas i detta sammanhang. Huruvida definitionen av medelstor aktör uppfylls eller överskrids ska bedömas i förhållande till trösklarna i kommissionens rekommendation och tolkningen av dem.

I kommissionens rekommendation 2003/361/EG fastställs den maximala storleken på mikroföretag, små företag och medelstora företag. En aktör uppfyller definitionen av medelstort företag när den överskrider ramvillkoren för definitionen av ett litet företag, men inte de övre gränserna för små och medelstora företag. En aktör uppfyller alltså definitionen av medelstor aktör om den har minst 50 anställda eller om dess årsomsättning och balansräkning överstiger 10 miljoner euro. Om en aktör har färre än 50 anställda, men både omsättningen och balansräkningen överstiger 10 miljoner, uppfylls definitionen av medelstor aktör. Om en aktör har färre än 50 anställda och antingen omsättningen eller balansräkningen, men inte båda, överskrider 10 miljoner euro, uppfylls inte definitionen av medelstor aktör. En aktör överskrider definitionen av medelstor aktör när den överskrider de trösklar för små och medelstora företag som anges i kommissionens rekommendation.

Om en aktör är verksam inom flera olika branscher och endast en del av verksamheten är sådan verksamhet som avses i bilaga I eller II, bedöms aktörens storlek utifrån dess totala verksamhet. Följaktligen ska omsättningen, balansräkningen och antalet anställda bedömas för hela aktören,

och bedömningen ska inte begränsas till omfattningen av den verksamhet som avses i bilaga I eller II. Bedömningen görs separat för varje aktör.

I *11 punkten* föreskrivs det på motsvarande sätt som i artikel 6.3 i NIS 2-direktivet om begreppet cybersäkerhet. Med cybersäkerhet avses cybersäkerhet enligt definitionen i artikel 2.1 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 (nedan *cybersäkerhetsakten*). Med cybersäkerhet avses således åtgärder som behövs för att skydda kommunikationsnät och informationssystem, användare av dessa nät och system och andra berörda personer mot cyberhot. Definitionen begränsar inte dessa åtgärders form eller art, utan det kan vara fråga om såväl tekniska som andra skyddsåtgärder oberoende av deras form och art. Vid sidan av användare av kommunikationsnät och informationssystem inbegriper definitionen till exempel personer som har anknytning till eller äger information som behandlas i kommunikationsnätet eller informationssystemet.

I *12 punkten* definieras på motsvarande sätt som i artikel 6.10 i NIS 2-direktivet begreppet cyberhot. Med cyberhot avses cyberhot enligt definitionen i artikel 2.8 i cybersäkerhetsakten. Med cyberhot avses en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka kommunikationsnät och informationssystem, användare av dessa nät och system och andra personer.

I *13 punkten* definieras tillhandahållare av betrodda tjänster. Med tillhandahållare av betrodda tjänster avses tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i eIDAS-förordningen. Enligt den definitionen avses med tillhandahållare av betrodda tjänster en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerad eller icke kvalificerad tillhandahållare av betrodda tjänster. Med betrodd tjänst avses enligt artikel 3.16 i eIDAS-förordningen en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av antingen skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

I *14 punkten* definieras tillbud. Definitionen motsvarar till sitt innehåll artikel 6.5 i NIS 2-direktivet. Med tillbud avses en händelse som kunde ha undergrävt 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, men som framgångsrikt hindrades från att utvecklas eller som av någon slumpmässig orsak inte uppstod.

I *15 punkten* definieras molntjänst på motsvarande sätt som i artikel 6.30 och skäl 33 i NIS 2-direktivet. Med molntjänst avses en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser. Definitionen av molntjänst i NIS 2-direktivet preciseras i direktivets skäl 33. Definitionen av molntjänst ska tolkas i enlighet med definitionen av molntjänst i NIS 2-direktivet. Beräkningstjänster kan därmed betyda t.ex. nätverk, servrar eller annan datateknisk infrastruktur, operativsystem, programvara, lagringsutrymme, applikationer och tjänster. Med beställtjänster avses att molnanvändaren har kapacitet att ensidigt, självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster. Med bred fjärråtkomst avses att

resurserna tillhandahålls över nätet och nås genom mekanismer som främjar användning av olika klientplattformar. Skalbarhet avser beräkningsresurser som leverantören av molntjänster kan fördela på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Med elastisk pool avses beräkningsresurser som tillhandahålls och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen delbar används för att beskriva beräkningsresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen distribuerad används för att beskriva beräkningsresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning. Tjänste- och distribueringsmodeller för molntjänster har liksom i skäl 33 i NIS 2-direktivet samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014.

I *16 punkten* definieras incident. Definitionen motsvarar till sitt innehåll artikel 6.6 i NIS 2-direktivet. Med incident avses 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.

I *17 punkten* definieras incidenthantering. Definitionen motsvarar till sitt innehåll artikel 6.8 i NIS 2-direktivet. Med incidenthantering avses alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

I *18 punkten* definieras risk. Med risk avses i lagen i likhet med definitionen i artikel 6.9 i NIS 2-direktivet dels sannolikheten för en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos uppgifter som lagras, överförs eller behandlas i eller hos tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem, dels arten av den störning som en sådan händelse orsakar. Vid bedömningen av hur allvarlig risken är ska hänsyn tas till sannolikheten för att risken realiseras samt omfattningen och betydelsen av den störning eller förlust som orsakas av att risken realiseras. Betydelsen av den förlust risken kan leda till ska bedömas i förhållande till samma omständigheter som är av betydelse med tanke på en betydande incident eller tröskeln för en incidentanmälan och konsekvenserna för dessa omständigheter. Sådana omständigheter är störningar i tjänsternas funktion, den berörda aktörens ekonomiska förluster samt materiell eller immateriell skada som påverkar andra fysiska eller juridiska personer. Till dessa omständigheter ska också räknas mängden och arten av de uppgifter som behandlas i kommunikationsnätet eller informationssystemet samt de negativa konsekvenser som en realisering av risken har för uppgifternas konfidentialitet och skyddet av personuppgifter.

I *19 punkten* definieras nätverk för leverans av innehåll. Definitionen motsvarar till sitt innehåll artikel 6.32 i NIS 2-direktivet. Med nätverk för leverans av innehåll avses 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.

Enligt *20 punkten* avses med teledirektivet Europaparlamentets och rådets direktiv (EU) 2018/1972 om en europeisk kodex för elektronisk kommunikation.

I *21 punkten* definieras på motsvarande sätt som i artikel 6.40 i NIS 2-direktivet leverantör av hanterade säkerhetstjänster. Med leverantör av hanterade säkerhetstjänster avses en i 8 punkten

avsedd leverantör av hanterade tjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

I *22 punkten* definieras IKT-tjänst. Definitionen av IKT-tjänst motsvarar innehållsmässigt definitionen av informations- och kommunikationsteknisk tjänst i artikel 2.13 i cybersäkerhetsakten (EU) 2019/881. Med IKT-tjänst avses en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via kommunikationsnät och informationssystem.

I *23 punkten* definieras IKT-produkt. Definitionen av IKT-produkt motsvarar innehållsmässigt definitionen av informations- och kommunikationsteknisk produkt i artikel 2.12 i cybersäkerhetsakten (EU) 2019/881. Med IKT-produkt avses en del, eller en grupp av delar, i kommunikationsnät och informationssystem.

I *24 punkten* definieras tillsynsmyndighet. Med tillsynsmyndighet avses inom varje verksamhetsområde en med stöd av 26 § i den föreslagna lagen behörig tillsynsmyndighet som har till uppgift att inom ansvarsområdet ordna tillsynen över efterlevnaden av den föreslagna lagen, de föreskrifter som meddelas med stöd av den och de författningar som utfärdats med stöd av NIS 2-direktivet. Med tillsynsmyndighet avses den behöriga myndigheten enligt artikel 8.1 i NIS 2-direktivet.

I *25 punkten* definieras på motsvarande sätt som i artikel 6.33 i NIS 2-direktivet plattform för sociala nätverkstjänster. Med plattform för sociala nätverkstjänster avses en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

I *26 punkten* definieras sökmotor. Definitionen motsvarar till sitt innehåll artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster. Med sökmotor avses en digital tjänst som gör det möjligt för användare att mata in sökfraser för att göra sökningar på i princip alla webbplatser eller alla webbplatser på ett visst språk på grundval av en fråga om vilket ämne som helst i form av ett nyckelord, en röstbegäran, en fras eller någon annan inmatning och som returnerar resultat i vilket format som helst som innehåller information om det begärda innehållet. Definitionen motsvarar definitionen i artikel 6.29 i NIS 2-direktivet. Med en sådan leverantör av sökmotorer som avses i bilaga till lagen avses en aktör som tillhandahåller tjänster enligt definitionen.

I *27 punkten* definieras internetbaserad marknadsplats. Med internetbaserad marknadsplats avses i likhet med definitionen i 6 kap. 8 § 4 punkten i konsumentskyddslagen (38/1978) en tjänst som erbjuder konsumenten möjlighet att ingå distansavtal med andra näringsidkare än den som tillhandahåller marknadsplatsen eller med privatpersoner och som utnyttjar den webbplats, applikation eller annat program eller en del av det som används av den som tillhandahåller marknadsplatsen eller på dennes vägnar. Definitionen motsvarar definitionen i artikel 6.28 i NIS 2-direktivet. Med en sådan tillhandahållare av internetbaserad marknadsplatser som avses i bilaga till lagen avses en aktör som tillhandahåller tjänster enligt definitionen.

I 28 *punkten* definieras kommunikationsnät och informationssystem. Definitionen motsvarar till sitt innehåll artikel 6.1 i NIS 2-direktivet. I stället för begreppet ”nätverks- och informationssystem” som används i översättningarna av NIS 1- och NIS 2-direktiven används i den nationella

lagen ”kommunikationsnät och informationssystem”, som är vedertaget i den nationella genomförandelagstiftningen för NIS 1-direktivet och i lagen om tjänster inom elektronisk kommunikation. I lagen föreskrivs det om begreppet kommunikationsnät och informationssystem på samma sätt som det i NIS 2-direktivet föreskrivs om nätverks- och informationssystem.

Med kommunikationsnät och informationssystem avses ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972 (teledirektivet), 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 eller digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av ovannämnda system för att de ska kunna drivas, användas, skyddas och underhållas. Begreppet kommunikationsnät och informationssystem ska tolkas på samma sätt som definitionen av nätverks- och informationssystem i NIS 2-direktivet.

I *29 punkten* definieras på motsvarande sätt som i artikel 6.2 i NIS 2-direktivet säkerhet i kommunikationsnät och informationssystem. Med säkerhet i kommunikationsnät och informationssystem avses kommunikationsnät och informationssystems förmåga att motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos uppgifter i dessa kommunikationsnät och informationssystem och att uppgifterna och tjänsterna kan utnyttjas av dem som har rätt att använda dem. Definitionen omfattar således informationssäkerhetens element, det vill säga att informationen i ett informationssäkert system är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen.

Enligt *30 punkten* avses med den allmänna dataskyddsförordningen Europaparlamentets och rådets förordning (EU) nr 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).

I *31 punkten* definieras tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster. Med tillhandahållare avses här den som tillhandahåller sådana kommunikationstjänster som avses i 3 § 1 mom. 37 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014). Enligt 3 § 1 mom. 37 punkten i den lagen avses med kommunikationstjänst en tjänst som helt eller huvudsakligen utgörs av överföring av meddelanden i kommunikationsnät samt överförings- och sändningstjänster i masskommunikationsnät och interpersonella kommunikationstjänster.

I *32 punkten* definieras tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät. Med tillhandahållare avses här den som tillhandahåller sådana kommunikationsnät som avses i 3 § 1 mom. 34 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014). Enligt 3 § 1 mom. 34 punkten i den lagen avses med nättjänst en tjänst som tillhandahålls av ett teleföretag (nätföretag) för att ett kommunikationsnät som det äger eller på någon annan grund förfogar över ska kunna användas för överföring och distribution av meddelanden.

3 §. *Aktörer*. I paragrafen föreskrivs det om de aktörer som omfattas av lagens tillämpningsområde. Definitionen av aktör är tvådelad och utgår dels från arten eller typen av aktörens verksamhet, dels från aktörens storlek. Dessutom kan lagens tillämpningsområde i vissa undantagsfall omfatta aktörer oavsett storlek, och till exempel kritiska aktörer som definierats med stöd av CER-direktivet omfattas alltid av lagens tillämpningsområde. Lagens tillämpningsområde och begreppet aktör avses motsvara artiklarna 2.1–2.4, 3.1 och 3.2 i NIS 2-direktivet så att det

omfattar alla väsentliga och viktiga aktörer som omfattas av NIS 2-direktivets minimitillämpningsområde.

I det föreslagna *1 mom.* föreskrivs det vilka aktörer som avses i lagen och således omfattas av lagens tillämpningsområde, om de överskrider de allmänna villkoren gällande storlek. Med aktör avses fysiska eller juridiska personer som bedriver sådan verksamhet som avses i bilaga I och II till lagen eller som är sådan typ av aktör som avses i dem och som uppfyller eller överskrider definitionen av medelstor aktör. Medelstor aktör definieras i 2 § 15 punkten. Med medelstor aktör avses en offentlig eller privat aktör som uppfyller villkoren för medelstora företag i artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG och som tillhandahåller tjänster eller bedriver verksamhet i unionen. Artikel 3.4 i bilagan till rekommendationen ska inte tillämpas vid definitionen av medelstor aktör. Definitionen av aktör påverkas inte av enhetens eller organisationens juridiska form, utan endast av huruvida aktören bedriver sådan verksamhet som avses i bilaga I eller II och uppfyller storlekskraven för aktörstypen.

Den föreslagna lagen tillämpas således i princip endast på medelstora och större aktörer. I det föreslagna 2 mom. föreskrivs det dock om vissa undantag från storleksavgränsningen, det vill säga om situationer där aktören är en aktör som avses i lagen oavsett dess storlek. Tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner och leverantörer av DNS-tjänster är oavsett storlek sådana aktörer som avses i lagen. Dessutom ska de aktörer som har identifierats som en kritisk aktör enligt CER-direktivet utgöra aktörer som avses i den föreslagna lagen oavsett storlek.

I *punkterna 1–4* i bilaga I definieras de aktörer inom transportsektorn som omfattas av lagens tillämpningsområde. När det gäller lufttransport föreslås tillämpningsområdet omfatta kommersiella lufttrafikföretag, vissa flygplatsoperatörer och leverantörer av flygkontrolltjänster. I fråga om spårtrafik föreslås tillämpningsområdet omfatta bannätsförvaltare och bolag som tillhandahåller trafikledningstjänster, järnvägsföretag samt tjänsteleverantörer. När det gäller sjöfart föreslås tillämpningsområdet omfatta transportföretag som bedriver

persontrafik och godstrafik, hamninnehavare och aktörer som sköter anläggningar och utrustning i hamnar samt VTS-tjänsteleverantörer. Aktörer som sköter anläggningar och utrustning i hamnar kan vara ovan nämnda hamninnehavare eller andra aktörer som hamninnehavaren, dvs. den som sköter hamnen, enligt avtal har bemyndigat att verka på området och tillhandahålla tjänster. Tidigare ägde hamnbolagen, dvs. hamninnehavarna, lager och andra konstruktioner samt olika lasthanteringsanordningar i hamnområdet. Numera är det vanligt att hamninnehavaren endast förvaltar området, medan en eller flera andra aktörer avtalsbaserat svarar för en del av eller alla funktioner som anknyter till tillhandahållande av hamntjänster. Sådana hamntjänster kan vara till exempel förtöjnings- och lösgöringstjänster för fartyg, bogsertjänster, lasthantering, leverans av anordningar och personal för lasthantering, skötsel av åtgärder i anslutning till hantering av lastdata, bevakningstjänster i hamnen samt tjänster i anslutning till passerkontroll och passerkort, om tjänsterna är av betydelse för hamnverksamheten. I fråga om vägtransport föreslås tillämpningsområdet omfatta vägmyndigheter med ansvar för trafikstyrning, med vissa undantag, samt de som tillhandahåller intelligenta transportsystem. Tillämpningsområdet i fråga om transportsektorn motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 2 i bilaga I till NIS 2-direktivet.

I *punkt 5* i bilaga I definieras de aktörer inom rymdsektorn som omfattas av lagens tillämpningsområde. Tillämpningsområdet för NIS 2-direktivet föreslås i enlighet med punkt 11 i bilaga I omfatta 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. Definitionen har ansetts omfatta åtminstone de verksamhetsutövare som avses i 2 § 1 mom. 5 punkten i markstationslagen. Lagens tillämpningsområde föreslås alltså omfatta åtminstone verksamhetsutövare som bedriver eller har för avsikt att bedriva markstations- eller radarverksamhet eller som faktiskt ansvarar för sådan verksamhet. Också andra aktörer inom rymdsektorn än verksamhetsutövare enligt markstationslagen som uppfyller definitionen i punkt 11 i bilaga I till NIS 2-direktivet ska omfattas av lagens tillämpningsområde. Tillämpningsområdet i fråga om rymdsektorn motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 11 i bilaga I till NIS 2-direktivet.

I *punkt 6* i bilaga I definieras de aktörer inom den digitala infrastrukturen som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar leverantörer av internetknutpunkter, leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, tillhandahållare av betrodda tjänster, tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät och leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster. De olika typerna av aktörer definieras närmare i 2 § 1, 3, 4, 13, 15, 19, 31 och 32 punkten. Tillämpningsområdet i fråga om digital infrastruktur motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 8 i bilaga I till NIS 2-direktivet.

I *punkt 7* i bilaga I definieras de aktörer inom förvaltning av IKT-tjänster som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster. De olika typerna av aktörer definieras närmare i 2 § 8 och 21 punkten. Tillämpningsområdet i fråga om förvaltning av IKT-tjänster motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 9 i bilaga I till NIS 2-direktivet.

I *punkterna 8–12* i bilaga I definieras de aktörer inom energisektorn som omfattas av lagens tillämpningsområde. När det gäller elbranschen ska tillämpningsområdet omfatta elleverantörer, distributionsnätsinnehavare , stamnätsinnehavare, elproducenter, elmarknadsoperatörer, tillhandahållare av aggregering, efterfrågeflexibilitet eller energilagring samt laddningsoperatörer. Tillämpningsområdet omfattar dessutom operatörer av fjärrvärme eller fjärrkyla, det vill säga distributörer av fjärrvärme och fjärrkyla. Operatörer av fjärrvärme eller fjärrkyla som inte alls bedriver distribution skulle uteslutas från tillämpningsområdet. I fråga om gassektorn ska lagens tillämpningsområde omfatta naturgasleverantörer, distributionsnätsinnehavare, överföringsnätsinnehavare, innehavare av en lagringsanläggning, innehavare av en behandlingsanläggning för kondenserad naturgas, vissa naturgasföretag samt innehavare av raffinaderier och bearbetningsanläggningar för naturgas. När det gäller oljebranschen omfattar tillämpningsområdet operatörer av oljeledningar, operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja samt centrala lagringsenheter. I fråga om vätgassektorn ska tillämpningsområdet omfatta aktörer som producerar, lagrar och transporterar vätgas. Tillämpningsområdet i fråga om energisektorn motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 1 i bilaga I till NIS 2-direktivet.

I *punkt 13* i bilaga I definieras de aktörer inom hälso- och sjukvårdssektorn som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar vårdgivare, EU-referenslaboratorier, aktörer som bedriver forskning och utveckling avseende läkemedel, aktörer som tillverkar farmaceutiska basprodukter och läkemedel samt aktörer som tillverkar vissa medicintekniska produkter. Tillämpningsområdet i fråga om hälso- och sjukvårdssektorn motsvarar minimitillämpningsområdet enligt punkt 5 i bilaga I till NIS 2-direktivet.

I *punkt 14* i bilaga I definieras de aktörer som i fråga om dricksvatten omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar både leverantörer och distributörer av dricksvatten. Tillämpningsområdet i fråga om dricksvatten motsvarar minimitillämpningsområdet enligt punkt 6 i bilaga I till NIS 2-direktivet.

I *punkt 15* i bilaga I definieras de aktörer som i fråga om spillvatten omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar företag som samlar in, bortskaffar eller behandlar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten. Tillämpningsområdet i fråga om spillvatten motsvarar minimitillämpningsområdet enligt punkt 7 i bilaga I till NIS 2-direktivet.

I *punkt 1* i bilaga II definieras de aktörer som i fråga om post- och budtjänster omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar både tillhandahållare av budtjänster och tillhandahållare av posttjänster. Tillämpningsområdet i fråga om post- och budtjänster motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 1 i bilaga II till NIS 2-direktivet.

I *punkt 2* i bilaga II definieras de aktörer inom digitala tjänster som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar tillhandahållare av en internetbaserad marknadsplats, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster. De olika typerna av aktörer definieras närmare i 2 § 25–27 punkten. Tillämpningsområdet i fråga om digitala leverantörer motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 6 i bilaga II till NIS 2-direktivet.

I *punkt 3* i bilaga II definieras de aktörer som i fråga om tillverkning av motorfordon, släpfordon och påhängsvagnar omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar företag som bedriver tillverkning som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2. Tillämpningsområdet i fråga om tillverkning av motorfordon, släpfordon och påhängsvagnar motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 e i bilaga II till NIS 2-direktivet.

I *punkt 4* i bilaga II definieras de aktörer som omfattas av lagens tillämpningsområde i fråga om tillverkning av andra fordon. Tillämpningsområdet omfattar företag som bedriver tillverkning som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2. Tillämpningsområdet i fråga om tillverkning av andra fordon motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 f i bilaga II till NIS 2-direktivet.

I *punkt 5* i bilaga II definieras de forskningsorganisationer som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar forskningsorganisationer vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte. Lagen tillämpas dock inte på högskolor eller andra utbildningsinstitutioner. Forskningsorganisationer ska anses inbegripa aktörer som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i ”Frascatimanualen 2015: Riktlinjer för insamling och rapportering av uppgifter om forskning och experimentell utveckling” från Organisationen för ekonomiskt samarbete och utveckling, i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållande av en tjänst, eller marknadsföring därav. Forskningsorganisationer som delar och utnyttjar forskningsresultat för kommersiella syften kan spela en viktig roll i värdekedjor, vilket gör säkerheten i deras kommunikationsnät och informationssystem till en viktig del av den övergripande cybersäkerheten på den inre marknaden. Definitionen av forskningsorganisation motsvarar definitionen i artikel 6.41 och skäl 36 i NIS 2-direktivet. Tillämpningsområdet i fråga om forskningsorganisationer motsvarar minimitillämpningsområdet enligt punkt 7 i bilaga II till NIS 2-direktivet.

I *punkt 6* i bilaga II definieras de aktörer inom kemikaliesektorn som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar tillverkning, produktion och distribution av kemikalier. Tillämpningsområdet i fråga om kemikaliesektorn motsvarar minimitillämpningsområdet enligt punkt 3 i bilaga II till NIS 2-direktivet.

I *punkt 7* i bilaga I definieras de aktörer inom livsmedelssektorn som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar livsmedelsföretag som bedriver grossisthandel, industriell produktion eller bearbetning. Företaget behöver inte vara verksamt inom alla nämnda verksamheter, utan det räcker att det bedriver någon av dem. Tillämpningsområdet i fråga om livsmedelssektorn motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 4 i bilaga II till NIS 2-direktivet.

I *punkt 8* i bilaga II definieras de aktörer inom avfallshantering som omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar företag som bedriver avfallshantering. Tillämpningsområdet i fråga om avfallshantering motsvarar minimitillämpningsområdet enligt punkt 2 i bilaga II till NIS 2-direktivet.

I *punkt 9 och 10* i bilaga II definieras de aktörer som omfattas av lagens tillämpningsområde i fråga om tillverkning av medicintekniska produkter. Tillämpningsområdet omfattar tillverkare av medicintekniska produkter som omfattas av tillämpningsområdet för den s.k. MD-förordningen samt tillverkare av medicintekniska produkter för in vitro-diagnostik. Aktörer som tillverkar medicintekniska produkter som anses kritiska vid ett hot mot folkhälsan hör dock på det sätt som beskrivs ovan till de aktörer inom hälsosektorn som avses i punkt 13 i bilaga I. Tillämpningsområdet i fråga om tillverkning av medicintekniska produkter motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 a i bilaga II till NIS 2-direktivet.

I *punkt 11* i bilaga II definieras de aktörer som i fråga om tillverkning av datorer, elektronikvaror och optik omfattas av lagens tillämpningsområde. Tillämpningsområdet omfattar företag som bedriver tillverkning som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2. Tillämpningsområdet i fråga om tillverkning av datorer, elektronikvaror och optik motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 b i bilaga II till NIS 2-direktivet.

I *punkt 12* i bilaga II definieras de aktörer som omfattas av lagens tillämpningsområde i fråga om tillverkning av elapparatur. Tillämpningsområdet omfattar företag som bedriver tillverkning som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2. Tillämpningsområdet i fråga om tillverkning av elapparatur motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 c i bilaga II till NIS 2-direktivet.

I *punkt 13* i bilaga II definieras de aktörer som omfattas av lagens tillämpningsområde i fråga om tillverkning av övriga maskiner. Tillämpningsområdet omfattar företag som bedriver tillverkning som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2. Tillämpningsområdet i fråga om tillverkning av övriga maskiner motsvarar innehållsmässigt minimitillämpningsområdet enligt punkt 5 d i bilaga II till NIS 2-direktivet.

Genom förslaget genomförs artiklarna 2.1–2.4, 3.1, 3.2 och 6.38 i NIS 2-direktivet, med undantag av artikel 2.2 b–e.

I *2 mom.* föreskrivs det att lagen tillämpas på en aktör som avses i bilaga I eller II oberoende av dess storlek, det vill säga när aktören inte överskrider tröskeln för en medelstor aktör.

Enligt artikel 2.2 b–e i NIS 2-direktivet ska tillämpningsområdet oavsett storlek omfatta aktörer inom de branscher som avses i bilaga I och II i de situationer som avses i artikel 2.2 b–e.

Med stöd av det föreslagna 2 mom. ska bestämmelser om tillämpningen av lagen på sådana aktörer utfärdas genom förordning av statsrådet. En överföring av lagstiftningsbehörigheten är lagtekniskt nödvändig, eftersom det är fråga om en mycket detaljerad definition av aktörer som på grund av verksamhetens särskilda art undantagsvis hör till tillämpningsområdet för skyldigheterna enligt lagen och NIS 2-direktivet oavsett storlek. Med hänsyn till arten av de kriterier som avses i artikel 2.2 b–e i NIS 2-direktivet, skulle tillämpningsområdet för dessa aktörer i fortsättningen också vara känsligt för förändringar, om aktörernas verksamhetskvalitet eller storlek förändras eller aktörer som är kritiska för vissa sektorer byts ut.

Genom det föreslagna bemyndigandet att utfärda förordning överförs rätten att föreskriva att lagen oberoende av storlek ska tillämpas på aktörer som bedriver verksamhet enligt bilagorna I eller II och på vilka lagen inte annars ska tillämpas, eftersom de inte uppfyller definitionen av medelstor aktör enligt 1 mom. En ytterligare förutsättning är att det för aktörens del är fråga om någon av de situationer som avses i 1–4 punkten. De föreslagna 1–4 punkterna motsvarar artikel 2.2 b–e i NIS 2-direktivet och förteckningen är uttömmande. Genom förordning kan det inte föreskrivas att lagen ska tillämpas på andra grunder än de som avses i 1–4 punkten eller på andra aktörer än sådana som bedriver verksamhet enligt bilaga I eller II. Om en aktör omfattas av lagens tillämpningsområde med stöd av en förordning, ska det samtidigt genom förordning bestämmas om aktören ska betraktas som en sådan väsentlig aktör som avses i 27 §.

Det föreslagna 2 mom. gäller andra aktörer än de som oavsett storlek omfattas av lagens tillämpningsområde med stöd av 1 mom. 2 eller 3 punkten.

Genom förslaget genomförs NIS 2-direktivets artikel 2.2 b–e om tillämpningsområde.

4 §. *Avgränsning av tillämpningsområdet.* I paragrafen föreskrivs det om vissa undantag från lagens tillämpningsområde.

Genom *1–3 mom.* utnyttjas det nationella handlingsutrymme för tillämpningsområdet som artikel 2.7–2.9 i NIS 2-direktivet tillåter.

I *1 mom.* föreslås ett undantag från tillämpningen av riskhanterings- och rapporteringsskyldigheterna i fråga om verksamhet eller tjänster som tillhandahålls för tryggande av försvaret, den nationella säkerheten, allmän ordning och säkerhet eller förebyggande av brott, brottsutredning och lagföring. Skyldigheten enligt 39 § att anmäla sig till förteckningen över aktörer ska fortfarande gälla för aktören.

I *2 mom.* föreskrivs det att lagen inte tillämpas på aktörer som endast tillhandahåller verksamhet eller tjänster som avses i 1 mom.

Med stöd av *3 mom.* omfattas med avvikelse från 1 och 2 mom. en aktör av lagens tillämpningsområde om aktören är en tillhandahållare av betrodda tjänster.

I *4 mom.* föreskrivs det att lagen inte tillämpas på aktörer på vilka DORA-förordningen inte tillämpas med stöd av artikel 2.4 i den förordningen. Genom det föreslagna 4 mom. avgränsas lagens tillämpningsområde i enlighet med artikel 2.10 i NIS 2-direktivet.

I *5 mom.* föreskrivs för tydlighetens skull om en avgränsning som motsvarar artikel 2.11 i NIS 2-direktivet. Lagen förpliktar därmed inte till att tillhandahålla information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed. I en sådan situation föreligger ingen skyldighet att lämna ut uppgifter med stöd av den föreslagna lagen. Genom bestämmelsen avgränsas inte de parter mellan vilka ett sådant utlämnande av information kan komma i fråga, utan det är av betydelse vilken typ av information som lämnas ut. Bestämmelsen kan i undantagsfall bli tillämplig till exempel när uppgifter lämnas ut från den gemensamma kontaktpunkten till Europeiska kommissionen, NIS-samarbetsgruppen eller Europeiska unionens cybersäkerhetsbyrå Enisa.**5 §.** *Förhållande till annan lagstiftning*. I paragrafen föreskrivs det om lagens förhållande till annan lagstiftning om riskhanterings- och rapporteringsskyldigheter inom cybersäkerheten. Eftersom lagen ska tillämpas horisontellt inom olika sektorer är det nödvändigt att förtydliga lagens förhållande till andra författningar genom den föreslagna bestämmelsen, som uttrycker lagens karaktär av allmän lag i förhållande till sektorsspecifik reglering som syftar till att uppnå en högre nivå på cybersäkerheten.

I lagen ställs horisontella allmänna minimikrav på riskhanteringen och incidentrapporteringen för cybersäkerheten för alla aktörer som omfattas av tillämpningsområdet för NIS 2-direktivet så att det i lagen föreskrivs om de riskhanterings- och rapporteringsskyldigheter för varje bransch som miniminivån enligt NIS 2-direktivet förutsätter. Sektorsvis är det dock möjligt att det i den nationella lagen eller EU-lagstiftningen för en viss bransch eller typ av aktör uppställs mer detaljerade eller exakta skyldigheter som syftar till att säkerställa en högre nivå på cybersäkerheten än de allmänna skyldigheterna enligt NIS 2-direktivet. Sådana skyldigheter kan exempelvis jämfört med den föreslagna lagen innehålla mer detaljerade bestämmelser om de delområden som ska beaktas i riskhanteringen, förutsätta att en viss standard eller certifiering tillämpas eller kräva en tätare eller snabbare rapportering till tillsynsmyndigheten. Sektorsspecifik reglering ska tillämpas utöver den föreslagna lagen till den del syftet med den sektorsspecifika regleringen är att säkerställa en högre cybersäkerhetsnivå.

I *1 mom.* föreskrivs det om lagens förhållande till bestämmelser i andra nationella lagar. I enlighet med artikel 5 är NIS 2-direktivet ett minimum av bindande verkan, vilket innebär att NIS 2-direktivet inte hindrar en medlemsstat från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten. Om det i någon annan lag finns bestämmelser som säkerställer en högre cybersäkerhetsnivå, ska dessa tillämpas utöver det som föreskrivs i den föreskrivna lagen.

I *2 mom.* föreskrivs det om lagens förhållande till krav som ställs på aktörer i sektorsspecifika unionsrättsakter. Genom förslaget genomförs artikel 4 i NIS 2-direktivet. Sektorsspecifika cybersäkerhetskrav finns åtminstone i unionens sektorsspecifika rättsakter i anslutning till finansmarknaden och flygtrafiken.

Enligt artikel 4.2 i NIS 2-direktivet ska kraven anses ha samma verkan om riskhanteringsåtgärderna för cybersäkerhet minst är likvärdiga som de åtgärder som föreskrivs i artikel 21.1 och 21.2, eller när respektive sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt direktivet och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i direktivet. Om den sektorsspecifika regleringen anses ha samma verkan som förpliktelserna enligt den föreslagna lagen, ska förpliktelserna enligt 2 kap. eller 43 § och bestämmelserna om tillsyn och påförande av påföljdsavgift i 4 och 5 kap. inte tillämpas på en

aktör. Trots sektorsspecifik reglering ska alla sektorer, branscher och typer av aktörer som avses i den föreslagna lagen beaktas vid beredningen av den nationella cybersäkerhetsstrategin och planen för hantering av omfattande cybersäkerhetsincidenter och cyberkriser samt i verksamheten vid CSIRT-enheten.

Kommissionen har publicerat närmare anvisningar om bedömningen av sektorsspecifik unionslagstiftning i förhållande till NIS 2-regleringen och, i det fall att den sektorsspecifika regleringen anses motsvara NIS 2-regleringen, om tillämpningen av NIS 2-regleringen på aktörer som omfattas av denna sektorsspecifika reglering. Kommissionen har genom meddelandet 2023/C 328/02 utfärdat anvisningar om tillämpningen av artikel 4.1 och 4.2 i NIS 2-direktivet.

6 §. *Jurisdiktion och territorialitet.* I paragrafen föreskrivs det om jurisdiktionen i Finland i fråga om internationella aktörer på det sätt som avses i artikel 26 i NIS 2-direktivet.

Med stöd av *1 mom.* ska, i enlighet med huvudregeln i artikel 26.1 i NIS 2-direktivet, finsk lag tillämpas på aktörer som är etablerade i Finland. Aktörer som är etablerade i Finland omfattas således i regel av jurisdiktionen i Finland och tillämpningsområdet för finsk lag. Om verksamhet som omfattas av tillämpningsområdet för NIS 2-direktivet i Finland bedrivs eller tjänster tillhandahålls av en aktör som är etablerad i en annan EU-medlemsstat, omfattas aktören i regel och på motsvarande sätt av lagstiftningen och laglighetsövervakningen i etableringsstaten. Enligt artikel 26.1 c i NIS 2-direktivet omfattas en offentlig förvaltningsaktör alltid av jurisdiktionen i den medlemsstat som inrättade den.

I *2 mom.* föreskrivs det om ett undantag från huvudregeln i 1 mom. i fråga om vissa aktörer på motsvarande sätt som i artikel 26.1 a i NIS 2-direktivet. Oberoende av i vilken stat de är etablerade ska tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Således omfattas de aktörer som tillhandahåller nämnda tjänster i Finland av jurisdiktionen i Finland. Om en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster endast tillhandahåller en allmänt tillgänglig rekursiv DNS-tjänst som en del av internetanslutningstjänsten, ska den aktören omfattas av jurisdiktionen i varje medlemsstat där dess tjänster tillhandahålls, i fråga om de tjänster som tillhandahålls i medlemsstaten.

I *3 mom.* föreskrivs det om ett undantag från huvudregeln i 1 mom. i fråga om vissa aktörer på motsvarande sätt som i artikel 26.1 b och 26.2–26.5 i NIS 2-direktivet. I fråga om skyldigheterna enligt NIS 2-direktivet omfattas de aktörer som avses i momentet av jurisdiktionen i den medlemsstat där aktören har sitt huvudsakliga etableringsställe enligt artikel 26.2 i NIS 2-direktivet. Dessa aktörer omfattas alltså av jurisdiktionen i endast en medlemsstat. Enligt artikel 26.2 i NIS 2-direktivet anses aktören ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda aktören har det etableringsställe som har flest anställda i unionen.

Om aktören har sitt huvudsakliga verksamhetsställe utanför Europeiska unionen men tillhandahåller tjänster inom Europeiska unionen, förutsätts aktören i enlighet med artikel 26.3 i NIS 2-direktivet utse en företrädare i Europeiska unionen. Aktören ska då anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om en aktör som är etablerad utanför

Europeiska unionen inte har utsett en sådan företrädare i Europeiska unionen som förutsätts och som avses i artikel 26.3 i NIS 2-direktivet och aktören tillhandahåller tjänster i Finland, omfattas aktören av jurisdiktionen i Finland och lagens tillämpningsområde.

En aktör som är etablerad utanför Europeiska unionen anses tillhandahålla tjänster inom Europeiska unionen om den avser att tillhandahålla tjänster till personer i en eller flera medlemsstater. Till exempel användning av ett språk eller en myntenhet som allmänt används i en eller flera medlemsstater och möjligheten att beställa tjänster på detta språk eller omnämnande av kunder eller användare i unionen kan visa att aktören har för avsikt att tillhandahålla tjänster till personer i en medlemsstat i unionen. Å andra sidan är det i allmänhet inte tillräckligt att enbart ha tillgång till webbplatser, e-postadresser eller andra kontaktuppgifter i unionen för att visa att en aktör avser att tillhandahålla sina tjänster i unionen.

Den namngivna företrädaren ska agera på aktörens vägnar, och det ska vara möjligt för de behöriga myndigheterna eller CSIRT-enheterna att vända sig till företrädaren. Företrädaren ska utses uttryckligen genom en skriftlig fullmakt från aktören att agera på dess vägnar med avseende på dess skyldigheter enligt direktivet, inklusive incidentrapportering. Att utse en företrädare skulle dock inte påverka medlemsstaternas möjligheter att vidta rättsliga åtgärder mot aktören själv.

I *4 mom.* föreskrivs det om tillsynsmyndighetens möjlighet att rikta tillsyns- och efterlevnadskontrollåtgärder mot en aktör som är etablerad i en annan medlemsstat i Europeiska unionen, men som tillhandahåller tjänster i Finland eller som har ett kommunikationsnät eller informationssystem i Finland. Tillsynsmyndigheten kan i Finland på det sätt som föreskrivs i lag utföra tillsyns- och efterlevnadskontrollåtgärder som avser aktörer etablerade i en annan medlemsstat i Europeiska unionen, om den behöriga myndigheten i etableringsstaten begär det. En ytterligare förutsättning är att aktören tillhandahåller tjänster i Finland eller har ett kommunikationsnät eller informationssystem på finskt territorium och att tillsynsmyndigheten har rätt att vidta den begärda åtgärden med stöd av den föreslagna lagen.

Bestämmelser om samarbetet mellan medlemsstaternas myndigheter finns i artikel 37 i NIS 2-direktivet, som tillsynsmyndigheten ska beakta vid genomförandet av samarbetet. Med stöd av artikel 37.1 andra stycket i NIS 2-direktivet får tillsynsmyndigheten inte avslå begäran, förutom om myndigheten inte är behörig att tillhandahålla det begärda biståndet, det begärda biståndet inte står i proportion till tillsynsmyndighetens tillsynsuppgifter eller begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot Finlands nationella säkerhetsintressen, allmänna säkerhet eller försvar. Före begäran ska tillsynsmyndigheten samråda med andra berörda behöriga myndigheter och, om en medlemsstat begär det, med Europeiska kommissionen och Enisa.

7 §. *Skyldighet att hantera cybersäkerhetsrisker*. I paragrafen föreskrivs det om en allmän skyldighet för aktörer som omfattas av tillämpningsområdet att identifiera, bedöma och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som de använder i sin verksamhet eller för att tillhandahålla sina tjänster.

Enligt *1 mom.* ska aktörerna genom riskhantering försäkra sig om att säkerhetsnivån och nivån på riskhanteringsåtgärderna i de kommunikationsnät och informationssystem som används i verksamheten eller tillhandahållandet av tjänster är tillräcklig och proportionell mot riskerna och kommunikationsnätets eller informationssystemets betydelse. Med riskhantering avses identifiering av risker som hänför sig till kommunikationsnät och informationssystem som är

av betydelse med tanke på verksamheten eller tillhandahållandet av tjänster, bedömning av hur allvarliga riskerna är samt vidtagande av tillräckliga åtgärder för att hantera riskerna.

Enligt skäl 77 i NIS 2-direktivet ska aktörerna främja och utveckla en riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna.

Med stöd av *2 mom.* ska aktören vidta säkerhets- och riskhanteringsåtgärder som är aktuella, proportionella och tillräckliga i förhållande till riskerna för de kommunikationsnät och informationssystem som används i verksamheten samt kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet och tillhandahållande av tjänster. Fastställandet av den identifierade riskens betydelse är både subjektivt på basis av aktörens egna affärs- eller serviceintressen och objektivt på basis av den allmänna och samhälleliga betydelsen och betydelsen av en tjänst som är beroende av tillförlitligheten hos aktörens kommunikationsnät och informationssystem. De objektiva kriterierna beskrivs närmare i 9 § och dess motivering. Syftet med riskhanteringen är att förhindra eller minimera att störningar i kommunikationsnäten och informationssystemen påverkar verksamheten, tjänstemottagarna eller andra tjänster vid störningssituationer oberoende av orsaken till störningen. Riskhanteringen ska alltså syfta till att trygga kontinuiteten i verksamheten i situationer där kommunikationsnätens och informationssystemens funktion störs på grund av illvillig verksamhet eller av någon annan orsak.

Skyldigheten att ordna riskhantering inom cybersäkerheten är fortlöpande till sin karaktär, eftersom riskerna för säkerheten i kommunikationsnät och informationssystem förändras och säkerhetsåtgärderna utvecklas med tiden. Riskhanteringsåtgärderna ska framför allt vara aktuella, dvs. motsvara aktuell teknisk utveckling och välkänd bästa praxis om hur cybersäkerhetsrisker kan skyddas eller deras effekter minimeras. Vid bedömningen av om riskhanteringen är tillräcklig och proportionell beaktas bland annat kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet eller tillhandahållande av tjänster, arten av de uppgifter som behandlas i kommunikationsnätet eller informationssystemet samt andra aktörers beroende av aktörens verksamhet, tillhandahållande av tjänster, kommunikationsnät eller informationssystem samt särskilt dess betydelse för samhällets kristålighet.

Syftet med bedömningen av cybersäkerhetsriskerna är att främja och utveckla en riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna. Ju större verkningarna blir om en risk realiseras och ju större sannolikheten är för att den realiseras, desto effektivare, högklassigare och dyrare åtgärder krävs det för att riskhanteringen ska vara proportionerlig.

Begreppet risk definieras i 2 § 18 punkten.

De föreslagna 7–10 § genomför artiklarna 20–22 i NIS 2-direktivet.

8 §. *Handlingsmodell för hantering av cybersäkerhetsrisker*. I paragrafen föreskrivs det om aktörers skyldighet att ha tillgång till en uppdaterad handlingsmodell för hantering av cybersäkerhetrisker för att uppfylla den föreskrivna riskhanteringsskyldigheten. I handlingsmodellen för hantering av cybersäkerhetrisker ska de risker identifieras som hänför sig till kommunikationsnät och informationssystem och deras fysiska miljö som aktören använder eller som påverkar tillhandahållandet av tjänster samt de åtgärder och förfaranden för riskhantering genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot risker och incidenter eller skadliga effekter. En aktör kan själv skapa en handlingsmodell för hantering av cybersäkerhetrisker eller lägga ut den på underentreprenad. Handlingsmodellen för hantering

av cybersäkerhetrisker kan också vara en del av aktörens mer omfattande riskhanteringsplan, som också beaktar andra risker som hänför sig till verksamheten, eller en del av den övriga säkerhetsberedskapen.

Handlingsmodellen för hantering av cybersäkerhetrisker ska i enlighet med en allriskansats (all-hazard approach) skapas så att den omfattar både kommunikationsnät och informationssystem och deras fysiska miljö. Syftet är att skydda kommunikationsnät och informationssystem samt den verksamhet som bedrivs eller de tjänster som tillhandahålls med hjälp av dem mot kränkningar av informationssäkerheten, systemfel, mänskliga misstag, avsiktligt skadliga handlingar och naturfenomen. I en allriskansats ska man alltså beakta alla rimligen förutsebara hot mot kommunikationsnät och informationssystem, oavsett om de beror på hot mot informationssäkerheten, orsakas av naturen eller människan eller om de följer olyckor eller är avsiktligt orsakade.

En allriskansats ska omfatta risker för informationssäkerheten i kommunikationsnät och informationssystem, såsom administrativa risker, risker i fråga om personal, hårdvara, programvara, informationsmaterial och användarsäkerhet samt i fråga om deras fysiska miljö, lokaler och nödvändiga resurser sådana händelser som stöld, brand, översvämning, störning av telekommunikationen eller elavbrott, obehörigt fysiskt tillträde till aktörens information eller informationshanteringsmiljö samt skada och störningar som kan äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten i fråga om den information eller de tjänster som hanteras i kommunikationsnäten och informationssystemen eller via dessa.

I riskhanteringen ska det beaktas i vilken utsträckning aktören är beroende av kommunikationsnäten och informationssystemen. Ju viktigare system det är fråga om med tanke på tjänsteproduktionen och ju större skadliga effekter en risk skulle få för systemet, desto högklassigare riskhantering ska det krävas till denna del.

Handlingsmodellen för hantering av cybersäkerhetrisker och de riskhanteringsåtgärder som grundar sig på den ska som en del av den fortlöpande identifiering och bedömning av risker som avses i 7 § uppdateras och hållas aktuell.

9 §. *Åtgärder för hantering av cybersäkerhetsrisker*. Aktörerna ska vidta proportionerliga åtgärder för att hantera, förebygga och förhindra eller minimera de risker som riktas mot säkerheten i kommunikationsnät och informationssystem. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till aktörens grad av riskexponering, aktörens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

I *2 mom.* föreskrivs det på motsvarande sätt som i artikel 21.2 i NIS 2-direktivet om de delområden som åtminstone ska beaktas vid utarbetandet av en handlingsmodell för hantering av cybersäkerhetsrisker och vid fastställandet av behövliga riskhanteringsåtgärder. Syftet med specificeringen av delområdena i punktens led är att definiera kraven å ena sidan så noggrant som möjligt för att aktörerna ska kunna förutse dem och å andra sidan teknikneutralt för att de ska lämpa sig för alla sektorer och för en cybersäkerhetsmiljö som ständigt förändras. Fastställandet av kraven främjar också att tillsynsmyndighetens grunder för tillsynsåtgärderna är tydliga och förutsägbara. Avsikten har varit att de termer som används i paragrafen ska samordnas med terminologin inom den tekniska sektorn. Med riktlinjer avses principerna för och fastställandet av aktörens allmänna mål, dvs. policyer. Med förfaranden avses olika processer och tekniska

förfaringssätt (procedures, processes). Med praxis avses funktionssätt (practises). Gränsdragningen mellan termerna är inte exakt och i tekniska källor, såsom standarder, kan termerna användas med olika betydelser.

Punkt 1 gäller riktlinjer för hantering av cybersäkerhetsrisker samt bedömning av effektiviteten i fråga om riskhanteringsåtgärderna. Genom denna punkt genomförs artikel 21.2 f och delvis 21.2 a i NIS 2-direktivet. Med riktlinjer för hantering av cybersäkerhetsrisker avses planering på högsta nivå i organisationen, genom vilken risker som hänför sig till organisationen eller dess verksamhet systematiskt identifieras, bedöms och hanteras, mål uppställs och förverkligandet av dem följs upp. Aktören ska ha en heltäckande handlingsmodell för hantering av cybersäkerhetsrisker genom vilken risker som hänför sig till kommunikationsnät och informationssystem samt deras fysiska miljö regelbundet identifieras, analyseras, utvärderas och hanteras. Riskhanteringen ska vara kontinuerlig till sin karaktär och utgöra en del av organisationens verksamhet, vilket förutsätter att bedömningen av strategins och åtgärdernas verkningsfullhet inkluderas i riskhanteringsåtgärderna. Det rekommenderas att riktlinjerna och handlingsmodell för hantering av cybersäkerhetsrisker baserar sig på aktuella bästa praxis och standarder inom branschen.

Vid riskhanteringen ska man följa en allriskansats och säkerställa att företagets företagsstyrning och riskhanteringsprocesser beaktar cybersäkerhetsriskerna. Utgångspunkten för riskhanteringen ska vara att identifiera de behov som hänför sig till konfidentialitet, integritet, tillgänglighet och äkthet samt de tjänster, system, processer och personer som är centrala med tanke på funktionerna. Denna identifiering preciseras i punkt 5 om tillgångsförvaltning. Dessutom ska man identifiera de hot som riktas mot aktören och bedöma sannolikheten för dem samt deras konsekvenser. Syftet med riskhanteringen är att hantera riskerna så att sannolikheten för eller verkan av dem minimeras, elimineras eller läggs ut på underentreprenad. De risker som kvarstår efter riskhanteringen ska godkännas på motiverade grunder. Riskhanteringens ändamålsenlighet ska regelbundet utvärderas med hjälp av lämpliga indikatorer så att de valda åtgärdernas ändamålsenlighet kan mätas och vid behov förbättras. Bedömningen kan göras exempelvis genom självbedömning eller med hjälp av oberoende tillhandahållare av informationssäkerhetstjänster.

Punkt 2 gäller riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem. Genom denna punkt genomförs artikel 21.2 a i NIS 2-direktivet. Med riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem avses aktörens syn på informationssäkerhetens mål, principer och genomförande under hela livscykeln. Dessa kan gälla administrativ säkerhet, personal-, maskinvaru-, programvaru-, kommunikationsnät- och datamaterialsäkerhet samt operativ säkerhet och säkerhet för den fysiska miljön. I ISO 27001 används termen ”informationssäkerhetspolicy” för motsvarande riktlinjer. Aktören ska ha skriftliga riktlinjer och förfaranden för säkerheten i kommunikationsnät och informationssystem. Dessa ska stå i rätt proportion till aktörens behov och de ska uppdateras. Aktörens personal ska känna till de säkerhetsförfarandena och förbinda sig att iaktta dem. Vid valet av lämpliga förfaranden kan de affärsmässiga behoven och identifierade cybersäkerhetsriskerna beaktas.

Punkt 3 gäller säkerhet vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter. Genom denna punkt genomförs artikel 21.2 e i NIS 2-direktivet. Aktören ska upprätthålla säkerheten i kommunikationsnät och informationssystem under hela deras livscykel. De system som förvärvas ska utifrån verksamhetens behov vara tillräckligt säkra, bland annat när det gäller integritet, tillgänglighet och konfidentialitet, och de ska kunna skydda sig mot de vanligaste angreppen. En säker konfiguration av systemen ska definieras, dokumenteras

och upprätthållas under hela livscykeln, och detta bör särskilt beaktas vid uppdateringar. Konfigurations- och programuppdateringar ska dokumenteras, vara utformade och detaljerade i enlighet med ändringshanteringsprocesserna och göras i rätt tid med tanke på objektets särdrag och uppdateringarnas kritiska natur. Otillåtna eller skadliga förändringar ska förhindras. De objekt som är mest kritiska med tanke på säkerheten ska identifieras och deras säkerhet ska dessutom tryggas till exempel genom regelbundna inspektioner av processer eller genom tekniska tester. Om aktören producerar nättjänster eller informationssystemtjänster, ska den sörja för deras säkerhet. Aktören ska se till att dessa kan konfigureras på ett säkert sätt och att de omfattas av säkerhetsuppdateringarna. Det ska finnas en rapporteringskanal för uppdagade sårbarheter och på förhand fastställda förfaranden och praxis för behandling av rapporter. Aktören ska försäkra sig om att produkterna har utvecklats med hjälp av välkänd god praxis så att processen omfattar hela utvecklingens livscykel. Om en aktör inte själv producerar nättjänster eller informationssystemtjänster, behöver den inte heller själv hantera anmälningar om sårbarheter eller delge information om sårbarheter. När det gäller kommunikationsnät ska aktören se till att dess struktur är säker. Objekt som är kritiska för funktionerna ska identifieras och vid behov skyddas genom uppdaterade tekniska metoder, till exempel genom zonindelning. Eventuell skadlig teknisk trafik ska kunna upptäckas och förhindras.

Punkt 4 gäller den övergripande kvaliteten och resiliensen hos leveranskedjan, leverantörernas och tjänsteleverantörernas produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos leverantörer och tjänsteleverantörer. Genom denna punkt genomförs artikel 21.2 d och 21.3 i NIS 2-direktivet. Aktören ska ha uppdaterad information om alla direkta leverantörer och tjänsteleverantörer som påverkar verksamheten och tillhandahållandet av tjänster. Vid riskhanteringen ska aktören beakta hur störningar i leveranskedjan påverkar dess egen verksamhet samt förbereda sig på leveransstörningar. Aktören ska beakta säkerhetsaspekterna i förhållande till de direkta leverantörerna av utrustning eller tjänster i leveranskedjan. När riskhanteringsåtgärder övervägs ska aktören beakta de sårbarheter som är typiska för en direkt leverantör eller tjänsteleverantör, den övergripande kvaliteten på produkterna och tjänsterna och deras motståndskraft mot störningar, de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i produkterna och tjänsterna samt cybersäkerhetspraxis hos leverantörer och tjänsteleverantörer. Dessa kan innehålla olika säkerhetskrav till exempel i fråga om tillgänglighet, kontinuitet och avtal. I fråga om kraven i den föreslagna lagen svarar aktören själv för att den för sin egen verksamhet förvärvar produkter och tjänster som uppfyller kraven på riskhanteringen. Kraven i lagen gäller alltså inte en underleverantör, om inte underleverantören själv är en aktör vars verksamhet omfattas av regleringen. Också då ansvarar underleverantören för att de krav i regleringen som ställs på den själv uppfylls och, i förhållande till den aktör som förvärvar tjänster eller produkter av underleverantören, för det som avtalats vid underleveransen. Aktörerna kan hantera cybersäkerhetsrisken i leveranskedjan genom att inkludera riskhanteringsåtgärder för cybersäkerhet i de avtalsarrangemang som de ingår med sina direkta leverantörer och tjänsteleverantörer. I enlighet med skäl 85 i NIS 2-direktivet är det med tanke på leveranskedjans stora betydelse särskilt viktigt att aktören hanterar risker som härrör från leveranskedjan och aktörens förhållande till leverantörerna.

I enlighet med artikel 22 i NIS 2-direktivet ska NIS-samarbetsgruppen, Europeiska kommissionen och Enisa i samarbete genomföra riskbedömningar av specifika leveranskedjor. I den mån sådana riskbedömningar har gjorts ska aktörerna utnyttja dem i tillämpliga delar.

Punkt 5 gäller tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på säkerheten. Genom denna punkt genomförs artikel 21.2 i) i NIS 2-direktivet. Med tillgångsförvaltning avses de förfaranden och åtgärder genom vilka aktören förvaltar tillgångar i maskinvara, programvara och kunskaper som är väsentliga för verksamheten. Tillgångsförvaltningen

är en central metod i hanteringen av cybersäkerhetsrisker. En omsorgsfull tillgångsförvaltning förebygger att risker realiseras och underlättar riskhanteringen. Aktören ska för tillgångsförvaltningen ha regelbundna och dokumenterade förfaranden och anvisningar som inbegriper identifiering av funktioner, processer och information. Med tillgångar avses t.ex. lokaler, maskinvara, programvara, tjänster, personer, immateriella tillgångar och resurser såsom immateriella rättigheter eller IP-adresser. Tillgångar i anknytning till kommunikationsnät och informationssystem ska identifieras och klassificeras utifrån skyddsbehoven. Aktören ska föra en uppdaterad förteckning över tillgångarna. Tillgångsförvaltningen ska vara en väsentlig del av hanteringen av förändringar i fråga om personal, externa aktörer och informationssystem samt livscykelhanteringen i fråga om utrustning från det att den tagits i bruk till det att den tas ur bruk på ett säkert sätt.

Punkt 6 gäller personalsäkerhet och utbildning i cybersäkerhet. Genom denna punkt genomförs NIS 2-direktivets artikel 21.2 i delvis och artikel 21.2 g. Med personalsäkerhet avses förfaranden som säkerställer personalens ansvar och skyldigheter i fråga om it-säkerhet, deras it-säkerhetskompetens samt bakgrundskontroller och hanteringen av nyckelpersonrisker. Dessutom omfattar dessa förfaranden förebyggande av missbruk, vilket bland annat innebär identifiering och undvikande av farliga arbetskombinationer, arbetsrotation samt upphörande av ett anställningsförhållande eller ett avtal. Aktören ska ha personalrelaterade förfaranden där också externa aktörer, såsom underleverantörer, beaktas. Förfaringssätten ska också beakta ansvar och skyldigheter efter det att anställningsförhållandet upphört och arbetsuppgifterna ändrats. Personalen och externa aktörer ska informeras om ansvar och skyldigheter i anslutning till säkerheten i deras arbetsuppgifter och tjänster, till exempel i fråga om sekretess. Om arbetsuppgifterna och ansvaren anses kräva särskild tillförlitlighet, kan det till exempel förutsättas att personen genomgår en ändamålsenlig bakgrundskontroll.

Aktören ska se till att personalen har förmåga att agera på ett sätt som motsvarar handlingsmodellen och åtgärderna för hantering av cybersäkerhetsrisker. För att uppnå detta ska personalen få utbildning som ökar medvetenheten om cybersäkerhet i allmänhet, kunskaper om aktuella förfaranden och aktuell praxis samt om kända cybersäkerhetsrisker. Genom utbildning eller på något annat motsvarande sätt bör det säkerställas att personalen med hänsyn till arbetsuppgifterna har tillräcklig kompetens i fråga om skydd av kommunikationsnät och informationssystem, identifiering av cybersäkerhetsrisker, riskhanteringspraxis och bedömning av deras konsekvenser för de tjänster som aktören tillhandahåller och att denna kompetens också upprätthålls på en tillräcklig nivå. Bestämmelser om skyldigheten för en aktörs ledning att upprätthålla tillräcklig förtrogenhet med riskhantering inom cybersäkerhet finns i 10 §.

Punkt 7 gäller förfaranden för åtkomsthantering och autentisering. Genom denna punkt genomförs NIS 2-direktivets artikel 21.2 i och j delvis. Med åtkomsthantering och autentisering avses förfaranden som säkerställer identifieringen av användare, utrustning, tillämpningar och system samt genomförandet av åtkomsten i enlighet med kraven på informationssäkerhet. Förfarandena för åtkomsthantering och autentisering ska gälla både fysiska användare, t.ex. personal och externa aktörer, och systemkoder, t.ex. koder som används av maskinvara, programvara, gränssnitt och andra väsentliga resurser. Åtkomsthanteringen ska gälla både åtkomst som kan autentiseras genom ett program och fysisk åtkomst. Förfarandena ska grunda sig på de verksamhetsrelaterade kraven samt på de krav som ställs på datanätverk och informationssystem med beaktande av systemens särdrag.

Aktören ska i anknytning till åtkomsthanteringen ha definitioner och praxis som övergripande säkerställer en tillförlitlig identifiering och tillåter åtkomst endast till nödvändiga kommunikat-

ionsnät och informationssystem, skyddade uppgifter och andra resurser. Aktören ska ha förfaranden som täcker användarnamnens och åtkomsträttigheternas hela livscykel, och åtkomsträttigheterna ska hanteras i enlighet med dem. Åtkomsträttigheterna och användningen av dem ska övervakas. Åtkomsträttigheter och roller ska fortgående dokumenteras och användarna ska endast ges de rättigheter som de behöver för att utföra sina arbetsuppgifter (principen om lägsta behörighet). Aktörerna ska ha förfaranden för hantering av användarkonton med stark behörighet och för huvudanvändarkonton. Huvudanvändarrättigheterna ska begränsas till så få användare som möjligt och dessa koder ska skyddas med starka metoder. Utövandet av huvudanvändarrättigheter ska övervakas.

De kontrollmetoder och kontrolltekniker som väljs ska grunda sig på kraven på åtkomst till informationen och på kontrollförfarandena. Kontrollmetoderna ska vara tillräckligt säkra för att i möjligaste mån förhindra obehörig användning. Vid behov ska som kontrollmetod användas stark autentisering, multifaktorautentisering (MFA) eller kontinuerlig autentisering, om dessa kan användas.

Punkt 8 gäller riktlinjer och förfaranden för användning av krypteringsmetoder. Genom denna punkt genomförs NIS 2-direktivets artikel 21.2 h samt artikel 21.2 j delvis. Med krypteringsmetoder avses kryptografiska metoder med vilka data omvandlas till ett format som en utomstående inte kan avläsa. Aktören ska fastställa riktlinjer och förfaranden för kryptografi för att vid behov skydda informationens konfidentialitet, äkthet och integritet. Det kan vara nödvändigt att kryptera information t.ex. om den överförs i ett öppet datanät eller förvaras utan tillräckligt fysiskt skydd. Aktören ska då välja en krypteringsteknik vars skyddsnivå är tillräcklig med tanke på den krypterade informationens art, krypteringsklassificering, skyddstid och prestandakrav. När det gäller krypteringsteknik ska man utöver algoritmer, användningssätt och nyckelstyrka också beakta åtkomsten till och säker förvaring, generering och hantering av nycklar. Kraven på krypteringsmetoden ska vara uppdaterade under hela systemets livscykel, så att t.ex. krypteringsalgoritmen kan bytas ut (kryptoagilitet).

Punkt 9 gäller upptäckande och hantering av incidenter i syfte att återställa och upprätthålla säkerheten och driftsäkerheten. Genom denna punkt genomförs artikel 21.2 b i NIS 2-direktivet. Med incident avses enligt 2 § i lagförslaget 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. Med incidenthantering avses enligt artikel 6.1.8 i NIS 2-direktivet alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident. Med återställande av säkerheten avses återställande av systemet till ett säkert läge efter en särskild situation eller en störning. Med upprätthållande av driftsäkerheten avses förfaranden som förbättrar systemets driftsäkerhet samt förmåga att fungera i särskilda situationer och att återhämta sig från störningar. För att hantera incidenter ska aktören ha på förhand dokumenterade förfaranden, roller och ansvar för att förebygga, upptäcka, analysera, hantera och rapportera incidenter samt för att återställa läget efter incidenter. För att upptäcka incidenter ska aktören ha rapporteringskanaler till interna och externa aktörer. Aktören ska ha verktyg och processer för att upptäcka och registrera händelserna.

Med tanke på observations- och analysförmågan är det nödvändigt att aktören har tillgång till tillräckliga logguppgifter om t.ex. underhåll, ändringar, användning och fel. Aktören ska bedöma händelserna för att utreda om de kan orsaka en incident. Aktören ska ha rutiner för bedömning och vid behov klassificering av incidentens allvarlighetsgrad och konsekvenser. Vid hanteringen av en incident ska det också finnas praxis för att reagera på den samt vid behov för

att begränsa och utreda den och eliminera dess konsekvenser. Efter en incident ska man utvärdera orsakerna till den och lära sig av erfarenheterna, så att man i fortsättningen bättre kan förbereda sig på risken för en liknande incident. För allvarliga incidenter och incidenter som kan påverka andra aktörer ska det finnas förfaranden, ansvar och kommunikationskanaler för att varna andra aktörer. Incidenthanteringen ska också inbegripa förfaranden för spridning av information så att incidenten inte utsätter aktören eller någon annan organisation för risk. Förfarandena för hantering av incidenter ska upprätthållas och utvecklas under hela livscykeln, och de ska uppdateras till exempel utifrån erfarenheterna.

Punkt 10 gäller säkerhetskopiering, katastrofhantering, krishantering och annan driftskontinuitet och vid behov användning av säkrade reservkommunikationssystem i aktörens verksamhet. Genom denna punkt genomförs NIS 2-direktivets artikel 21.2 c och artikel 21.2 j delvis. Med säkerhetskopiering avses kopiering av uppgifter till en säker plats. Med katastrofhantering avses processer och metoder med vilka systemet kan fås i funktionsdugligt skick t.ex. genom reservarrangemang eller säkerhetskopior. Med driftskontinuitet avses processer och förfaranden med hjälp av vilka organisationen bereder sig på att hantera störningssituationer och fortsätta verksamheten på en på förhand bestämd och godtagbar nivå. Med säkrade reservkommunikationssystem avses kommunikationskanaler som inte är beroende av något annat system och som har tillräcklig funktionssäkerhet och konfidentialitet.

Aktören ska ha dokumenterade förfaranden för driftskontinuitet och återhämtning från störningssituationer. Kontinuiteten ska säkerställas, vilket kan göras till exempel genom en återställningsplan och en kontinuitetsplan som utarbetats på grundval av riskhantering. Planerna kan till exempel innehålla de omständigheter under vilka de ska aktiveras samt planer som gäller behövliga roller, resurser, åtgärder och kommunikationskanaler samt behövliga säkrade reservkommunikationssystem. Planerna ska åtminstone innehålla krishanteringsförfaranden för synnerligen allvarliga incidenter. I enlighet med den övriga riskhanteringen ska planerna uppdateras och utvecklas regelbundet och genomförandet av planerna övas.

När det gäller säkerhetskopiering ska aktören t.ex. bestämma till vilka delar säkerhetskopior ska tas och ur vilka system och reservsystem. Aktören kan fastställa praxis för hur ofta säkerhetskopior ska tas, förvaringstiden för säkerhetskopior, skyddet av säkerhetskopior och testningen av återställning i ett läge där det ursprungliga systemet inte är tillgängligt.

Behovet av säkrade reservkommunikationssystem kan till exempel grunda sig på att det i riskbedömningen har konstaterats vara nödvändigt att säkra kommunikationskanalerna också när vanliga system (t.ex. telefon, e-post, snabbmeddelanden) inte finns att tillgå. I sådana fall ska aktören definiera de reservkommunikationssystem som ska användas och behovet av dem samt hur de ska tas i bruk.

Punkt 11 gäller grundläggande praxis för cyberhygien för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet. Genom denna punkt genomförs delvis artikel 21.2 g i NIS 2-direktivet. Aktören ska skydda sitt kommunikationsnät och sina informationssystem genom grundläggande praxis för cyberhygien. Aktören ska se till att grundläggande praxis för cyberhygien tillämpas och att arbetstagarna följer praxis. Nivån på dessa förfaranden ska dimensioneras så att de är tillräckliga med hänsyn till hur kritiska funktionerna är. De valda åtgärderna ska bygga på allmän god praxis och riskbedömning.

Med cyberhygienpraxis avses allmänna goda informationssäkerhetsåtgärder som säkerställer en säker grundläggande användning av system, program och tjänster. Det innebär tekniska och

andra åtgärder på basnivå för att säkerställa säkerheten i de objekt som beskrivs i punkten. Cyberhygienpraxis kan bland annat omfatta säkerhetsstrukturen i kommunikationsnätet, upptäckt och förhindrande av skadlig trafik, spårbarhet för och övervakning av funktioner, säker konfiguration av maskinvara och programvara, uppdateringar av programvara, heltäckande och tillförlitlig identifiering samt förbättrande av användarnas kompetens och medvetenhet. Grundläggande praxis för cyberhygien kan omfatta till exempel principen om noll förtroende (zero-trust), aktuella programuppdateringar, säker konfiguration av maskinvara och programvara, nätsegmentering, identitetshantering och åtkomsthantering samt förbättrande av användarnas kompetens och vid behov införande av teknik som förbättrar säkerheten i kommunikationsnät och informationssystem. Punkten överlappar delvis andra punkter i fråga om de omständigheter som förutsätts, men för tydlighets skull och på grund av dess betydelse anges den också separat.

Punkt 12 gäller åtgärder för att säkerställa den fysiska miljön och säkerheten i lokalerna samt nödvändiga resurser. Genom denna punkt genomförs inledningsfrasen i artikel 21.2 i NIS 2-direktivet när det gäller åtgärder för att skydda den fysiska miljön för kommunikationsnät och informationssystem. Enligt skäl 79 i ingressen till NIS 2-direktivet ska dessa åtgärder vara förenliga med CER-direktivet. Artikel 13 i CER-direktivet gäller kritiska aktörers åtgärder för att säkerställa motståndskraft mot störningar. I artikeln föreskrivs bland annat om fysiskt skydd av lokaler, till exempel stängsel, barriärer, detektionsutrustning och passerkontroll samt återhämtning från incidenter, med hänsyn till åtgärder identifiering av alternativa försörjningskedjor.

Med fysisk säkerhet avses fysiskt och tekniskt skydd som skyddar system, lokaler, nät och andra resurser mot obehörig åtkomst samt andra skador och störningar. Med nödvändiga resurser avses identifierade stödfunktioner, stödtjänster och stödsystem som är kritiska med tanke på verksamheten och vars tillgänglighet ska säkerställas. Aktören ska identifiera faktorer i den fysiska miljön vars säkerhet är viktig med tanke på kommunikationsnätens och informationssystemens funktion och skydda dem mot effekterna och störningarna av hot som kan påverka verksamheten. Aktören ska också beakta fysiska miljöer som påverkar kommunikationsnät och informationssystem. Dessa kan vara mycket olika och till exempel geografiskt omfattande eller begränsade. Fysiska hot är miljöfaktorer och illvilliga aktörer. Kommunikationsnäten och informationssystemen ska övervakas och skyddas mot obehörig fysisk åtkomst, skada och störning. Dessutom måste man skydda sig mot naturrelaterade och sociala händelser, såsom eldsvådor, översvämningar och oroligheter. Aktören ska förbereda sig på störningar i de nödvändiga resurserna, såsom eldistributionen, datakommunikationsförbindelserna och kylningen, och förhindra att kommunikationsnät och informationssystem förstörs eller skadas eller att aktörens kritiska funktioner avbryts på grund av brist på nödvändiga resurser eller på grund av störningar.

I det föreslagna *3 mom.* föreskrivs det om nivån på proportionaliteten hos de åtgärder som aktören förutsätts vidta. Åtgärderna för hantering av cybersäkerhetsrisker ska stå i rätt proportion till risken, dvs. till sannolikheten för skadliga effekter och följderna av att risken realiseras. I momentet föreskrivs det om de grunder enligt vilka aktören kan lägga sina riskhanteringsåtgärder på rätt nivå.

Åtgärderna ska ställas i relation till verksamhetens art och omfattning, eftersom verksamhetens art och omfattning står i direkt samband både med aktörens resurser för att avvärja cyberhot och med betydelsen av de tjänster aktören erbjuder med tanke på samhällets funktioner. Åtgärderna ska ställas i relation till de direkta konsekvenser som rimligtvis kan förutses följa av att ett förutsett hot realiseras. Konsekvenserna ska bedömas särskilt med tanke på viktiga samhällsfunktioner, och ju större konsekvenser genomförandet av hotet kan bedömas ha ur samhällets eller ekonomins synvinkel, desto viktigare hanteringsåtgärder bör vidtas. Konsekvenserna ska således bedömas inte bara för aktören själv utan också för dem som använder eller är beroende

av aktörens tjänster. Åtgärderna ska också stå i proportion till aktörens riskexponering i fråga om kommunikationsnät och informationssystem. Vissa tekniska lösningar kan vara förknippade med kända hot mot informationssäkerheten, och dessutom inverkar arten av aktörens verksamhet eller aktörens roll på hur lockande det är för en illvillig aktör att inrikta sig på verksamheten. Åtgärderna ska också ställas i relation till sannolikheten för att en incident inträffar och hur allvarlig den är, vilket sammanhänger med helhetsbedömningen av hotets art och natur och riskdefinitionen. Dessutom ska åtgärderna med beaktande av den senaste tidens utveckling ställas i relation till aktuella tekniska möjligheter att avvärja identifierade hot. Med den senaste utvecklingen avses i synnerhet utvecklingen av tekniska hanteringsåtgärder och riskhanteringsmetoder samt utvecklingen av kända riskhanteringsmetoder till exempel i fråga om kända hotttyper, hotande aktörer, angreppssätt och ny teknik.

Med stöd av *4 mom.* kan tillsynsmyndigheten inom sitt ansvarsområde meddela närmare tekniska föreskrifter om de omständigheter som anges i momentet. Myndighetens behörighet att meddela föreskrifter gäller precisering av de skyldigheter som avses i 2 mom. De närmare föreskrifterna kan dock gälla endast tekniska omständigheter, dvs. de får inte utvidga skyldigheterna enligt 9 §. Bestämmelserna ska vara teknikneutrala. Genom NIS 2-direktivet ges kommissionen befogenhet att anta genomförandeakter för att fastställa tekniska och metodologiska specifikationerna för åtgärderna och, i tillämpliga fall, sektorsspecifika krav. Kommissionens genomförandeakter tillämpas i första hand i förhållande till tillsynsmyndighetens föreskrifter. Till den del kommissionen har utövat sina befogenheter och antagit genomförandeakter som preciserar NIS 2-direktivet ska tillsynsmyndigheterna beakta dessa vid utarbetandet av föreskrifterna och se till att de föreskrifter som de utfärdar är anpassade till kommissionens genomförandeakter.

Med stöd av *5 mom.* ska handlingsmodellen för hantering av risker och hanteringsåtgärderna dessutom iaktta de genomförandeakter som kommissionen antar med stöd av artikel 21.5 i NIS 2-direktivet. Mer detaljerade sektorsspecifika krav som föreskrivs med stöd av NIS 2-direktivet kan till exempel vara de genomförandeakter som kommissionen antagit med stöd av artikel 21.5 första stycket i NIS 2-direktivet om tekniska krav och metodkrav med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster samt tillhandahållare av betrodda tjänster. Dessutom kan med stöd av artikel 21.5 andra stycket i NIS 2-direktivet mer detaljerade sektorsvisa krav föreskrivas genom de genomförandeakter som kommissionen antar för att fastställa tekniska och metodologiska krav på riskhanteringsåtgärder samt, vid behov, sektorskrav som gäller andra aktörer än de som avses ovan.

10 §. *Ledningens ansvar*. Aktörens högsta ledning ska svara för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker i aktörens kommunikationsnät och informationssystem. Ansvaret innebär ett ansvar i sista hand för att ordna riskhanteringen och avsätta lämpliga resurser för den samt att övervaka dess verksamhet. Aktörens ledning godkänner handlingsmodellen för hantering av cybersäkerhetrisker samt övervakar genomförandet av riskhanteringen, resursfördelningen, åtgärderna, riskbedömningarnas aktualitet och åtgärdernas genomslag. Aktörens ledning ska också ha tillräcklig och aktuell förtrogenhet med hantering av cybersäkerhetsrisker, vilket förutsätter förtrogenhet antingen genom utbildning eller på något annat motsvarande sätt med regelbundna intervaller. Som en del av de hanteringsåtgärder som avses i 9 § sörjer ledningen också för att personalen får cybersäkerhetsutbildning.

Med ledning avses en aktörs styrelse, förvaltningsråd, verkställande direktör eller någon annan i motsvarande ställning som faktiskt leder aktörens verksamhet. En sådan ställning kan till exempel innehas av en bolagsman i ett öppet bolag, en ansvarig bolagsman i ett kommanditbolag, en personmedlem i en europeisk ekonomisk intressegruppering eller en enskild näringsidkare. Med ledning avses också en person som lyder direkt under verkställande direktören, om personen sköter sådana högsta ledningsuppgifter i vilka den faktiska ledningen av aktörens verksamhet bedrivs.

Genom förslaget genomförs artikel 20.1 och 20.2 i NIS 2-direktivet.

11 §. *Incidentanmälningar till myndigheten*. I paragrafen föreskrivs det om aktörernas skyldighet att underrätta tillsynsmyndigheten om en betydande incident. De föreslagna 11–13 § genomför artikel 23.1–23.4 i NIS 2-direktivet. Anmälningsskyldigheten gäller endast betydande incidenter.

Med betydande incident avses en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda aktören, eller en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. Om en aktör upptäcker en betydande incident i verksamheten hos någon annan, t.ex. en direkt underleverantör, ska aktören rapportera incidenten, om den har orsakat eller kan orsaka en allvarlig driftsstörning i aktörens egna tjänster eller om den har orsakat eller kan orsaka betydande materiell eller immateriell skada för aktören. Aktören ska i sin inledande bedömning av hur betydande incidenten är ta hänsyn åtminstone till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av aktörens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt aktörens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om driftsstörningen är allvarlig.

Anmälningsskyldigheten ska gälla i tre steg, dvs. aktören ska inom 24 timmar från det att en händelse upptäcktes lämna en första anmälan till tillsynsmyndigheten och inom 72 timmar från det att en avvikelse upptäcktes lämna en uppföljande anmälan. När incidenten har upphört ska aktören lämna tillsynsmyndigheten den slutrapport som avses i 13 §. Syftet med anmälningsskyldigheten i tre steg är å ena sidan att säkerställa snabb rapportering av händelser och skapande av en uppdaterad lägesbild och å andra sidan att möjliggöra att aktörens resurser i första hand riktas till funktioner i anslutning till incidenthanteringen. Aktören kan göra den första anmälan och den uppföljande anmälan på en och samma gång, om aktören inom tidsfristen för den första anmälan, dvs. utan dröjsmål och senast inom 24 timmar från det att incidenten upptäckte, har de uppgifter som förutsätts i båda anmälningarna.

Den första anmälan ska göras utan dröjsmål och inom 24 timmar från det att incidenten upptäcktes. Den första anmälan ska åtminstone innehålla uppgift om att en betydande incident har upptäckts, en preliminär bedömning av huruvida den betydande incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar samt en preliminär bedömning av huruvida den observerade betydande incidenten kan ha verkningar för andra EU-medlemsstater och sannolikheten för sådana gränsöverskridande verkningar. Den första anmälan ska också innehålla andra uppgifter som gör det möjligt för den behöriga myndigheten att fastställa incidentens eventuella gränsöverskridande verkningar.

Den uppföljande anmälan ska göras utan dröjsmål och inom 24 timmar från det att incidenten upptäcktes. I den uppföljande anmälan ska aktören lägga fram en preliminär bedömning av den betydande incidenten, dess allvarlighetsgrad och verkningar samt angreppsindikatorer (Indicator of Compromise, IOC), om sådana finns tillgängliga. Dessutom ska aktören uppdatera uppgifterna i den första anmälan, om det har skett ändringar i eller preciseringar av dem.

Med stöd av *5 mom.* kan tillsynsmyndigheten vid behov inom sitt ansvarsområde meddela närmare tekniska föreskrifter om när en incident som avses i 1 mom. är betydande, om de uppgifter som ska lämnas i slutrapporten samt om förfarandet för anmälan av betydande incidenter och uppgifter enligt 12 och 13 §. Genom NIS 2-direktivet ges kommissionen befogenhet att anta genomförandeakter för att precisera innehållet i, formatet för och rapporteringsförfarandet för incidentanmälningar samt i vilka fall en incident ska betraktas som betydande. Kommissionens genomförandeakter tillämpas i första hand i förhållande till tillsynsmyndighetens föreskrifter. Till den del kommissionen har utövat sina befogenheter och antagit genomförandeakter som preciserar NIS 2-direktivet ska tillsynsmyndigheterna beakta dessa vid utarbetandet av föreskrifterna och se till att de föreskrifter som de utfärdar är anpassade till kommissionens genomförandeakter.

Enligt *6 mom.* ska, med avvikelse från tidsfristen i 2 mom., en tillhandahållare av betrodda tjänster göra en uppföljande anmälan inom 24 timmar från det att den betydande incidenten upptäcktes.

12 §. *Delrapport om incident.* I paragrafen föreskrivs det om aktörens skyldighet att lämna tillsynsmyndigheten ytterligare information eller en delrapport om statusuppdateringar som gäller incidenten. Utöver den första och den uppföljande anmälan ska aktören på begäran av tillsynsmyndigheten lämna ytterligare information eller en delrapport om statusuppdateringar som gäller incidenten och om hur hanteringen framskrider. Om incidenten är långvarig, dvs. om incidenthanteringen inte har avslutats inom en månad från det att en uppföljande anmälan lämnades in, varvid en slutrapport skulle ha lämnats för andra än långvariga incidenter, ska aktören på eget initiativ lämna tillsynsmyndigheten en delrapport om hur behandlingen av avvikelsen framskrider. Delrapporten ska lämnas på eget initiativ senast en månad efter den uppföljande anmälan. Syftet med delrapporten är att beskriva hur incidenthanteringen framskrider, dess konsekvenser och andra väsentliga faktorer som hänför sig till ärendets verkningar samt ändringar i uppgifterna i den första anmälan och den uppföljande anmälan. Aktören ska på begäran av tillsynsmyndigheten lämna ytterligare information eller en delrapport om statusuppdateringar som gäller incidenten och om hur behandlingen framskrider.

13 §. *Slutrapport om incident.* Enligt *1 mom.* ska aktören lämna tillsynsmyndigheten en slutrapport när hanteringen av incidenten har avslutats. Slutrapporten ska lämnas in senast en månad efter det att den uppföljande anmälan lämnades in. Om det är fråga om en långvarig incident som har behandlats mer än en månad från det att den uppföljande anmälan lämnades in, ska aktören i stället för slutrapporten lämna en i 12 § avsedd delrapport om statusuppdateringar som gäller incidenten och om hur hanteringen framskrider. Slutrapporten ska då lämnas in senast en månad efter det att hanteringen av incidenten avslutades.

I *2 mom.* föreskrivs det om slutrapportens minimiinnehåll. Syftet med slutrapporten är att för aktören själv och tillsynsmyndigheten klarlägga det hot eller den orsak som sannolikt har utlöst incidenten samt ge en beskrivning av incidentens art, allvarlighetsgrad och konsekvenser samt vilka åtgärder som vidtagits för begränsa incidentens negativa verkningar. Dessutom ska slutrapporten innehålla en beskrivning av de gränsöverskridande konsekvenserna av den betydande incidenten, om den medförde sådana konsekvenser. Syftet med slutrapporten är att för aktören

förtydliga dess erfarenheter och iakttagelser om orsakerna till, konsekvenserna av och hanteringen av en incident och därigenom genom efterhandsutvärdering av incidenten i framtiden förbättra motståndskraften mot cyberstörningar och cyberattacker både hos den aktör som varit föremål för incidenten och hos andra aktörer. Slutrapporten erbjuder ett sätt att få kännedom om orsakerna till och följderna av incidenten samt att få goda lärdomar av incidenten så att motsvarande betydande incidenter kan förebyggas. Avsikten med slutrapporten är inte att rikta påföljder eller andra sanktioner mot aktören.

14 §. *Rapportering om incidenter och cyberhot till andra än myndigheter.* Enligt *1 mom.* ska aktörerna utan dröjsmål underrätta de mottagare av sina tjänster som kan påverkas av en betydande incident. Dessutom ska aktörerna i enlighet med *2 mom.* utan dröjsmål underrätta de tjänstemottagare som kan påverkas av ett betydande cyberhot. Aktören ska informera tjänstemottagarna om förekomsten av ett cyberhot och om alla åtgärder eller korrigerande insatser som tjänstemottagarna kan vidta för att hantera hotet eller minska de risker som det innebär. Den underrättelse som avses i det föreslagna 2 mom. påverkar dock inte aktörens skyldighet att vidta lämpliga och direkta åtgärder för att förebygga eller avhjälpa hot och återställa tjänstens normala säkerhetsnivå. Sådan information om betydande cyberhot ska tillhandahållas tjänstemottagarna kostnadsfritt och vara formulerad på ett lättbegripligt sätt.

Med betydande cyberhot avses ett i 2 § 10 punkten definierat cyberhot som på basis av sina tekniska egenskaper kan antas allvarligt påverka en aktörs kommunikationsnät och informationssystem eller användare av en aktörs tjänster genom att orsaka betydande materiell eller immateriell skada.

Om det ligger i allmänt intresse att allmänheten underrättas om en incident, kan tillsynsmyndigheten ålägga aktören att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Genom den föreslagna bestämmelsen genomförs artikel 23.1, 23.2 och 23.7 i NIS 2-direktivet.

15 §. *Frivillig underrättelse.* I paragrafen föreskrivs det om möjligheten till frivillig underrättelse om andra än betydande incidenter, cyberhot och tillbud. Aktörer som omfattas av lagens tillämpningsområde uppmuntras att göra frivilliga anmälningar om cyberhot för att förhindra att hoten realiseras som incidenter. För att främja cybersäkerheten är det dock viktigt att också aktörer eller privatpersoner som inte omfattas av tillämpningsområdet för den föreslagna lagen frivilligt anmäler incidenter, cyberhot och tillbud.

Syftet med den anmälningsskyldighet som åläggs aktörerna är inte att förhindra frivillig underrättelse. Frivillig underrättelse kan göras också på något annat sätt än vad som föreskrivs i förslaget eller om andra saker än de som nämns i förslaget. För genomförandet av NIS 2-direktivet är det dock nödvändigt att på lagnivå ta in en bestämmelse om vissa frivilliga anmälningar som tillsynsmyndigheten åtminstone ska ta emot. Tillsynsmyndigheten ska reagera på dessa anmälningar på samma sätt som på en anmälan som en aktör som avses i denna lag är skyldig att göra.

I paragrafen föreskrivs det också om tillsynsmyndighetens skyldighet att allmänt inom sitt ansvarsområde ta emot frivilliga incidentanmälningar om betydande incidenter, cyberhot och tillbud. Frivilliga anmälningar ska tas emot också från andra aktörer än sådana som omfattas av de riskhanterings- och rapporteringsskyldigheter som avses i NIS 2-direktivet. Tillsynsmyndigheten ska behandla frivilliga incidentanmälningar i enlighet med förfarandet i 16 och 17 §. Tillsynsmyndigheten kan prioritera behandlingen av obligatoriska anmälningar framför behandlingen av frivilliga anmälningar.

Syftet med bestämmelsen är inte att frivillig anmälan ska begränsas endast till situationer enligt bestämmelsen eller till ett förfarande enligt bestämmelsen. För genomförandet av NIS 2-direktivet är det fråga om en minimibestämmelse som fastställer tillsynsmyndighetens skyldighet att ta emot åtminstone de angivna anmälningarna. Frivilliga anmälningar om cyberstörningar, cyberhot, tillbud och andra iakttagelser som är väsentliga för upprätthållandet av cybersäkerheten kan i fortsättningen göras till myndigheten också på något annat sätt än det som beskrivs i bestämmelsen.

På aktörer som frivilligt rapporterar betydande incidenter, cyberhot och tillbud och som inte omfattas av riskhanterings- och rapporteringsskyldigheterna enligt den föreslagna lagen, tillämpas inte lagen till övriga delar på grund av den frivilliga rapporteringen.

Tillsynsmyndigheten ska också underrätta den gemensamma kontaktpunkt som avses i 18 § om anmälningar som grundar sig på frivillighet och som har lämnats till den.

Genom den föreslagna bestämmelsen genomförs delvis artikel 30 i NIS 2-direktivet.

16 §. *Mottagande av incidentanmälan.* I *1 mom.* föreskrivs det om tillsynsmyndighetens skyldighet att svara på en incidentanmälan. Skyldigheten att svara gäller både sådana anmälningar som avses i 11 § och sådana frivilliga anmälningar som avses i 15 §.

Tillsynsmyndigheten ska efter att ha fått en incidentanmälan enligt 11 eller 15 § utan dröjsmål svara den som lämnat incidentanmälan. Svaret ska om möjligt ges inom 24 timmar, dock inom ramen för tjänstetiderna. Av tillsynsmyndigheten förutsätts alltså inte till exempel beredskap att dejourera under veckoslut, nattetid eller på helgdag som infaller på en vardag. Svaret ska innehålla initial återkoppling om den betydande incidenten samt anvisningar om hur den ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet. Med initial återkoppling avses tillsynsmyndighetens syn på incidentens betydelse och andra omständigheter som behövs för att hantera incidenten. Tillsynsmyndigheten kan i sitt svar också ta med andra omständigheter som den anser behövliga, såsom allmänna anvisningar eller råd om åtgärder för att lindra verkningarna.

Med stöd av 2 mom. får tillsynsmyndigheten prioritera besvarandet av obligatoriska anmälningar och behandlingen av dem i förhållande till frivilliga underrättelser. Det ska vara möjligt att prioritera behandlingen av anmälningar till exempel när antalet frivilliga anmälningar är så stort i förhållande till tillsynsmyndighetens resurser att behandlingen av de obligatoriska anmälningarna fördröjs eller äventyras. Tillsynsmyndigheten och CSIRT-enheten ska prioritera behandlingen av obligatoriska anmälningar för att minimera de skadliga konsekvenser som betydande incidenter medför.

Genom den föreslagna bestämmelsen genomförs artiklarna 23.5 och 30.2 i NIS 2-direktivet.

17 §. *Hantering av incidentanmälningar.* I paragrafen föreskrivs det om behandlingen av incidentanmälningar, det vill säga vilka åtgärder tillsynsmyndigheten ska vidta med anledning av en incidentanmälan utöver den skyldighet att svara som föreskrivs i 16 §.

Enligt paragrafens *1 mom.* ska tillsynsmyndigheten lämna de anmälningar och rapporter som avses i 11–13 § och 15 § till CSIRT-enheten, så att enheten på begäran av en aktör kan ge kompletterande vägledning eller operativa råd i samarbete med tillsynsmyndigheten. CSIRT-enheten ska på begäran av en aktör ge vägledning eller operativa råd om begränsande åtgärder

för att minimera de negativa verkningarna. Vid behov kan anvisningar eller råd också ges i samarbete mellan tillsynsmyndigheten och CSIRT-enheten.

Med stöd av *2 mom.* ska tillsynsmyndigheten förse de behöriga myndigheterna enligt CER-direktivet med information om betydande incidenter, cyberhot och tillbud om vilka de blivit underrättade av aktörer som med stöd av CER-direktivet identifierats som kritiska.

Enligt *3 mom.* ska tillsynsmyndigheten informera dataombudsmannen om upptäckten av en incident som har lett till en sådan kränkning av personuppgiftsskyddet som avses i artikel 33 i den allmänna dataskyddsförordningen och som enligt den förordningen ska anmälas till den behöriga myndighet som övervakar skyddet av personuppgifter. Anmälan ska göras till dataombudsmannen om en omständighet som upptäckts i samband med tillsynen i Finland, även om den behöriga tillsynsmyndigheten med stöd av den allmänna dataskyddsförordningen är etablerad i en annan EU-medlemsstat. Dataombudsmannen överväger med stöd av den allmänna dataskyddsförordningen och dataskyddslagen de åtgärder som behövs i situationen.

Enligt *4 mom.* ska tillsynsmyndigheten, om en betydande incident påverkar andra EU-medlemsstater eller andra sektorer, informera den gemensamma kontaktpunkten om den betydande incidenten och sända anmälningar, rapporter och annat om den till den gemensamma kontaktpunkten. Bestämmelser om den gemensamma kontaktpunkten finns i 18 §.

Den gemensamma kontaktpunkten ska utan onödigt dröjsmål underrätta Europeiska unionens cybersäkerhetsbyrå och de medlemsstater som berörs av incidenten. Informationen till medlemsstaterna ska ske via den gemensamma kontaktpunkten för varje medlemsstat som utsetts enligt NIS 2-direktivet. Den gemensamma kontaktpunkten ska i detta syfte ha rätt att lämna information om incidentanmälningar och delrapporter och slutrapporter till den gemensamma kontaktpunkten i en annan EU-medlemsstat och till Enisa. Den gemensamma kontaktpunkten ska särskilt förse de övriga medlemsstaterna och Enisa med information som gör det möjligt att fastställa incidentens verkningar i en annan medlemsstat och de gränsöverskridande verkningarna på unionsnivå. Den gemensamma kontaktpunkten ska beakta konfidentialiteten i fråga om de uppgifter som rör aktören, säkerhets- och affärsintressen samt undvika onödigt äventyrande av dessa intressen och onödigt utlämnande av uppgifter. Den gemensamma kontaktpunktens anmälningsskyldighet omfattar med stöd av 4 § 5 mom. inte utlämnande av uppgifter vars utlämnande skulle strida mot Finlands centrala intressen i fråga om den nationella säkerheten, den allmänna säkerheten eller försvaret.

Genom den föreslagna bestämmelsen genomförs artikel 23.1 och 23.5 delvis, artikel 23.6, 23.8 och 23.10 samt artikel 13.2 och 13.3 i NIS 2-direktivet.

18 §. *Gemensam kontaktpunkt.* I paragrafen föreskrivs det om en sådan gemensam kontaktpunkt som avses i artikel 8.3 i NIS 2-direktivet. Det föreslås att Cybersäkerhetscenter vid Transport- och kommunikationsverket, som har haft en motsvarande uppgift i och med genomförandet av NIS 1-direktivet, ska vara den gemensamma kontaktpunkten i Finland.

Den gemensamma kontaktpunkten ska i första hand sköta kontakterna enligt NIS 2-direktivet med andra EU-medlemsstater och Europeiska unionens cybersäkerhetsbyrå Enisa. Den gemensamma kontaktpunkten ska ansvara för de uppgifter som ålagts den i NIS 2-direktivet när det gäller både mottagande och avsändande av anmälningar. Bestämmelser om den gemensamma kontaktpunktens roll vid behandlingen av incidentanmälningar finns i 17 § 5 mom.

Den gemensamma kontaktpunkten ska också främja samarbetet mellan de nationella tillsynsmyndigheterna för att de ska kunna utföra sina uppgifter enligt den föreslagna lagen. Den gemensamma kontaktpunkten kan främja samarbetet och informationsutbytet mellan tillsynsmyndigheterna samt ge rekommendationer till tillsynsmyndigheterna i syfte att samordna kraven och tillsynen enligt den föreslagna lagen.

Den gemensamma kontaktpunkten spelar också en central roll i kontakterna med andra EU-medlemsstater och Enisa. Dessutom ska den gemensamma kontaktpunkten var tredje månad lämna en sammanfattande rapport till Enisa om betydande incidenter, incidenter, cyberhot och tillbud som rapporterats i Finland.

Genom paragrafen genomförs artiklarna 8.3, 8.4 och 23.9 i NIS 2-direktivet.

19 §. *CSIRT-enheten.* I paragrafen föreskrivs det om den enhet enligt artiklarna 10 och 11 i NIS 2-direktivet som hanterar it-säkerhetsincidenter, dvs. CSIRT-enheten.

Enligt *1 mom.* är CSIRT-enheten i Finland en enhet vid Transport- och kommunikationsverket och dess verksamhet ska ordnas separat från de tillsynsmyndigheter som övervakar olika aktörer. CSIRT-enheten ska övervaka och analysera cyberhot, sårbarheter och incidenter och samla in information och tillhandahålla aktörerna i samhället tidiga varningar samt sköta andra, i det föreslagna 2 mom. angivna, operativa och tekniska myndighetsuppgifter som hänför sig till hanteringen av cybersäkerhetsrisker i samhället. CSIRT har till uppgift att tillhandahålla operatörerna stöd och vägledning på operativ och teknisk nivå för att förebygga, upptäcka och hantera betydande incidenter och risker och mildra deras konsekvenser, om det behövs, om en aktör begär det och om CSIRT kan tillhandahålla stöd inom ramen för sina resurser. CSIRT-enhetens uppgift är inte att övervaka aktörer som avses i denna lag, och därför ska verksamheten ordnas separat från tillsynsfunktionen vid Transport- och Kommunikationsverket. Dessutom ska CSIRT-enheten uppfylla de krav som avses i artikel 11.1 i NIS 2-direktivet, dvs. se till att bland annat kommunikationskanaler finns tillgängliga, att lokaler och de informationssystem som de använder sig av är belägna på säkra platser samt att personalen har fått tillräcklig och lämplig utbildning.

I paragrafens *2 mom.* föreskrivs det närmare om uppgifterna för CSIRT-enheten. Enligt 2 mom. *1 punkten* ska CSIRT-enheten på nationell nivå övervaka och analysera cyberhot, sårbarheter och incidenter. Den får också samla in information om dem och enligt vad situationen kräver exempelvis tillhandahålla tidiga varningar, larm, meddelanden och information om upptäckta sårbarheter. Det är fråga om allmän information som riktar sig exempelvis till i denna lag avsedda väsentliga eller viktiga aktörer eller tillsynsmyndigheter eller till andra intressentgrupper, såsom olika nätverk eller allmänheten. Uppgiften ska i mån av möjlighet genomföras samordnat med Transport- och kommunikationsverkets uppgift enligt 304 § 7 punkten i lagen om tjänster inom elektronisk kommunikation.

Enligt 2 mom. *2 punkten* ska CSIRT-enheten på begäran tillhandahålla stöd avseende realtidsövervakning eller nära realtidsövervakning av kommunikationsnät och informationssystem. Stödet kan från fall till fall avse till exempel anvisningar, råd eller tekniskt bistånd. En CSIRT-enhet kan tillhandahålla tjänster eller stöd och ge råd både till aktörer som avses i denna lag och till andra aktörer för förvärv av en tredje parts övervakningstjänster. Vid övervakningen ska det beaktas vad som särskilt föreskrivs om behandling av personuppgifter och skydd för konfidentiell kommunikation. CSIRT-enheten ska särskilt ha en styrande och rådgivande roll som inte inverkar på aktörens skyldighet att sörja för säkerheten i de kommunikationsnät och informationssystem som den använder.

Enligt 2 mom. *3 punkten* ska CSIRT-enheten reagera på incidentanmälningar och vid behov bistå den anmälande parten i incidenthanteringen. I princip kan vem som helst anmäla en incident till CSIRT-enheten, och enheten ska då reagera på dessa anmälningar. CSIRT-enheten reagerar på incidentanmälningar på ett ändamålsenligt sätt t.ex. genom att svara på dem, ge anvisningar och råd till den anmälande parten, samordna svaren på incidenter, undersöka den anmälda incidenten eller erbjuda behövligt tekniskt stöd. CSIRT-enheten ska alltså också svara på anmälningar från andra väsentliga eller viktiga aktörer än de som avses i denna lag och vid behov bistå dem i incidenthanteringen. Den som gjort anmälan ska dock huvudsakligen själv ansvara för incidenthanteringen och för att behövliga åtgärder vidtas.

Enligt 2 mom. *4 punkten* ska CSIRT-enheten samla in och analysera information om hot och om utredning av kränkningar av informationssäkerheten, dvs. forensisk information. Med forensisk information avses digitala bevis, prover, angreppsindikatorer, dvs. IOC-uppgifter, eller andra tekniska kännetecken och spår som har samband med säkerhetsincidenten. Forensisk information kan samlas in t.ex. från maskinvara, data eller loggar. Dessutom kan uppgifter om hot inhämtas till exempel från intressentgrupper.

Enligt 2 mom. *5 punkten* ska CSIRT-enheten utarbeta risk- och incidentanalyser och stödja upprätthållandet av en lägesbild över cybersäkerheten. Med stöd av 3 § i lagen om Transport- och kommunikationsverket upprätthåller Cybersäkerhetscentralen vid Transport- och kommunikationsverket en lägesbild över cybersäkerheten. CSIRT-enhetens uppgift är att stödja upprätthållandet av lägesbilden. Risk- och incidentanalyserna kan behandla antingen en enskild händelse eller mera omfattande fenomen och de kan vid behov uppdateras fortgående, dvs. vara dynamiska.

Enligt 2 mom. *6 punkten* ska CSIRT-enheten delta i det CSIRT-nätverk som avses i artikel 15 i NIS 2-direktivet. CSIRT-nätverket består av CSIRT-enheterna i alla EU-medlemsstater. Syftet med CSIRT-nätverket är att främja förtroende och tillit och ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna. CSIRT-enheten kan också, beroende på sin kapacitet och kompetens, bistå andra medlemmar i CSIRT-nätverket på deras begäran, till exempel genom att dela information om aktuella händelser, fenomen och trender eller genom att tillhandahålla tekniskt bistånd. CSIRT-enheten har till uppgift att delta i sådant samarbete i den mån det är möjligt inom ramen för dess tillgängliga resurser.

Enligt 2 mom. *7 punkten* kan CSIRT-enheten utse experter som deltar i sådana sakkunnigbedömningar som avses i artikel 19 i NIS 2-direktivet. De sakkunnigbedömningar som avses i artikel 19 i NIS 2-direktivet ska utföras av cybersäkerhetsexperter som utses på grundval av kriterier som fastställs särskilt. Det är dock frivilligt att delta i sakkunnigbedömningar, dvs. CSIRT-enheten kan bedöma behovet av att delta från fall till fall och bestämmelsen medför inte skyldighet för CSIRT-enheten att delta i bedömningar.

Enligt 2 mom. *8 punkten* ska CSIRT-enheten främja införandet av säkra verktyg för informationsutbyte. CSIRT-enheten ska ha tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med aktörer och andra relevanta intressenter. Verktygen för informationsutbyte ska uppfylla kraven i informationshanteringslagen. Eftersom den information som hanteras i dem kan vara säkerhetsklassificerad ska verktygen också uppfylla kraven i förordningen om säkerhetsklassificering av handlingar inom statsförvaltningen. När CSIRT-enheten använder sådana verktyg för informationsutbyte främjar enheten också användningen av dem i samhället i stort.

Enligt 2 mom. *9 punkten* kan CSIRT-enheten främja samarbetet med intressentgrupper inom den privata sektorn genom att ge anvisningar och rekommendationer till exempel för godkännande och användning av gemensam eller standardiserad praxis, klassificeringssystem och taxonomier. CSIRT-enheten kan ge anvisningar och rekommendationer om hantering av incidenter, krishantering inom cybersäkerheten och samordnad delgivning av information om sårbarheter.

I *3 mom.* föreskrivs det om möjligheten för CSIRT-enheten att prioritera sina uppgifter. Prioriteringen ska göras på grundval av en riskbaserad metod. Med riskbaserad metod avses i första hand att fokus läggs på risker, hot och incidenter som kan ha betydande eller omfattande skadliga verkningar i samhället eller som med stor sannolikhet kommer att realiseras. Till exempel incidentanmälningar kan klassificeras utifrån hur betydande IT-säkerhetsincidenten eller cyberhotet är, och vid denna bedömning kan man beakta till exempel angreppstypen, föremålet för incidenten eller hotet samt incidentens eller hotets omfattning.

Genom paragrafens 1–3 mom. genomförs artikel 10.1, 10.3 a–d, f och h, 10.5 samt artikel 11.1, 11.3 och 11.5 i NIS 2-direktivet.

I *4 mom.* föreskrivs det om CSIRT-enhetens uppgift att stödja frivilliga arrangemang för informationsutbyte om cybersäkerhet mellan aktörer som omfattas av tillämpningsområdet för lagen, andra parter och CSIRT-enheten. Bestämmelser om frivilliga arrangemang för informationsutbyte om cybersäkerhet finns i 22 §. Genom momentet genomförs artikel 29 i NIS 2-direktivet.

I *5 mom.* föreskrivs det om möjligheten för CSIRT-enheten att producera en tjänst för upptäckande av kränkningar av informationssäkerheten. Genom tjänsten kan aktörerna få stöd för övervakningen av informationssäkerheten i kommunikationsnät och informationssystem i realtid eller nästan i realtid. Tjänsten främjar också åtgärder för att upptäcka och utreda incidenter samt förebygga cyberhot. Bestämmelser om informationsbehandling i anslutning till tjänsten för upptäckande av kränkningar av informationssäkerheten finns i 23 §. Bestämmelsen ålägger inte någon skyldighet att producera tjänsten, utan gör det möjligt att tillhandahålla tjänsten om CSIRT-enheten anser att det behövs. CSIRT-enheten kan tillhandahålla tjänsten för upptäckande av kränkningar av informationssäkerheten direkt till de aktörer eller andra parter som begär det samt till sådana leverantörer av hanterade säkerhetstjänster som tillhandahåller aktörer eller andra parter en tjänst för upptäckande av kränkningar av informationssäkerheten i egenskap av servicecenter. Tjänsten ska tillhandahållas av CSIRT-enheten för att främja dess lagstadgade uppgift, och verksamhetsutövaren eller den som beställt tjänsten beslutar själv om den vill anlita tjänsten. I bestämmelsen är det fråga om att på lagnivå precisera befogenheten att producera en tjänst för upptäckande av kränkningar av informationssäkerheten. Cybersäkerhetscentralen vid Trafiksäkerhetsverket har producerat en tjänst för upptäckande av kränkningar av informationssäkerheten för att fullgöra sina uppgifter enligt lagen om tjänster inom elektronisk kommunikation. Genom bestämmelsen förtydligas författningsgrunden för produktionen av tjänsten. Dessutom främjar tillhandahållandet av tjänsten skötseln av CSIRT:s uppgifter.

I *6 mom.* föreslås ett bemyndigande för kommunikationsministeriet att utfärda förordning om de avgifter, eller grunderna för dem, som CSIRT-enheten kan ta ut för tjänster som avses i 2 mom. 1 och 2 punkten och som tillhandahållits på begäran av en aktör eller någon annan part. Avgiftsbelagd verksamhet kan vara till exempel riktad sårbarhetskartläggning enligt 20 § 4 mom. som gjorts på begäran samt en tjänst för upptäckande av kränkningar av informationssäkerheten och andra tjänster enligt 2 mom. 1 och 2 punkten som tillhandahålls på begäran av en aktör eller någon annan part. För en avgiftsbelagd prestation betalas en ersättning för en tjänst

som riktas till en aktör eller någon annan part och som produceras av en myndighet och som är frivillig för aktören eller parten.

20 §. *Nätbaserad kartläggning av sårbarheter i allmänna kommunikationsnät och informationssystem.* Paragrafen innehåller bestämmelser om CSIRT-enhetens rätt att observera allmänt tillgängliga kommunikationsnät, dvs. till dem anslutna kommunikationsnät och informationssystem, för att upptäcka sårbarheter och för att varna föremålet för kartläggningen om iakttagelserna (*kartläggning av sårbarheter*). I *4 mom.* föreskrivs det dessutom om riktad kartläggning av sårbarheter som utförs på aktörens begäran. Genom den föreslagna befogenheten genomförs de uppgifter som föreskrivs för CSIRT-enheten i artikel 11.3 första stycket led e och artikel 11.3 andra stycket i NIS 2-direktivet.

Syftet med sårbarhetskartläggningen är att identifiera sårbarheter, cyberhot och osäkert konfigurerade kommunikationsnät och informationssystem samt att informera berörda parter om dessa observationer, vilket förbättrar parternas möjligheter att skydda sig mot utnyttjande av sårbarheter och cyberhot.

Sårbarhetskartläggningen ska genomföras på ett proaktivt och icke-inkräktande sätt. Med proaktivt avses sambandet mellan sårbarhetskartläggningen och kända eller förutsebara sårbarheter eller cyberhot. Med icke-inkräktande karaktär avses observation av kommunikationsnät och informationssystem som är tillgängliga med hjälp av kommunikationsnät på ett sätt som inte förutsätter intrång i nätet eller informationssystemet. Vid icke-inkräktande observation kan man t.ex. skicka tekniska förfrågningar eller meddelanden i maskinläsbar form till ett kommunikationsnät eller ett informationssystem, en tjänst, dess server eller en serverapplikation, t.ex. en port, för att upptäcka öppna portar eller oskyddade tekniska lösningar i systemet. Förfrågningar kan också i syfte att avvärja sårbarheter eller cyberhot sändas för att samla in information om tekniska lösningar, såsom vilken programvara som används i kommunikationsnät och informationssystem, för att fastställa om sårbara eller oskyddade tekniska lösningar används i kommunikationsnät och informationssystem.

Som inkräktande och därmed förbjuden sårbarhetskartläggning ska betraktas åtminstone sådan verksamhet där intrång görs i kommunikationsnät och informationssystem utan den berörda aktörens samtycke genom utnyttjande av en sårbarhet. I paragrafen förutsätts det särskilt också att kartläggningen inte får medföra olägenhet för funktionen hos de berörda systemen eller tjänsterna. Det är enligt momentet också förbjudet att påverka kommunikationsnätets och informationssystemets funktion vid sårbarhetskartläggningen på ett sätt som avviker från tjänstens normala funktion eller annars orsakar störningar eller att obehörigen behandla information i kommunikationsnätet eller informationssystemet. Det är enligt förslaget alltså inte tillåtet att genomföra en sårbarhetskartläggning på dessa sätt. Till exempel ett enskilt försök med en kombination av ett känt eller på förhand känt standardanvändarnamn och lösenord till ett system för att avgöra om systemet är ändamålsenligt skyddat ska inte betraktas som ett inkräktande och därmed förbjudet intrång i kommunikationsnätet och informationssystemet, om verksamheten i kommunikationsnätet och informationssystemet inte fortsätter eller uppgifterna i systemet inte behandlas efter ett sådant försök. Det är inkräktande och därför förbjudet att upprepat testa en kombination av ett standardanvändarnamn och ett lösenord på ett sätt som gör att koderna låses av IT-säkerhetsskäl. För bedömningen av intrånget är det väsentligt vad som görs i informationssystemet. Om en sårbarhet upptäcks så att säkerhetsarrangemanget ger åtkomst till informationssystemet, ska verksamheten inte tolkas som inkräktande, i det fall att förbindelsen till informationssystemet avbryts omedelbart efter observationen och verksamheten i informations-

systemet upphör. Om man efter en sådan observation obehörigen skulle behandla vilken information som helst i informationssystemet, skulle verksamheten vara inkräktande och därmed förbjuden.

I sårbarhetskartläggningen kan man bara observera eller kartlägga kommunikationsnät och informationssystem. Det är alltså inte tillåtet att genom sårbarhetskartläggning inhämta och behandla information som omfattas av skyddet för konfidentiell kommunikation, såsom förmedlingsuppgifter eller innehållet i meddelanden där CSIRT-enheten inte är part i kommunikationen. Genom sårbarhetskartläggningen ingriper man således inte i konfidentiell kommunikation. Vid sårbarhetskartläggningen är det inte tillåtet att behandla personuppgifter som registrerats i kommunikationsnätet eller informationssystemet, eftersom en sådan behandling är inkräktande. För att genomföra kartläggning av sårbarheter har CSIRT-enheten rätt att inhämta information om identifieringsuppgifter om teleterminalutrustning och informationssystem som är kopplade till ett allmänt kommunikationsnät samt om deras datakommunikationsarrangemang, de programvaror som används och deras funktion och tekniska genomförande och de tjänster som tillhandahållits med hjälp av dem. Sårbarhetskartläggningen kan också gälla sådan nätutrustning i det allmänna kommunikationsnätet som faller under begreppet kommunikationsnät.

CSIRT-enheten får använda sådan information som upptäckts vid kartläggningen av sårbarheter endast för att informera föremålet för kartläggningen om sårbarheter och risker som riktas mot kommunikationsnätet eller informationssystemet samt för att identifiera cyberhot, upprätthålla en lägesbild över cybersäkerheten och informera om sårbarheter. Identifieringen av cyberhot omfattar också behandling av uppgifter som samlats in genom kartläggningen i syfte att hitta tidigare oidentifierade hot. Bestämmelser om Transport- och kommunikationsverkets uppgift att upprätthålla en lägesbild över den nationella cybersäkerheten finns i 3 § 1 mom. i lagen om Transport- och kommunikationsverket (935/2018). Informationen får inte innehålla uppgifter som kan kopplas till föremålet för kartläggningen, men informationen kan användas exempelvis för att rikta delgivningen. Information får dock lämnas ut i situationer som avses i 319 § 2 mom. i lagen om tjänster inom elektronisk kommunikation.

Onödig information ska utplånas utan dröjsmål. Med detta avses att information som fåtts genom kartläggningen ska bevaras endast till den del de behövs för ovan nämnda ändamål. Det hindrar inte förvaring av information som förväntas behövas för att identifiera framtida sårbarheter i materialet så att man kan reagera effektivt på dem.

Enligt det föreslagna *4 mom.* har CSIRT-enheten 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 av sårbarheter för att upptäcka en sårbarhet som kan ha en betydande inverkan på kommunikationsnätet eller informationssystemet eller de tjänster som tillhandahålls med hjälp av dem. En sådan kartläggning som CSIRT-enheten genomför på begäran och i samarbete med den berörda parten kan avvika från de villkor som anges i 1–3 mom. CSIRT-enheten är inte skyldig att på begäran utföra en kartläggning av sårbarheter, utan den kan utifrån den riskbaserade prioriteringen av uppgifterna överväga om det är ändamålsenligt att en separat sårbarhetskartläggning på begäran utförs uttryckligen av CSIRT-enheten.

I en kartläggning av sårbarheter eller en riktad kartläggning av sårbarheter får uppgifter om innehållet i elektroniska meddelanden inte behandlas. Vid en riktad kartläggning av sårbarheter har CSIRT-enheten dock rätt bedriva observation av och använda förmedlingsuppgifter, om det behövs för att upptäcka en sårbarhet, ett cyberhot eller en osäker konfiguration.

CSIRT-enheten ska utplåna den information som den fått vid kartläggningen av sårbarheter, när informationen inte längre behövs för att informera den berörda verksamhetsutövaren om sårbarheten eller för att upprätthålla en lägesbild över cybersäkerheten.

Grunden för behandling av personuppgifter vid sårbarhetskartläggning är artikel 6.1 c och e i den allmänna dataskyddsförordningen.

21 §. *Samordnad delgivning av information om sårbarheter.* I paragrafen föreskrivs det om en samordnad process för delgivning av information om sårbarheter. Genom förslaget genomförs artikel 12.1 i NIS 2-direktivet.

Enligt 1 mom. är CSIRT-enheten den samordnare för den samordnade delgivningen av informationen om sårbarheter som avses i artikel 12 i NIS 2-direktivet. För delgivning av information om sårbarheter tar CSIRT-enheten emot rapporter om upptäckta sårbarheter. Rapporter kan lämnas till CSIRT-enheten av vem som helst och även anonymt. CSIRT-enheten ska alltid säkerställa anonymitet för en fysisk eller juridisk person som rapporterar en sårbarhet, såvida inte den rapporterande personen uttryckligen samtycker till att hans eller hennes identitet avslöjas. CSIRT-enheten ska också se till att uppföljningsåtgärder vidtas med anledning av rapporterna, såsom att information om en sårbarhet lämnas till tillverkaren eller leverantören av en IKT-produkt eller IKT-tjänst och till den europeiska sårbarhetsdatabasen samt att aktören vidtar behövliga uppföljningsåtgärder med anledning av upptäckten. Europeiska unionens cybersäkerhetsbyrå Enisa förvaltar den europeiska sårbarhetsdatabasen och dess författningsgrund finns i artikel 12 i NIS 2-direktivet.

Enligt *2 mom.* ska CSIRT-enheten i egenskap av samordnare identifiera och kontakta de berörda aktörerna, stödja dem som rapporterar sårbarheter, förhandla om tidsramar för delgivning av information och hantera sårbarheter som påverkar flera aktörer. Vid behov ska CSIRT-enheten också fungera som en betrodd mellanhand mellan den som rapporterar en sårbarhet och tillverkaren eller leverantören av IKT-produkten eller IKT-tjänsten. Dessutom kan CSIRT-enheten ge vägledning och råd om hur information rapporteras till och söks i den europeiska sårbarhetsdatabasen. CSIRT-enheten har också rätt att rapportera sårbarheter som den själv har kännedom om till den europeiska sårbarhetsdatabasen. CSIRT-enheten kan till den europeiska sårbarhetsdatabasen rapportera de uppgifter om en sårbarhet som avses i 3 mom.

Enligt *3 mom.* ska CSIRT-enheten vid behov samarbeta med andra enheter inom CSIRT-nätverket, om den får kännedom om en sårbarhet som kan ha en betydande påverkan på andra EU-medlemsstater.

22 §. *Frivilliga arrangemang för informationsutbyte om cybersäkerhet.* I paragrafen finns det bestämmelser om frivilliga arrangemang för informationsutbyte om cybersäkerhet som samordnas av CSIRT-enheten. Syftet med de frivilliga arrangemangen är att utbyta cybersäkerhetsinformation mellan aktörer och CSIRT-enheten i syfte att förebygga och upptäcka cyberhot samt reagera på och återhämta sig från incidenter eller begränsa deras inverkan.

Paragrafen tillämpas endast på sådana arrangemang för informationsutbyte om cybersäkerhet som samordnas av CSIRT-enheten. Trots vad som föreskrivs i 1 mom. kan tillsynsmyndigheten inom sitt ansvarsområde stödja också andra sammanslutningar för informationsutbyte. Aktörerna kan också komma överens om att inrätta andra sådana sammanslutningar.

De som deltar i ett frivilligt arrangemang för informationsutbyte om cybersäkerhet kan särskilt utbyta den information som avses i 2 mom. De som deltar i det frivilliga arrangemanget för

informationsutbyte om cybersäkerhet kan också utbyta annan information som behövs för att avvärja cyberhot och incidenter, såsom rekommendationer om konfiguration av cybersäkerhetsverktyg som används för att upptäcka cyberattacker. Bestämmelser om möjligheten att lämna ut information om förmedlingsuppgifter eller om ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando finns i 24 § 1 mom. Parterna i arrangemanget för informationsutbyte ska trots bestämmelsen ha möjlighet att komma överens om förfaranden och tillvägagångssätt vid behandlingen av information som utbyts eller i fråga om informationens konfidentialitet.

När CSIRT-enheten stöder ett arrangemang för informationsutbyte genom att sprida cybersäkerhetsinformation till dem som deltar i arrangemanget, har en deltagande part särskild lagstadgad rätt att få ta del av den information som utbyts inom arrangemanget. Således kan de aktörer som deltar i det frivilliga arrangemanget för informationsutbyte om cybersäkerhet få informationen i fråga på det sätt som avses i 22 och 24 § i informationshanteringslagen.

Genom den föreslagna 22 § genomförs artikel 29 i NIS 2-direktivet.

23 §. *Behandling av information i anslutning till tjänsten för upptäckande av kränkningar av informationssäkerheten.* I paragrafen föreskrivs det om behandling av information i den tjänst för upptäckande av kränkningar av informationssäkerheten som avses i 19 § 5 mom., vilket behövs till den del elektroniska meddelanden eller förmedlingsuppgifter behandlas i tjänsten. Paragrafen är en specialbestämmelse i förhållande till bestämmelserna om behandling av elektroniska meddelanden och förmedlingsuppgifter i 17 kap. i lagen om elektronisk kommunikation.

Enligt *1 mom.* får en part som använder en tjänst för upptäckande av kränkningar av informationssäkerheten, servicecentret och CSIRT-enheten till varandra lämna ut information som behövs för att följa upp informationssäkerheten i kommunikationsnät och informationssystem i syfte att förebygga och upptäcka cyberhot samt reagera på och återhämta sig från incidenter eller begränsa deras inverkan. CSIRT-enheten får lämna ut uppgifter som avses i 1 mom. med hjälp av en elektronisk förbindelse eller ett tekniskt gränssnitt på det sätt som föreskrivs i 24 § i informationshanteringslagen. 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 part som använder tjänsten har begärt att ska behandlas i tjänsten och som parten har rätt att behandla med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation.

De uppgifter som lämnas ut kan alltså utöver andra uppgifter också innehålla elektroniska meddelanden som den som använder tjänsten har begärt att ska behandlas i tjänsten eller förmedlingsuppgifter i anslutning till dem i den utsträckning det är nödvändigt för att utföra tjänsten för upptäckande av kränkningar av informationssäkerheten. I tjänsten kan behandlas annan information än konfidentiell elektronisk kommunikation eller förmedlingsuppgifter, men det är nödvändigt att föreskriva särskilt om denna typ av information på grund av de begränsningar av behandlingen som föreskrivs i lagen om tjänster inom elektronisk kommunikation. Syftet med bestämmelsen är att förtydliga att denna typ av information med stöd av det föreslagna 1 mom. får lämnas ut och behandlas trots 136 § 4 mom. i lagen om tjänster inom elektronisk kommunikation, om de förutsättningar som anges i paragrafen uppfylls. Bestämmelsen förtydligar också hur behandlingen av information i tjänsten förhåller sig till förutsättningarna i 137 § i lagen om tjänster inom elektronisk kommunikation. Till de typer av information som en part har rätt att behandla med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation hör till exempel elektronisk kommunikation som begärs bli behandlad i en tjänst, förmedlingsuppgifter i

anslutning till den och andra logguppgifter eller metadata som beskriver kommunikationen samt behövliga identifieringskoder, dvs. angreppsindikatorer, som används för att identifiera kränkningar av och hot mot informationssäkerheten.

En förutsättning för utlämnande av meddelanden eller förmedlingsuppgifter är utöver nödvändighet att den aktör som använder tjänsten för upptäckande av kränkningar av informationssäkerheten har rätt att behandla informationen med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation. I 272 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om rätten för kommunikationsförmedlare och leverantörer av mervärdestjänster samt för dem som handlar för deras räkning att vidta nödvändiga åtgärder för att sörja för informationssäkerheten. De förutsättningar för behandling av information som anges i 272 § 3 och 4 mom. i lagen om tjänster inom elektronisk kommunikation ska också tilllämpas på tjänsten för upptäckande av kränkningar av informationssäkerheten. Åtgärderna ska vidtas omsorgsfullt och stå i proportion till den störning som ska avvärjas. När åtgärderna vidtas får yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet inte begränsas mer än vad som är nödvändigt. Åtgärderna ska avslutas, om det enligt paragrafen inte längre finns förutsättningar för att vidta dem.

I *2 mom.* preciseras de bestämmelser som alltid ska tillämpas vid tillhandahållandet av en tjänst oberoende av om servicecentret eller CSIRT-enheten är en leverantör av mervärdestjänster enligt lagen om tjänster inom elektronisk kommunikation eller inte. Villkoret i 1 mom. för rätten att behandla meddelanden och förmedlingsuppgifter med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation inbegriper förutsättningen att parten ska vara en sådan kommunikationsförmedlare som avses i lagen om tjänster inom elektronisk kommunikation. CSIRT-enheten har rätt att använda förmedlingsuppgifter och andra uppgifter som den fått i samband med produktionen av tjänsten för att upprätthålla en lägesbild över den nationella cybersäkerheten.

I *3 mom.* preciseras det att meddelanden och förmedlingsuppgifter som lämnats ut till CSIRT-enheten för att utföra en tjänst för upptäckande av kränkningar av informationssäkerheten också ska omfattas av vad som i 316 § 4 mom. i lagen om tjänster inom elektronisk kommunikation föreskrivs om utplåning av information om utredning av betydande kränkningar av eller hot mot informationssäkerheten och i 319 § 1 mom. om tystnadsplikt.

24 §. *Utlämnande av vissa uppgifter om cyberhot och incidenter.* Paragrafen innehåller vissa bestämmelser om utlämnande av uppgifter om cyberhot och incidenter som behövs för tillämpningen av lagen. Paragrafen är en specialbestämmelse i förhållande till lagen om tjänster inom elektronisk kommunikation.

I *1 mom.* föreskrivs det om möjligheten för en aktör eller någon annan part som deltar i ett frivilligt informationsutbyte om cybersäkerhet att trots 136 § 4 mom. i lagen om tjänster inom elektronisk kommunikation på eget initiativ till CSIRT-enheten, tillsynsmyndigheten eller någon annan part 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. För att hantera cyberhot och händelser och förebygga skadliga effekter är det nödvändigt att aktören har möjlighet att på eget initiativ lämna information om ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando och om dess förmedlingsuppgifter, särskilt till den del informationen gäller de tekniska egenskaperna och spåren hos ett skadligt datorprogram eller kommando. Bestämmelsen omfattar till exempel utlämnande av information om logguppgifter i anslutning till ett skadligt datorprogram. Aktören kan med stöd av 1 mom.

lämna ut uppgifter till tillsynsmyndigheten som en del av den obligatoriska eller frivilliga rapporteringen och till CSIRT-enheten till exempel när skadliga verkningar av en betydande incident elimineras. För att genomföra det frivilliga arrangemanget för informationsutbyte om cybersäkerhet är det nödvändigt att de som deltar i det frivilliga arrangemanget på motsvarande sätt sinsemellan kan utbyta information om skadliga datorprogram och kommandon. Om den information som utlämnas med stöd av paragrafen är personuppgifter, ska också bestämmelserna om personuppgifter i den allmänna dataskyddsförordningen och dataskyddslagen iakttas separat.

I *2 mom.* föreskrivs det att CSIRT-enheten har rätt att lämna ut information som den fått och inhämtat med stöd av den föreskrivna lagen på det sätt som föreskrivs i 319 § 2 och 3 mom. i lagen om tjänster inom elektronisk kommunikation. Bestämmelsen behövs för att CSIRT-enheten ska kunna utföra sina uppgifter. Med stöd av bland annat 319 § 3 mom. i lagen om tjänster inom elektronisk kommunikation får uppgifter lämnas ut endast i den omfattning som behövs för att förebygga och utreda kränkningar av dataskyddet, och utlämnandet får inte begränsa skyddet för konfidentiella meddelanden och integritetsskyddet mer än nödvändigt.

I *3 mom.* föreskrivs det om en begränsning av rätten att använda information. Bestämmelsen avser skydda den som frivilligt lämnar ut uppgifter till CSIRT-enheten och begränsar användningen av information som frivilligt lämnats ut till CSIRT-enheten i brottsutredningar, förvaltningsförfaranden eller annat beslutsfattande som gäller den som lämnat ut informationen. Om CSIRT-enheten i samband med skötseln av uppgifter enligt den föreslagna lagen får annan information än sådan som omfattas av rapporteringsskyldigheten enligt lagen, får sådan information inte användas i en straffprocess eller förvaltningsprocess som riktar sig mot den som frivilligt lämnat ut informationen. Bestämmelsen är nödvändig för att möjliggöra ett förtroendefullt samarbete mellan aktörerna och CSIRT-enheten i bekämpningen av skadliga effekter av cyberhot och incidenter, i synnerhet eftersom CSIRT-enheten är placerad vid Transport- och kommunikationsverket, som också sköter tillsynsmyndighetens uppgifter i fråga om vissa aktörer. Begränsningen gäller dock endast brottsutredning eller beslutsfattande som riktar sig mot den som har lämnat informationen. Begränsningen hindrar inte heller den som lämnat informationen från att själv göra till exempel en polisanmälan i ärendet. Om det är fråga om en misstänkt uppsåtlig och allvarlig lagstridig verksamhet och anmälan behövs för att avvärja ett betydande cyberhot, har CSIRT-enheten utifrån sin riskbedömning likväl rätt att på basis av informationen göra en anmälan till tillsynsmyndigheten.

Bestämmelsen motsvarar skäl 41 i NIS 2-direktivet. Där sägs det att för att stärka förtroendeförhållandet mellan aktörerna och CSIRT-enheterna ska medlemsstaterna, när en CSIRT-enhet är en del av de behörig myndighet, kunna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till aktörerna, och de behöriga myndigheternas tillsynsverksamhet. Genom den begränsning som föreskrivs för att skydda den som frivilligt lämnar ut uppgifter åtskiljs uppgifter som används i tillsynsverksamheten och i den operativa verksamheten vid CSIRT-enheten och främjas tillgodoseendet av aktörens rättsskydd.

25 §. *Tillsynsmyndigheter.* I paragrafen föreskrivs det om de myndigheter som utövar tillsyn över att lagen följs. Med tillsynsmyndighet avses i lagen den behöriga myndighet som avses i NIS 2-direktivet.

I *1 mom.* anges sektorsspecifika tillsynsmyndigheter som övervakar efterlevnaden av lagen, de bestämmelser som utfärdats med stöd av den samt de bestämmelser som utfärdats med stöd av

NIS 2-direktivet, det vill säga kommissionens genomförandeakter, i fråga om aktörerna inom respektive sektor.

Transport- och kommunikationsverket är enligt lagförslaget tillsynsmyndighet inom trafik- och rymdsektorn, i fråga om tjänster inom digital infrastruktur, IKT-tjänster, post- och budtjänster och digitala tjänster, i fråga om tillverkning av motorfordon, släpvagnar, påhängsvagnar och andra fordon samt i fråga om forskningsorganisationer.

Energimyndigheten är tillsynsmyndighet i fråga om innehavare av distributions- eller överföringsnät för el, fjärrvärme och fjärrkyla samt naturgas.

Säkerhets- och kemikalieverket är enligt lagförslaget tillsynsmyndighet i fråga om andra aktörer inom gasbranschen, aktörer inom olje- och vätgasbranschen samt i fråga om tillverkning, produktion och distribution av kemikalier samt även i fråga om tillverkning av datorer, elektronikvaror och optik, elmateriel och tillverkning av övriga maskiner.

Tillstånds- och tillsynsverket för social- och hälsovården är enligt lagförslaget tillsynsmyndighet i fråga om tillhandahållande av tjänster inom hälso- och sjukvårdssektorn.

Närings-, trafik- och miljöcentralen i Södra Savolax är tillsynsmyndighet i fråga om behandling av dricksvatten och spillvatten samt avfallshanteringstjänster.

Livsmedelsverket är tillsynsmyndighet i fråga om tillhandahållande av tjänster inom livsmedelssektorn.

Säkerhets- och utvecklingscentret för läkemedelsområdet är tillsynsmyndighet i fråga om andra tillverkare av medicintekniska produkter än tillverkare av sådana medicintekniska produkter som anses kritiska vid ett hot mot folkhälsan.

I *2 punkten* föreskrivs det om tillsynsmyndighetens uppgift. Tillsynsmyndigheten ska inom sitt ansvarsområde övervaka att den föreslagna lagen, de föreskrifter som utfärdas med stöd av den och de rättsakter som antagits med stöd av NIS 2-direktivet följs.

I *3 mom.* föreskrivs det om tillsyn i situationer där en aktör bedriver verksamhet på bred front inom flera sektorer så att fler än en myndighet med stöd av 1 mom. är behörig att utöva tillsyn över aktören. Respektive tillsynsmyndighet utövar då tillsyn över aktören endast i fråga om den verksamhet som står under dess tillsyn. Om samma aktör är verksam inom flera olika sektorer, ska tillsynen över dess olika verksamheter alltså utövas av olika tillsynsmyndigheter. Tillsynsmyndigheterna förutsätts då samarbeta för att genomföra tillsynen på ett sätt som sparar resurser för tillsynsobjektet och tillsynsmyndigheterna. Tillsynsmyndigheterna ska till exempel samordna de tillsynsåtgärder som gäller aktören i fråga och i tillämpliga delar utnyttja varandras riskbedömningar. Aktören ska inte bli föremål för överlappande tillsynsåtgärder i fråga om ett och samma ärende.

26 §. *Inriktning av tillsynen.* I enlighet med minimikraven i NIS 2-direktivet ska förhandstillsyn av efterlevnaden av den föreslagna lagen, de bestämmelser som utfärdats med stöd av den samt de bestämmelser som utfärdats med stöd av NIS 2-direktivet riktas till de väsentliga aktörerna. En väsentlig aktör definieras enligt kriterierna för en väsentlig aktör i NIS 2-direktivet. Med andra än väsentliga aktörer avses viktiga aktörer enligt NIS 2-direktivet, dvs. andra än väsentliga aktörer som omfattas av tillämpningsområdet.

Av artiklarna 32.1 och 33.1 och skäl 122 i NIS 2-direktivet framgår utgångspunkten att tillsynen delas upp i förhandstillsyn och efterhandstillsyn för de väsentliga respektive de viktiga aktörerna. De väsentliga aktörerna ska i princip omfattas av proaktiv tillsyn och de viktiga, dvs. icke väsentliga, aktörerna ska i princip endast omfattas av efterhandskontroll om det finns bevis, indikationer eller uppgifter som tyder på att de väsentliga aktörerna inte uppfyller skyldigheterna enligt NIS 2-direktivet och de bestämmelser som genomför direktivet.

Väsentliga aktörer är de aktörer som avses i bilaga I och som överskrider de trösklar som avses i definitionen av medelstora aktörer. Väsentliga aktörer är utifrån storleken således stora företag som har minst 250 anställda eller en årlig omsättning på över 50 miljoner euro och en balansräkning på över 43 miljoner euro. Om en aktör har färre än 250 anställda, men både årsomsättningen och balansräkningen överskrider trösklarna, uppfylls definitionen av medelstor aktör. När det bestäms om en aktör är en medelstor aktör ska man beakta omfattningen av aktörens verksamhet i dess helhet, inte bara i fråga om den verksamhet som avses i bilaga I.

Väsentliga aktörer är dessutom, oberoende av storlek, kvalificerade tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner, leverantörer av DNS-tjänster, aktörer som definierats som kritiska med stöd av CER-direktivet samt aktörer som har definierats som väsentliga i en statsrådsförordning som utfärdats med stöd av 3 § 2 mom.

Väsentliga aktörer är tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, om de motsvarar eller överskrider definitionen av en medelstor aktör.

Tillsynsmyndigheten kan inrikta tillsynen och åtgärder enligt 29 och 30 § gentemot andra aktörer än väsentliga aktörer, om det finns grundad anledning att misstänka att aktören i fråga inte har iakttagit den föreslagna lagen, föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet. Med grundad anledning avses bevis, indikationer eller uppgifter som tillsynsmyndigheten får kännedom om och enligt vilka aktören påstås underlåta sina lagstadgade skyldigheter, särskilt i fråga om riskhantering eller rapportering. Icke väsentliga aktörer kan i princip bli föremål för tillsyn endast om tillsynsmyndigheterna får kännedom om grundad anledning, dvs. bevis, indikationer eller uppgifter som ger anledning att misstänka att aktören inte har iakttagit den föreslagna lagen, föreskrifter som utfärdats med stöd av den eller författningar som utfärdats med stöd av NIS 2-direktivet. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som andra myndigheter, aktörer, medborgare, medier eller andra källor lämnar eller offentligt tillgänglig information eller en angivelse till tillsynsmyndigheten, om den inte är uppenbart ogrundad.

Antalet aktörer som står under tillsyn varierar sektorsvis, liksom också aktörernas betydelse för samhällets kritiska funktioner och omfattningen av de cybersäkerhetsrisker som de utsätts för. Därför är det nödvändigt att tillsynsmyndigheten utifrån en riskbaserad bedömning vid behov kan prioritera sina tillsynsuppgifter enligt den föreslagna lagen. Tillsynen, det vill säga arten och omfattningen av de tillsynsåtgärder som riktas mot aktörerna, ska vara proportionell och grunda sig på en bedömning av cybersäkerhetsriskerna. Vid bedömningen ska hänsyn tas till arten och omfattningen av de cybersäkerhetsrisker som aktörerna utsätts för, konsekvenserna för samhället av en eventuell incident, arten av aktörernas allmänna cybersäkerhetsmaturitet, tillsynsmyndigheternas tillgängliga resurser samt samarbetet med andra myndigheter. Tillsynen kan vara riskbaserad exempelvis genom att tillsynsmyndigheten utarbetar en tillsynsplan där tillsynsobjekten indelas i olika riskklasser och utifrån dem fastställer tillsynsåtgärder och deras frekvens eller vilken information som regelbundet ska begäras av aktörerna och vilka detaljkrav som ska ställas på informationen. Tillsynsmyndigheterna är dock inte skyldiga att göra upp en

tillsynsplan, utan uppgifterna kan också prioriteras på något annat sätt. Tillsynen och prioriteringen av uppgifterna ska genomföras i enlighet med artikel 31.1 och 31.2 i NIS 2-direktivet.

När tillsynsmyndigheten inriktar tillsynen och beslutar om efterlevnadskontrollåtgärder ska den beakta åtminstone arten och omfattningen av den verksamhet som avses i bilaga I eller II, dvs. till exempel hur betydande aktören är inom sektorn i fråga och vilka konsekvenser störningar i verksamheten skulle ha för samhället. Dessutom ska tillsynsmyndigheten i ärenden som gäller enskilda informationssystem eller kommunikationsnät beakta informationssystemets eller kommunikationsnätets betydelse för den verksamhet som avses i bilaga I eller II. Med tanke på lagens syften skulle sådana informationssystem och kommunikationsnät som är väsentliga med tanke på den verksamhet som avses i bilagorna till lagförslaget ha större betydelse än sådana informationssystem och kommunikationsnät vars störning inte skulle inverka på den verksamhet som avses i bilagorna. Om det exempelvis har upptäckts brister i verksamhet som bedrivs av en aktör som omfattas av lagens tillämpningsområde och aktören konstateras ha brutit mot sina skyldigheter, ska de omständigheter som anges i artikel 32.7 i NIS 2-direktivet, bland annat överträdelsens allvar och varaktighet, aktörens tidigare överträdelser, överträdelsens konsekvenser för andra tjänster samt den skada som aktören har orsakat och de åtgärder som aktören har vidtagit för att förebygga eller lindra skadan, beaktas när åtgärderna mot aktören bestäms.

I *4 mom.* föreskrivs dessutom om tillsynsmyndighetens rätt att lämna ett ärende utan prövning, om det är fråga om en uppenbart ogrundad begäran. Beslut om att lämna ett ärende utan prövning ska fattas utan dröjsmål. Momentet behövs till exempel i en situation där någon försöker störa tillsynsmyndighetens verksamhet genom att göra ogrundade anmälningar som belastar resurserna. Momentet är ett nationellt tillägg till genomförandet.

Genom paragrafen genomförs artiklarna 3.1 och 3.2, 31.1 och 31.2 samt 32.1 och 33.1 i NIS 2-direktivet.

27 §. *Tillsynsmyndighetens rätt att få information.* I paragrafen föreskrivs om den rätt att få information som tillsynsmyndigheten behöver för att fullgöra sin tillsynsuppgift.

I *1 mom.* föreskrivs det om tillsynsmyndighetens rätt att trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information få den information som är nödvändig för utförande av myndighetens uppgifter enligt lagförslaget. Utövandet av rätten att få information är den primära och huvudsakliga åtgärden som riktar sig till aktörerna och genom vilken tillsynsmyndigheten utövar tillsyn. Myndigheten har rätt att få tillgång till handlingar och uppgifter som aktören har i sin besittning, såsom en handlingsmodell för hantering av cybersäkerhetrisker, samt att få bevis på att cybersäkerhetsprinciperna har följts, såsom eventuella resultat av säkerhetsrevisioner och den bevisning som de baserar sig på, aktörens egna riskbedömningar eller logguppgifter om cyberhot och incidenter. Med hjälp av rätten att få uppgifter kan myndigheten kartlägga uppgifter om den handlingsmodell för riskhantering som gjorts och om godkännandet av den, uppgifter om utbildning för ledningen, uppgifter om upptäckta incidenter, cyberhot och tillbud, uppgifter om genomförandet av informationssäkerheten, uppgifter om genomförandet av incidenthanteringen samt uppgifter om säkerställandet av kontinuiteten i verksamheten och tjänsterna. En förutsättning för begäran om information trots sekretessbestämmelserna är att uppgifterna är nödvändiga för utförandet av tillsynsuppgiften. När tillsynsmyndigheten med stöd av bestämmelsen begär information av en aktör, ska tillsynsmyndigheten uppge syftet med begäran och precisera vilken information som begärs. Aktören ska lämna ut informationen utan dröjsmål, i den form som myndigheten begärt och avgiftsfritt.

Om en aktör som är föremål för tillsyn har lagt ut en del av eller alla sina cybersäkerhetsprocesser på underentreprenad och tillsynsmyndigheten framställer en begäran om information till aktören, är aktören skyldig att lämna informationen oberoende av om uppgiften innehas av aktören eller av den part till vilken verksamheten har lagts ut. Aktören är vid behov skyldig att skaffa den begärda informationen av sin leverantör och lämna den till tillsynsmyndigheten.

Enligt *2 mom.* har tillsynsmyndigheten trots sekretessbestämmelserna 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 samt att röja sekretessbelagd information för en annan tillsynsmyndighet och en CSIRT-enhet, om det är nödvändigt för skötseln av de uppgifter som föreskrivits för tillsynsmyndigheten eller CSIRT-enheten. Det kan vara nödvändigt att lämna ut sekretessbelagd information, såsom information som hänför sig till tryggande av informationssystemen, till en annan tillsynsmyndighet till exempel när en aktör övervakas av fler än en myndighet, och för att tillsynen ska kunna ordnas effektivt eller ändamålsenligt ska det vara möjligt att utbyta information om aktören mellan myndigheterna. Det kan vara nödvändigt att lämna ut sekretessbelagd information till CSIRT-enheten exempelvis för att utreda incidenter eller för att bistå den övervakade aktören i hanteringen av en incident. Sekretessen gäller också den myndighet som tar emot informationen. En förutsättning är dessutom att informationen är nödvändig för skötseln av ett lagstadgat uppdrag.

Genom paragrafen genomförs artikel 32.2 första stycket led e-g och delvis led d, artikel 32.3 samt artikel 33.2 första stycket led c–f och 33.3 i NIS 2-direktivet.

28 §. *Tillsynsmyndighetens rätt till information om förmedlingsuppgifter, lokaliseringsuppgifter och elektroniska meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando.*

I *1 mom.* föreskrivs det om tillsynsmyndighetens rätt till information om förmedlingsuppgifter, lokaliseringsuppgifter och elektroniska meddelanden. Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att få förmedlingsuppgifter, lokaliseringsuppgifter eller meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för att övervaka de skyldigheter som gäller hantering av cybersäkerhetsrisker eller för att utreda betydande incidenter. Bestämmelser om skyldigheten att hantera risker inom cybersäkerheten finns i 7–9 § och i fråga om vissa aktörer också i de genomförandeförordningar som kommissionen antagit med stöd av NIS 2-direktivet. Dessutom kan innehållet i riskhanteringsskyldigheterna för cybersäkerheten preciseras genom föreskrifter av tillsynsmyndigheterna. Rätten att få information gäller dessutom utredning av betydande incidenter. Med betydande incident avses en betydande incident enligt 11 § 1 mom. Med utredning av en betydande incident avses utredning av orsakerna till den betydande incidenten samt begränsning eller förebyggande av dess negativa konsekvenser. En lagstadgad separat och exakt rätt till information om dessa omständigheter behövs av de skäl som skyddet för konfidentialitet vid kommunikation förutsätter.

I *2 mom.* föreskrivs det om sekretess för samt utlämnande och utplåning av den information som avses i 1 mom. Bestämmelserna i 316 § 4 mom. och 319 § i lagen om tjänster inom elektronisk kommunikation ska tillämpas på information som tillsynsmyndigheten fått och skaffat med stöd av den föreslagna paragrafen. Informationen ska vara sekretessbelagd hos myndigheterna och får inte lämnas ut annat än under de förutsättningar som anges i lagen. I fråga om information om betydande incidenter är det i situationer som avses i 319 § 2 mom. i lagen om tjänster inom elektronisk kommunikation möjligt att lämna ut information i nödvändig utsträckning exempelvis till aktörer som kan utsättas för motsvarande kränkningar av informationssäkerheten, för att

de ska kunna förbereda sig på hotet. Av hänvisningen följer också att tillsynsmyndigheten ska utplåna de uppgifter om meddelanden, förmedlingsuppgifter och lokaliseringsuppgifter som den fått med stöd av paragrafen när uppgifterna inte längre behövs för skötseln av de uppgifter som avses i paragrafen.

Genom paragrafen genomförs delvis artikel 32.2 första stycket led f och artikel 33.2 första stycket led e i NIS 2-direktivet.

29 §. *Inspektionsrätt.* I paragrafen föreskrivs om tillsynsmyndighetens inspektionsrätt. Genom paragrafen genomförs artiklarna 32.2 första stycket led a och delvis led d, 32.4 g samt 33.2 första stycket led a och delvis led c i NIS 2-direktivet.

Enligt *1 mom.* har tillsynsmyndigheten rätt att i den omfattning det behövs förrätta inspektion av aktörer för tillsynen över att skyldigheterna enligt den föreslagna lagen eller föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet fullgörs. Inspektioner kan utföras i aktörens lokaler eller informationssystem. En inspektion i informationssystemet kan till exempel vara observation av tekniska riskhanteringsmetoder eller identifiering av svagheter i databaser, maskinvara, brandväggar, kryptering och nät. En inspektion i aktörens lokaler kan exempelvis gälla tillträdeskontroll och omständigheter som gäller lokalens säkerhet. Annan inspektion som utförs i aktörens lokaler kan också vara inspektion på basis av skriftligt material, såsom granskning av drifthandböcker, anvisningar, processbeskrivningar, utbildningsbokföring, resultaten av externa inspektioner eller annat relevant material som aktören utarbetat samt bedömning av överensstämmelse med kraven.

Tillsynsmyndigheten ska utifrån sin riskbedömning och med beaktande av de omständigheter som ska beaktas vid styrningen av tillsynen ha rätt att bestämma hur inspektioner ska riktas mot aktörerna. Inspektioner kan vara slumpmässiga, göras till följd av en betydande incident eller vara regelbundna och bygga på en riskbedömning för de aktörer som är mest kritiska med tanke på samhällets funktion. Inspektionsbefogenheten omfattar också tillsynen enligt artikel 32.4 g i NIS 2-direktivet över att aktören fullgör sina skyldigheter i fråga om riskhantering och rapportering. Inspektionen kan gälla antingen aktören som helhet eller fokusera på vissa delområden inom riskhanteringen eller aktörens verksamhet. Den som förrättar inspektionen ska ha den utbildning och erfarenhet som behövs för inspektionen.

I *2 mom.* föreskrivs det om tillsynsmyndighetens möjlighet att genom sitt beslut för inspektionen anlita eller begära att inspektionen utförs av en annan tillsynsmyndighet, ett godkänt bedömningsorgan för informationssäkerhet eller en utomstående sakkunnig inom informationsteknik, om inspektionens art eller omfattning kräver det. Myndigheten kan i ett uppdrag som anvisats ett bedömningsorgan för informationssäkerhet eller en utomstående sakkunnig bestämma vilken kompetens bedömningsorganet eller den sakkunniga förutsätts ha och vilka kriterier bedömningsorganet eller den sakkunniga ska tillämpa. Möjligheten att överföra inspektionsuppdraget på en annan myndighet eller en utomstående sakkunnig behövs när inspektionen förutsätter teknisk specialkompetens som tillsynsmyndigheten inte har. Den andra tillsynsmyndigheten är dock inte skyldig att ge handräckning för detta ändamål, utan det är fråga om myndighetssamarbete enligt 10 § i förvaltningslagen. När en utomstående sakkunnig anlitas är det till denna del fråga om överföring av en offentlig förvaltningsuppgift på en enskild, så på den sakkunniga ska strafflagens bestämmelser om tjänsteansvar tillämpas. Också kravet på utbildning och erfarenhet enligt 1 mom. tillämpas när inspektionsuppgiften överförs på en annan myndighet eller en utomstående sakkunnig. Den tillsynsmyndighet som beslutat om inspektionen svarar för kostnaderna för inspektionen.

I *3 mom.* föreskrivs det om rätten för den som utför inspektionen att få information och att i den omfattning som inspektionen kräver få tillträde till det kommunikationsnät eller informationssystem och de lokaler som inspektionen gäller. Aktören ska ge inspektören tillträde till de lokaler som behövs för inspektionen. Vilka lokaler som behövs för inspektionen beror på verksamhetens art och kan till exempel vara aktörens lokaler, produktionsanläggningar eller infrastruktur eller, i synnerhet inom transportsektorn, transportmedel. Inspektioner får inte utföras i utrymmen som är avsedda för boende av permanent natur. Inspektören kan granska de säkerhetsarrangemang som vidtagits för att skydda företagets lokaler, informationssystem och datakommunikation samt andra säkerhetsarrangemang. Den som utför en inspektion har rätt att för granskning få 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. Inspektören ska kunna utföra nödvändiga tester och mätningar, såsom intrångs- eller belastningstestning, som en del av inspektionen.

Paragrafens *4 mom.* är en materiell hänvisning enligt vilken det som i förvaltningslagen föreskrivs om inspektion också ska tillämpas på det som avses i paragrafen.

30 §. *Säkerhetsrevision.* I *1 mom.* föreskrivs om tillsynsmyndighetens rätt att genom sitt beslut ålägga en aktör att låta utföra en säkerhetsrevision som gäller hanteringen av cybersäkerhetsrisker. Det innebär en skyldighet för aktören att på egen bekostnad låta utföra en säkerhetsrevision. En förutsättning är att aktören har drabbats av en betydande incident som har orsakat en allvarlig funktionsstörning i tjänsterna eller betydande materiell eller immateriell skada eller att aktören har konstaterats väsentligt och allvarligt ha försummat hanteringen av cybersäkerhetsrisker eller i övrigt väsentligt och allvarligt handlat i strid med en skyldighet som föreskrivs i lag eller med stöd av lag eller NIS 2-direktivet. Ett åläggande att låta utföra en säkerhetsrevision kan komma i fråga endast om dess syfte inte kan nås med lindrigare medel.

I *2 mom.* föreskrivs det om tillsynsmyndighetens rätt att få information om resultatet av en säkerhetsrevision som aktören låtit utföra. I momentet föreskrivs det också om tillsynsmyndighetens rätt att genom ett beslut ålägga aktören att vidta de rimliga och proportionella åtgärder för att utveckla hanteringen av cybersäkerhetsrisker som säkerhetsrevisionen rekommenderar.

Genom paragrafen genomförs artikel 32.2 första stycket led b delvis, 32.2 första stycket led c, 32.2 andra stycket delvis, 32.2 tredje stycket och 32.4 f i NIS 2-direktivet. Genom paragrafen genomförs också artikel 33.2 första stycket led b, 33.2 andra och tredje stycket och 33.4 f i NIS 2-direktivet.

31 §. *Tillsynsbeslut, anmärkning och varning*. I *1 mom.* föreskrivs det om tillsynsmyndighetens behörighet att meddela aktören ett förpliktande beslut för att rätta till verksamhet som strider mot lag, föreskrifter som meddelats med stöd av lag eller föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan genom ett beslut ålägga aktören att inom en tidsfrist avhjälpa bristerna i fullgörandet av skyldigheterna, om det vid tillsynen upptäcks fel, försummelser eller andra brister i fullgörandet av skyldigheterna enligt den föreslagna lagen, föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan till exempel ålägga aktören att avhjälpa upptäckta brister eller försummelser, upphöra med verksamhet som strider mot bestämmelserna och i framtiden avstå från sådan verksamhet samt ålägga aktören att fullgöra sin rapporteringsskyldighet på ett bestämt sätt och inom en viss tid. Tillsynsmyndigheten kan också ålägga aktören att offentliggöra dessa brister eller andra omständigheter som har samband med överträdelser av den föreslagna lagen, föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet.

I *2 mom.* föreskrivs det om tilldelande av varning eller anmärkning. Tillsynsmyndigheten kan också ge en väsentlig aktör en anmärkning eller varning. En anmärkning eller varning är en påföljd som kan hänföra sig till ett beslut om skyldighet att avhjälpa brister, men också till ett beslut om att tillsynsprocessen avslutas utan skyldighet att avhjälpa brister.

Genom paragrafen genomförs artiklarna 32.4 a–e och h, 33.4 a–g och 21.4 i NIS 2-direktivet.

32 §. *Begränsning av tillståndspliktig eller certifierad verksamhet och återkallande av tillstånd eller certifiering.* Den begränsning av verksamheten och det återkallande av tillstånd eller certifiering som avses i paragrafen gäller endast sådana väsentliga aktörer vars verksamhet förutsätter tillstånd eller certifiering som beviljats av en myndighet. Befogenheten gör det alltså inte möjligt att begränsa eller förbjuda till exempel anmälningspliktig verksamhet. Tillsynsmyndigheten kan begränsa eller återkalla ett tillstånd eller en certifiering som den själv har beviljat. I fråga om andra aktörer som bedriver tillståndspliktig verksamhet eller verksamhet som kräver certifiering ska det fortfarande föreskrivas om begränsning av tillståndet eller certifieringen i speciallagstiftningen om verksamheten i fråga. Tillsynsmyndigheten kan dock föreslå för en annan behörig myndighet att den begränsar verksamheten eller återkallar tillståndet eller certifieringen. Behörigheten gäller endast väsentliga aktörer.

Tillsynsmyndigheten ska ge aktören en varning eller anmärkning och reservera en skälig tid att avhjälpa bristen eller försummelsen innan den fattar ett beslut eller lägger fram ett förslag till ett beslut enligt paragrafen. En begränsning av tillståndspliktig eller certifierad verksamhet eller återkallande av tillstånd eller certifiering är därför en tillsynsåtgärd som vidtas i sista hand, och före det ska tillsynsmyndigheten använda lindrigare metoder för att rätta till aktörens verksamhet. Ett återkallande av tillstånd ska bindas till allvarliga eller väsentliga förseelser eller försummelser och till att eventuella anmärkningar eller varningar till tillståndshavaren inte har lett till att bristerna i verksamheten har korrigerats. Villkoren för återkallande av tillstånd är bundna till de viktigaste skyldigheterna för väsentliga aktörer som omfattas av tillämpningsområdet för NIS 2-direktivet.

En förutsättning för begränsning av tillståndspliktig eller certifierad verksamhet och återkallande av tillstånd eller certifiering är att aktören väsentligt och allvarligt har underlåtit att iaktta sina skyldigheter. Ett exempel på en väsentlig försummelse är till exempel att aktören inte alls har skapat en sådan handlingsmodell för hantering av cybersäkerhetsrisker som avses i 8 § eller inte alls vidtagit de hanteringsåtgärder som modellen förutsätter och försummat myndighetens uppmaning eller ett förpliktande beslut om att vidta korrigerande åtgärder. En väsentlig och allvarlig försummelse av skyldigheter förutsätter också en så specificerad och entydig försummelse av en skyldighet som klart gäller aktören att det inte lämnar rum för tolkning.

Tillsynsmyndigheten ska överväga om tillståndet eller certifieringen ska återkallas temporärt eller om det räcker att delvis begränsa verksamheten. Begränsning av verksamheten bör vara det primära sättet att ingripa mot lagstridig verksamhet, och i synnerhet om aktören tillhandahåller den aktuella tjänsten eller infrastrukturen som enda aktör i Finland. I vilket fall som helst kan det föreläggas att begränsningen av verksamheten samt återkallandet av tillståndet eller certifieringen ska gälla endast en viss tid avvägd enligt hur allvarliga bristerna eller försummelserna i verksamheten är. Tidsfristen kan till exempel vara några månader. En begränsning av verksamheten och återkallande av tillstånd eller certifiering kan dock gälla högst tills behövliga åtgärder för att avhjälpa bristen eller försummelsen har vidtagits. Om bristerna inte har avhjälpts inom utsatt tid, kan tillsynsmyndigheten också besluta eller föreslå att beslut ska fattas om ändring av tillståndsvillkoren i syfte att begränsa verksamheten eller permanent återkalla tillståndet eller certifieringen.

Genom denna punkt genomförs artikel 32.5 första stycket led a i NIS 2-direktivet. Befogenheten kan endast tillämpas på väsentliga aktörer, eftersom NIS 2-direktivet inte förutsätter motsvarande tillsynsbehörighet i fråga om andra än väsentliga aktörer.

33 §. *Begränsning av ledningens verksamhet.* I paragrafen föreskrivs det om tillsynsmyndighetens befogenheter att begränsa verksamheten för de personer som hör till ledningen för en väsentlig aktör, om dessa upprepade gånger och allvarligt bryter mot sina skyldigheter enligt den föreslagna 10 §. Det är fråga om ett tidsbegränsat förbud för en enskild person att sköta de högsta ledningsuppdragen i bolaget i fråga, till vilka hör till exempel styrelsens ledamöter och suppleanter, förvaltningsrådets ledamöter och suppleanter, verkställande direktören eller något annat därmed jämförbart uppdrag samt uppdrag som är direkt underställda verkställande direktören och där de som sköter uppdraget har faktisk beslutanderätt i frågor som gäller efterlevnaden av den föreslagna lagen. Beroende på organisationsstrukturen skulle sådana uppdrag kunna åligga till exempel ekonomidirektören, den verkställande direktören, förvaltningsdirektören eller någon annan ansvarig högre ledande person. Paragrafen gäller dock inte privata näringsidkare eller personbolag, det vill säga öppna bolag eller kommanditbolag.

Begränsningen av ledningens verksamhet är en sträng påföljd, och att påföra ett förbud ska vara en exceptionell åtgärd. Innan ledningens verksamhet begränsas ska tillsynsmyndigheten ge aktören en anmärkning eller varning samt en skälig tidsfrist för att rätta till den lagstridiga verksamheten. Överträdelserna förutsätts vara upprepade och allvarliga, vilket förutsätter att aktören redan tidigare har påförts en administrativ påföljd för förseelsen eller försummelsen eller att tillsynsmyndigheten på något annat sätt har ingripit i aktörens lagstridiga eller bristfälliga verksamhet. Det är alltså fråga om en sista utväg för att förhindra att ett rättsstridigt förfarande upprepas. Tillsynsmyndigheten ska i varje enskilt fall bedöma om ett verksamhetsförbud är den mest ändamålsenliga tillsynsåtgärden.

Ledningens verksamhet får dock inte begränsas med stöd av den föreslagna paragrafen, om den väsentliga aktör är en aktör inom den offentliga förvaltningen.

Genom denna punkt genomförs artikel 32.5 första stycket led b i NIS 2-direktivet. Befogenheten kan endast tillämpas på väsentliga aktörer, eftersom NIS 2-direktivet inte förutsätter motsvarande tillsynsbehörighet i fråga om andra än väsentliga aktörer.

34 §. *Anmälan till dataombudsmannen.* NIS 2-direktivet begränsar inte tillämpningen av den allmänna dataskyddsförordningen. Tillsynsmyndigheten ska därför underrätta dataombudsmannen, om den i samband med tillsyn eller efterlevnadskontroll upptäcker en försummelse som kan leda till eller redan har lett till en sådan personuppgiftsincident som med stöd av den allmänna dataskyddsförordningen ska rapporteras till dataombudsmannen.

Anmälningsskyldigheten enligt artikel 33 i den allmänna dataskyddsförordningen ska inte tillämpas på personuppgiftsincidenter som begåtts i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster, eftersom särskild lagstiftning ska tillämpas i stället för den (Europeiska dataskyddsstyrelsens yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, punkt 44). Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska underrätta Transport- och kommunikationsverket om säkerhetsincidenter i enlighet med 275 § i lagen om tjänster inom elektronisk kommunikation och kommissionens förordning (EU) 611/2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rå-

dets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation. Således ska skyldigheten enligt paragrafen inte gälla sådana kränkningar av dataskyddet för personuppgifter som gäller televerksamhet och som kommit till Transport- och kommunikationsverkets kännedom och som verket behandlar i egenskap av behörig myndighet enligt direktivet om dataskydd vid elektronisk kommunikation.

Genom paragrafen genomförs artikel 35.1 och 35.3 i NIS 2-direktivet.

35 §. *Vite, hot om tvångsutförande och hot om avbrytande.* I paragrafen föreskrivs det om tillsynsmyndighetens möjlighet att förena ett beslut med vite, hot om tvångsutförande eller hot om avbrytande. Bestämmelser om föreläggande och verkställande av administrativa sanktioner finns i viteslagen, som ska tillämpas på åtgärden.

36 §. *Begäran om omprövning.* I paragrafen föreskrivs det om hur omprövning av tillsynsmyndighetens beslut ska begäras. Omprövning får begäras endast i fråga om beslut som tillsynsmyndigheten fattat med stöd av 30–33 § i den föreslagna lagen. Bestämmelser om begäran om omprövning finns i förvaltningslagen. I beslut som tillsynsmyndigheten har fattat med anledning av begäran om omprövning får ändring sökas på det sätt som föreskrivs i lagen om rättegång i förvaltningsärenden. Med stöd av 2 mom. kan myndigheten dock bestämma att myndighetens beslut ska iakttas trots att det inte vunnit laga kraft, om inte besvärsmyndigheten bestämmer något annat.

37 §. *Administrativ påföljdsavgift.* I paragrafen föreskrivs det om en administrativ påföljdsavgift. Påföljdsavgiften är en administrativ påföljd för överträdelse av lagen. Vid påförandet av påföljdsavgiften iakttas förvaltningslagens bestämmelser om behandling av förvaltningsärenden. Påföljdsavgiften ska påföras av en påföljdsavgiftsnämnd som består av de sektorsspecifika tillsynsmyndigheterna. Genom paragrafen genomförs tillsammans med övriga bestämmelser i 5 kap. artikel 34 i NIS 2-direktivet.

I *1 mom.* definieras de gärningar för vilka en aktör kan påföras en administrativ påföljdsavgift. Påföljdsavgift kan påföras för försummelse av riskhanteringsskyldigheten, för försummelse att vidta riskhanteringsåtgärder, för försummelse att göra obligatoriska incidentanmälningar och incidentrapporter och för försummelse att anmäla sig till förteckningen över aktörer.

I 2 mom. föreskrivs det att påföljdsavgift inte får påföras statliga myndigheter, statliga affärsverk, kommunala myndigheter, självständiga offentligrättsliga institutioner, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland, ortodoxa kyrkan i Finland och de två sistnämndas församlingar, kyrkliga samfälligheter och övriga organ. I momentet utnyttjas det nationella handlingsutrymmet enligt artikel 34.7 i NIS 2-direktivet för att offentliga aktörer inte ska åläggas de administrativa sanktioner som direktivet förutsätter.

38 §. *Påföljdsavgiftsnämnd.* I paragrafen föreskrivs det om en påföljdsavgiftsnämnd som påför en administrativ påföljdsavgift. Påföljdsavgiftsnämnden är ett nytt organ som består av medlemmar som utses av tillsynsmyndigheterna. Påföljdsavgiftsnämnden arbetar inte med uppgiften som huvudsyssla, utan den ska vid behov sammankomma för att behandla ett ärende som gäller påförande av påföljdsavgift. Påföljdsavgiften påförs på framställning av den sektorsvisa tillsynsmyndigheten.

I *1 mom.* föreskrivs det att den administrativa påföljdsavgiften påförs av påföljdsavgiftsnämnden på framställning av tillsynsmyndigheten. Tillsynsmyndigheten kan föreslå för påföljdsav-

giftsnämnden att en administrativ påföljdsavgift påförs, om den i sin tillsynsverksamhet observerar ett lagstridigt förfarande. Tillsynsmyndigheten ska i sin tillsynsverksamhet se till att ärendet utreds tillräckligt så att det i framställningen om påförande av påföljdsavgift kan inkluderas en utredning om den förseelse eller försummelse som ligger till grund för framställningen. Den administrativa påföljdsavgiften betalas till staten.

I *2 mom.* föreskrivs det om påföljdsavgiftsnämndens sammansättning. Varje tillsynsmyndighet ska utnämna en ledamot och en ersättare i nämnden. Transport- och kommunikationsverket ska utse nämndens ordförande och vice ordförande. Det allmänna behörighetsvillkoret för ledamöterna och ersättarna i påföljdsavgiftsnämnden är förtrogenhet med hantering av cybersäkerhetsrisker samt NIS 2-direktivet och de skyldigheter som ställs i den reglering som genomför direktivet inom den ifrågavarande tillsynsmyndighetens tillsynsområde. Ordföranden och vice ordföranden för nämnden förutsätts ha sådan tillräcklig juridisk sakkunskap som uppdraget förutsätter. Nämnden tillsätts för en period på tre år. Nämndens ledamöter ska agera oberoende och opartiskt i sitt uppdrag. Nämndens uppgift ska vara bisyssla för medlemmarna och ersättarna.

I *3 mom.* föreskrivs det om påföljdsavgiftsnämndens beslutsfattande. Beslut fattas efter föredragning. Föredraganden i ett ärende kommer från den tillsynsmyndighet som har tillsynsbehörighet i ärendet. Föredragande är en tjänsteman vid den tillsynsmyndighet som utövar tillsyn över den typ av aktör som det ärende som ska avgöras gäller. 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.

I *4 mom.* föreskrivs det om påföljdsavgiftsnämndens rätt till information. Nämnden har trots sekretessbestämmelserna rätt att avgiftsfritt få de uppgifter som är nödvändiga för skötseln av nämndens uppgifter. Nämnden måste kunna inhämta information om relevanta omständigheter för att påföra eller avstå från att påföra en påföljdsavgift.

39 §. *Påförande av påföljdsavgift.* I paragrafen föreskrivs det om de omständigheter som ska beaktas när en administrativ påföljdsavgift påförs. Beloppet av den administrativa påföljdsavgiften baserar sig på en helhetsbedömning där omständigheterna i fallet och de omständigheter som nämns i bestämmelsen ska beaktas. De omständigheter som ska beaktas motsvarar de omständigheter som anges i artikel 32.7 i NIS 2-direktivet och som också ska beaktas vid bedömningen av tillsynsåtgärder som gäller aktören.

När storleken på påföljdsavgiften övervägs ska det säkerställas att påföljden och dess belopp står i rätt proportion till gärningen eller försummelsen och till hur allvarlig den risk som gärningen eller försummelsen medför är och sannolikheten för att risken realiseras. Vid helhetsbedömningen ska alltså beaktas överträdelsens eller försummelsens art och omfattning, graden av klandervärdhet, gärningens varaktighet och aktörens strävan att på eget initiativ agera i enlighet med sin skyldighet. Frågan huruvida en överträdelse eller försummelse är klandervärd ska särskilt bedömas mot bakgrund av de rättsobjekt som den föreslagna lagen och NIS 2-direktivet syftar till att skydda.

Genom bestämmelsen genomförs artikel 34.3 i NIS 2-direktivet, som förutsätter att de omständigheter som avses i artikel 32.7 i NIS 2-direktivet beaktas när en administrativ påföljdsavgift påförs.

40 §. *Påföljdsavgiftens maximibelopp.* I paragrafen föreskrivs det om ett maximibelopp för den administrativa påföljdsavgiften. Den högsta administrativa påföljdsavgiften är det lägsta tillåtna

maximibeloppet enligt den nivå som förutsätts i artikel 34.4 och 34.5 i NIS 2-direktivet. Maximibeloppet är antingen i euro eller en procentandel av omsättningen beroende på vilket belopp som är högst. Maximibeloppet för en väsentlig aktör är större än för andra aktörer. Med en väsentlig aktör avses en väsentlig aktör i enlighet med 26 § 2 mom.

41 §. *Avstående från och verkställighet av påföljdsavgift.* I paragrafen föreskrivs det om avstående från och verkställighet av påföljdsavgift.

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

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

2) överträdelsen eller försummelsen ska anses vara ringa, eller

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

Grundlagsutskottet har i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljd ska vara bunden prövning, och att påföljdsavgift inte ska påföras om de villkor som anges i lag uppfylls (se GrUU 49/2017 rd och GrUU 39/2017 rd).

Syftet med bestämmelsen är att säkerställa att påföljdsavgift alltså inte påförs om den antingen med stöd av de omständigheter som avses i 1 mom. 1 eller 2 punkten eller annars med stöd av någon motsvarande omständighet eller andra omständigheter är uppenbart oskälig.

I *2 mom.* föreskrivs det om preskription av rätten att påföra påföljdsavgift. Påföljdsavgift får inte påföras, om det har förflutit mer än fem år sedan överträdelsen eller försummelsen har skett. Om överträdelsen eller försummelsen har varit fortlöpande räknas tidsfristen från det att överträdelsen eller försummelsen har upphört.

I 3 *mom.* föreskrivs det att påföljdsavgift inte får påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom. Bestämmelsen motsvarar principen ne bis in idem, det vill säga förbudet mot dubbel straffbarhet.

I *4 mom.* föreskrivs det att påföljdsavgift inte kan påföras om det vid en överträdelse eller försummelse är fråga om samma gärning för vilken det har påförts en påföljdsavgift enligt artikel 83 i den allmänna dataskyddsförordningen. Genom momentet genomförs artikel 35.2 i NIS 2-direktivet. Det kan till exempel vara fråga om brister i identifieringen eller genomförandet av behövliga riskhanteringsåtgärder eller om behandling och lagring av personuppgifter eller om förfarande som annars strider mot artikel 5 i den allmänna dataskyddsförordningen, varvid den behöriga myndigheten påför en påföljdsavgift enligt artikel 83 i den allmänna dataskyddsförordningen för kränkning av personuppgifter.

I *5 mom.* föreskrivs det om verkställigheten av påföljdsavgifter. Rättsregistercentralen svarar för verkställigheten av påföljdsavgiften. En påföljdsavgift som påförts med stöd av lag verkställs i den ordning som föreskrivs i lagen om verkställighet av böter (672/2002). Påföljdsavgiften preskriberas fem år efter det att beslutet om påförande av avgiften har vunnit laga kraft.

42 §. *Sökande av ändring.* I ett beslut om en administrativ påföljdsavgift får ändring sökas i den ordning som föreskrivs i lagen om rättegång i förvaltningsärenden.

43 §. *Förteckning över aktörer.* Genom förslaget genomförs artikel 3.3–3.6 i NIS 2-direktivet, där det förutsätts att medlemsstaterna ska föra en förteckning över väsentliga och viktiga aktörer. Bestämmelser om motsvarande skyldighet för aktörer som tillhandahåller domännamnsregistreringstjänster finns i 165 § i lagen om tjänster inom elektronisk kommunikation. Genom förslaget genomförs dessutom artikel 27 i NIS 2-direktivet, som för vissa aktörers del förutsätter att närmare uppgifter samlas in och anmäls till Enisa för det register som Enisa inrättat, samt artikel 29.4 i NIS 2-direktivet, som förutsätter en anmälan till tillsynsmyndigheten om deltagande i det frivilliga arrangemang för informationsutbyte om cybersäkerhet som avses i 22 §.

I det föreslagna *1 mom.* föreskrivs det om aktörernas skyldighet att för förande av en förteckning över aktörer lämna tillsynsmyndigheten de uppgifter som avses i artikel 3.4 i NIS 2-direktivet. Med tanke på inriktningen av tillsynen förutsätts det dessutom att det uppges om aktören är en sådan väsentlig aktör som avses i 26 §. Tillsynsmyndigheten ska med stöd av artikel 29.4 i NIS 2-direktivet också underrättas om deltagande i ett sådant frivilligt arrangemang för informationsutbyte om cybersäkerhet som avses i 22 §. När uppgifter lämnas och förteckningen över aktörer förs kan Europeiska kommissionens eller Europeiska unionens cybersäkerhetsbyrå Enisas anvisningar och mallar beaktas.

I det föreslagna *2 mom.* föreskrivs det att leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster ska lämna kompletterande uppgifter utöver de uppgifter som anges i 1 mom. Dessa aktörer förutsätts dessutom lämna de uppgifter som avses i artikel 27.2 i NIS 2-direktivet.

Med stöd av det föreslagna *3 mom.* kan tillsynsmyndigheten meddela närmare tekniska föreskrifter om hur uppgifterna ska lämnas till förteckningen över aktörer. För att underlätta upprättandet och upprätthållandet av förteckningen över aktörer ska tillsynsmyndigheten, om möjligt, ge aktören möjlighet att själv både registrera sig och uppdatera uppgifterna i förteckningen. Dessutom föreskrivs det i momentet i överensstämmelse med maximitiderna enligt artiklarna 3 och 27 i NIS 2-direktivet att ändringar i de uppgifter som avses i 1 mom. ska anmälas inom högst två veckor och i de uppgifter som avses i 2 mom. inom högst tre månader från tidpunkten för ändringen.

I det föreslagna *4 mom.* föreskrivs det om upprätthållande av den förteckning över aktörer som förutsätts i artikel 3 i NIS 2-direktivet, om anmälan till Europeiska kommissionen och NIS-samarbetsgruppen enligt artikel 3.5 i direktivet samt om lämnande av uppgifter till Enisa enligt artikel 27.4.

Enligt artikel 3.5 i NIS 2-direktivet ska tillsynsmyndigheterna senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och NIS-samarbetsgruppen om antalet väsentliga aktörer inom varje sektor och delsektor. Dessutom ska kommissionen med stöd av artikel 2.2

b–e i NIS 2-direktivet underrättas om antalet aktörer som omfattas av lagens tillämpningsområde, den sektor och delsektor som avses i bilaga I eller II, typen av tjänst som tillhandahålls samt om det led i punkten som utgör skäl för att de omfattas av tillämpningsområdet.

Med stöd av artikel 27.4 i NIS 2-direktivet ska den gemensamma kontaktpunkten utan dröjsmål vidarebefordra den information som avses i artikel 27.2 och 27.3, med undantag för den information som avses i artikel 27.2 f, dvs. aktörens IP-adressintervall, till Enisa. Tillsynsmyndigheten ska ha rätt att lämna den nationella kontaktpunkten de uppgifter som är nödvändiga för anmälan, dvs. de uppgifter som avses i artikel 27.2 och 27.3, med undantag för IP-adressintervall.

44 §. *Nationell strategi för cybersäkerhet.* I paragrafen föreskrivs det om utarbetande och uppdatering av den nationella cybersäkerhetsstrategin, om dess minimiinnehåll och om anmälan till Europeiska kommissionen. Genom förslaget genomförs artikel 7 i NIS 2-direktivet.

Med den nationella cybersäkerhetsstrategin avses i enlighet med artikel 6.4 i NIS 2-direktivet en enhetlig ram som fastställer strategiska mål och prioriteringar på cybersäkerhetsområdet och en styrningsram för att uppnå dem på nationell nivå. I enlighet med artikel 7.1 i NIS 2-direktivet ska den nationella strategin för cybersäkerhet fastställa strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå.

Den nationella strategin för cybersäkerhet ska åtminstone omfatta de aspekter som avses i artikel 7.1 och 7.2 i NIS 2-direktivet. Den nationella strategin för cybersäkerhet ska bedömas regelbundet och minst vart femte år. Strategin ska vid behov uppdateras på grundval av resultatindikatorer i enlighet med artikel 7.4 i NIS 2-direktivet. Vid utvecklingen eller uppdateringen av den nationella strategin för cybersäkerhet och de centrala resultatindikatorer som används vid bedömningen av den kan man på begäran få stöd av Europeiska unionens cybersäkerhetsbyrå Enisa.

Den nationella strategin för cybersäkerhet kan vara en självständig strategi eller en del av ett annat dokument, en annan strategi eller av statsrådets principbeslut. Förslaget innehåller således inga bestämmelser om eller begränsningar av strategins utformning. Statsrådet svarar för godkännandet och uppdateringen av den nationella strategin för cybersäkerhet och för att den delges Europeiska kommissionen.

Den nationella strategin för cybersäkerhet ska i enlighet med artikel 7.3 i NIS 2-direktivet meddelas till kommissionen inom tre månader efter det att den antagits. I meddelandet kan man utesluta information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed. Offentligheten för den nationella strategin för cybersäkerhet i övrigt bestäms enligt offentlighetslagen.

45 §. *Plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser.* I paragrafen föreskrivs det om utarbetande av en nationell plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser samt om cyberkrishanteringsmyndigheten. Genom förslaget genomförs artikel 9 i NIS 2-direktivet.

I *1 mom.* föreskrivs det om utarbetande av en nationell plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser enligt artikel 9 i NIS 2-direktivet. Transport- och kommunikationsverket svarar för utarbetandet av planen. Planen ska utarbetas i samarbete med de tillsynsmyndigheter som avses i 25 §, polisstyrelsen, skyddspolisen, Försvarsmakten och försörjningsberedskapscentralen. Även andra myndigheter kan vid behov delta i utarbetandet

av planen. Med storskalig cybersäkerhetsincident avses en incident som orsakar en så omfattande störning att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan också en annan medlemsstat.

I *2 mom.* föreskrivs det om de uppgifter som planen ska innehålla. Planen ska innehålla de uppgifter som avses i artikel 9 i NIS 2-direktivet. Syftet med bestämmelsen är inte att avgränsa vilka uppgifter som kan tas in i planen. I 2 mom. föreskrivs det dessutom om den cyberkrishanteringsmyndighet som avses i artikel 9 i NIS 2-direktivet. I Finland är respektive myndighet i enlighet med sina lagstadgade uppgifter en sådan cyberkrishanteringsmyndighet som avses i artikel 9.1 i NIS 2-direktivet. Dessa myndigheter är de tillsynsmyndigheter som avses i den föreslagna lagen, polisen, skyddspolisen, Försvarsmakten och Transport- och kommunikationsverket. Samordnare mellan cyberkrishanteringsmyndigheterna är Cybersäkerhetscentret vid Transport- och kommunikationsverket. Uppgifterna, ansvarsfördelningen och samarbetet mellan cyberkrishanteringsmyndigheterna preciseras i planen.

I *3 mom.* föreskrivs det om skyldighet att lämna uppgifter om den nationella planen för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser. I enlighet med artikel 9.5 i NIS 2-direktivet ska planen delges Europeiska kommissionen och det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) inom tre månader från det att planen antagits. I meddelandet kan man utesluta delar av planen eller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed. Offentligheten för den nationella planen för hantering av cybersäkerhetskriser i övrigt bestäms enligt offentlighetslagen.

46 §. *Myndighetssamarbete.* Paragrafen innehåller särskilda bestämmelser om samarbetet mellan myndigheterna. Ett informationsutbyte ger inte i sig rätt att avvika från sekretessbestämmelserna. Vid fastställandet av omfattningen av det nödvändiga samarbetet ska särskild vikt läggas vid tolkningen av artikel 13 i NIS 2-direktivet och dess mål. Genom paragrafen genomförs artikel 13.1, 13.4 och 13.5, artikel 32.9 och 32.10 samt artikel 33.6 i NIS 2-direktivet.

I *1 mom.* föreskrivs det om tillsynsmyndighetens och CSIRT-enhetens skyldighet att samarbeta vid fullgörandet av de uppgifter som föreskrivs i den föreslagna lagen och NIS 2-direktivet. Genom momentet genomförs tillsammans med 10 § i förvaltningslagen artikel 13.1 i NIS 2-direktivet.

I *2 mom.* föreskrivs det om tillsynsmyndighetens, CSIRT-enhetens och den gemensamma kontaktpunktens skyldighet att vid behov samarbeta med polisen eller någon annan förundersökningsmyndighet, dataombudsmannen, den myndighet som ansvarar för säkerheten inom den civila luftfarten, de tillsynsorgan som avses i eIDAS-förordningen, den behöriga myndighet som avses i DORA-förordningen, den nationella regleringsmyndighet som avses i teledirektivet och den behöriga myndighet som avses i CER-direktivet. Genom momentet genomförs tillsammans med 10 § i förvaltningslagen artikel 13.4 i NIS 2-direktivet. Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska vid behov samarbeta också med andra myndigheter, såsom Försvarsmakten och skyddspolisen, på det sätt som föreskrivs i 10 § i förvaltningslagen.

I *3 mom.* finns en specialbestämmelse om samarbete mellan tillsynsmyndigheten och den behöriga myndighet som avses i CER-direktivet.

Tillsynsmyndigheten och den behöriga myndigheten enligt CER-direktivet ska regelbundet utbyta information avseende identifieringen av kritiska aktörer, om risker, cyberhot och incidenter

samt icke-cyberrelaterade risker, hot och incidenter som berör aktörer som identifierats som kritiska i enlighet med CER-direktivet, samt om de åtgärder som vidtagits för att hantera sådana risker, hot och incidenter.

Tillsynsmyndigheterna ska underrätta den behöriga myndigheten enligt CER-direktivet när de utövar befogenheter enligt 4 kap. gentemot en aktör som identifierats som kritisk med stöd av CER-direktivet. Dessutom kan tillsynsmyndigheten på motiverad begäran av en behörig myndighet enligt CER-direktivet rikta befogenheter enligt 4 kap. gentemot en aktör som identifierats som kritisk med stöd av CER-direktivet.

Genom momentet genomförs artikel 13.5 delvis och artikel 32.9 i NIS 2-direktivet.

I *4 mom.* föreskrivs det om tillsynsmyndigheten skyldighet att informera det tillsynsforum som inrättats med stöd av artikel 32.1 i DORA-förordningen när den 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. Genom momentet genomförs artiklarna 32.10 och 33.6 i NIS 2-direktivet.

I 5 mom. föreskrivs det om skyldighet för tillsynsmyndigheten och tillsynsorganen enligt eIDAS-förordningen, den behöriga myndigheten enligt DORA-förordningen och den nationella regleringsmyndigheten enligt teledirektivet att regelbundet utbyta information om betydande incidenter och cyberhot. Genom momentet genomförs delvis artikel 13.5 i NIS 2-direktivet.

47 §. *Ikraftträdande.* Lagen föreslås träda i kraft vid den tidpunkt som anges för det nationella genomförandet i artikel 41 i NIS 2-direktivet, dvs. den 18 oktober 2024.

Det föreslås dock att lagens 43 § om aktörernas skyldighet att anmäla uppgifter till tillsynsmyndigheten träder i kraft först den 1 januari 2025, vilket ger aktörerna och tillsynsmyndigheterna en övergångsperiod och tid att upprätta en förteckning över aktörer och anmäla uppgifter till den. NIS 2-direktivet förutsätter inte att en anmälan till kommissionen angående de uppgifter som ska anmälas görs före 2025.

7.2 Lag om ändring av lagen om informationshantering inom den offentliga förvaltningen

1 §. *Lagens syfte.* Det föreslås att ett nytt *2 mom.* fogas till paragrafen. I momentet ska konstateras att NIS 2-direktivet genom lagen genomförs inom den offentliga förvaltningen. I momentet ska NIS 2-direktivet också definieras. Bestämmelser om de skyldigheter och den tillsyn över att de skyldigheter som gäller cybersäkerhet enligt direktivet iakttas inom den offentliga förvaltningen ska enligt förslaget finnas i ett nytt 4 a kap. Dessutom ska det föreslagna 2 mom. innehålla en informativ hänvisning till lagen om hantering av cybersäkerhetsrisker, det vill säga den allmänna lag genom vilken NIS 2-direktivet ska genomföras. En materiell hänvisning till den lagen ska ingå i den 18 h § som föreslås, där det ska föreskrivas om Transport- och kommunikationsverkets uppgifter.

2 §. *Definitioner*. Till paragrafen ska fogas de definitioner som krävs för genomförande av NIS 2-direktivet och som används i det nya 4 a kap., det vill säga nya punkter 17–26, av vilka de

övriga utom definitionen på betydande incident ingår i artikel 6 i direktivet. Betydande incident har definierats i artikel 23.3 i direktivet.

De nya definitioner som föreslås i informationshanteringslagen motsvarar till innehållet de motsvarande definitionerna i 2 § i den föreslagna lagen om hantering av cybersäkerhetsrisker. I detaljmotiveringarna motiveras också ändrade formuleringar av några definitioner i förhållande till direktivet. I informationshanteringslagens definitioner används begreppet myndighet i stället för aktör, eftersom de aktörer inom offentliga sektorn som det föreskrivs om i den lagen är myndigheter.

Betydande cyberhot som definieras i den föreslagna *21 punkten* har inte definierats i den föreslagna lagen om hantering av cybersäkerhetsrisker. Med betydande cyberhot avses cyberhot som på grund av dess tekniska egenskaper eventuellt kan antas kan antas ha potential att ha en allvarlig påverkan på en myndighets nätverks- och informationssystem eller användarna av dess tjänster genom att vålla betydande materiell eller immateriell skada.

En betydande incident som definieras i den föreslagna *25 punkten* har definierats i 11 § 1 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker.

Eftersom det föreslås att nya punkter fogas till paragrafen måste den föregående 16 punkten ändras så, att det inte finns någon punkt mellan punkterna.

3 §. *Lagens tillämpningsområde och begränsningar i det.* Det föreslås att paragrafen ändras så, att ett nytt 2 mom., där det föreskrivs om tillämpningsområdet för det nya 4 a kap., fogas till momentet. De gällande 3 § 2–5 mom. blir i stället 3–6 mom. Det föreslås att även paragrafens 5 mom. som gäller Åland (6 mom. efter det 2 mom. som fogas till) ändras.

I artikel 2 i direktivet föreskrivs om minimivillkoret för dess tillämplighet på aktörer inom offentlig förvaltning. Enligt artikel 2.2 f är direktivet tillämpligt om entiteten är en offentlig förvaltningsentitet i) på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller ii) på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

Enligt det föreslagna nya 2 mom. ska 4 a kap. tillämpas på statliga ämbetsverk och inrättningar som avses i 4 § 1 mom. 1 punkten, statliga affärsverk, självständiga offentligrättsliga inrättningar som avses i 4 § 1 mom. 9 punkten samt välfärdsområden, välfärdssammanslutningar och Helsingfors stad när de sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar. Dessutom ska 4 a kap. tillämpas på aktörer som med stöd av [CER-lagen] har definierats som kritiska aktörer inom offentlig förvaltning.

Den reglering som föreslås i 2 mom. täcker det minimitillämpningsområde för aktörer inom offentlig förvaltning som föreskrivs i direktivet. Statliga ämbetsverk och inrättningar, även statliga regionförvaltningsmyndigheter såsom regionförvaltningens ämbetsverk och närings-, trafik- och miljöcentraler kan enligt vår nationella lagstiftning anses vara aktörer inom offentlig

förvaltning på regional nivå som avses i direktivet. Till statliga ämbetsverk och inrättningar som avses i momentet räknas statliga ämbetsverk och inrättningar enligt 4 § 1 mom. 1 punkten i informationshanteringslagen inklusive de myndigheter som finns inom dem.

Regleringen ska också tillämpas på statliga affärsverk och på självständiga offentligrättsliga inrättningar med vissa undantag. Av affärsverk omfattas till exempel Senatsfastigheter och Forststyrelsen av tillämpningsområdet. Regleringen ska inte tillämpas på Försvarsfastigheter, eftersom dess verksamhet huvudsakligen gäller försvaret och den nationella säkerheten, såsom Försvarsmakten, som regleringen inte heller ska tillämpas på.

Självständiga offentligrättsliga inrättningar som avses i 4 § 1 mom. 9 punkten i informationshanteringslagen är bland annat Folkpensionsanstalten, Finlands Bank, Arbetshälsoinstitutet, Finlands viltcentral, Finlands skogscentral, Pensionsskyddscentralen, Keva och Kommunernas garanticentral. Av dem tillämpas 4 a kap. på de övriga utom på Finlands Bank. Regleringen ska inte tillämpas på offentligrättsliga universitet enligt universitetslagen (558/2009), eftersom universiteten nämns i en egen punkt, 4 § 1 mom. 10 punkten i informationshanteringslagen. De är alltså inte självständiga offentligrättsliga inrättningar som avses i 4 § 1 mom. 9 punkten i lagen. En offentligrättslig inrättning är en självständig offentligrättslig juridisk person som i allmänhet har inrättats genom en särskild lag i ställningen som offentligrättslig inrättning. Självständiga offentligrättsliga inrättningar har vanligen också egen ekonomi och förvaltning. Självständiga offentligrättsliga inrättningar har rättskapacitet. Offentligrättsliga inrättningar hör inte till det egentliga förvaltningsmaskineriet, men de sköter offentliga uppgifter som fastställts separat och utövar offentlig makt. De beslutar om rättigheter och skyldigheter som berör människor och deras verksamhet är lagstadgad. En inrättnings självständighet innebär närmast dess utpräglade oberoende av förvaltningsmaskineriets styrning. Deras verksamhet övervakas dock av staten. Valet mellan olika organisationsformer (till exempel statligt verk eller offentligrättslig inrättning) har varit osystematiskt och delvis slumpmässigt. Med beaktande av det ovan konstaterade bör självständiga offentligrättsliga inrättningar räknas till de aktörer inom offentlig förvaltning på regional nivå som avses i bilaga I punkt 10 i NIS 2-direktivet som direktivet i regel ska tillämpas på.

Dessutom ska välfärdsområden, välfärdssammanslutningar och Helsingfors stad höra till tillämpningsområdet för 4 a kap. De ska enligt den nationella lagstiftningen anses som offentliga aktörer på regional nivå när de utför uppgifter som hör till organiseringsansvaret för välfärdsområden. Till organiseringsansvaret för välfärdsområden, välfärdssammanslutningar och Helsingfors stad hör enligt lag social- och hälsovården samt räddningsväsendet. Vårdgivare inom offentlig och privat hälso- och sjukvård hör enligt bilaga I punkt 5 i NIS 2-direktivet till Hälso- och sjukvårdssektorn. För den ska bestämmelser om de skyldigheter och den tillsyn som det föreskrivs om i direktivet finnas i lagen om hantering av cybersäkerhetsrisker. Då kommer den reglering som föreslås i informationshanteringslagen att utvidga direktivets skyldigheter till att också gälla välfärdsområdenas och välfärdssammanslutningarnas förvaltning samt Helsingfors stads förvaltning i fråga om social- och hälsovården samt räddningsväsendet. Dessutom ska regleringen gälla myndigheterna inom socialvården och räddningsväsendet i välfärdsområden, välfärdssammanslutningar och Helsingfors stad. Att förvaltningen fungerar är en förutsättning

för att välfärdsområdena och välfärdssammanslutningarna samt Helsingfors stad ska kunna utföra de uppgifter som räknas som kritiska funktioner i samhället.

Enligt artikel 2.7 är direktivet inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Enligt skäl 8 i ingressen till direktivet bör undantaget för offentliga förvaltningsentiteter från detta direktivs tillämpningsområde ”omfatta entiteter vars verksamhet till övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet verksamhet som rör utredning, förebyggande, upptäckt och lagföring av brott. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av detta direktiv anses entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för detta direktiv.” Enligt detta ska 4 a kap. i lagen inte omfatta sådana statliga myndigheter och inrättningar som bedriver verksamhet på de nämnda områdena. Således ska 4 a kap. inte tillämpas på Försvarsmakten, Försvarsfastigheter, de polisenheter som avses i polisförvaltningslagen (110/1992) (polisenheter är enligt 1 § i den lagen Polisstyrelsen och enheter under den samt skyddspolisen), Gränsbevakningsväsendet, Tullens brottsbekämpning, Åklagarväsendet, eller på tjänsteproduktion i säkerhetsnätet och användning av dess tjänster som nämns i säkerhetsnätslagen. Den begränsning som gäller tjänsteproduktion och användning av tjänster i säkerhetsnätet innebär att 4 a kap. inte ska tillämpas på verksamhet enligt säkerhetsnätslagen i Statens center för informations- och kommunikationsteknik Valtori. På Suomen Erillisverkot Oy ska 4 a kap. inte tillämpas ens utan den begränsning som gäller säkerhetsnät, för Suomen Erillisverkot Oy hör inte till någon grupp av myndigheter som huvudregeln i början av 4 a kap. 3 § tillämpas på. Vad gäller användningen av tjänster i säkerhetsnätet innebär begränsningen att de användare av tjänsterna (till exempel republikens presidents kansli, ministerierna och Migrationsverket), som ska omfattas av tillämpningsområdet för 4 a kap., inte ska vara skyldiga att anmäla säkerhetsnätets IP-adresser eller att anmäla om incidenter i säkerhetsnätet. Transport- och kommunikationsverkets tillsynsbefogenheter eller rätt att få upplysningar och göra inspektioner ska inte heller gälla säkerhetsnätets tjänster eller användning av dem. Bestämmelser om begränsningar av rätten att få upplysningar och att göra inspektioner ska enligt förslaget också finnas i de paragrafer som gäller detta.

Enligt artikel 6.35 i direktivet räknas nationella rättsväsenden, parlament och centralbanker inte till begreppet aktörer inom offentlig förvaltning. Enligt detta omfattas inte domstolarna, nämnder som inrättats för att behandla besvärsärenden, Finlands Bank samt riksdagens riksmöte och riksdagens ämbetsverk av tillämpningsområdet för 4 a kap. Av dem nämns Finlands Bank separat i 3 § 2 mom. som en aktör som inte omfattas av tillämpningsområdet för 4 a kap. Domstolarna, nämnder som inrättats för att behandla besvärsärenden och riksdagens ämbetsverk finns som egna punkter (2 och 3 punkten) avskilda från andra statliga ämbetsverk och inrättningar i förteckningen i 4 § 1 mom. i informationshanteringslagen. De ska därför inte heller i den 3 § 2 mom. som föreslås anses som statliga ämbetsverk och inrättningar som avses i 4 § 1 mom. 1 punkten i lagen, och ska inte omfattas av tillämpningsområdet för 4 a kap.

Enligt den sista meningen i 2 mom. tillämpas inte tillsynsmyndigheters tillsynsbefogenheter eller rätt att få upplysningar och göra inspektioner på republikens presidents kansli, verksamhet som bedrivs av justitiekanslern i statsrådet eller Folkpensionsanstalten. Begränsningarna beror huvudsakligen på den ställning som dessa organisationer, som hör till offentliga sektorn, har enligt grundlagen. På grund av den ställningen kan inte styrning av myndigheter som hör till statens centralförvaltning utvidgas till styrning av dessa organisationers inre administration (t.ex. GrUU 46/2010).

Trots att det föreslås att en del av aktörerna inom offentlig förvaltning samt tjänsteproduktion och användning av tjänster i ett säkerhetsnät på det sätt som direktivet tillåter lämnas utanför tillämpningsområdet för NIS 2-regleringen utesluter detta inte rätten för de offentligrättsliga aktörerna i fråga att utnyttja till exempel CSIRT-tjänster som är avskilda från Trafik- och kommunikationsverket, vilka – och om vilkas databehandling – det föreskrivs om i lagen om hantering av cybersäkerhetsrisker. Dessutom kan dessa aktörer utanför regleringen i 4 a kap. göra frivilliga anmälningar som avses i 18 f § till Trafik- och kommunikationsverket. Bestämmelser om överlåtande av information i samband med frivilliga anmälningar finns i 18 f §.

Regleringen i det gällande 5 mom. övergår enligt förslaget till 6 mom. Till slutet av detta 6 mom. fogas en mening enligt vilken 4 a kap. i lagen ska tillämpas på statliga myndigheter i landskapet Åland, om inget annat följer av 2 mom. I NIS 2-direktivet finns reglering enligt vilken den offentliga sektorn ska utvärdera myndigheters verksamhet, varvid granskning av lagstiftningsbehörigheten mellan landskapet och riket ska grunda sig på regleringen i självstyrelselag för Åland (1144/1991, nedan självstyrelselagen) om landskapets och rikets myndigheter. I självstyrelselagen finns bestämmelser om landskapets självstyrelse och om fördelningen av lagstiftningsbehörigheten mellan landskapet och riket. I 4 kap. i lagen föreskrivs om landskapets behörighet och i 5 kap. om rikets behörighet. Enligt bestämmelserna i lagens 18 § 1 punkten i självstyrelselagen har landskapet lagstiftningsbehörighet i fråga om lagtingets organisation och uppgifter samt val av lagtingets ledamöter, landskapsregeringen och under denna lydande myndigheter och inrättningar. Enligt 27 § 3 punkten i självstyrelselagen har riket lagstiftningsbehörighet i fråga om statsmyndigheternas organisation och verksamhet. Rikets myndigheter på Åland ska anses vara aktörer på regional inom offentlig förvaltning som direktivet ska tillämpas på. Därför ska det som regleras i 4 a kap. tillämpas också på de statliga myndigheter som finns på Åland. På statliga myndigheter som också finns på Åland tillämpas enligt förslaget begränsningarna enligt 2 mom. – det vill säga 4 a kap. tillämpas till exempel inte heller på Åland på Gränsbevakningsväsendets verksamhet.

10 §. *Den offentliga förvaltningens informationshanteringsnämnd.* Det föreslås att 1 mom. 2 punkten ändras så, att informationshanteringsnämndens uppgift som gäller främjande inte ska gälla vad som föreskrivs i 4 a kap. Enligt vad som föreslås i propositionen ska Transport- och kommunikationsverket utöva tillsyn över att av bestämmelserna i 4 a kap. iakttas. Trots att informationshanteringsnämnden inte med stöd av den nämnda punkten kan ge myndigheter bindande anvisningar eller föreskrifter, och trots att dess ställningstaganden och rekommendationer med stöd av punkten inte är bindande, kan informationshanteringsnämndens främjande uppgift i fråga om 4 a kap. strida mot iakttagandet av verksamheten som tillsynsmyndighet enligt 4 a kap. och äventyra oberoendet i tillsynsmyndighetens verksamhet. Därför är det motiverat att

informationshanteringsnämndens främjande uppgift inte gäller bestämmelserna i 4 a kap. Informationshanteringsnämnden och Trafik- och kommunikationsverket ska samarbeta kring upprättandet av anvisningar och rekommendationer som gäller informationssäkerhet och cybersäkerhet så att de anvisningar de ger till de delar det behövs stämmer överens.

18 §. *Handlingar som ska säkerhetsklassificeras inom statsförvaltningen.* Det föreslås att 1 mom. ändras så, att skyldigheten att säkerhetsklassificera utvidgas till att gälla även Suomen Erillisverkot Oy och dess helägda dotterbolag när de sköter uppgifter som avses i säkerhetsnätslagen.

Informationshanteringslagen tillämpas till vissa delar även på statliga bolag med specialuppgifter som sköter offentliga förvaltningsuppgifter. Till exempel 4 kap. i lagen tillämpas på dem. På grund av innehållet i 18 § 1 mom. får dock de nämnda aktörerna inte heller för närvarande använda den säkerhetsklassificering av handlingar i den egna verksamheten som avses i informationshanteringslagen.

Ändringen innebär att Suomen Erillisverkot Oy och dess helägda dotterbolag är skyldiga att i den verksamhet som avses i säkerhetsnätslagen klassificera handlingar som har samband med deras verksamhet på samma sätt som statliga ämbetsverk och inrättningar. Behov av säkerhetsklassificering har ur informationshanteringens perspektiv uppkommit i Suomen Erillisverkot Oy, som utövar verksamhet som är kritisk med tanke på säkerhet eller beredskap. På Suomen Erillisverkot Oy och dess dotterbolag som sköter uppgifter i enlighet med säkerhetsnätslagen tillämpas enligt 19 § 1 mom. i den lagen offentlighetslagen när de sköter uppgifter som föreskrivs för dem i denna lag. De upprättar alltså handlingar som avses i offentlighetslagen och deras verksamhet samt en del av handlingarna är sekretessbelagda och betydelsefulla med tanke på Finlands säkerhet som nämns som grund för säkerhetsklassificeringen. Vid informationsutbyte och i samarbete med myndigheter som säkerhetsklassificerar handlingar är det viktigt att det finns enhetliga krav på klassificering, registrering och de förfaranden som ska iakttas vid behandlingen av dem.

4 a kap. Skyldigheter som gäller cybersäkerhet och tillsynen över att de fullgörs

Det föreslås att ett nytt 4 a kap. fogas till informationshanteringslagen där det enbart ska finnas bestämmelser om de omständigheter som genomförandet av NIS 2-direktivet kräver. Det är motiverat att placera de bestämmelser som föreslås i ett eget kapitel för att bestämmelserna i kapitlet ska gälla endast ett begränsat antal informationshanteringsenheter och myndigheter. Också den behöriga myndighetens, det vill säga tillsynsmyndighetens uppgifter, som i 4 a kap. föreslås för Transport- och kommunikationsverket och som avses i NIS 2-direktivet, ska begränsas till tillsyn över fullgörandet av de skyldigheter som föreskrivs i 4 a kap.

18 a §. *Aktörsindelning och anmälan om verksamhet.* I paragrafen ska det föreskrivas om den anmälningsskyldighet för aktörer till den behöriga myndigheten som grundar sig på artikel 3.4 och artikel 29.4 i NIS 2-direktivet. Motsvarande bestämmelser i lagen om hantering av cybersäkerhetsrisker som föreslås ska ingå i 43 § i den lagen.

Enligt artikel 3.3 i direktivet ska medlemsstaterna senast den 17 april 2025 upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år därefter se över förteckningen och när det är lämpligt att uppdatera den. Enligt artikel 3.5 a i direktivet ska de behöriga myndigheterna senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och den samarbetsgrupp som avses i artikel 14 om antalet väsentliga och viktiga entiteter som förtecknats för varje sektor och delsektor som avses i bilaga I eller II. Enligt artikel 29.4 ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter underrättar de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet som avses i artikel 29.42 när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

Enligt *1 mom.* är de informationshanteringsenheter som omfattas av tillämpningsområdet för 4 a kap. väsentliga aktörer inom offentlig förvaltning enligt punkt 10 i bilaga I till NIS 2 -direktivet, med undantag för välfärdsområdena och välfärdssammanslutningarna samt Helsingfors stad, vilka är viktiga aktörer. Enligt artikel 3.1 d i direktivet ska en entitet som är en offentlig förvaltningsentitet anses vara en väsentlig entitet som avses i direktivet. En aktör som med stöd av CER-direktivet fastställts vara en kritisk entitet ska enligt artikel 3.1 f i NIS 2-direktivet anses som en väsentlig entitet. Övriga aktörer inom offentlig förvaltning ska anses som viktiga aktörer.

Huruvida en aktör är väsentlig eller viktig påverkar det antal aktörer som kommissionen och samarbetsgruppen enligt artikel 3.5 a ska underrättas om, och huruvida de tillsyns- och efterlevnadskontrollåtgärder i fråga om väsentliga entiteter som avses i artikel 32 (förhandstillsyn) eller de tillsyns- och efterlevnadskontrollåtgärder i fråga om väsentliga entiteter (tillsyn i efterhand) som avses i artikel 33 ska gälla en aktör.

I *2 mom.* ska det föreskrivas om skyldighet för en informationshanteringsenhet att anmäla vissa uppgifter om sig själv till den behöriga myndigheten. Transport- och kommunikationsverket kan till exempel inrätta en digital tjänst för anmälan om uppgifter på sin webbplats.

En informationshanteringsenhet ska anmäla enhetens namn, adress och aktuell kontaktinformation, inklusive e-postadresser och telefonnummer. Dessutom ska aktören anmäla de IP-adressintervall som den använder. Aktören ska dessutom anmäla om den är en väsentlig eller en viktig aktör inom sektorn offentlig förvaltning, en förteckning över övriga medlemsstater i Europeiska unionen där enheten tillhandahåller sina tjänster och om den deltar i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 22 § i lagen om hantering av cybersäkerhetsrisker.

Enligt 3 mom. ska en informationshanteringsenhet utan dröjsmål, senast inom två veckor från en ändring, anmäla alla ändringar i de uppgifter som lämnats med stöd av 1 mom.

Informationshanteringsenheten ska sörja för att den för anmälningarna får de uppgifter om IP-adressintervall den behöver av den som levererar informations- och kommunikationstekniska tjänster till den. Statens center för informations- och kommunikationsteknik Valtori ska också

höra till området för anmälningsskyldighet för den del av sin verksamhet som inte gäller tjänsteproduktion i säkerhetsnätet och användning av dess tjänster. Valtori ska också sörja för att de informationshanteringsenheter som använder dess tjänster känner till de IP-adressintervall som de använder och ändringar i dem, så att de för sin del kan uppfylla anmälningsskyldigheten och hålla sina uppgifter uppdaterade. Naturligtvis kan en informationshanteringsenhet även ha egna IP-adresser för vilkas uppgifter de ansvarar självständigt. IP-adressintervall är rätt stabila, så det borde inte utgöra något större besvär att hålla uppgifterna om dem uppdaterade.

Enligt artikel 3.4 d tredje stycket ska kommissionen, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar för uppfyllande av anmälningsskyldigheterna. Tillsynsmyndigheten ska beakta kommissionens riktlinjer på ett ändamålsenligt sätt när den ger anvisningar och råd till informationshanteringsenheterna.

18 b §. *Skyldighet att hantera cybersäkerhetsrisker och handlingsmodell för hantering av cybersäkerhetsrisker.* I paragrafen föreskrivs det om hantering av cybersäkerhetsrisker och om en handlingsmodell för hantering av cybersäkerhetsrisker samt om ledningens ansvar. Bestämmelserna grundar sig på artiklarna 20–22 i direktivet. Den förteckning över riskhanteringsåtgärder för cybersäkerhet som finns i artikel 21 i direktivet ingår i 18 c §. I 7–10 § i den föreslagna lagen om hantering av cybersäkerhetsrisker föreskrivs det om de riskhanteringsskyldigheter enligt NIS 2-direktivet som motsvarar de föreslagna 18 b och 18 c § i informationshanteringslagen. I specialmotiveringen till de nämnda paragraferna i lagen om hantering av cybersäkerhetsrisker anges bland annat det som konstateras om riskhantering i direktivets skäl samt andra lämpliga exempel på riskhantering.

Enligt *1 mom.* ska en informationshanteringsenhet identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som används i dess verksamhet. I momentet beskrivs också syftet med riskhanteringen, dvs. att skydda kommunikationsnät och informationssystem, deras användare och andra personer mot cyberhot. Informationshanteringsenheten ska genom metoder för identifiering, utvärdering och hantering av riskerna försäkra sig om att säkerhetsnivån och nivån på riskhanteringsåtgärderna i de nätverks- och informationssystem som används i verksamheten är tillräcklig och proportionell i förhållande till riskerna. Bestämmelsen motsvarar i stor utsträckning det som i 13 § i informationshanteringslagen sägs om att dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Begreppet cybersäkerhet motsvarar inte helt begreppet informationssäkerhet, eftersom informationssäkerheten skyddar informationen i alla dess former – inte bara i informationssystem. På definitionsnivå inbegriper cybersäkerheten dessutom en dimension av skydd för personer, vilket visserligen också följer av genomförandet av informationssäkerheten.

Enligt det föreslagna *2 mom.* ska informationshanteringsenheten utarbeta en handlingsmodell för hantering av cybersäkerhetsrisker och hålla den uppdaterad. I handlingsmodellen ska de risker som riktas mot kommunikationsnät och informationssystem och deras fysiska miljö identifieras i enlighet med ett tillvägagångssätt som beaktar alla riskfaktorer. Dessutom ska målen, förfarandena och ansvaren för hanteringen av cybersäkerhetsrisker samt de tekniska, driftsrelaterade och organisatoriska åtgärder för hantering av cybersäkerhetsrisker som avses i 18 c §

beskrivas. Riskhanteringens mål, förfaranden och ansvar i allmänhet ska beskrivas i de riktlinjer för riskhanteringen som avses i den föreslagna 18 c § 2 mom. 1 punkten, men beskrivningen av dem betonas också i det föreslagna 18 b § 2 mom. för att beskrivningen ska utgöra ett tydligt krav oberoende av hur innehållet i riktlinjerna för riskhantering förstås. Riskhanteringen är till sin karaktär kontinuerlig, och den handlingsmodell för riskhantering som upprättas ska också hållas uppdaterad, eftersom riskerna för nät- och informationssystemens säkerhet förändras och utvecklas med tiden på samma sätt som skyddsåtgärderna.

Åtgärderna för hantering av cybersäkerhetsrisker ska bygga på en strategi som tar hänsyn till alla riskfaktorer och som syftar till att skydda nätverks- och informationssystemen och deras fysiska miljö mot händelser som stöld, brand, översvämning eller avbrott i telekommunikationen eller elförsörjningen. Riskhanteringen skyddar också nätverks- och informationssystem mot obehörig fysisk tillgång till information samt informationsmiljön mot skada och störningar som kan äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos uppgifter som lagras, överförs eller behandlas i eller hos tjänster som erbjuds genom eller är tillgängliga via kommunikationsnäten och informationssystemen.

Enligt 5 § i informationshanteringslagen ska en informationshanteringsenhet upprätthålla en informationshanteringsmodell som definierar och beskriver informationshanteringen i dess verksamhetsmiljö. Enligt den paragrafens 2 mom. 5 punkt ska informationshanteringsmodellen innehålla information om informationssäkerhetsåtgärder. Enligt 5 § 3 mom. ska man vid planeringen av väsentliga administrativa reformer som har konsekvenser för innehållet i informationshanteringsmodellen och i samband med att informationssystem tas i bruk bedöma de förändringar som hänför sig till åtgärderna och deras konsekvenser i förhållande till de bestämmelser i informationshanteringslagen som specificeras i paragrafen.

I propositionen föreslås inga bestämmelser om att cybersäkerhetsåtgärder ska inkluderas i informationshanteringsmodellen eller att bestämmelserna i 4 a kap. ska beaktas vid bedömningen av konsekvenserna av ändringar i informationshanteringsmodellen. Enligt den föreslagna regleringen ska informationshanteringsenheten dock ha dokumenterat de omständigheter som gäller hantering av cybersäkerhetsrisker och som avses i 18 b och 18 c §. Dessutom motsvarar åtgärderna i praktiken delvis de åtgärder som myndigheten ska beakta som en del av informationssäkerhetsåtgärderna enligt 4 kap. Därför är det ändamålsenligt att de informationshanteringsenheter som omfattas av tillämpningsområdet för 4 a kap. enligt prövning tar in de åtgärder som föreslås i 18 b och 18 c § i sin informationshanteringsmodell, även om det inte föreskrivs särskilt om en skyldighet till detta. Detta skulle också vara till nytta för myndigheterna, eftersom det material som definierar och beskriver deras informationshantering skulle finnas samlat i samma dokumentation.

Enligt *3 mom.* ska informationshanteringsenhetens ledning ordna genomförandet och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänna handlingsmodellen för hantering av cybersäkerhetsrisker och övervaka genomförandet av den. Informationshanteringsenheten ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

Med informationshanteringsenhetens ledning (i direktivet ledningsorganet, på engelska management body) avses den verkschef eller det ledande organ som fastställts i ämbetsverkens och inrättningarnas arbetsordningar eller i de olika aktörernas förvaltningsstadgor. Med ledning avses chefen för ett statligt ämbetsverk eller en statlig inrättning som typiskt har tjänstebenämningen generaldirektör eller överdirektör. Enligt 38 § 2 mom. i kommunallagen (410/2015) leder kommunstyrelsen kommunens verksamhet, förvaltning och ekonomi. Således ska Helsingfors stadsstyrelse i princip vara den i momentet avsedda ledningen för informationshanteringsenheten, om inte ansvaret har delegerats till något annat organ eller någon annan tjänsteinnehavare, såsom stadsdirektören, i förvaltningsstadgan. Med självständiga offentligrättsliga inrättningars ledning avses den ledning som fastställts på basis av de bestämmelser som gäller varje inrättning och som kan delegera sitt ansvar till en annan ledning.

I praktiken svarar ledningen för att hanteringen av cybersäkerhetsrisker genomförs vid informationshanteringsenheten och för att den utvecklas. Ledningen ska också se till att handlingsmodellen för hantering av cybersäkerhetsrisker, inklusive riskhanteringsåtgärderna inom cybersäkerheten, uppdateras. Dessutom ska ledningen ordna tillsynen över hanteringen av cybersäkerhetsrisker.

Aktörens ledning ska också ha tillräcklig och aktuell förtrogenhet med hantering av cybersäkerhetsrisker, vilket förutsätter förtrogenhet antingen genom utbildning eller på något annat motsvarande sätt med regelbundna intervaller. Som en del av de riskhanteringsåtgärder inom cybersäkerheten som avses i 18 c § sörjer ledningen också för att personalen får cybersäkerhetsutbildning. Syftet med utbildningen i hantering av cybersäkerhetsrisker är att ge tillräckliga kunskaper och färdigheter för att kunna identifiera riskerna och bedöma praxis för hantering av cybersäkerhetsrisker och deras inverkan på verksamheten vid informationshanteringsenheten, inklusive de tjänster som enheten tillhandahåller.

I 4 § 2 mom. i informationshanteringslagen föreskrivs en skyldighet för informationshanteringsenhetens ledning att se till att ansvaret för uppgifterna i anslutning till genomförandet av informationshanteringen har fastställts vid enheten. Ledningen ska också se till att det finns aktuella anvisningar och att det tillhandahålls utbildning för att säkerställa att personalen och de som arbetar för informationshanteringsenhetens räkning har tillräcklig kännedom om gällande författningar och föreskrifter om informationshantering, databehandling samt handlingars offentlighet och sekretess och om enhetens anvisningar på dessa områden. Vidare ska ledningen se till att det ordnats tillräcklig tillsyn över att författningarna, föreskrifterna och anvisningarna i anslutning till informationshanteringen följs. Utöver den gällande regleringen betonas i den föreslagna bestämmelsen hanteringen av cybersäkerhetsrisker i personalutbildningen samt förpliktas ledningen att också ordna sin egen utbildning för att ledningen ska ha förutsättningar att ansvara för hanteringen av cybersäkerhetsrisker och tillsynen över den.

Enligt artikel 20.1 i NIS 2-direktivet ska medlemsstaterna se till att väsentliga och viktiga aktörers ledningsorgan kan ställas till svars för aktörernas överträdelser av artikel 21. Dessutom konstateras det att tillämpningen av den punkten inte påverkar nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner, samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner. Tjänstemän kan med stöd av 40 kap. 9 eller 10 § i

strafflagen ställas till svars exempelvis för brott mot tjänsteplikt eller brott mot tjänsteplikt av oaktsamhet.

18 c §. *Åtgärder för hantering av cybersäkerhetsrisker.* I paragrafen föreskrivs det om riskhanteringsåtgärder i enlighet med artikel 21 i direktivet. I *1 mom.* föreskrivs det om informationshanteringsenhetens skyldighet att genomföra åtgärder för hantering av cybersäkerhetsrisker och fastställs på en allmän nivå vad som ska beaktas vid valet av riskhanteringsåtgärder och beskrivningen av dem i handlingsmodellen för hantering av cybersäkerhetsrisker. Enligt bestämmelsen ska åtgärderna vara lämpliga och stå i rätt proportion till riskerna för de kommunikationsnät och informationssystem som använd, kommunikationsnätets eller informationssystemets betydelse för informationshanteringsenhetens verksamhet samt de samhälleliga och ekonomiska konsekvenserna av en incident i dessa. Vid dimensioneringen av åtgärderna ska hänsyn dessutom tas till informationshanteringsenhetens storlek, verksamhetens art, 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.

Enligt skäl 83 i direktivet bör de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i direktivet tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om dessa entiteter underhåller sina nätverks- och informationssystem internt eller lägger ut underhållet på entreprenad. Informationshanteringsenheten svarar för hanteringen av cybersäkerhetsrisker och för genomförandet av proportionella riskhanteringsåtgärder också när enheten skaffar informations- och kommunikationstekniska tjänster av en utomstående leverantör. Statens center för informations- och kommunikationsteknik Valtoris verksamhet som producent och utvecklare av statens gemensamma grundläggande informationstekniktjänster och informationssystemtjänster grundar sig på lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013) och den förordning som utfärdats med stöd av den (132/2014). Valtori avtalar om de tjänster som produceras i de serviceavtal som ingås med informationshanteringsenheterna. Den föreslagna paragrafen förpliktar Valtori att genomföra riskhanteringsåtgärder för cybersäkerheten som är ändamålsenliga och proportionella i förhållande till de gemensamma grundläggande informationstekniktjänster och informationssystemtjänster som Valtori producerar. Valtori ska också beskriva dessa åtgärder i sina tjänstebeskrivningar och göra dem tillgängliga för den informationshanteringsenhet som använder tjänsten till exempel i klientlokaler där det finns också andra beskrivningar av tjänsterna, såsom konsekvensbedömningar enligt den allmänna dataskyddsförordningen.

I *2 mom.* föreskrivs det om syftet med riskhanteringsåtgärderna för cybersäkerheten och uppräknas de åtgärdshelheter som åtminstone ska ingå.

Enligt det inledande stycket i det föreslagna 2 mom. ska riskhanteringsåtgärderna för cybersäkerheten identifiera incidentrisker, förebygga, upptäcka och hantera incidenter, bidra till återhämtning efter incidenter och lindra konsekvenserna av dem. I bestämmelsen preciseras dessutom att riskhanteringsåtgärderna för cybersäkerheten skyddar kommunikationsnät och informationssystem och deras fysiska miljö mot cyberhot och incidenter samt minimerar incidenternas inverkan på informationshanteringsenhetens verksamhet, mottagarna av dess tjänster och andra tjänster.

Den förteckning i 12 punkter med åtgärder för hantering av cybersäkerhetsrisker som ges i 2 mom. motsvarar förteckningen i 9 § 2 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker. I specialmotiveringen till de bestämmelserna beskrivs innehållet i 1–12 punkten i momentet närmare. Här beskrivs endast de omständigheter i anknytning till åtgärdshelheterna som särskilt gäller den offentliga förvaltningens verksamhetsområde.

Enligt *1 punkten* ska informationshanteringsenheten som riskhanteringsåtgärd ha riktlinjer för hantering av cybersäkerhetsrisker och bedöma effektiviteten i fråga om åtgärder för hantering av cybersäkerhetsrisker. Enligt *2 punkten* ska informationshanteringsenheten också ha riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem. Bestämmelserna motsvarar delvis det som i 13 §1 mom. föreskrivs om att utifrån riskbedömningen säkerställa informationssäkerheten, även om det i 13 § inte uttryckligen förutsätts att riktlinjer för informationssäkerheten ska utarbetas.

Enligt *3 punkten* ska informationshanteringsenheten som en riskhanteringsåtgärd sörja för och i handlingsmodellen för hantering av cybersäkerhetsrisker beskriva säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter. På delvis samma sätt ska enligt 13 § 4 mom. i lagen myndigheten vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga informationssäkerhetsåtgärder.

I *4 punkten* förutsätts det att säkerheten i leveranskedjorna tryggas som en åtgärdshelhet inom riskhanteringen. Enligt artikel 22 i direktivet får den samarbetsgrupp som avses i artikel 14, i samarbete med kommissionen och Enisa, utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter, med beaktande av tekniska och, i relevanta fall, icke-tekniska riskfaktorer. Dessa bedömningar av säkerhetsrisker kan också gälla den offentliga förvaltningen. I den mån sådana riskbedömningar har gjorts ska informationshanteringsenheten utnyttja dem i tillämpliga delar.

Enligt *5 punkten* omfattar riskhanteringsåtgärderna tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på säkerheten.

Enligt *6 punkten* ska enheten sörja för personalsäkerheten och cybersäkerhetsutbildningen. Bestämmelser om personalsäkerhetsfrågor och personalutbildning finns också bland annat i 4 § 2 mom. och 12 § i informationshanteringslagen.

I *punkt 7* förutsätts att informationshanteringsenheten sörjer för förfarandena för åtkomsthantering och autentisering. Informationshanteringsenheten ska vid behov använda lösningar för stark identifiering och autentisering, multifaktorautentisering eller kontinuerlig autentisering. Också 14, 16 och 17 § i informationshanteringslagen anknyter till åtkomsthantering och förfaranden för autentisering.

Enligt *punkt 8* förutsätts enheten ha riktlinjer och förfaranden för kryptering samt vid behov för en säker elektronisk kommunikation. I informationshanteringslagen anknyter särskilt 14 § till krypteringsmetoder.

I *punkt 9* förutsätts upptäckande och hantering av incidenter i syfte att upprätthålla och återställa säkerheten och driftsäkerheten.

I *punkt 10* förutsätts säkerhetskopiering, katastrofhantering, krishantering och annan driftskontinuitet. Syftet med 13 a § i informationshanteringslagen är i stor utsträckning detsamma – dvs. att föreskriva om behandlingen av informationsmaterial, utnyttjandet av informationssystem och verksamhetens kontinuitet. Enligt 13 a § ska en informationshanteringsenhet utreda väsentliga risker som hänför sig till behandlingen av informationsmaterial, utnyttjandet av informationssystem och verksamhetens kontinuitet. Utifrån riskbedömningen ska informationshanteringsenheten genom beredskapsplaner och förberedelser för verksamhet i störningssituationer samt genom andra åtgärder se till att behandlingen av informationsmaterial, utnyttjandet av informationssystem och verksamheten fortsätter så störningsfritt som möjligt i störningssituationer under normala förhållanden samt under undantagsförhållanden som avses i beredskapslagen. I den föreslagna 10 punkten nämns dessutom på samma sätt som i NIS 2-direktivet särskilt att informationshanteringsenheten som en del av kontinuitetshanteringen vid behov ska sörja för tillgången till säkrade reservkommunikationssystem.

I den föreslagna *punkt 11* förutsätts grundläggande praxis för cyberhygien för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet. Praxis för cyberhygien nämns inte särskilt i informationshanteringslagen, men ingår åtminstone delvis i skyldigheten enligt 13 § att säkerställa säkerheten för informationsmaterialen genom informationssäkerhetsåtgärder som grundar sig på riskhantering.

Enligt den föreslagna *12 punkten* ska informationshanteringsenheten vidta och med stöd av 18 b § beskriva åtgärderna för att skydda kommunikationsnätens och informationssystemens fysiska miljö och säkerställa säkerheten i lokalerna samt nödvändiga resurser. Enligt 15 § i informationshanteringslagen ska informationsmaterial behandlas och förvaras i verksamhetslokaler som är tillräckligt säkra för att tillgodose kraven på tillförlitlighet, integritet och tillgänglighet.

Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019) innehåller dessutom mer detaljerade krav på hanteringen av säkerhetsklassificerade handlingar än vad som anges i de ovan nämnda punkterna 1–12.

18 d §. *Skyldighet att anmäla betydande incidenter.* I paragrafen föreskrivs det om myndighetens skyldighet att i tre steg rapportera betydande incidenter till den myndighet som utövar tillsyn över den offentliga förvaltningen, dvs. Transport- och kommunikationsverket. Paragrafen grundar sig på artikel 23 i direktivet. Bestämmelser om anmälningsskyldigheten i fråga om de övriga sektorerna i direktivets bilagor finns i 11–13 § i lagen om hantering av cybersäkerhetsrisker. Motiveringarna till de paragraferna innehåller kompletterande exempel i anknytning till incidentanmälningar.

I *1 mom.* föreskrivs det om rapporteringens första fas, det vill säga den första anmälan som myndigheten ska lämna utan obefogat dröjsmål och senast inom 24 timmar efter att ha fått kännedom om den betydande incidenten. I den första anmälan ska det anges om den betydande

incidenten misstänks bero på en olaglig eller avsiktligt skadlig handling och om den kan ha gränsöverskridande verkningar samt sannolikheten för sådana verkningar. Det är fråga om en slags tidig varning som endast bör innehålla den information som är nödvändig för att Transport- och kommunikationsverket ska få kännedom om en betydande incident och för att den berörda aktören vid behov ska kunna begära hjälp. Anmälningsskyldigheterna enligt denna paragraf, särskilt den första anmälan och den i 2 mom. avsedda uppföljande anmälan, ska fullgöras endast i sådan omfattning att åtgärder för att hantera incidenten kan vidtas effektivt. Syftet med den slutrapport som avses i 3 mom. är att ge tillsynsmyndigheten och aktören värdefulla erfarenheter av incidenten och att med tiden förbättra både aktörens och den offentliga förvaltningens och andra sektorers cyberresiliens.

Den tidsgräns på 24 timmar som nämns i bestämmelsen räknas från det att myndigheten har fått kännedom om en betydande incident. Tidpunkten för när myndigheten får kännedom om incidenten kan bero på om incidenten inträffar under tjänstetid eller på natten eller under ett veckoslut. Bestämmelsen förpliktar inte myndigheten att ordna jour dygnet runt för att kunna göra en första anmälan. Behovet av jour samt föremålet för och omfattningen av jouren ska enligt 18 b och 18 c § bedömas i myndigheternas riskhantering.

Myndigheten ska se till att dess underleverantör lämnar myndigheten de uppgifter som behövs för en incidentanmälan och samarbetar med myndigheten så att myndigheten kan fullgöra sina skyldigheter i fråga om en incidentanmälan. En privat underleverantör kan omfattas av anmälningsskyldigheten enligt den allmänna lagen, om den tillhandahåller IKT-tjänster eller digitala infrastrukturtjänster enligt bilagorna till direktivet. Detta undanröjer dock inte myndighetens att anmäla incidenten till tillsynsmyndigheten för den offentliga förvaltningens verksamhetsområde.

Statens center för informations- och kommunikationsteknik Valtori har en självständig anmälningsskyldighet när det gäller betydande incidenter i anknytning till statens gemensamma informations- och kommunikationstekniska tjänster. Valtori är skyldigt att anmäla incidenten till de användarmyndigheter som berörs av incidenten, så att dessa myndigheter för sin del kan göra en anmälan till Transport- och kommunikationsverket. Enbart en anmälan från Valtoris är inte tillräcklig i fråga om den myndighet som anlitar tjänsten, eftersom Valtori inte nödvändigtvis kan bedöma de omständigheter som förutsätts i anmälan, såsom de slutliga verkningarna av incidenten inklusive eventuella gränsöverskridande verkningar. Valtoris anmälningsskyldighet gäller endast dess egen verksamhet och gäller inte betydande incidenter i de sektorbundna informationssystemen hos den myndighet som anlitar dess tjänster, om inte incidenten yppar sig också i Valtoris tjänst.

I *2 mom.* föreskrivs det om rapporteringens andra fas, det vill säga den uppföljande anmälan som myndigheten ska lämna utan obefogat dröjsmål och senast inom 72 timmar från det att myndigheten fått kännedom om den betydande incidenten. I den uppföljande anmälan ska myndigheten uppdatera de uppgifter som lämnats i den första anmälan och lägga fram en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och verkningar samt angreppsindikatorer (Indicator of Compromise, IOC), om sådana finns tillgängliga. Den första anmälan

och den uppföljande anmälan kan göras på en och samma gång, om myndigheten inom tidsfristen för den första anmälan, dvs. utan dröjsmål och senast inom 24 timmar från det att incidenten upptäckte, har de uppgifter som förutsätts i båda anmälningarna.

I paragrafens *3 mom.* föreskrivs det om en slutrapport om en betydande incident. Slutrapporten ska lämnas senast en månad efter den uppföljande anmälan. Slutrapporten ska innehålla en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser. Slutrapporten ska också innehålla en beskrivning av vilken typ av hot eller grundorsak som sannolikt har utlöst incidenten samt vilka åtgärder som genomförts och håller på att genomföras för att mildra konsekvenserna. Om en incident har gränsöverskridande konsekvenser, ska också dessa beskrivas.

Enligt det föreslagna *4 mom.* ska en delrapport lämnas i stället för en slutrapport, om incidenten fortfarande pågår när den slutrapport som avses i 3 mom. ska lämnas in. Slutrapporten ska därefter lämnas in inom en månad efter det att myndigheten har behandlat incidenten. Syftet med delrapporten är att beskriva hur incidenthanteringen framskrider, incidentens verkningar och andra väsentliga faktorer som hänför sig till konsekvenserna av händelsen samt ändringar i uppgifterna i den första anmälan och den uppföljande anmälan. Om en incident fortgår kan Transport- och kommunikationsverket begära ytterligare information av myndigheten eller en delrapport om statusuppdateringar i ärendet och om hur hanteringen framskrider.

18 e §. *Mottagande av incidentanmälan.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets svar på en incidentanmälan. Paragrafen grundar sig på artikel 23.5 i direktivet.

Enligt paragrafen ska Transport- och kommunikationsverket svara myndigheten utan obefogat dröjsmål och om möjligt inom 24 timmar från mottagandet av den första anmälan som avses i 18 d § 1 mom. Det förutsätter dock inte jour under veckoslut, nätter eller söckenhelger. Svaret ska innehålla initial återkoppling om den betydande incidenten och, på myndighetens begäran, anvisningar eller operativa råd om hanteringen av incidenten samt anvisningar om hur en betydande incident ska anmälas till förundersökningsmyndigheten, om det finns misstanke om brott. Enligt artikel 23.5 i NIS 2-direktivet ska den behöriga myndigheten, om CSIRT-enheten inte är mottagaren av anmälan, utfärda instruktioner i samarbete med CSIRT-enheten. Den i NIS 2-direktivet avsedda CSIRT-enheten vid Transport- och kommunikationsverket ska på behövligt sätt delta i behandlingen av incidentanmälan.

18 f §. *Frivillig underrättelse.* I paragrafen föreskrivs det om möjlighet för myndigheter och andra aktörer inom den offentliga förvaltningen att också frivilligt underrätta Transport- och kommunikationsverket om incidenter, cyberhot och tillbud. Paragrafen grundar sig på artikel 30 i direktivet. I den föreslagna lagen om hantering av cybersäkerhetsrisker föreskrivs det om frivillig underrättelse i 15 §.

Enligt skäl 105 i direktivet är en proaktiv strategi mot cyberhot en viktig del av riskhanteringsåtgärderna för cybersäkerhet som bör göra det möjligt för de behöriga myndigheterna att effektivt förhindra att cyberhot blir incidenter som kan vålla betydande materiell eller immateriell skada.

Det är därför av avgörande vikt att cyberhot anmäls. I detta syfte uppmuntras aktörer att rapportera cyberhot på frivillig basis.

Enligt *1 mom.* kan myndigheten underrätta Transport- och kommunikationsverket också om andra än betydande incidenter samt om cyberhot och tillbud. Också andra i 3 § i informationshanteringslagen avsedda samfund och personer som inte omfattas av anmälningsskyldigheten kan underrätta verket om betydande incidenter, incidenter, cyberhot och tillbud.

Enligt 304 § 7 punkten i lagen om tjänster inom elektronisk kommunikation ska Transport- och kommunikationsverket samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem samt om fel och störningar i kommunikationsnät och kommunikationstjänster. Transport- och kommunikationsverket tar redan i nuläget emot och behandlar rapporter om kränkningar av och hot mot informationssäkerheten och behandlar dem i den mån dess resurser tillåter. Avsikten med bestämmelsen är inte att begränsa den beskrivna möjligheten att frivilligt underrätta Transport- och kommunikationsverket. I direktivet förutsätts det dock att dessa frivilliga underrättelser i princip behandlas på samma sätt som de anmälningar som omfattas av anmälningsskyldigheten enligt 18 d §.

Om en incident har gränsöverskridande verkningar ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i tillämpliga fall och särskilt om den betydande incidenten berör minst två medlemsstater, utan onödigt dröjsmål informera de övriga berörda medlemsstaterna och Enisa om den betydande incidenten (artikel 23.6). Den gemensamma kontaktpunkten ska dessutom var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats på basis av anmälningsskyldighet eller frivilligt (artikel 23.9). Bestämmelser om dessa samarbetsskyldigheter finns i 17 och 18 § i lagen om hantering av cybersäkerhetsrisker, och det hänvisas till dessa skyldigheter i det föreslagna 18 h § 3 mom. i informationshanteringslagen.

Enligt *2 mom.* ska Transport- och kommunikationsverket behandla frivilliga underrättelser med iakttagande av det förfarande som anges i 18 e §, men verket får prioritera behandlingen av anmälningar som avses i 18 d § framför behandlingen av frivilliga underrättelser.

I *3 mom.* föreskrivs det om utlämnande av information i samband med frivillig underrättelse. Myndigheter och andra som nämns i 3 § kan i samband med en frivillig underrättelse till Transport- och kommunikationsverket lämna ut sådan information som verket har rätt att få med stöd av 18 i § 1 och 2 mom. På utlämnande av uppgifter tillämpas också vad som i 18 i § 3 mom. föreskrivs om utlämnande av vissa sekretessbelagda uppgifter.

18 g §. *Informationsskyldighet om betydande cyberhot och incidenter.* I paragrafen föreskrivs det om informationshanteringsenhetens skyldighet att informera om betydande cyberhot mot och incidenter i anknytning till dess tjänster. Paragrafen grundar sig på artikel 23.1, 23.2 och 23.7 samt artikel 32.4 e i NIS 2-direktivet. I lagen om hantering av cybersäkerhetsrisker finns motsvarande bestämmelser i 14 §.

Enligt paragrafens *1 mom.* ska en myndighet 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 enligt *2 mom.* 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.

I *3 mom.* föreskrivs det om en situation där det ligger i allmänt intresse att en betydande incident offentliggörs. Det är till exempel fråga om en situation av allmänt intresse när allmänhetens medvetenhet behövs för att förhindra en betydande incident eller för att hantera en pågående betydande incident. Om det ligger i allmänt intresse att allmänheten underrättas, kan tillsynsmyndigheten ålägga myndigheten att informera om den betydande incidenten eller, efter att ha hört myndigheten, själv informera om saken. Enligt artikel 23.7 i NIS 2-direktivet får en medlemsstats CSIRT-enhet eller, i tillämpliga fall, dess behöriga myndighet och, om det är lämpligt, CSIRT-enheterna eller de behöriga myndigheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om den betydande incidenten eller ålägga aktören att göra detta.

18 h §. *Behörig myndighet.* I paragrafen föreskrivs det om uppgifterna för den i NIS 2-direktivet avsedda behöriga myndigheten inom den offentliga förvaltningen samt om den tillsynsuppgift som hör till den. Paragrafen grundar sig på artiklarna 8.1, 8.2, 31, 32.4 g, 32.7 och 33.1 i NIS 2-direktivet.

Enligt *1 mom.* ska Transport- och kommunikationsverket vara den behöriga myndighet inom den offentliga förvaltningen som avses i artikel 8.1 i NIS 2-direktivet. Den offentliga förvaltningens verksamhetsområde definieras i 18 a §. Enligt momentets andra mening ska Transport- och kommunikationsverket, utöver vad som ovan i kapitlet föreskrivs om behandlingen av incidentanmälningar, utöva tillsyn över att de skyldigheter som föreskrivs i kapitlet och i författningar eller rättsakter som utfärdats med stöd av det eller 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 §.

Till skillnad från den tillsynsmyndighet som avses i den föreslagna lagen om hantering av cybersäkerhetsrisker har Transport- och kommunikationsverket inte behörighet att meddela föreskrifter. Däremot kan Transport- och kommunikationsverket givetvis utarbeta anvisningar och rekommendationer om åtgärder för hantering av cybersäkerhetsrisker och om god praxis. Transport- och kommunikationsverket och informationshanteringsnämnden ska samarbeta vid utarbetandet av anvisningar och rekommendationer som gäller informationssäkerhet och cybersäkerhet så att deras anvisningar till behövliga delar är enhetliga.

Enligt *2 mom.* ska Transport- och kommunikationsverket när det utför sina tillsynsåtgärder och fattar ett tillsynsbeslut enligt 18 l § beakta de omständigheter som anges i artikel 32.7 i NIS 2-direktivet, på det sätt som förutsätts i den punkten i direktivet. Dessutom möjliggörs i 2 mom. på det sätt som direktivet tillåter att Transport- och kommunikationsverket med tillämpning av

ett riskbaserat synsätt kan prioritera sina tillsynsuppgifter enligt den föreslagna lagen. Myndighetens tillsyn, det vill säga arten och omfattningen av de åtgärder som riktas mot aktörerna, ska vara proportionell och grunda sig på en bedömning av cybersäkerhetsriskerna. Enligt skäl 124 i direktivet kan den behöriga myndigheten klassificera de väsentliga aktörerna i riskkategorier och fastställa motsvarande tillsynsåtgärder och tillsynsmedel som rekommenderas per riskkategori, såsom användning av frekvens för eller typ av inspektion på plats, riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information. Sådana tillsynsmetoder skulle även kunna åtföljas av arbetsprogram och utvärderas och ses över regelbundet, inklusive med avseende på aspekter som resursfördelning och resursbehov. När det gäller offentliga förvaltningsaktörer bör tillsynsbefogenheterna utövas i överensstämmelse med nationella lagstiftningsmässiga och institutionella ramar.

Dessutom föreskrivs det i 2 mom. att Transport- och kommunikationsverket får utöva tillsyn över ett välfärdsområde, en välfärdssammanslutning eller Helsingfors stad endast om det finns grundad anledning att misstänka att aktören i fråga inte har iakttagit bestämmelserna i 4 a kap. eller i författningar som utfärdats med stöd av 4 a kap. eller NIS 2-direktivet. Enligt direktivet ska endast väsentliga aktörer bli föremål för förhandstillsyn. Andra (viktiga) aktörer är endast föremål för efterhandstillsyn. Välfärdsområdena, välfärdssammanslutningarna och Helsingfors stad är viktiga aktörer enligt NIS 2-direktivet. Med grundad anledning avses bevis, indikationer eller uppgifter som tillsynsmyndigheten får kännedom om och enligt vilka aktören påstås underlåta sina lagstadgade skyldigheter, särskilt i fråga om riskhantering eller rapportering. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som andra myndigheter, aktörer, medborgare, medier eller andra källor lämnar eller offentligt tillgänglig information eller en angivelse till tillsynsmyndigheten, om den inte är uppenbart ogrundad.

Enligt artikel 32.4 g i direktivet ska den behöriga myndigheten kunna utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda aktörerna efterlever artiklarna 21 och 23. Transport- och kommunikationsverket kan även utan särskilda bestämmelser i lag ge en tjänsteman i dess tjänst särskilda uppgifter i anslutning till tillsynen och rikta särskild tillsyn mot en aktör eller aktörer.

I *3 mom.* föreslås en materiell hänvisning till den föreslagna lagen om hantering av cybersäkerhetsrisker. I informationshanteringslagen föreskrivs endast om aktörernas skyldigheter och tillsynen över att skyldigheterna fullgörs samt om tillsynsåtgärder inom den offentliga förvaltningens verksamhetsområde enligt 10 punkten i bilaga I till NIS 2-direktivet. I övrigt genomförs bestämmelserna i direktivet genom den föreslagna lagen om hantering av cybersäkerhetsrisker.

Transport- och kommunikationsverket ska vid behandlingen av de anmälningar om verksamhet som avses i 18 a §, av sådana anmälningar och underrättelser om incidenter som avses i 18 d och f § och av annan information som erhållits i tillsynsuppdraget och i samarbetet med de övriga myndigheter och Europeiska unionens organ, decentraliserade byråer och samarbetsorgan som avses i NIS 2-direktivet och vid utlämnandet av uppgifter till dem iaktta vad som i 6 § 4 mom., 15 § 3 mom., 17 §, 25 § 3 mom., 27 § 2 mom., 34 §, 43 § 4 mom. och 46 § i lagen om hantering av cybersäkerhetsrisker föreskrivs om behandling av information vid tillsynsmyndigheten och om tillsynsmyndighetens samarbete med andra myndigheter, Europeiska unionens

organ, byråer och samarbetsorgan som avses i NIS 2-direktivet samt om utlämnande av uppgifter till dem.

I momentet konstateras det dessutom informativt att bestämmelser om den gemensamma kontaktpunkt och den CSIRT-enhet som avses i NIS 2-direktivet och om deras uppgifter, behandlingen av information samt samarbetet med andra myndigheter, Europeiska unionens organ, byråer och samarbetsorgan som avses i NIS 2-direktivet finns i lagen om hantering av cybersäkerhetsrisker.

18 i §. *Den behöriga myndighetens rätt att få information.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets rätt att få information. Paragrafen grundar sig på artikel 32.2 första stycket led e-g, 32.2 tredje stycket och 32.3. I det föreslagna 2 mom. är det fråga om en nationell reglering som förtydligar behandlingen av uppgifter om kommunikationen hos den behöriga myndigheten.

Enligt *1 mom.* har Transport- och kommunikationsverket när det utför uppgifter enligt 4 a kap. trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av myndigheter på vilka 4 a kap. tillämpas få den information som är nödvändig för skötseln av verkets uppgifter. Myndigheten ska lämna ut informationen utan dröjsmål, i den form som begärts och avgiftsfritt.

Transport- och kommunikationsverket har rätt att få tillgång till data, handlingar och information samt att få bevis på att cybersäkerhetsprinciperna har följts, såsom eventuella resultat av bedömningar som gjorts med stöd av 18 k § eller på något annat sätt och den bevisning som ligger till grund för dessa resultat. Rätten att få information gäller också när myndigheten har lagt ut en del eller alla sina cybersäkerhetsprocesser på underentreprenad. Myndigheten är då skyldig att skaffa den begärda informationen av underleverantören. Transport- och kommunikationsverket har dessutom rätt att få till exempel information om underentreprenaden, såsom avtal som anknyter till den. När tillsynsmyndigheten begär information av en myndighet, ska tillsynsmyndigheten uppge syftet med begäran och precisera vilken information som begärs.

Enligt *2 mom.* har Transport- och kommunikationsverket trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en myndighet få förmedlingsuppgifter, lokaliseringsuppgifter eller meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för att övervaka de skyldigheter enligt 18 b och 18 c § som gäller hantering av cybersäkerhetsrisker eller för att utreda betydande incidenter.

Dessutom föreskrivs det i 2 mom. att på behandlingen av nämnda information vid Transport- och kommunikationsverket tillämpas vad som i 316 § 4 mom. och 319 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om sekretess för och utlämnande och utplåning av uppgifter som Transport- och kommunikationsverkets har fått och skaffat om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar. Transport- och kommunikationsverket har med stöd av 319 § 2 mom. i lagen om tjänster inom elektronisk kommunikation rätt att lämna ut förmedlingsuppgifter och

andra uppgifter som verket fått i samband med insamling av information om och utredning av kränkningar av informationssäkerheten till en kommunikationsförmedlare, en leverantör av mervärdestjänster, ett företag, en organisation, en abonnent och en användare, om denna har blivit utnyttjad i samband med kränkningen av informationssäkerheten eller har blivit eller sannolikt kan bli utsatt för en sådan kränkning, och om det enligt Transport- och kommunikationsverkets bedömning finns skäl att misstänka att det har begåtts ett sådant brott som nämns i 316 § 2 mom. 1–12 punkten, Bestämmelsen gör det möjligt att utnyttja uppgifter som lämnats till Transport- och kommunikationsverket eller som verket fått i samband med tillsynen för att avvärja cybersäkerhetshot och för att hantera incidenter också hos andra aktörer än den myndighet som uppgifterna härstammar från. Med stöd av 319 § 3 mom. i lagen om tjänster inom elektronisk kommunikation får uppgifter lämnas ut endast i den utsträckning som behövs för att förebygga och utreda kränkningar av informationssäkerheten, och utlämnandet får inte begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt.

I *3 mom.* föreskrivs det om begränsningar i Transport- och kommunikationsverkets rätt att få information. Enligt den första meningen i bestämmelsen ska den rätt att få information som föreskrivs i paragrafen inte förplikta till att till Transport- och kommunikationsverket lämna ut information om sådan tjänsteproduktion eller användning av tjänster i säkerhetsnätet som avses i säkerhetsnätslagen och inte heller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

Enligt den andra meningen i bestämmelsen får en myndighet dock (frivilligt och enligt eget beslut) inom de gränser som anges i en sekretessbestämmelse som innehåller en offentlighets- eller sekretesspresumtion enligt lagen om offentlighet i myndigheternas verksamhet till Transport- och kommunikationsverket lämna ut information också om tjänsteproduktion och användning av tjänster i säkerhetsnätet samt information som har samband med försvaret och den nationella säkerheten och som är sekretessbelagd för allmänheten. Avsikten med den andra meningen är att förtydliga att även om den nämnda informationen i princip är undantagen från Transport- och kommunikationsverkets rätt att få information, kan de enligt myndighetens prövning liksom hittills lämnas ut till Transport- och kommunikationsverket på det sätt som är tillåtet enligt offentlighetslagen. Möjligheten kan bli tillämplig till exempel när en myndighet som inte omfattas av 4 a kap. därför att verksamheten anknyter till försvaret eller den nationella säkerheten frivilligt vill anmäla ett cyberhot eller en incident till Transport- och kommunikationsverket. Offentlighetslagen gör det möjligt att lämna ut en handling som är sekretessbelagd för allmänheten (vanligen till en annan myndighet), om sekretessbestämmelsen innehåller ett skaderekvisit och det intresse som skyddas av sekretessbestämmelsen inte äventyras om uppgiften lämnas ut. I handlingen antecknas då uppgift om sekretess och om eventuell säkerhetsklass för att visa vilka informationssäkerhetsåtgärder som ska vidtas när handlingen behandlas. Anteckningen påvisar samtidigt antecknarens uppfattning att handlingen ska vara sekretessbelagd. Den ovan beskrivna möjligheten att till en annan myndighet lämna ut handlingar och uppgifter som är sekretessbelagda för allmänheten gäller också Transport- och kommunikationsverket. Transport- och kommunikationsverket får alltså inom de gränser som anges i offentlighetslagen lämna ut sekretessbelagda uppgifter som verket fått till andra myndigheter, till exempel för att avvärja ett cybersäkerhetshot eller för att hantera en incident. Utlämnandet av uppgifter får inte äventyra de intressen som skyddas genom sekretessbestämmelsen eller sekretessbestämmelserna. Vid

utlämnande av uppgifter ska man också beakta utgångspunkten för säkerhetsklassificerad information, enligt vilken den myndighet som upprättat handlingen beslutar om utlämnande av den.

I momentets tredje mening föreskrivs det i fråga om säkerhetsklassificerad information att om en myndighet till Transport- och kommunikationsverket överlämnar en handling som faller utanför verkets rätt att få information enligt 1 och 2 mom. och som en annan myndighet har säkerhetsklassificerat eller som bedömningen av arten av den information som handlingen innehåller i sin helhet hör till, ska beslutet om utlämnande av handlingen eller informationen fattas av den myndighet som utfört klassificeringen eller den myndighet som bedömningen av ärendet i sin helhet hör till.

Särskilt när uppgifter enligt 3 mom. lämnas ut är det skäl att överväga att begränsa ett vidare utlämnande, om utlämnandet av uppgifterna skulle äventyra Finlands centrala säkerhetsintressen. I detta sammanhang bör det också bedömas om det är möjligt att lämna ut information om hot eller incidenter på allmän nivå så att Finlands centrala säkerhetsintressen inte äventyras. NIS 2-direktivet förutsätter inte att uppgifter som avses i det föreslagna 3 mom. lämnas ut t.ex. till EU:s institutioner, decentraliserade organ, samarbetsorgan eller andra myndigheter. Särskilt i fråga om säkerhetsklassificerad sekretessbelagd information framhävs bedömningen av den myndighet som har förutsättningar att bedöma informationens natur i förhållande till det intresse som skyddas genom sekretessbestämmelserna. I 15 § 3 mom. i offentlighetslagen föreskrivs det att om någon hos en myndighet begär att få ta del av en handling i vilken det enligt lagen om informationshantering inom den offentliga förvaltningen ska göras en anteckning om säkerhetsklass i fråga om de informationssäkerhetskrav som ska uppfyllas vid hantering av handlingen och som har upprättats av en annan myndighet, ska myndigheten överföra ärendet för avgörande av den myndighet som har upprättat handlingen.

I momentets fjärde mening konstateras för tydlighetens skull att vid hantering av särskilt känsligt informationsmaterial enligt lagen om internationella förpliktelser som gäller informationssäkerhet ska bestämmelserna i den lagen iakttas. Förutsättningarna för utlämnande av särskilt känsligt informationsmaterial ska således bedömas utifrån den lagen och den internationella förpliktelse som lämpar sig för informationsmaterialet.

18 j §. *Inspektionsrätt.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets inspektionsrätt. Paragrafen grundar sig på artikel 32.2 första stycket led a–d samt andra och tredje stycket.

Enligt 1 mom. har Transport- och kommunikationsverket rätt att i den omfattning som behövs utföra inspektioner hos myndigheter för att övervaka att de skyldigheter som föreskrivs i 4 a kap. eller i författningar som utfärdats med stöd av 4 a kap. eller NIS 2-direktivet fullgörs. Inspektionen kan utföras antingen på plats eller någon annanstans. Inspektionen kan omfatta tekniska åtgärder såsom identifiering av databasernas, utrustningens, brandväggarnas, krypteringens och nätens svagheter genom säkerhetsskanning. I lagen om hantering av cybersäkerhetsrisker föreskrivs det särskilt om CSIRT-enhetens sårbarhetskartläggningar och de tillåtna

användningsändamålen för information som erhållits genom dem. Transport- och kommunikationsverket kan utföra regelbundna inspektioner, sporadiska inspektioner eller inspektioner från fall till fall (t.ex. efter en betydande incident). Inspektionerna kan vara mindre omfattande, inriktade på ett visst ämnesområde eller mer omfattande, heltäckande inspektioner av verksamheten.

Enligt *2 mom.* ska den som utför inspektionen ha tillräcklig utbildning och erfarenhet med hänsyn till inspektionens art och omfattning. Transport- och kommunikationsverket ska säkerställa att den som utför inspektionen har de färdigheter som krävs för att utföra uppgifterna i fråga och att inspektionen utförs objektivt.

Enligt *3 mom.* har den som utför en inspektion för utförande av inspektionen rätt att få tillträde till andra utrymmen än sådana som är avsedda för boende av permanent natur och till det kommunikationsnät eller informationssystem som inspektionen gäller samt rätt att trots sekretessbestämmelserna få granska den information och de handlingar, maskinvaror och programvaror som behövs för inspektionsuppdraget. Den som utför inspektionen har också rätt att utföra behövliga tester och mätningar samt granska de säkerhetsarrangemang som myndigheten har genomfört. Med stöd av sin rätt att få information har Transport- och kommunikationsverket rätt att också före och under inspektionen få granska myndighetens skriftliga material, såsom drifthandböcker, anvisningar, processbeskrivningar, utbildningsbokföring och resultaten av bedömningar av informationssäkerheten som aktören utarbetat.

Dessutom innehåller momentet en materiell hänvisningsbestämmelse om att 39 § i förvaltningslagen ska tillämpas på förfarandet vid inspektionen. Den bestämmelsen lämpar sig inte i övrigt för inspektioner av tillsynstyp. I 39 § i förvaltningslagen föreskrivs det bland annat att en myndighet ska underrätta en part om tidpunkten för en inspektion, såvida syftet med inspektionen inte äventyras av en sådan underrättelse. Dessutom föreskrivs det om en parts rätt att närvara vid en inspektion och om att inspektionen ska utföras utan att den som är föremål för inspektionen eller dess innehavare orsakas oskälig olägenhet. Enligt skäl 123 i NIS 2-direktivet bör ”utförande av tillsynsuppgifter [...] inte i onödan hämma den berörda entitetens affärsverksamhet. När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom inspektioner på plats och distansbaserad tillsyn, utredning av överträdelser av detta direktiv, säkerhetsrevisioner eller säkerhetsskanningar, bör de minimera konsekvenserna för den berörda entitetens affärsverksamhet.” I 39 § 2 mom. i förvaltningslagen föreskrivs det om en skriftlig inspektionsberättelse.

Paragrafens *4 mom.* innehåller en hänvisning till de begränsningar av rätten att få information som föreslås i 18 i § 3 mom. och som också kan tillämpas på inspektioner.

18 k §. *Tilldelande av biträdande uppgift till godkänt bedömningsorgan samt att låta utföra bedömning.* I paragrafen föreslås bestämmelser om utnyttjande av sådana godkända bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011, nedan *lagen om bedömningsorgan*) i tillsynsverksamheten samt i situationer där Transport- och kommunikationsverket i egenskap av tillsynsmyndighet ålägger en myndighet att själv låta utföra en bedömning av hanteringen av cybersäkerhetsrisker. Med stöd

av 3 § i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation får statsförvaltningsmyndigheterna för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation bara använda sig av Transport- och kommunikationsverkets tjänster eller av ett sådant bedömningsorgan som har godkänts av Kommunikationsverket enligt lagen om bedömningsorgan. I motiveringen till bestämmelsen (RP 45/2011 rd, s. 11) konstateras det att avsikten är att säkerställa att statsförvaltningsmyndigheterna anlitar bara tillförlitliga externa tjänster för bedömning av informationssäkerheten och att bestämmelsen behövs för att informationssäkerheten inom statsförvaltningen ska utvecklas på ett enhetligt sätt och utan kostnader vars grund är osaklig. På samma grunder avgränsas i den föreslagna bestämmelsen uppgiften att utföra inspektioner och bedömningar till godkända bedömningsorgan.

Enligt *1 mom.* kan Transport- och kommunikationsverket ge ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet en biträdande uppgift i anslutning till ett inspektionsuppdrag enligt 18 j §. I bestämmelsen ingår också en definition av godkänt bedömningsorgan. Transport- och kommunikationsverket kan anförtro en uppgift av biträdande art åt ett bedömningsorgan vars kompetensområde lämpar sig för uppgiften.

Enligt *2 mom.* kan Transport- och kommunikationsverket ålägga en myndighet att låta ett godkänt bedömningsorgan utföra en bedömning av hanteringen av cybersäkerhetsrisker, om myndigheten har drabbats av en betydande incident som har orsakat en allvarlig driftsstörning för tjänsterna eller vållat betydande materiell eller immateriell skada, eller myndigheten väsentligt och allvarligt har försummat att iaktta skyldigheterna att hantera cybersäkerhetsrisker enligt 18 b eller 18 c §. Bedömningen beställs av den myndighet som bedömningen gäller. Den myndigheten svarar också för kostnaderna för bedömningen. Om det kan dröja att få tillgång till bedömningsorganens tjänster, ska Transport- och kommunikationsverket beakta detta när verket ålägger myndigheten att låta utföra en bedömning, till exempel om verket sätter ut en tidsfrist för utförandet.

Enligt *3 mom.* ska på den som är anställd vid ett godkänt bedömningsorgan och som förrättar inspektion eller utför bedömning tillämpas vad som i 18 j § 2–4 mom. föreskrivs om inspektionsförrättarens erfarenhet och utbildning samt inspektionsförrättarens rättigheter. Kompetensen hos personalen vid ett godkänt bedömningsorgan säkerställs i princip när bedömningsorganet godkänns i ett förfarande enligt lagen om bedömningsorgan. Den som utför inspektioner eller utvärderingar och som är anställd hos ett godkänt bedömningsorgan ska ha samma inspektionsbefogenheter och rätt att få information som en anställd hos Transport- och kommunikationsverket som utför inspektioner. Transport- och kommunikationsverket har naturligtvis med stöd av den föreslagna 18 i § rätt att få information om resultaten av en inspektion eller bedömning som myndigheten låtit utföra samt med stöd av 18 l § rätt att ålägga en myndighet att vidta korrigerande åtgärder, om det vid inspektionen eller bedömningen framgår att myndigheten inte har fullgjort de skyldigheter som föreskrivs i 4 a kap. eller i författningar som utfärdats med stöd av 4 a kap. eller NIS 2-direktivet.

I 3 mom. föreskrivs dessutom om straffrättsligt tjänsteansvar för den som är anställd hos ett godkänt bedömningsorgan. I momentet ingår också en informativ hänvisning till skadeståndslagen.

18 l §. *Påföljder.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets tillsynsbeslut, det vill säga rätten att ålägga en informationshanteringsenhet att fullgöra de skyldigheter som föreskrivs i 4 a kap. eller med stöd av det kapitlet eller NIS 2-direktivet. Paragrafen grundar sig på artikel 32.1, 32.4 och 32.7 i NIS 2-direktivet.

Enligt *1 mom.* kan Transport- och kommunikationsverket genom sitt beslut ålägga en myndighet att inom utsatt tid avhjälpa brister i fullgörandet av de skyldigheter som föreskrivs i 4 a kap. eller i författningar som utfärdats med stöd av det kapitlet eller NIS 2-direktivet. Transport- och kommunikationsverket kan också ålägga en myndighet att offentliggöra dessa brister eller andra omständigheter som anknyter till överträdelser av de nämnda bestämmelserna. Transport- och kommunikationsverket kan i sitt beslut specificera vilka åtgärder som ska vidtas för att förebygga eller avhjälpa en incident eller för att avhjälpa någon annan brist. Ett tillsynsbeslut enligt momentet är ett förvaltningsbeslut på vilket förvaltningslagen tillämpas. Vid utredningen och avgörandet av ett ärende ska därför, utöver vad som föreskrivs i denna paragraf, beaktas bland annat vad som i förvaltningslagen föreskrivs om utredning av ärenden, hörande av parter och motivering av beslut.

Enligt *2 mom.* kan Transport- och kommunikationsverket ge myndigheten en anmärkning eller en varning. En varning kan ges om en anmärkning inte kan anses tillräcklig med beaktande av omständigheterna i ärendet som helhet.

I *3 mom.* föreskrivs det om Transport- och kommunikationsverkets möjlighet att förena ett tillsynsbeslut med vite. Paragrafen grundar sig på artikel 32.1 i NIS 2-direktivet, enligt vilken medlemsstaterna ska säkerställa att de tillsyns- eller efterlevnadskontrollåtgärder som åläggs väsentliga entiteter angående de skyldigheter som anges i direktivet är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall, samt på artikel 34.6, enligt vilken medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en väsentlig eller viktig entitet att upphöra med en överträdelse av direktivet i enlighet med ett föregående beslut av den behöriga myndigheten. Enligt artikel 32.5 i direktivet krävs det inom den offentliga sektorn inte skyldigheter som gör det möjligt att avbryta verksamheten, och enligt artikel 34.7 i direktivet är det inte nödvändigt att inom den offentliga sektorn tillämpa administrativa böter som efterlevnadskontrollåtgärd. Avsikten är inte att de nämnda efterlevnadskontrollåtgärderna ska tillämpas inom den offentliga förvaltningen, vilket innebär att efterlevnaden, utöver att den är förenad med tjänsteansvar, också förenas med vite. Momentet innehåller också en informativ hänvisning till viteslagen.

18 m §. *Sökande av ändring.* Paragrafen innehåller en bestämmelse om möjlighet att begära omprövning av Transport- och kommunikationsverkets tillsynsbeslut samt informativa hänvisningar till de allmänna lagarna om omprövning och sökande av ändring.

7.3 Lag om ändring av lagen om tjänster inom elektronisk kommunikation

2 §. *Tillämpning av vissa bestämmelser.* Det föreslås att 2 mom. upphävs. I momentet föreskrivs det om tillämpning av lagstiftning mellan medlemsländerna i EU enligt NIS 1-direktivet på verksamhet ho en leverantör av internetbaserade marknadsplatser, sökmotortjänster och molntjänster enligt 247 a §, som enligt förslaget ska upphävas. Momentet ska på grund av upphävandet av 247 a § upphävas som onödigt, eftersom den reglering som gäller dessa aktörer enligt NIS 2-direktivet genomförs genom det första lagförslaget. En bestämmelse med motsvarande innehåll finns i 2 § 3 mom. i det första lagförslaget.

165 §. *Registrarens anmälningsskyldighet.* Det föreslås att *1 mom.* ändras så, att registrarens anmälningsskyldighet ska utvidgas till att täcka de uppgifter som avses i artikel 27.2 i NIS 2-direktivet. Registrarerna ska således till den myndighet som administrerar domännamnsregistret, det vill säga Transport- och kommunikationsverket, även anmäla vissa adressuppgifter och övrig aktuell kontaktinformation, IP-adressintervall samt en förteckning över de medlemsstater där registraren tillhandahåller tjänster. Genom förslaget genomförs artikel 27.2 i NIS 2-direktivet i fråga om registrarer.

Dessutom ska till bestämmelsen även fogas ett nytt *4 mom.* enligt vilket Transport- och kommunikationsverket ska lämna den gemensamma kontaktpunkt som avses i 19 § i lagen om hantering av cybersäkerhetsrisker vissa uppgifter om registrarernas anmälningar för att göra en anmälan som avses i artikel 27.4 i NIS 2-direktivet.

167 §. *Anteckning av uppgifter i domännamnsregistret och offentliggörande av uppgifter.* Enligt förslaget ändras *1 mom.* i bestämmelsen på det sätt som artikel 28.1 och 28.2 i NIS 2-direktivet kräver. Domännamnsanvändaren ett ska vara skyldig att anmäla korrekta och uppdaterade användar- och kontaktuppgifter som identifierar domännamnsanvändaren samt ändringar i dem. Registraren eller en aktör som handlar för dess räkning, såsom en tillhandahållare eller återförsäljare av privata tjänster eller förmedlingstjänster, ska, utöver de uppgifter som gäller domännamnsanvändaren, även anteckna uppgifter som gäller det registrerade domännamnet, såsom uppgift om det registrerade domännamnet och registreringsdag.

Det föreslås att ett nytt *2 mom.* fogas till bestämmelsen enligt vilket 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. Transport- och kommunikationsverket ska ändå först uppmana registraren att bevisa att uppgifterna är riktiga inom en skälig utsatt tid. Transport- och kommunikationsverket ska offentliggöra sina riktlinjer och förfaranden för säkerställande av att användaruppgifterna är korrekta.

De tidigare 2–4 mom. i bestämmelsen blir 3–5 mom. på grund av det nya 2 mom. som fogas till. Det föreslås att *3 mom.* i bestämmelsen ändras så, att Transport- och kommunikationsverket

ska vara skyldigt att offentliggöra uppgifterna i domännamnsregistret. Uppgifterna ska offentliggöras utan obefogat dröjsmål och antingen på Transport- och kommunikationsverkets webbsidor eller i någon annan elektronisk tjänst. Skyldigheten ska dock inte gälla personuppgifter som registret innehåller. Särskilda bestämmelser om utlämnande av personuppgifter ur register som myndigheter upprätthåller finns i 16 § 3 mom. i lagen om offentlighet i myndigheternas verksamhet (1999/621, nedan offentlighetslagen). Med avvikelse från offentlighetslagen ska Transport- och kommunikationsverket dock besvara en begäran om åtkomst till registeruppgifter om domännamn utan obefogat dröjsmål och senast inom 72 timmar från mottagandet av begäran. Den tidsfrist som ska sättas ut för svarandet innebär inte att begäran om information i sin helhet måste behandlas inom tidsfristen 72 timmar. Om en begäran om information som har lämnats till exempel till Transport- och kommunikationsverket är bristfällig eller oklar på så sätt att det utifrån den inte kan bedömas om det är i enlighet med dataskyddslagstiftningen att lämna ut uppgifter ska verket svara den som framfört begäran till exempel med att begära mer information inom den tidsfrist som satts ut i lagen. Transport- och kommunikationsverket ska dessutom offentliggöra de riktlinjer och förfaranden som verket har till förfogande för utlämnande av registreringsinformation om domännamn.

I bestämmelsens *5 mom.* föreskrivs om det bemyndigande att utfärda föreskrifter som Transport- och kommunikationsverket ska ges. Det föreslås att Transport- och kommunikationsverkets bemyndigande att utfärda föreskrifter ska utvidgas så, att verket får utfärda närmare föreskrifter också om säkerställande av uppgifter som gäller domännamnsanvändare. Med det avses till exempel riktlinjer och förfaranden som registrarer ska ta i bruk för att de ska kunna säkerställa att de uppgifter som avses i 1 mom. och som meddelas av domännamnsanvändare är korrekta och uppdaterade.

Genom de föreslagna ändringarna genomförs artikel 28.1 och 28.2 samt 28.3–5 i NIS 2-direktivet i fråga om registreringsenhet för toppdomäner.

170 §. *Registrarens övriga skyldigheter.* Till 1 mom. i bestämmelsen ska fogas en ny 8 punkt enligt vilken registraren ska offentliggöra de riktlinjer och förfaranden som den har till förfogande för att säkerställa att uppgifterna i domännamnsregistret överensstämmer med 167 § 1 mom. Enligt 167 § ska registraren eller en aktör som handlar för dess räkning, såsom en tillhandahållare eller återförsäljare av privata tjänster eller förmedlingstjänster, 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. Dessutom föreslås det att en *ny 9 punkt* fogas till momentet enligt vilken registraren utan obefogat dröjsmål ska göra andra registreringsuppgifter om domännamn än personuppgifter offentligt tillgängliga Registraren ska dessutom enligt den föreslagna *10 punkten* i enlighet med dataskyddslagstiftningen och avgiftsfritt ge åtkomst till registreringsuppgifter om domännamn. Registraren ska dessutom svara den som ber om åtkomst till registeruppgifter utan obefogat dröjsmål och senast inom 72 timmar efter det att registraren har mottagit en laglig och vederbörligen motiverad begäran. Om en begäran om information är bristfällig eller oklar på så sätt att det utifrån den inte kan bedömas om det är i enlighet med dataskyddslagstiftningen att lämna ut uppgifter ska verket svara den som framfört begäran till exempel med att begära mer information inom den tidsfrist som ställts i lagen. Dessutom föreslås det att en ny *11 punkt* fogas till 1

mom. Enligt den ska en registrar offentliggöra de riktlinjer och förfaranden som den använder vid utlämnande av registreringsuppgifter för domännamn.

I bestämmelsens *2 mom.* föreskrivs om det bemyndigande att utfärda föreskrifter som Transport- och kommunikationsverket ska ges. Det föreslås att Transport- och kommunikationsverkets bemyndigande att utfärda föreskrifter på grund av 8–11 punkten som ska fogas till 1 mom. utvidgas så, att verket får ge närmare föreskrifter även om uppgifter som avses att offentliggöras, om givande av åtkomst till uppgifter, om riktlinjer och förfaranden.

Det föreslås att ett *nytt 3 mom*., som klargör 1 mom. 6–7 punktens förhållande till den föreslagna lagen om hantering av cybersäkerhetsrisker, fogas till bestämmelsen. Vad gäller de leverantörer av DNS-tjänster som hör till tillämpningsområdet för NIS 2-direktivet ska bestämmelser om deras skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem i fortsättningen finnas i lagen om hantering av cybersäkerhetsrisker. I stället ska motsvarande skyldigheter för registrarer som inte är leverantörer av DNS-tjänster även i fortsättningen finnas i 1 mom. 6–7 punkten.

Genom de föreslagna ändringarna genomförs artikel 28.3–5 i NIS 2-direktivet för registrarers del.

247 §. *Skyldighet att sörja för informationssäkerheten vid kommunikationsförmedling och tillhandahållande av mervärdestjänster.* Det föreslås att till bestämmelsen fogas ett klargörande moment om att lagen om hantering av cybersäkerhetsrisker även tillämpas på skyldigheten att sörja för informationssäkerheten och för de risker som riktas mot den för kommunikationsförmedlare och leverantörer av mervärdestjänster som omfattas av tillämpningsområdet för NIS 2-direktivet.

247 a §. *Skyldighet för den som tillhandahåller internetbaserade marknadsplatser, sökmotortjänster och molntjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem.* Det föreslås att bestämmelsen upphävs när motsvarande skyldighet överförs till lagen om hantering av cybersäkerhetsrisker. Syftet med bestämmelsen har för de aktörers del som avses i den varit att genomföra NIS 1-direktivet. I fortsättningen ska det föreskrivas om den motsvarande skyldigheten till riskhantering för de aktörer som avses i 247 a § i lagen om hantering av cybersäkerhetsrisker. Det föreslås således att bestämmelsen upphävs som obehövlig.

275 §. *Störningsanmälningar till Transport- och kommunikationsverket.* Det föreslås att Transport- och kommunikationsverkets skyldighet att enligt 1 mom. årligen sända kommissionen och Europeiska unionens cybersäkerhetsbyrå en sammanfattande informationsrapport om de anmälningar som lämnats med stöd av momentet stryks i momentet. Skyldigheten har fogats till lagen för genomförande av artikel 40 i kodexdirektivet. Genom NIS 2-direktivet upphävs artikel 40 i kodexdirektivet, så den nationella bestämmelse som genomför direktivet upphävs enligt förslaget som onödig.

Det föreslås att 2 mom. i bestämmelsen upphävs där det föreskrivs om skyldighet för de aktörer som avses i 247 a §, som enligt förslaget ska upphävas, att anmäla om en betydande informationssäkerhetsrelaterad störning. Momentet har fogats till lagen för genomförande av NIS 1-direktivet i fråga om aktörer som avses i 247 a §. I fortsättningen ska det föreskrivas i lagen om hantering av cybersäkerhetsrisker om motsvarande anmälningsskyldighet enligt NIS 2-direktivet för de aktörer som avses i 247 a §. Det föreslås således att bestämmelsen upphävs som obehövlig.

Samtidigt blir nuvarande 3–5 mom. nya 2–4 mom., och hänvisningarna i dem till det 2 mom. som ska upphävas stryks. För de aktörers del som avses i 247 a §, som ska upphävas, ska en bestämmelse som motsvarar det gamla 275 § 3 mom. ingå i 11 § i det första lagförslaget, bemyndigandet att utfärda föreskrifter som motsvarar det gamla 4 mom. ska ingå i 11 § i det första lagförslaget och en bestämmelse som motsvarar det gamla 5 mom. ska ingå i 17 § i det första lagförslaget. För föreskrifter som meddelats med stöd av 275 § 4 mom. gäller en övergångsbestämmelse.

308 §. *Myndighetssamarbete*. Det föreslås att 3 mom. ändras så att hänvisningen till den samarbetsgrupp som avses i artikel 11 i direktivet om nät- och informationssäkerhet ändras till en hänvisning till den samarbetsgrupp som avses i artikel 14 i NIS 2-direktivet. Till momentet ska också fogas en hänvisning till CSIRT-nätverket som avses i artikel 15 och det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) som avses i artikel 16. I momentet stryks hänvisningen till sändande av en sammanfattande rapport enligt artikel 10.3 i direktivet om nät- och informationssäkerhet eftersom direktivet är upphävt. För NIS 2-direktivets del ska det föreskrivas om motsvarande rapporteringsskyldighet till Transport- och kommunikationsverket i 19 § i lagen om hantering av cybersäkerhetsrisker.

313 §. *Behandling av tillsynsärenden vid Transport- och kommunikationsverket.* Det föreslås att 2 mom. 2 punkten ändras så att hänvisningen till 247 a §, som enligt förslaget ska upphävas, stryks i punkten. I fortsättningen ska det föreskrivas om rätten att lämna ett ärende obehandlat i 26 § i lagen om hantering av cybersäkerhetsrisker.

318 §. Det föreslås att 4 mom. ändras delvis av lagstiftningstekniska skäl. I momentet ska hänvisningen till det nuvarande 2 mom. i 275 § strykas då momentet enligt förslaget upphävs. Dessutom ska hänvisningen till den samarbetsgrupp som avses i artikel 11 i direktivet om nät- och informationssäkerhet ändras till en hänvisning till den samarbetsgrupp som avses i artikel 14 och till CSIRT-nätverket som avses i artikel 15 i NIS 2-direktivet.

7.4 Lag om upphävande av 128 a § och 128 b § i luftfartslagen

Genom förslaget upphävs 128 a § och 128 b § i luftfartslagen som gäller skyldighet för leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och att anmäla myndigheten om inform-

ationssäkerhetsrelaterade händelser. Bestämmelserna har fogats till luftfartslagen för genomförande av NIS 1-direktivet. Bestämmelserna ska strykas, för i den föreslagna lagen om hantering av cybersäkerhetsrisker ingår motsvarande skyldigheter som gäller leverantörer av flygtrafiktjänster och flygplatsoperatörer.

Genom förslaget upphävs även statsrådets förordning om samhällsviktiga flygplatser och hamnar (361/2018) tillsammans med förslaget som gäller upphävande av 7 e § och 7 f § i lagen om sjöfartskydd Den förordning som ska upphävas har utfärdats med stöd av 128 a § i luftfartslagen och 7 e § i lagen om sjöfartskydd Eftersom det föreslås att de båda bestämmelserna som innehåller bemyndigande att utfärda förordning ska upphävas ska den statsrådets förordning som utfärdats med stöd av dem inte vara i kraft. Skyldigheterna ska i fortsättningen tillämpas på flygplatser och hamnar som omfattas av tillämpningsområdet för NIS 2-direktivet och den föreslagna allmänna lagen, och därför behöver inte samhällsviktiga flygplatser eller hamnar fastställas separat i lag eller med stöd av lag.

7.5 Lag om upphävande av 169 § i spårtrafiklagen

Genom förslaget upphävs 169 § i spårtrafiklagen som gäller skyldighet för förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och att anmäla myndigheten om störningar i kommunikationsnät och informationssystem. Bestämmelsen ska upphävas, för den föreslagna lagen om hantering av cybersäkerhetsrisker ska i fortsättningen innehålla samma skyldighet för förvaltaren av bannät och den som tillhandahåller trafikledningstjänster.

7.6 Lag om ändring av lagen om transportservice

140 §. *Informationssäkerhet inom vägtrafikstyrnings- och vägtrafikledningstjänster.* Det föreslås att paragrafen ändras så att de nuvarande 1–4 mom. upphävs. Den föreslagna lagen om hantering av cybersäkerhetsrisker ska i fortsättningen innehålla motsvarande skyldighet för en leverantör av vägtrafikstyrnings- och vägtrafikledningstjänster. Ett nytt 1 mom. ska innehålla en informativ hänvisning till den lagen. Paragrafens nuvarande 5 mom. övergår oförändrad till att bli ett nytt 2 mom.

161 §. *Skyldighet för den som tillhandahåller intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten.* Det föreslås att paragrafen upphävs. Paragrafen gäller skyldighet för den som tillhandahåller intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt att anmäla om störningar i dem till myndigheten. Bestämmelsen ska strykas, för i den föreslagna lagen om hantering av cybersäkerhetsrisker ingår i fortsättningen motsvarande skyldigheter för den som tillhandahåller intelligenta trafiksystem.

7.7 Lag om upphävande av 18 a § i lagen om fartygstrafikservice.

Genom propositionen upphävs 18 a § i lagen om fartygstrafikservice som gäller VTS-tjänsteleverantörens skyldighet att lämna Transport- och kommunikationsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem. Bestämmelsen ska strykas, för i den föreslagna lagen om hantering av cybersäkerhetsrisker ingår i fortsättningen motsvarande skyldigheter för VTS-tjänsteleverantörer.

7.8 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

Enligt förslaget upphävs 7 e § och 7 f § i lagen om sjöfartskydd som gäller skyldighet för innehavare av samhällsviktiga hamnar att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder samt att anmäla om störningar i dem till myndigheten. Bestämmelserna ska strykas, för i den föreslagna lagen om hantering av cybersäkerhetsrisker ingår i fortsättningen motsvarande skyldigheter som gäller hamninnehavare.

Genom förslaget upphävs även statsrådets förordning om samhällsviktiga flygplatser och hamnar (361/2018) tillsammans med förslaget som gäller upphävande av 128 a § och 128 b § i luftfartslagen. Skyldigheterna ska i fortsättningen tillämpas enligt tillämpningsområdet för NIS 2-direktivet och den föreslagna allmänna lagen.

7.9 Lag om ändring av lagen om behandling av kunduppgifter inom social- och hälsovården

2 §. *Tillämpningsområde och förhållande till annan lagstiftning*. Det föreslås att 2 § *3mom.* i lagen ändras så, att genom lagen utfärdas 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 och lagen om hantering av cybersäkerhetsrisker (/) 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. Samtidigt ändras hänvisningen till att motsvara det nya NIS 2-direktivet som trätt i kraft den 14 december 2022.

Bestämmelser som kompletterar och preciserar NIS 2-direktivet och lagen om hantering av cybersäkerhetsrisker finns i lagens 10 kap. Egenkontroll av informationssäkerhet och dataskydd. I 77 § i lagen finns bestämmelser om tjänstetillhandahållares skyldighet att utarbeta en informationssäkerhetsplan och i den redogöra för hur de krav som hänför sig till behandlingen av de

klient- och patientuppgifter som det redogörs närmare för i paragrafen säkerställs. Kraven gäller till exempel att informationssystemens driftmiljö är lämplig för en sådan ändamålsenlig användning av informationssystemen som säkerställer informationssäkerheten och dataskyddet och att det sörjs för riskhanteringen i fråga om driftmiljön och informationssystemen. Kravet gäller både offentliga och privata tjänstetillhandahållare inom hälso- och sjukvården. Institutet för hälsa och välfärd får meddela närmare föreskrifter om de redogörelser och krav som ska tas in i informationssäkerhetsplanen och om verifiering av informationssäkerheten. Kompletterande och specificerande bestämmelser finns också i lagens 78 § där det föreskrivs om genomförande av och ansvar för egenkontroll av informationssäkerheten, bland annat om skyldigheten för den ansvariga föreståndaren hos en tjänstetillhandahållare att se till att en informationssäkerhetsplan utarbetas och iakttas.

90 §. *Underrättelse om avvikelser från de väsentliga kraven på ett informationssystem eller en välbefinnandeapplikation samt om störningar i informationssäkerheten avseende informationsnät.* I 2 mom. ska det i fråga om skyldighet för tjänstetillhandahållare inom hälso- och sjukvården hänvisas till 12–15 § i lagen om hantering av cybersäkerhetsrisker. Lagen om hantering av cybersäkerhetsrisker tillämpas inom hälso- och sjukvården även i andra situationer än vid behandling av kunduppgifter, så med tanke på tillämpningen är det åskådligt att iaktta samma reglering i alla situationer. För åskådlighetens skull ska det ändå i kunduppgiftslagen finnas en hänvisning till lagen om hantering av cybersäkerhetsrisker. I momentet ska det vidare föreskrivas om motsvarande skyldigheter för en tjänstetillhandahållare inom socialvården, ett apotek, Folkpensionsanstalten och en producent av en informationssystemtjänst eller en tillverkare av ett informationssystem eller en mellanhand på vilkas verksamhet lagen om hantering av cybersäkerhetsrisker inte ska tillämpas.

Det föreslås att *3 mom.* ska ändras så, att i stället för tjänstetillhandahållaren ska regleringen gälla endast tjänstetillhandahållaren inom socialvården eftersom det i fortsättningen föreskrivs om skyldigheter för tjänstetillhandahållare inom hälso- och sjukvården i lagen om hantering av cybersäkerhetsrisker.

Paragrafens *4 mom.* ska enligt förslaget upphävas eftersom det har gällt enbart offentlig hälso- och sjukvård och motsvarande reglering i fortsättningen finns i lagen om hantering av cybersäkerhetsrisker.

7.10 Lag om ändring av elmarknadslagen

29 a §. *Nätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten.* Det föreslås att paragrafen ska upphävas, för i fortsättningen ska det föreskrivas om nätinnehavarens skyldighet att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som nätinnehavaren använder i den föreslagna lagen om hantering av cybersäkerhetsrisker.

62 §. *Specialbestämmelser som gäller slutna distributionsnät.* Paragrafens 1 mom. ändras genom att hänvisningen till 29 a § i momentet stryks. Ändringen är av lagstiftningsteknisk natur.

7.11 Lag om upphävande av 34 a § i naturgasmarknadslagen

Genom förslaget upphävs 34 a § i naturgasmarknadslagen som gäller överföringsnätsinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt skyldighet att anmäla om betydande störningar i informationssäkerheten. Bestämmelserna ska upphävas, för i den föreslagna lagen om hantering av cybersäkerhetsrisker ingår i fortsättningen motsvarande skyldigheter som gäller överföringsnätsinnehavare.

7.12 Lag om ändring av 1 § i lagen om Energimyndigheten

1 §. *Uppgifter*. I 1 § finns bestämmelser om Energimyndighetens uppgifter. Det föreslås att en ny 21 punkt fogas till 2 mom. Enligt den ska Energimyndigheten sköta de uppgifter som myndigheten har enligt lagen om hantering av cybersäkerhetsrisker. Energimyndigheten är en av de tillsynsmyndigheter som avses i 24 § i lagen om hantering av cybersäkerhetsrisker.

7.13 Lag om ändring av 28 § i lagen om tillsyn över el- och naturgasmarknaden

28 §. *Energimyndighetens rätt att lämna ut uppgifter till andra myndigheter.* Det föreslås att 1 mom. 1 punkten ändras så, att i den stryks omnämnandet av att trots bestämmelserna om sekretess lämna ut uppgifter till Transport- och kommunikationsverket. Det föreslås att punkten i fråga stryks, för 27 § i den föreslagna lagen om hantering av cybersäkerhetsrisker ska i fortsättningen innehålla motsvarande möjlighet att lämna ut sekretessbelagd information till en annan myndighet.

7.14 Lag om ändring av 35 § i lagen om vattentjänster

Enligt förslaget upphävs 35 § 2 mom. 3 punkten som gäller utlämnande av uppgifter som är nödvändiga för skötseln av informationssäkerhetsrelaterade uppgifter till Transport- och kommunikationsverket trots tystnadsplikten. Det föreslås att punkten i fråga upphävs, för 27 § i den föreslagna lagen om hantering av cybersäkerhetsrisker ska i fortsättningen innehålla motsvarande möjlighet att lämna ut sekretessbelagd information till en annan myndighet.

8 Bestämmelser på lägre nivå än lag

8.1 Propositionens nya bemyndiganden att utfärda bestämmelser på lägre nivå än lag

I propositionen föreslås det att bestämmelserna på lagnivå ska kompletteras med bestämmelser på lägre nivå än lag. Bestämmelser på lägre nivå som preciserar de föreslagna nya bestämmelserna utfärdas genom förordning av statsrådet, genom förordning av ministeriet och genom normer som utfärdas av andra myndigheter. Dessutom innehåller propositionen förslag till upphävande av bestämmelser på lägre nivå än lag och av bemyndigande att utfärda sådana.

Hänförande av vissa aktörer till tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker genom förordning av statsrådet.

I propositionen ingår ett förslag till bemyndigande att genom förordning av statsrådet föreskriva om ett undantag från tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker i fråga om dess storlekskriterium. Det genomförs med stöd av det bemyndigande som föreslås i 3 § 2 mom. i lagen om hantering av cybersäkerhetsrisker, enligt vilket det genom förordning av statsrådet föreskrivs om tillämpning av lagen på sådana aktörer som bedriver verksamhet enligt bilaga I eller II eller som är en typ av aktör som avses i bilaga I eller II, oavsett storlek, om de i lagen angivna förutsättningar som gäller aktörerna uppfylls.

Genom förordning av statsrådet får det således föreskrivas att lagen ska tillämpas på en aktör på vilken lagen inte annars skulle tillämpas eftersom aktören inte uppfyller definitionen av ett medelstort företag. En förutsättning är att aktören är en sådan typ av aktör som avses i en bilaga till lagen eller bedriver sådan verksamhet som avses i en bilaga och att aktören omfattas av ett lagstadgat kriterium som motsvarar artikel 2.2 b–e i NIS 2-direktivet.

Enligt artikel 2.2 b–e i NIS 2-direktivet ska, inom de sektorer som omfattas av direktivet, riskhanterings- och rapporteringsskyldigheterna enligt NIS 2-direktivet tillämpas på de aktörer som avses i leden, oberoende av aktörernas storlek. Kriterierna för dessa aktörer är följande:

b) aktören är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
c) en störning av den tjänst som aktören tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa,
d) en störning av den tjänst som aktören tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser,
e) 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 medlemsstaten som är beroende av denna aktör.

Enligt propositionen ska sådana aktörer oavsett storlek med stöd av förordning av statsrådet kunna omfattas av tillämpningsområdet för den föreslagna lagen om hantering av cybersäkerhetsrisker.

I lagen om hantering av cybersäkerhetsrisker föreskrivs det om skyldigheterna enligt NIS 2-direktivet för de aktörer som omfattas av direktivets minimitillämpningsområde och som också är de aktörer som avses i dessa punkter. När lagens tillämpningsområde utsträcks till sådana aktörer är det fråga om en mycket detaljerad definition av aktör eller typ av aktör. Dessa aktörer, oavsett storlek, omfattas på grund av verksamhetens särskilda art undantagsvis av tillämpningsområdet för skyldigheterna enligt lagen och NIS 2-direktivet. Med beaktande av kriterierna kan tillämpningsområdet för dessa aktörer förändras om aktörernas verksamhet eller verksamhetsmiljö förändras. Därför är det lagtekniskt nödvändigt att överföra lagstiftningsbehörighet. En utvidgning av tillämpningsområdet till att omfatta de beskrivna aktörerna kan förväntas utgöra en exceptionell åtgärd, och gruppen aktörer och aktörstyper som omfattas av tillämpningsområdet skulle förändras i takt med samhällsutvecklingen.

Bemyndigandet att utfärda förordning uppfyller kraven i 80 § i grundlagen. Genom förordning kan man inte avvika från bestämmelserna i lagen eller föreskriva om annat än att lagens tillämpningsområde ska utsträckas till aktörer som uppfyller de kriterier som anges i lagen. Genom förordning kan det inte föreskrivas om ändringar i de rättigheter och skyldigheter som aktörerna har enligt lagen om hantering av cybersäkerhetsrisker. Bestämmelsen om bemyndigande att utfärda förordning har bedömts vara ändamålsenlig och noga avgränsad. *Kommunikationsministeriets bemyndigande att utfärda förordning om avgifter*

I 19 § 6 mom. i lagen om hantering av cybersäkerhetsrisker föreslås ett bemyndigande för kommunikationsministeriet att utfärda förordning om de avgifter, eller grunderna för dem, som CSIRT-enheten kan ta ut för tjänster som avses i paragrafens 2 mom. 1 och 2 punkt och som tillhandahållits på begäran av en aktör eller någon annan part. Bemyndigande att utfärda förordning behövs, eftersom det är fråga om att fastställa grunderna för de avgifter som tas ut för tillhandahållande av en ny typ av tjänst. CSIRT-enheten är placerad vid Transport- och kommunikationsverkets Cybersäkerhetscenter. Bemyndigandet att utfärda förordning ska i stället för statsrådet anvisas kommunikationsministeriet, eftersom en ministerieförordning är en tillräcklig författningsnivå med tanke på ärendets innehåll och eftersom det genom förordning av kommunikationsministeriet av hävd har utfärdats bestämmelser om grunderna för avgifter för Transport- och kommunikationsverkets prestationer.

Myndigheternas behörighet att meddela föreskrifter

Propositionen innehåller flera förslag om normgivningsbemyndigande för tillsynsmyndigheten eller Transport- och kommunikationsverket. Bemyndigandena att meddela föreskrifter är noggrant avgränsade, och föreskrifter kan meddelas endast för precisering av de i lag föreskrivna omständigheterna för en begränsad målgrupp. Bemyndigandena behövs för att precisera tekniska detaljer och beakta sektorspecifika särdrag. Bemyndigandena anses vara sakliga på så sätt att de är noggrant avgränsade och gäller bestämda frågor för vilka det finns särskilda skäl som hänför sig till föremålet för regleringen, och regleringens betydelse i sak kräver inte reglering genom lag eller förordning.

I 9 § 4 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker föreskrivs det om bemyndigande för tillsynsmyndigheten att inom sitt ansvarsområde meddela närmare tekniska föreskrifter om de omständigheter som i fråga om riskhanteringen avses i momentet. Myndighetens bemyndigande att meddela föreskrifter gäller förtydligande och precisering av innehållet i de omständigheter enligt momentet som hänför sig till skyldigheten att hantera risker inom cybersäkerheten. De närmare föreskrifterna kan dock endast gälla tekniska omständigheter, dvs. de får inte utvidga skyldigheterna enligt 9 § eller ändra skyldigheternas innehåll i sak. Föreskrifterna ska vara teknikneutrala. Bemyndigandet att meddela föreskrifter behövs, eftersom det med tanke på tillämpningen kan vara nödvändigt att precisera nämnda omständigheter inom riskhanteringen särskilt med beaktande av särdragen i den sektorspecifika verksamheten. Med tanke på den tekniska utvecklingen är det dessutom nödvändigt att tillsynsmyndigheten genom en föreskrift kan uppdatera omständigheter som gäller riskhanteringen. Genom föreskrifter kan man alltså hålla den obligatoriska riskhanteringen uppdaterad och bättre beakta sektorspecifika särdrag i fråga om genomförandet av riskhanteringen. Det bidrar till uppnåendet av NIS 2-direktivets mål att vidta riskhanteringsåtgärder som är lämpliga i förhållande till den föreliggande risken.

I 11 § 5 mom. i lagen om hantering av cybersäkerhetsrisker föreskrivs det att tillsynsmyndigheten vid behov inom sitt ansvarsområde kan meddela närmare tekniska föreskrifter om när en incident som avses i 1 mom. är betydande, om de uppgifter som ska lämnas i slutrapporten samt om förfarandet för anmälan av betydande incidenter och uppgifter enligt 12 och 13 §. Bemyndigandet att meddela föreskrifter behövs, eftersom det genom föreskrifterna kan föreskrivas mer detaljerat om omständigheter som är av sektorspecifik betydelse och med beaktande av sektorernas särdrag.

I förslaget till ändring av 90 § 2 mom. i lagen om behandling av kunduppgifter inom social- och hälsovården finns ett bemyndigande för Institutet för hälsa och välfärd att meddela närmare föreskrifter om när en störning är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bemyndigandet att meddela föreskrifter ändras inte genom propositionen, men det föreslås att bemyndigandet också ska gälla störningar som orsakas av informationssystem och kommunikationsnät.

I 165 § 3 mom. i förslaget till lag om ändring av lagen om tjänster inom elektronisk kommunikation finns ett bemyndigande för Transport- och kommunikationsverket att meddela föreskrifter om hur registrarens anmälan ska göras innan verksamheten inleds och om innehållet i anmälan. Propositionen ändrar inte bemyndigandet att meddela föreskrifter jämfört med nuläget, men de ändringar som föreslås i 1, 2 och 4 mom. i samma paragraf är av betydelse för tillämpningsområdet för bemyndigandet att meddela föreskrifter.

I 167 § 5 mom. i den föreslagna lagen om ändring av lagen om tjänster inom elektronisk kommunikation föreskrivs det om Transport- och kommunikationsverkets behörighet att meddela föreskrifter. Det föreslås att bemyndigandet utvidgas så att verket kan meddela närmare föreskrifter också om verifiering av uppgifterna om domännamnsanvändaren. Med detta avses till

exempel de riktlinjer och förfaranden som en registrar ska införa för att säkerställa att de uppgifter som avses i 1 mom. och som lämnats av domännamnsanvändaren är korrekta och uppdaterade.

I 170 § 2 mom. i förslaget till lag om ändring av lagen om tjänster inom elektronisk kommunikation föreskrivs det om bemyndigande för Transport- och kommunikationsverkets att meddela föreskrifter. Bemyndigandet för Transport- och kommunikationsverket att meddela föreskrifter föreslås med anledning av de nya punkter 8–11 som fogas till 1 mom. bli utvidgat så att verket kan meddela närmare föreskrifter också om information som ska göras offentligt tillgänglig, om givande av åtkomst till uppgifter samt om riktlinjer och förfaranden.

I 275 § 3 mom. i förslaget till lag om ändring av lagen om tjänster inom elektronisk kommunikation föreskrivs det om ett bemyndigande för Transport- och kommunikationsverket att meddela föreskrifter. Med stöd av bemyndigandet får verket 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.

8.2 De bemyndiganden att utfärda bestämmelser på lägre nivå än lag som upphävs genom propositionen.

Statsrådets förordning om samhällsviktiga flygplatser och hamnar

Genom förslaget upphävs 128 a § i luftfartslagen. I paragrafens 3 mom. finns ett bemyndigande för statsrådet att utfärda förordning om när en flygplats ska betraktas som samhällsviktig. Genom förslaget upphävs 7 e § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet. Enligt 7 e § 3 mom. föreskrivs det genom förordning av statsrådet när en hamn som avses i 1 mom. ska betraktas som samhällsviktig.

Genom förslaget upphävs tillsammans med förslaget om upphävande av 7 e och 7 f § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet också statsrådets förordning om samhällsviktiga flygplatser och hamnar (361/2018). Den förordning som upphävs har utfärdats med stöd av 128 a § i luftfartslagen och 7 e § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, vilka föreslås bli upphävda. Eftersom det föreslås att båda dessa bestämmelser som innehåller ett bemyndigande att utfärda förordning upphävs, kan den statsrådsförordning som utfärdats med stöd av dem inte förbli i kraft. Bemyndigandet att utfärda förordning om samhällsviktiga flygplatser och hamnar behövs inte i fortsättningen, eftersom skyldigheterna enligt NIS 2-direktivet i fortsättningen, i enlighet med storlekskriteriet i fråga om tillämpningsområdet för NIS 2-direktivet och den föreslagna allmänna lagen, ska tillämpas på de flygplatser och hamnar som omfattas av tillämpningsområdet. I fortsättningen är det därför inte nödvändigt att genom lag eller genom förordning av statsrådet som utfärdats med stöd av lag föreskriva särskilt om samhällsviktiga flygplatser och hamnar.

Bemyndigande att meddela föreskrifter

Genom propositionen upphävs de sektorspecifika genomförandebestämmelserna i NIS 1-direktivet, eftersom motsvarande bestämmelser i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker. De bemyndiganden att meddela föreskrifter som myndigheterna getts med anledning av bestämmelserna i NIS 1-direktivet upphävs i de ovan nämnda lagarna, eftersom det i fortsättningen ska föreskrivas i den föreslagna lagen om hantering av cybersäkerhetsrisker om en incidents betydelse samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Tillsynsmyndigheternas bemyndigande att meddela föreskrifter om incidentens betydelse, innehållet i slutrapporten om incidenten samt förfarandet för anmälan av uppgifter enligt delrapporten och slutrapporten om betydande incidenter ska i fortsättningen ingå i 11 § 4 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 128 b § i luftfartslagen. Enligt paragrafens 4 mom. får Transport- och kommunikationsverket meddela närmare föreskrifter om när en händelse som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 169 § i spårtrafiklagen. Enligt paragrafens 5 mom. får Transport- och kommunikationsverket meddela närmare föreskrifter om när en sådan störning som avses i 2 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 34 a § i naturgasmarknadslagen. Enligt paragrafens 5 mom. får Energimyndigheten meddela närmare föreskrifter om när en händelse som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 29 a § i elmarknadslagen. Enligt paragrafens 5 mom. får Energimyndigheten meddela närmare föreskrifter om när en störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Samtidigt upphävs 49 a § 5 mom., som innehåller ett bemyndigande för Energimyndigheten att meddela närmare föreskrifter om innehållet i anmälningarna, om anmälningarnas form och om hur de lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bestämmelser och anknytande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 7 f § i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet. Enligt paragrafens 4 mom. får Transport- och kommunikationsverket meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 18 a § i lagen om fartygstrafikservice. Enligt paragrafens 4 mom. får Transport- och kommunikationsverket meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

Genom förslaget upphävs 18 kap. 161 § i lagen om transportservice. Enligt paragrafens 5 mom. får Transport- och kommunikationsverket meddela närmare föreskrifter om när en sådan störning som avses i 2 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in. Bestämmelsen behövs inte, eftersom motsvarande bemyndigande att meddela föreskrifter i fortsättningen ska ingå i lagen om hantering av cybersäkerhetsrisker.

9 Ikraftträdande

Lagarna föreslås i huvudsak träda i kraft den 18 oktober 2024. Det föreslås att 43 § i lagförslag 1 träder i kraft den 1 januari 2025. Paragrafen gäller registrering av aktörer och lämnande av uppgifter till tillsynsmyndigheterna.

NIS 2-direktivet förutsätter att medlemsstaterna senast den 17 oktober 2024 antar och offentliggör de bestämmelser som är nödvändiga för att följa direktivet och tillämpar dem från och med den 18 oktober 2024. Lagen föreslås träda i kraft vid den tidpunkt som i artikel 41 i NIS 2-direktivet anges för det nationella genomförandet, dvs. den 18 oktober 2024.

Det föreslås dock att skyldigheten att lämna uppgifter för förande av den förteckning över aktörer som avses i 43 § ska träda i kraft den 1 januari 2025, vilket ger tillsynsmyndigheterna och aktörerna en längre övergångsperiod för anmälan till aktörsförteckningen. NIS 2-direktivet förutsätter inte att myndigheterna före 2025 gör anmälningar som baserar sig på uppgifterna i aktörsförteckningen.

10 Verkställighet och uppföljning

I artikel 40 i NIS 2-direktivet föreskrivs det om skyldighet för kommissionen att se över hur direktivet fungerar.

Senast den 17 oktober 2027 och därefter var 36:e månad ska kommissionen se över hur direktivet fungerar och rapportera resultatet till Europaparlamentet och rådet. Rapporten ska särskilt bedöma relevansen av de berörda enheternas storlek och sektorer, delsektorer och typer när det gäller den entitet som avses i bilagorna I och II till NIS 2-direktivet för ekonomins och samhällets funktion när det gäller cybersäkerhet. För detta ändamål och för att ytterligare främja det strategiska och operativa samarbetet ska kommissionen beakta rapporterna från den samarbetsgrupp som avses i artikel 14 i NIS 2-direktivet och CSIRT-nätverket om de erfarenheter som förvärvats på strategisk och operativ nivå. Rapporten om översynen ska vid behov åtföljas av ett lagstiftningsförslag.

På nationell nivå följs verkställandet av de föreslagna lagarna av kommunikationsministeriet. Uppföljningen bedömer särskilt konsekvenserna för de aktörer som omfattas av tillämpnings-

området, hanteringsåtgärderna för cybersäkerheten och antalet anmälningar om betydande incidenter samt utfallet av myndighetssamarbetet och den sektorsvis decentraliserade tillsynsmodellen i förhållande till syftena med lagen och de bedömda konsekvenserna av den. En efterhandsutvärdering av lagen om hantering av cybersäkerhetsrisker ska genomföras 2026–2027.

Transport- och kommunikationsverket fortsätter verksamheten i den nationella samarbetsgrupp för tillsynsmyndigheter som inrättades i samband med genomförandet av NIS 1-direktivet. Samarbetsgruppen ska stödja genomförandet av regelverket vid tillsynsmyndigheterna. Tillsynsmyndigheterna ska vid behov stödja aktörerna i verkställandet av regleringen med hjälp av anvisningar, rekommendationer, information och rådgivning.

11 Förhållande till andra propositioner

11.1 Samband med andra propositioner

Propositionen har samband med det nationella lagstiftningsprojektet för genomförande av Europaparlamentets och rådets direktiv om kritiska entiteters motståndskraft (CER-direktivet, (EU) 2022/2557) (SM047:00/2022) och den regeringsproposition som bereds i projektet. Uppgifterna om projektet finns i statsrådets projektportal (https://valtioneuvosto.fi/sv/projektet?tunnus=SM047:00/2022) och en proposition som hänför sig till verkställigheten ska lämnas till riksdagen/har lämnats till riksdagen [xx]. Med stöd av CER-direktivet ska de aktörer som identifieras som samhällets kritiska aktörer omfattas av skyldigheterna enligt NIS 2-direktivet. Därför föreslås det att tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker också ska omfatta aktörer som med stöd av CER-direktivet identifieras som samhällets kritiska aktörer i samband med detta projekt. Propositionen innehåller också förslag i fråga om samarbetet mellan de myndigheter som utövar tillsyn över den reglering som utfärdats med stöd av CER-direktivet och NIS 2-direktivet.

Propositionen har samband med det nationella lagstiftningsprojektet (VM067:00/2022) för genomförande av Europaparlamentets och rådets direktiv om digital operativ motståndskraft för finanssektorn (DORA-förordningen, (EU) 2022/2554) och den proposition som bereds i projektet. Uppgifterna om projektet finns i statsrådets projektportal (https://vm.fi/sv/projekt?tunnus=VM067:00/2023) och en proposition som kompletterar förordningen ska lämnas till riksdagen/har lämnats till riksdagen [xx]. DORA-förordningen innehåller mer detaljerade krav på riskhantering i fråga om cybersäkerhet för de aktörer som omfattas av förordningens tillämpningsområde än NIS2-direktivet. Förordningen ska i enlighet med artikel 1.2 i DORA-förordningen och artikel 4 i NIS2-direktivet tillämpas på dessa aktörer i stället för NIS 2-direktivet. DORA-förordningen och NIS 2-direktivet innehåller dessutom bestämmelser om samarbete mellan tillsynsmyndigheterna.

11.2 Förhållande till budgetpropositionen

[Kompletteras senare.]

12 Förhållande till grundlagen samt lagstiftningsordning

Propositionen innehåller konstitutionellt relevanta förslag i förhållande till lagbundenheten vid utövning av offentlig makt enligt 2 § 3 mom. i grundlagen, skyddet för privatlivet, personuppgifter och förtroliga meddelanden enligt 10 § i grundlagen, näringsfriheten enligt 18 § i grundlagen, rättsskyddet enligt 21 § i grundlagen, bestämmelserna om utfärdande av förordning och delegering av lagstiftningsbehörighet i 80 § i grundlagen, bestämmelserna om avgifter för statlig verksamhet i 81 § i grundlagen och bestämmelserna om överföring av förvaltningsuppgifter på andra än myndigheter i 124 § i grundlagen.

12.1 Skyddet för förtrolig kommunikation

I förslaget ingår flera bestämmelser som är av betydelse med tanke på det skydd för förtrolig kommunikation som tryggas i 10 § i grundlagen. Sådana bestämmelser finns särskilt i 20 § om nätbaserad kartläggning av sårbarheter, och dessutom i 22, 24 och 28 §, som gäller utlämnande av information i samband med förmedlingsuppgifter och meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando.

Enligt 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Dessutom är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Enligt 4 mom. i paragrafen kan det genom lag föreskrivas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång, vid säkerhetskontroll och under frihetsberövande samt för att inhämta information om militär verksamhet eller sådan annan verksamhet som allvarligt hotar den nationella säkerheten. Grundlagsutskottet har konstaterat att utgångspunkten för det skydd för privatlivet som tryggas i 10 § i grundlagen är individens rätt att leva sitt eget liv utan godtycklig eller ogrundad inblandning av myndigheter eller andra utomstående (GrUU 53/2005 rd, s. 2, GrUU 36/2002 rd, s. 5/II, GrUU 9/2004 rd, s. 5/II).

I artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna föreskrivs det att var och en har rätt till respekt för sina kommunikationer. Skyddet för förtroliga meddelanden tryggas också i artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna (FördrS 63/1999), enligt vilken var och en har rätt till skydd för sin korrespondens. Offentliga myndigheter får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Vid bedömningen av förslagen är det dessutom relevant att beakta artikel 5 i direktivet om integritet och elektronisk kommunikation, dvs. Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (2002/58/EG), enligt vilken medlemsstaterna ska säkerställa konfidentialiteten vid elektronisk kommunikation. Enligt artikel 15 i direktivet om integritet och elektronisk kommunikation får en medlemsstat genom lagstiftning vidta åtgärder för att begränsa konfidentialiteten vid elektronisk kommunikation, om sådana begränsningar är nödvändiga, lämpliga och proportionella bland annat för att förebygga, undersöka och avslöja obehörig användning av ett elektroniskt kommunikationssystem.

Kartläggning av sårbarheter

Konfidentialiteten vid kommunikation ska för det första granskas med avseende på den kartläggning av sårbarheter som avses i 20 § i förslaget. Enligt förslaget ska CSIRT-enheten ha rätt att på eget initiativ, på ett proaktivt och icke-inkräktande sätt upptäcka och kartlägga sårbarheter eller osäkra kommunikationsnät, anordningar eller system i allmänt tillgängliga kommunikationsnät och informationssystem. Syftet med observationen är att få information om ett sårbart objekt innan sårbarheten utnyttjas och att förmedla information om sårbarheten till den aktör som administrerar det sårbara objektet, så att korrigerande åtgärder kan vidtas och eventuella kränkningar av informationssäkerheten i anslutning till sårbara anordningar eller system kan undvikas. Det har alltså ansetts finnas en vägande grund för kartläggningen i anknytning till förberedelserna inför cyberhot och förebyggande av skadliga verkningar av cyberattacker i samhället.

Det tekniska genomförandet av sårbarhetskartläggningen behandlas närmare i specialmotiveringen till paragrafen, men utifrån motiveringen kan det konstateras att verksamheten inte bedöms ha betydande konsekvenser för de grundläggande fri- och rättigheterna annat än i fråga om de uppgifter som behandlas i samband med den. Förslaget möjliggör inte intrång i kommunikationsnät eller system, utan det handlar om observation av öppna och oskyddade anordningar och system i det allmänna kommunikationsnätet. Vid sårbarhetskartläggningen hanteras inte information eller kommunikation i kommunikationsnät eller informationssystem. I sårbarhetskartläggningen hanteras dock förmedlingsuppgifter som är av betydelse med tanke på kommunikationens konfidentialitet. Förmedlingsuppgifterna fungerar som tekniska identifieringsuppgifter för skadlig verksamhet, och därför är det nödvändigt att behandla dem för att identifiera sårbara objekt eller sårbarheter i vissa tekniska situationer, såsom till exempel för att upptäcka ett skadligt datorprogram. Förslaget utesluter hanteringen av information om meddelandets innehåll från observationsverksamheten, och därför behöver förslaget till denna del inte bedömas i ljuset av de frågor som gäller de grundläggande fri- och rättigheterna i fråga om meddelandets innehåll.

När det gäller skyddet för förtroliga meddelanden har grundlagsutskottet konstaterat att meddelandens identifieringsuppgifter, för vilka termen förmedlingsuppgifter sedermera har börjat användas, inte omfattas av kärnområdet i den rättighet som gäller sekretess i fråga om konfidentiella meddelanden. Utskottet har därför till exempel ansett det möjligt att rätten att få identifieringsuppgifter inte binds till vissa typer av brott, om bestämmelserna i övrigt uppfyller de allmänna kraven på begränsningar av de grundläggande fri- och rättigheterna (GrUU 7/1997 rd, s 2/I, GrUU 26/2001 rd, s. 3/II). Grundlagsutskottet har dock konstaterat att identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6/II). Det kan konstateras att ändamålet med behandlingen enligt förslaget inte är en sådan sammanställning eller sammanställning av uppgifter som har betydande konsekvenser med tanke på skyddet för privatlivet, eftersom det snarare är fråga om användning av förmedlingsuppgifter som en teknisk identifiering för att upptäcka en sårbar anordning.

Förslaget bedöms också uppfylla kravet på exakthet och noggrann avgränsning. Förslaget innehåller ett flertal faktorer som avgränsar verksamheten. För det första är verksamheten avgränsad till allmänt tillgängliga kommunikationsnät och informationssystem, dvs. förslaget utesluter bland annat privata nät. Syftet med verksamheten har avgränsats till att upptäcka sårbara eller osäkert konfigurerade kommunikationsnät och informationssystem och informera de berörda

parterna om iakttagelserna samt till att upprätthålla en lägesbild över cybersäkerheten. Verksamheten kan således inte bedrivas för något annat ändamål. Information får genom teknisk förfrågning inhämtas om identifieringsuppgifter för teleterminalutrustning och informationssystem samt deras datakommunikationsarrangemang, de programvaror som används och deras funktion och tekniska genomförande och de tjänster som tillhandahållits med hjälp av dem. Dessa uppgifter har bedömts vara nödvändiga bland annat för att upptäcka utrustning som innehåller kritiska sårbarheter och bedöma hur allvarligt cyberhotet är. I förslaget finns en uttömmande förteckning över uppgifterna. Förslaget har dessutom avgränsats så att verksamheten inte får orsaka olägenhet för den utrustning eller det system som kartläggningen gäller. Genom verksamheten får inte heller inhämtas information om kommunikation som förmedlas i ett allmänt kommunikationsnät eller i en allmänt tillgänglig kommunikationstjänst, vilket är av betydelse också med tanke på proportionalitetsprincipen.

De begränsningar av de grundläggande fri- och rättigheterna som gäller de uppgifter som behandlas under sårbarhetskartläggningen har bedömts stå i rätt proportion till nyttan. Kartläggningen ger betydande fördelar genom att förebygga informationssäkerhetskränkningar som kan ha rentav betydande konsekvenser för individer och samhället till exempel i form av dataintrång eller störningar av verksamheten. Förslaget har också avgränsats på det sätt som beskrivs ovan så att det i sin helhet uppfyller proportionalitetskravet.

Förslaget bedöms inte vara problematiskt med tanke på rättsskyddet, eftersom förslagets uttryckliga syfte är att kunna lämna information om sårbara anordningar och system till dem som administrerar dem. Dessutom innehåller förslaget betydande avgränsningar, i synnerhet med tanke på rättsskyddet, i fråga om vad uppgifterna kan användas till. Informationen får användas endast för att underrätta föremålet för kartläggningen om sårbarheter och risker som riktas mot kommunikationsnätet eller informationssystemet samt för att identifiera cyberhot, upprätthålla en lägesbild över cybersäkerheten och informera om sårbarheter. Förslaget innehåller också en skyldighet att radera onödig information.

Förslaget har inte heller bedömts vara problematiskt med tanke på människorättsförpliktelserna. Europeiska unionens domstol (EUD) och Europadomstolen har i flera avgöranden behandlat främst statliga aktörers oriktade inhämtande, behandling och förvaring av information, som typiskt har beröringspunkter med civil eller militär underrättelseinhämtning. I de fall som gäller artiklarna 8 och 10 i Europakonventionen har man allmänt beaktat de i artiklarna angivna grunderna för begränsning av rättigheter. Inskränkningsgrundernas centrala innehåll är kravet på att bestämmelser ska utfärdas genom lag och att det i ett demokratiskt samhälle är nödvändigt, till exempel för att trygga den nationella och allmänna säkerheten. Därför ska oriktat inhämtande av information (bulk interception) inom ramen för Europakonventionen till exempel för att trygga den nationella säkerheten ske så att det genom nationell lag utfärdas bestämmelser om inhämtande av information och att intrång i enskildas rätt är nödvändigt i ett demokratiskt samhälle. (t.ex. Kennedy mot Förenade kungariket, punkt 155; Roman Sacharov mot Ryssland, punkt 236). Europadomstolen har i sina avgöranden *Big Brother Watch och andra mot Förenade kungadömet* och *Centrum för Rättvisa mot Sverige* skapat en ram för bedömning av särskilda villkor för lagstiftningsåtgärderna och för hur väl åtgärderna räcker till. Det är värt att notera att grundlagsutskottet i sin utlåtandepraxis inte heller har ansett det möjligt att i underrättelseverksamhet övervaka all datatrafik på ett allmänt, oriktat och heltäckande sätt (GrUB 4/2018 rd, s. 8). Det nu aktuella förslaget handlar inte om sådan informationsinhämtning eller övervakning av datatrafik.

Den föreslagna sårbarhetskartläggningen avviker på två viktiga sätt från det oriktade inhämtande av information som Europadomstolen och EUD behandlat i de nämnda fallen. Verksamhet som avses i de nämnda avgörandena innebär i praktiken inhämtning av information i telekommunikationen genom att fånga själva trafiken mellan parterna i kommunikationen. Kartläggningen av sårbarheter innefattar inte att kommunikationen mellan parterna kapas eller analyseras. Den som genomför sårbarhetskartläggningen är i stället själv en part i kommunikationen genom att sända begäranden till en server i det allmänna kommunikationsnätet och analysera de tekniska svar som servern skickar, vilket gör det möjligt att upptäcka en sårbarhet. I denna situation handlar man på en annan nivå av datakommunikationen, som inte på motsvarande sätt är problematisk med tanke på människorättsförpliktelser eller konfidentiell kommunikation, eftersom det inte är fråga om att övervaka kommunikationen. En annan betydande skillnad är syftet med verksamheten. Domstolarnas avgöranden har ofta fokuserat på underrättelsemyndigheternas verksamhet, det vill säga inhämtande av information om verksamhet som hotar säkerheten. Syftet med förslaget är däremot att förbättra informationssäkerheten för de aktörer som är föremål för kartläggningen genom att upptäcka allmänt tillgängliga tekniska egenskaper hos kommunikationsnät och informationssystem och därigenom bland annat främja konfidentialiteten vid kommunikation samt skydda och förbättra säkerheten för kommunikation eller information som förmedlas i kommunikationsnätet och informationssystemet.

I förslaget ingår också en mer riktad kartläggning än den som nämns ovan och som görs på objektets begäran. Kartläggning av sårbarheter som görs på begäran har inte bedömts vara särskilt problematisk med tanke på de grundläggande fri- och rättigheterna, uttryckligen för att det är fråga om en åtgärd som genomförs på objektets begäran och i den omfattning som denne fastställer. En riktad kartläggning av sårbarheter inbegriper inte någon möjlighet att behandla innehållet i kommunikationen utan samtycke av kommunikationsparten. Genom kartläggning av sårbarheter får information inte inhämtas om kommunikation som förmedlas i kommunikationsnätet eller i allmänt tillgängliga kommunikationstjänster.

På de grunder som anförts ovan bedöms förslaget om kartläggning av sårbarheter vara förenligt med förutsättningarna i 10 § i grundlagen.

Informationsutbyte om förmedlingsuppgifter och skadligt innehåll

I 22, 24 och 28 § i förslaget finns bestämmelser om utlämnande av information om meddelanden som innehåller förmedlingsuppgifter och skadliga datorprogram eller skadliga kommandon. I 22 § i förslaget är det fråga om informationsutbyte mellan aktörer som deltar i ett frivilligt arrangemang. CSIRT-enheten kan lämna ut ett meddelande som innehåller ett skadligt datorprogram eller kommando till aktörer som deltar i arrangemanget för informationsutbyte, om det behövs för att förebygga och upptäcka cyberhot samt reagera på och återhämta sig från incidenter eller begränsa deras inverkan.

Dessutom innehåller 24 § möjligheten för en aktör eller för en part som deltar i ett frivilligt arrangemang för informationsutbyte enligt 22 § att på eget initiativ lämna ut förmedlingsuppgifter eller ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando till CSIRT-enheten, tillsynsmyndigheten eller någon annan aktör som deltar i ett sådant arrangemang som avses i förslaget, när det är fråga om förmedlingsuppgifter som har samband med ett cyberhot eller en incident.

Enligt 28 § i förslaget har tillsynsmyndigheten trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få förmedlingsuppgifter, lokaliseringsuppgifter eller meddelanden som innehåller ett skadligt datorprogram eller ett

skadligt kommando, om det är nödvändigt för att övervaka de skyldigheter som gäller hantering av cybersäkerhetsrisker eller för att utreda betydande incidenter.

När det gäller kommunikationens konfidentialitet har grundlagsutskottets praxis i fråga om förmedlingsuppgifter redan lyfts fram. Grundlagsutskottet har ansett det möjligt att rätten att få identifieringsuppgifter inte binds till vissa typer av brott, om bestämmelserna i övrigt uppfyller de allmänna kraven på begränsningar av de grundläggande fri- och rättigheterna, eftersom förmedlingsuppgifterna inte har ansetts höra till kärnområdet för 10 § i grundlagen. I sin senare praxis har grundlagsutskottet dock konstaterat att identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är (GrUU 18/2014 rd, s. 6/II). I det informationsutbyte som avses i förslaget bedöms det inte vara fråga om en begränsning som är betydande med tanke på skyddet för privatlivet. Med hjälp av informationen kan man identifiera och förhindra skadlig trafik, och informationen används som teknisk identifiering för ovan beskrivna ändamål och inte som information om privatlivet.

Ett meddelande som innehåller ett skadligt datorprogram eller kommando kan dock tänkas gälla meddelandets innehåll. Meddelandets innehåll har som sådant traditionellt åtnjutit ett starkt skydd inom ramen för de grundläggande fri- och rättigheterna och innehållet i ett privat meddelande har ansetts höra till kärnområdet för skyddet för konfidentialitet vid kommunikation. I ett meddelande som innehåller ett skadligt datorprogram eller kommando är det å andra sidan ofta fråga om ett automatiserat phishingmeddelande som syftar till att vilseleda mottagaren att exekvera ett skadligt datorprogram eller att förse angriparen med användbar information. Syftet med behandlingen av ett meddelande som innehåller ett skadligt datorprogram eller kommando är inte att få reda på innehållet i meddelande. Ett sådant meddelande innehåller i regel inte personlig kommunikation som hör till kärnan i skyddet för konfidentiell kommunikation utan är endast avsett att tas emot av den ena parten. Ett meddelande som innehåller ett skadligt datorprogram eller kommando är i regel ett phisingmeddelande som genereras automatiskt av ett skadligt datorprogram eller som en aktör som utför cyberattacker sänder till en okänd mottagargrupp. Man kan med fog också komma fram till en tolkning där ett meddelande med ett skadligt datorprogram eller ett skadligt kommando som skapats för att genomföra en cyberattack inte hör till kärnan i skyddet för konfidentiell kommunikation. Syftet med behandlingen av ett meddelande är att undersöka eller utreda de tekniska egenskaperna hos ett skadligt program samt att varna allmänheten för motsvarande meddelanden. Grundlagsutskottet bedömer i vilken utsträckning sådan kommunikation med skadliga program åtnjuter skydd för konfidentialitet vid kommunikation eller placerar sig inom kärnan av skyddet för konfidentialitet vid kommunikation till exempel i fråga om meddelandets tekniska egenskap av skadligt datorprogram eller dess förmedlingsuppgifter.

Syftet med förslagen är att förbättra informationssäkerheten genom informationsutbyte om skadlig teknik. Det innebär att uppgifter om ett skadligt datorprogram eller kommando eller förmedlingsuppgifter kan användas för att identifiera verksamhet som äventyrar informationssäkerheten samt för att skydda sig mot motsvarande meddelanden som innehåller ett skadligt datorprogram eller kommando och för att utreda deras tekniska egenskaper. Det är ofta nödvändigt att i detta syfte behandla ett meddelande som innehåller ett skadligt datorprogram eller kommando. Ett meddelande som innehåller ett skadligt datorprogram eller kommando har ofta genererats automatiskt av ett skadligt datorprogram och det har inte sänts av en fysisk person utan av ett skadligt program eller den som programmerat det. Behandlingen av ett meddelande

som innehåller ett skadligt datorprogram eller kommando gör det möjligt att utreda dess tekniska egenskaper och varna allmänheten för motsvarande meddelanden. Dessutom kan man med tanke på det i rättssystemet etablerade förbudet mot rättsmissbruk hävda att skyddet för konfidentiell kommunikation inte ska tolkas på ett sätt som hindrar att teknisk information om ett meddelande som innehåller ett skadligt datorprogram behandlas i syfte att förebygga verkningarna av programmet, i det fall att skyddet för konfidentiell kommunikation skulle skydda en verksamhet vars syfte är att allvarligt äventyra just skyddet för konfidentiell kommunikation i elektronisk kommunikation. Det är särskilt med tanke på cyberberedskapen hos kritiska samhällsaktörer viktigt att information om de skadliga datorprogram som används vid angrepp kan delas mellan de potentiella objekten för angreppen.

I lagen om militär underrättelseverksamhet (590/2019) föreskrivs det i fråga om underrättelseinhämtning som avser datatrafik att det är möjligt att till företag, sammanslutningar och myndigheter lämna ut information om ett skadligt datorprogram eller ett skadligt kommando. Förslaget motiveras med att det med tanke på det övergripande skyddet av samhället är viktigt att uppgifter om skadliga datorprogram som används vid angrepp i så stor utsträckning som möjligt kan lämnas ut till de potentiella offren för angreppen. Genom att föreskriva om rätt att överlåta dylika uppgifter kan man garantera möjligheter för företagen och sammanslutningarna att vidta sådana åtgärder för att sörja för sin datasäkerhet om vilka det föreskrivs i 272 § i lagen om tjänster inom elektronisk kommunikation. Åtgärder i överenstämmelse med bestämmelsen i fråga kan innehålla bl.a. automatisk utredning av innehållet i ett meddelande, automatiskt förhindrande eller begränsande av förmedling och mottagande av meddelanden samt automatiskt avlägsnande ur meddelanden av skadliga datorprogram som äventyrar datasäkerheten (RP 203/2017 rd). I sitt utlåtande om propositionen i ärendet lyfte grundlagsutskottet inte fram den föreslagna bestämmelsen som problematisk med avseende på de grundläggande fri- och rättigheterna.

Allmänt taget har förslagen i första hand en begränsande effekt på skyddet för förtroliga meddelanden i samband med informationsutbyte. Å andra sidan grundar sig informationsutbytet bland annat på att konfidentiell kommunikation skyddas genom beredskap för och skydd mot cyberhot, varvid skyddet för konfidentiell kommunikation indirekt främjas genom att det begränsas i en enskild situation. Den konsekvens som skyddet av förtroliga meddelanden har för de grundläggande fri- och rättigheterna är således en indirekt följd av myndigheternas åtgärder i samband med undersökning, förebyggande och eliminering av kränkningar av informationssäkerheten.

Grundlagsutskottet har konstaterat att meddelandens identifieringsuppgifter, för vilka termen förmedlingsuppgifter sedermera har börjat användas, inte omfattas av kärnområdet i den rättighet som gäller sekretess i fråga om konfidentiella meddelanden, och utskottet har därför till exempel ansett det möjligt att rätten att få identifieringsuppgifter inte binds till vissa typer av brott, om bestämmelserna i övrigt uppfyller de allmänna kraven på begränsningar av de grundläggande fri- och rättigheterna (GrUU 7/1997 rd, s 2/I, GrUU 26/2001 rd, s. 3/II). I förslaget är det fråga om en situation av det slaget, eftersom förslagen bedöms uppfylla de allmänna kraven på begränsningar, bland annat att de ska föreskrivas genom lag, vara exakta och noggrant avgränsade, godtagbara, proportionella och inte inkräkta på kärnområdet för rättigheten.

Behandlingen av ett meddelande som innehåller ett skadligt datorprogram eller kommando av det slag som beskrivs bedöms ligga utanför kärnan i skyddet för konfidentiell kommunikation, med beaktande av behandlingens syfte och mål i förhållande till begränsningens art och betydelse. Eftersom det är förpliktande att genomföra direktivet måste det dessutom finnas möjlighet att behandla dessa uppgifter för att uppnå målen i förslaget. Förslaget uppfyller också i övrigt

de allmänna kraven på begränsningar. Förslagen om informationsutbyte bedöms därför vara förenliga med grundlagen och bedöms därmed kunna behandlas i vanlig lagstiftningsordning. Med anledning av förslaget om behandling av ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando är det dock nödvändigt att begära grundlagsutskottets utlåtande om propositionen.

12.2 Överföring av förvaltningsuppgifter på andra än myndigheter och avgifter för myndigheters prestationer

Anlitande av utomstående sakkunniga vid inspektion.

Med stöd av 29 § i den föreslagna lagen om hantering av cybersäkerhetsrisker kan tillsynsmyndigheten anlita eller bemyndiga ett godkänt bedömningsorgan för informationssäkerhet eller en utomstående expert i informationsteknik att förrätta inspektionen, om det är nödvändigt på grund av inspektionens art eller omfattning. Med stöd av den föreslagna 18 k § i informationshanteringslagen kan Transport- och kommunikationsverket tilldela ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011) en biträdande uppgift i anslutning till ett inspektionsuppdrag. Förslagen är betydelsefulla med tanke på 124 § i grundlagen, där det sägs att offentliga förvaltningsuppgifter kan anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter.

I grundlagsutskottets utlåtandepraxis har det betonats att kravet på ändamålsenlighet i 124 § i grundlagen är en rättslig förutsättning som kräver bedömning från fall till fall i fråga om varje offentlig förvaltningsuppgift som föreslås bli anförtrodd någon utanför myndighetsorganisationen. Då ska man beakta bl.a. förvaltningsuppgiftens karaktär (GrUU 44/2016 rd, s. 5, GrUU 26/2017 rd, s. 49, GrUU 5/2014 rd, s.3/I–II, GrUU 8/2014 rd, s.3/II, GrUU 23/2013 rd, s.3/I, GrUU 65/2010 rd, s.2/II). Enligt förarbetena till grundlagen ska man vid bedömning av ändamålsenligheten uppmärksamma dels förvaltningens effektivitet och övriga interna behov, dels enskilda personers och sammanslutningars behov (GrUU 44/2016 rd, s. 5, RP 1/1998 rd, s. 179/II).

Utgångspunkten är att tillsynsmyndigheten själv utför inspektionen. Med stöd av grundlagsutskottet utlåtandepraxis kan det i vissa fall vara lämpligt att inspektioner på grund av särskilda yrkesmässiga och tekniska aspekter på de omständigheter som tillsynen gäller utförs av sakkunniga som myndigheterna befullmäktigat därtill (GrUU 40/2002 rd, s. 3/I, GrUU 44/2016 rd, s. 5). Nödvändighetskravet kan bli uppfyllt i fall där granskningen förutsätter kompetens eller resurser som saknas hos myndigheterna (GrUU 29/2013 rd, s. 2/I). Enligt det föreslagna 29 § 2 mom. är det möjligt att anlita en utomstående expert endast om inspektionens art och omfattning förutsätter det. I praktiken gäller förslaget alltså en situation där inspektionen gäller sådana omständigheter vars granskning kräver sådan teknisk specialkompetens eller exceptionell kompetens som myndigheten själv inte innehar.

Grundlagsutskottet har ansett att kravet på rättssäkerhet och god förvaltning ska skrivas in i lag när förvaltningsuppgifter förs över på någon annan än en myndighet (GrUU 26/2001 rd, 5/II och GrUU 2/2001 rd, s. 2). Dessutom har grundlagsutskottet i sin senare utlåtandepraxis ansett att det i regleringen av granskningar av tillsynskaraktär hos företag för klarhetens skull bör hänvisas till den allmänna bestämmelsen om inspektioner i 39 § i förvaltningslagen (GrUU

44/2016 rd, s. 6, GrUU 35/2014 rd, s.4/I och GrUU 29/2013 rd, s. 2). Grundlagsutskottets utlåtandepraxis har i propositionen beaktats i 29 § 4 mom. i lagen om hantering av cybersäkerhetsrisker och 18 j § 3 mom. i informationshanteringslagen, enligt vilka 39 § i förvaltningslagen ska tillämpas på förfarandet vid inspektioner.

Grundlagsutskottet har ansett att respekten för de grundläggande fri- och rättigheterna, rättssäkerheten och kraven på god förvaltning kan tryggas med hjälp av de berörda personernas kompetens och lämplighet (GrUU 5/2006 rd, s. 8/I, GrUU 67/2002 rd, s.5/I–II och GrUU 2/2002 rd, s. 2/II). Dessutom ska den offentliga tillsynen över dem som sköter uppgifterna vara ändamålsenlig (GrUU 2/2002 rd, s. 2, GrUU 5/2006 rd, s. 8, och RP 1/1998 rd, s. 179/II). I 29 § 2 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker och i 18 j § 2 mom. i informationshanteringslagen föreskrivs det att inspektören ska ha den utbildning och erfarenhet som behövs för uppdraget med hänsyn till inspektionens art och omfattning. Detta behörighetskrav gäller också en utomstående expert som kan förordnas att utföra en inspektion med stöd av 27 § 2 mom. Grundlagsutskottet har i fråga om respekten för de grundläggande fri- och rättigheterna, kraven på rättssäkerhet och god förvaltning ansett att inspektionerna ska utföras i enlighet med de allmänna förvaltningslagarna och att de som behandlar ärendena handlar under tjänsteansvar (GrUU 20/2006 rd, s. 2, GrUU 46/2002 rd, s. 9, GrUU 33/2004 rd, s. 7/II, GrUU 11/2006 rd, s. 3). Enligt 29 § 2 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker och 18 k § 3 mom. i informationshanteringslagen ska bestämmelserna om straffrättsligt tjänsteansvar tilllämpas på utomstående experter och anställda hos godkända bedömningsorgan när de sköter offentligrättsliga förvaltningsuppgifter som getts i enlighet med ifrågavarande paragraf. Det är numera inte nödvändigt att med anledning av 124 § i grundlagen ta in en hänvisning till de allmänna förvaltningslagarna i lagen, om det av förslaget klart framgår att de allmänna förvaltningslagarna tillämpas på verksamhet som avses i 124 § i grundlagen (GrUU 20/2006 rd, s. 2) när det är fråga om aktörer som avses i 4 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999).

Enligt 124 § i grundlagen får uppgifter som innebär betydande utövning av offentlig makt dock ges endast myndigheter. I 29 § i den föreslagna lagen om hantering av cybersäkerhetsrisker och i 18 k § i informationshanteringslagen är det inte fråga om betydande utövning av offentlig makt. Grundlagsutskottet har i sina utlåtanden ansett att som betydande utövning av offentlig makt kan betraktas till exempel ingrepp i de grundläggande fri- och rättigheterna (RP 1/1998 rd, s. 179/II, GrUU 28/2001 rd, s. 5), på självständig prövning baserad användning av maktmedel (RP 1/1998 rd, s. 180/I, GrUU 28/2001 rd, s. 5) och inspektionsbefogenheter som gäller hemfridsskyddade platser (GrUU 40/2002 rd, s.3/II, GrUU 46/2001 rd, s.3/II). Utomstående inspektörer kan åtminstone inte förordnas att ensamma göra inspektioner i hemfridsskyddade lokaler (GrUU 29/2013 rd, s. 2). Grundlagsutskottets utlåtandepraxis har beaktats i 29 § 3 mom. i förslaget och i 18 j § 3 mom. i informationshanteringslagen, enligt vilka en inspektör ska ges tillträde till andra utrymmen än sådana som används för boende av permanent natur.

På de grunder som anförts ovan bedöms förslaget om anlitande av utomstående experter vid inspektion inte stå i strid med 124 § i grundlagen.

Avgifter för myndigheters prestationer

Med stöd av förslaget till 19 § 6 mom. i propositionen kan CSIRT-enheten ta ut en avgift för vissa prestationer och bestämmelser om avgiftens belopp och grunder utfärdas genom förordning av kommunikationsministeriet. Förslaget är av betydelse med tanke på 81 § 2 mom. i grundlagen, enligt vilket bestämmelser om avgifter samt de allmänna grunderna för storleken

av avgifter för de statliga myndigheternas tjänsteåtgärder, tjänster och övriga verksamhet utfärdas genom lag. Enligt förarbetena till grundlagen ska det genom lag föreskrivas om de allmänna principer som ska följas vid fastställandet av avgifternas storlek, exempelvis om vilka självkostnadsvärden eller företagsekonomiska principer som ska iakttas (RP 1/1998 rd, s 135/II).

Enligt grundlagsutskottets etablerade praxis är det kännetecknande för avgifter i konstitutionellt hänseende att de är ersättningar eller vederlag för service som det allmänna ger. I bedömningen av om det finns en motprestation till betalningen eller inte bör hänsyn tas till bl.a. om betalningen går att specificera, om den motsvarar kostnaderna och om den är frivillig eller obligatorisk (GrUU 49/2006 rd, s. 2 och de utlåtanden av grundlagsutskottet som det hänvisas till där).

I den föreslagna 19 § 6 punkten är det fråga om en myndighetsprestation som gäller en specificerad och enskild aktör och som för myndigheten medför väsentliga kostnader som är bundna till hur mycket tjänsten används. Det ska vara frivilligt för aktören att anlita och ta emot en tjänst som myndigheten tillhandahåller, och betalningsskyldigheten ska i sista hand grunda sig på aktörens egen prövning av behovet av tjänsten. I lagen föreslås bestämmelser om de tjänster som tillhandahålls av CSIRT-enheten och som kan utgöra grund för den avgift som tas ut. En förutsättning för avgiften är dessutom att tjänsten tillhandahålls på begäran av aktören och att myndighetsinitierade prestationer inte kan utgöra grund för avgiften. Förslaget bedöms motsvara de villkor som 81 § 2 mom. i grundlagen föreskriver för statliga avgifter.

12.3 Näringsfrihet

Aktörernas skyldighet att anmäla sig hos tillsynsmyndigheten

I propositionen ingår ett förslag till skyldighet för aktörer som omfattas av tillämpningsområdet att lämna tillsynsmyndigheten de uppgifter som avses i 43 § i lagen om hantering av cybersäkerhetsrisker för förande av en förteckning över aktörer. I förslaget till 165 § i lagen om tjänster inom elektronisk kommunikation föreskrivs det dessutom mer detaljerat än för närvarande om de uppgifter som registraren ska lämna innan verksamheten inleds. Förslagen innebär i praktiken att en aktör som omfattas av tillämpningsområdet är skyldig att underrätta tillsynsmyndigheten om sin verksamhet. Bestämmelserna är därför av betydelse med tanke på näringsfriheten enligt 18 § i grundlagen.

Genomförandet av NIS 2-direktivet förutsätter att de uppgifter som omfattas av anmälningsskyldigheten samlas in hos dessa aktörer. Genom anmälningsskyldigheten informeras tillsynsmyndigheten dessutom om vilka aktörer som omfattas av tillämpningsområdet för lagen om hantering av cybersäkerhetsrisker och gör det möjligt att rikta tillsynen till dessa aktörer.

Enligt 43 § i lagen om hantering av cybersäkerhetsrisker ska aktörerna lämna tillsynsmyndigheten de uppgifter som anges i paragrafens 1 mom. a–f punkten för förande av en förteckning över aktörer. Utöver dessa uppgifter ska leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster lämna tillsynsmyndigheten de uppgifter som avses i 3 § 2 mom. a–c punkten: I 3 mom. föreskrivs det dessutom om aktörens skyldighet att anmäla ändringar och om tillsynsmyndighetens rätt att meddela närmare föreskrifter om rapporteringen av uppgifter. Tillsynsmyndigheten för en förteckning över aktörerna utifrån anmälningarna.

Grundlagsutskottet har i sitt utlåtande GrUU 54/2002 rd ansett att bestämmelser om anmälningsskyldighet

i sig inte utgör något problem ur näringsfrihetssynpunkt, i synnerhet inte då myndigheten inte förväntas fatta några beslut med anledning av anmälan. I den föreslagna anmälningsskyldigheten är det fråga om en situation av detta slag. Å andra sidan har grundlagsutskottet i sin utlåtandepraxis ansett att skyldigheten att anmäla verksamheten hos tillsynsmyndigheten och att lämna uppgifter till tillsynsmyndigheten i en situation där underlåtelse att göra anmälan leder till negativa konsekvenser ofta kan jämställas med tillståndsplikt och således innebära ett ingrepp i näringsfriheten (GrUU 45/2001 rd). Anmälningsskyldighet är dock en skyldighet som lindrigare ingriper i näringsfriheten än tillståndsplikt. Grundlagsutskottet har inte ansett att anmälningsplikt är problematisk med tanke på näringsfriheten, när en försummelse i detta avseende inte innebär ett förbud att bedriva näringsverksamhet (GrUU 16/2009 rd) eller när myndigheten inte förväntas fatta något beslut med anledning av anmälan (GrUU 54/2002 rd). I propositionen åläggs aktören skyldighet att till myndigheten lämna de uppgifter som krävs när den omfattas av anmälningsskyldigheten enligt NIS 2-direktivet. Anmälan är inte en förutsättning för verksamheten och tillsynsmyndigheten förutsätts inte fatta några beslut med anledning av anmälan. Försummelse av anmälningsskyldigheten ska dock leda till en administrativ påföljd, och tillsynsmyndigheten har rätt att förordna att försummelsen ska avhjälpas med stöd av vite eller hot om avbrytande. Dessutom ska tillsynsmyndigheten ytterst ha rätt att utöva andra lagstadgade befogenheter för att rätta till ett lagstridigt förfarande. Tillsynsmyndigheten ska också utifrån anmälningar föra en förteckning över aktörer.

Den föreslagna anmälningsskyldigheten innebär en begränsning av näringsfriheten och förslaget ska uppfylla de allmänna kraven på en lag som begränsar de grundläggande fri- och rättigheterna, såsom kraven på godtagbarhet, exakthet och noggrann avgränsning (GrUU 58/2014 rd, s. 5, GrUU 19/2009 rd, s. 2). Enligt grundlagsutskottet ska det finnas godtagbara och vägande skäl att begränsa näringsfriheten (GrUU 15/2008 rd, s. 2). Syftet med propositionen är att stärka förmågan att hantera cybersäkerhetsrisker hos de aktörer som omfattas av tillämpningsområdet och därigenom säkerställa kontinuiteten i kritiska samhällsfunktioner. Det bedöms finnas vägande och godtagbara skäl för att föreskriva om anmälningsskyldighet.

Aktörernas skyldighet att anmäla sig hos tillsynsmyndigheten och tillsynsmyndighetens skyldighet att föra en förteckning över aktörerna gör det möjligt att övervaka de skyldigheter som åläggs aktörerna samt att vid en omfattande cyberstörning bedöma dess konsekvenser både i Finland och på EU-nivå. Genomförandet av NIS 2-direktivet förutsätter bestämmelser om anmälningsskyldighet. Det förutsätts att bestämmelser om begränsningar är *exakta och noggrant avgränsade* (GrUU 15/2008 rd, s. 2, GrUU 33/2005 rd, s. 2) och att den centrala innebörden av begränsningarna i näringsfriheten ska framgå av lagen, t.ex. deras omfattning och villkoren (GrUU 19/2009 rd, s. 2). I lagen anges vilka aktörer anmälningsskyldigheten gäller, och de uppgifter som ska anmälas har definierats uttömmande på lagnivå. Dessutom har grundlagsutskottet i sin utlåtandepraxis ansett att myndighetsverksamhet bör vara förutsägbar. Förutsägbarheten i myndighetsverksamheten stöds av att det finns bestämmelser om villkoren för registrering och om registreringens beständighet (GrUU 19/2009 rd, s. 2, GrUU 15/2008 rd, s. 2). Utifrån anmälningarna ska tillsynsmyndigheten föra en förteckning över de aktörer som omfattas av tillämpningsområdet för tillsynsområdet. Grundlagsutskottet har i sin utlåtandepraxis förutsatt att det av lagen framgår att var och en som utövar sådan verksamhet som regleras i lagen ska föras in i registret (GrUU 45/2001 rd). Av den föreslagna 43 § framgår att tillsynsmyndigheten i fråga om sitt tillsynsområde för en aktörsförteckning utifrån de uppgifter som lämnats.

Bestämmelserna i 43 § i lagen om hantering av cybersäkerhetsrisker och de ändringar som föreslås i 165 § i lagen om tjänster inom elektronisk kommunikation motsvarar de krav som enligt grundlagsutskottets praxis ställs på en bestämmelse som begränsar näringsfriheten. De bedöms därför inte strida mot näringsfriheten enligt 18 § 1 mom. i grundlagen på ett sätt som hindrar att lagförslaget behandlas i vanlig lagstiftningsordning.

Begränsning av tillståndspliktig eller certifierad verksamhet

I 32 § i förslaget finns bestämmelser om begränsning av tillståndspliktig eller certifierad verksamhet och återkallande av tillstånd eller certifiering. Genom förslaget genomförs NIS 2-direktivets artikel 32.5 om befogenheter för tillsynsmyndigheten. Förslaget om begränsning av i synnerhet tillståndspliktig verksamhet eller återkallande av tillstånd är av betydelse med tanke på näringsfriheten enligt 18 § i grundlagen. En myndighet kan beviljas befogenhet att begränsa företagens tillståndsenliga verksamhet. Grundlagsutskottet har dock förutsatt att begränsningar i sådana situationer ska stödas av godtagbara och vägande skäl med avseende på de grundläggande fri- och rättigheterna. Grundlagsutskottet har i sina utlåtanden bland annat framfört att till exempel grunder som hänför sig till strävan att garantera stabiliteten på den finansiella marknaden och som därmed också skyddar kunderna talar för reglering som innebär kraftfulla ingrepp i det grundlagsskyddade egendomsskyddet och den grundlagsskyddade näringsfriheten (t.ex. GrUU 43/2004 rd, s.2/I eller GrUU 35/2014 rd, s. 3). Det nu aktuella förslaget gäller hantering av cybersäkerhetsrisker i tjänster som är kritiska med tanke på samhällets funktion och säkerställandet av kontinuiteten i dessa tjänster, så det bedöms att det finns vägande och godtagbara skäl för att begränsa tillståndspliktig verksamhet på det föreslagna sättet.

Återkallande av tillstånd har i samband med reglering av näringsverksamhet ansetts vara en åtgärd som ingriper kraftigare i individens rättsliga ställning än till exempel avslag på en ansökan om tillstånd. Därför är det nödvändigt att koppla återkallande av tillstånd till allvarliga eller väsentliga förseelser eller försummelser samt till att eventuella anmärkningar eller varningar till tillståndshavaren eller en skälig tidsfrist för att avhjälpa bristen eller försummelsen inte har lett till att bristerna i verksamheten har korrigerats (t.ex. GrUU 13/2014 rd, s. 3, eller GrUU 34/2012 rd, s. 2). Villkoren för återkallande av tillstånd i förslaget är kopplade till direktivets viktigaste skyldighet för aktörerna, dvs. till den handlingsmodell för hantering av cybersäkerhetsrisker som avses i förslaget och till att de riskhanteringsåtgärder som anknyter till den inte har vidtagits. Dessutom kan ett tillstånd återkallas om den väsentliga aktören väsentligt har underlåtit att iaktta andra skyldigheter som ålagts den med stöd av den föreslagna lagen eller NIS 2-direktivet. I förhållande till andra tillsynsbefogenheter ska åtgärderna enligt 32 § tillämpas i sista hand.

Återkallande av tillstånd kan endast gälla de väsentliga aktörer som avses i 26 §. Återkallande av tillstånd förutsätter en väsentlig och allvarlig överträdelse eller försummelse av lagen samt att anmärkningar eller varningar till tillståndshavaren eller en skälig tidsfrist för avhjälpande av bristen eller försummelsen inte har lett till att bristerna avhjälpts. Den myndighet som beviljat tillståndet ska i sista hand pröva om en tillståndspliktig verksamhet ska återkallas eller avbrytas.

Utifrån det som sägs ovan anses förslaget om begränsning av tillståndspliktig verksamhet inte stå i strid med grundlagen.

Begränsning av ledningens verksamhet

Enligt 33 § i propositionen kan tillsynsmyndigheten för viss tid, högst fem år, 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 samt att sköta

uppdrag som är direkt underställda verkställande direktören, med vilket avses de högsta ledningsuppdragen hos den väsentliga aktören eller uppdrag där dess verksamhet de facto leds, om personen upprepade gånger och allvarligt har brutit mot skyldigheterna i 11 §. Genom förslaget genomförs NIS 2-direktivets artikel 32.5 om befogenheter för tillsynsmyndigheten. Förslaget är relevant för näringsfriheten, som tryggas i 18 § i grundlagen, där det föreskrivs att var och en i enlighet med lag har rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt.

Bestämmelser om begränsning av ledningens verksamhet har stiftats med grundlagsutskottets medverkan (GrUU 67/2002 rd, s. 3 och GrUU 28/2008, s. 2). Enligt grundlagsutskottets utlåtandepraxis ska ett verksamhetsförbud vara definierat i lag, det ska finnas en godtagbar grund för det och bestämmelserna om det ska vara exakta (GrUU 16/2003 rd, s. 3, GrUU 67/2002 rd, s. 3, GrUU 52/2001 rd, s. 4).

Bestämmelser om begränsning av ledningens verksamhet ska i enlighet med grundlagsutskottets utlåtandepraxis utfärdas på lagnivå. Bestämmelser om detta finns i 32 § i lagförslag 1. Grundlagsutskottet har förutsatt att det ska finnas en godtagbar grund för en bestämmelse som begränsar ledningens verksamhet. Grunden är i detta fall genomförandet av en förpliktande EU-bestämmelse som syftar till att förbättra motståndskraften mot störningar hos de aktörer som är väsentliga med tanke på samhällets funktion. NIS 2-direktivet förutsätter att aktörens ledning personligen ansvarar för att aktören fullgör sina riskhanterings- och rapporteringsskyldigheter i fråga om cybersäkerheten samt att det finns möjlighet att förbjuda att en person utövar ledningsfunktioner i en central aktör, om aktören trots en anmärkning eller varning inte inom en skälig tid avhjälper bristen eller försummelsen att iaktta bestämmelserna. Om en aktörs ledning upprepade gånger och allvarligt handlar i strid med en lagstadgad skyldighet, ska enligt förslaget ledningens verksamhet kunna begränsas. Begränsningen gäller fysiska personers verksamhet i ledningen för en enskild aktör. Syftet med bestämmelsen är att göra de åtgärder som anges i lagen effektivare och mer avskräckande.

Grundlagsutskottet har i sina utlåtanden betonat att en omständighet som stärker grundlagsenligheten är att förbudsmöjligheten bara kan omfatta ett fåtal uppgifter och att målgruppen för regleringen är snäv (GrUU 52/2001 rd, s. 4, GrUU 16/2003 rd, s. 3). I lagförslaget begränsas möjligheten att begränsa ledningens verksamhet så att den endast kan gälla aktörens högsta ledning, det vill säga de personer som definieras i 33 § i lagförslaget. Förbudet är inte heller ett allmänt förbud, utan gäller endast en fysisk persons verksamhet i den högsta ledningen för en viss aktör. Förbudet begränsar inte en fysisk persons övriga näringsutövning eller möjligheter att utöva ett yrke som han eller hon själv väljer. En förutsättning är dessutom att förfarandet tillämpas i sista hand. Tillsynsmyndigheten ska innan den fattar ett beslut ge den väsentliga aktören en anmärkning eller varning samt reservera en skälig tid för att avhjälpa bristen eller försummelsen. Dessa villkor säkerställer att ledningens verksamhet endast kan begränsas i sista hand och undantagsvis.

Med tanke på begränsning av näringsfriheten lindras konsekvenserna av ett förbud också av att en person som är föremål för förbudet har möjlighet att söka sig till andra uppgifter i samma eller en annan organisation. Förbudet kommer dessutom inte att gälla enskilda näringsidkare eller personbolag, det vill säga öppna bolag eller kommanditbolag där en enskild näringsidkare eller bolagsmännen i ett personbolag personligen ansvarar för bolagets skulder. Det faktum att möjligheten att begränsa ledningens verksamhet avgränsas till att gälla endast vissa personer som anges i bestämmelsen när det är fråga om allvarliga och upprepade överträdelser av skyldigheten enligt 10 § stöder grundlagsutskottets krav på att bestämmelserna ska vara exakta och stärker regleringens grundlagsenlighet. Åtgärden kan endast riktas mot en väsentlig aktör.

12.4 Administrativ påföljdsavgift

I 5 kap. i lagen om hantering av cybersäkerhetsrisker föreskrivs det på det sätt som förutsätts i NIS 2-direktivet om påförande av en administrativ påföljdsavgift för en aktör som uppsåtligen eller av grov oaktsamhet försummar den lagstadgade riskhanteringsskyldigheten, skyldigheten att anmälan en betydande incident eller den lagstadgade anmälan för aktörsförteckningen. Det är fråga om en administrativ påföljd av sanktionskaraktär som påförs för en lagstridig gärning och som kan uppgå till ett betydande belopp.

Enligt grundlagsutskottets utlåtandepraxis ska de allmänna grunderna för administrativa påföljder i enlighet med 2 § 3 mom. i grundlagen fastställas i lag. Dessutom är det fråga om betydande utövning av offentlig makt, som endast kan anförtros myndigheter. Lagen måste exakt och tydligt föreskriva om grunderna för betalningsskyldigheten och avgiftens storlek, rättsskyddet för den betalningsskyldige och grunderna för verkställigheten av lagen. Utskottet har också ansett att även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen, som framgår av grundlagens 8 §, inte direkt gäller administrativa påföljder kan det allmänna kravet på exakthet ändå inte åsidosättas i ett sådant sammanhang (GrUU 43/2013 rd, GrUU 14/2012 rd, GrUU 32/2012 rd och de utlåtanden som nämns där).

Grundlagsutskottets hävdvunna tolkning har varit att administrativa påföljdsavgifter är administrativa påföljder av sanktionskaraktär som påförs för en lagstridig gärning. I sak har utskottet i sina utlåtanden jämställt en ekonomisk påföljd av straffkaraktär med en straffrättslig påföljd (GrUU 17/2012 rd, s. 5, GrUU 9/2012 rd, s. 2). Påförande av en administrativ påföljdsavgift innebär enligt grundlagsutskottet betydande utövning av offentlig makt (GrUU 34/2012 rd, s. 3, GrUU 17/2012 rd, s. 5, GrUU 9/2012 rd, s. 2). Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag. Enligt sista meningen i 124 § i grundlagen får uppgifter som innebär betydande utövning av offentlig makt ges endast myndigheter. I förslaget om påförande av påföljdsavgift har grundlagsutskottets utlåtandepraxis beaktats. I lagen ska det på ett exakt, noggrant avgränsat och uttömmande sätt föreskrivas om den gärning eller försummelse som kan ligga till grund för påförande av påföljdsavgift för en aktör.

Grundlagsutskottet har i sin bedömning av dataskyddsförordningen konstaterat att rättssäkerhetsintresset i fråga om administrativa påföljdsavgifter är starkt accentuerat, med hänsyn till att påföljdsavgiften är sträng och har karaktär av sanktion. Grundlagsutskottet förutsatte att beslut om påföljdsavgift för att säkerställa att förfarandet är behörigt, oavhängigt och rättvist på det sätt som krävs i 21 § i grundlagen ska fattas av ett kollegialt organ för att förslaget ska kunna behandlas i vanlig lagstiftningsordning. Dataombudsmannen kan ges i uppdrag att ha hand om utredning, övrig beredning och föredragning innan påföljdsavgiften påförs i ärendet (GrUU 14/2018 rd).

Av rättssäkerhetsskäl föreslås det att påföljdsavgift ska påföras av ett kollegialt organ. Påföljdsavgift ska påföras av påföljdsavgiftsnämnden, som består av medlemmar som utses av tillsynsmyndigheterna. Transport- och kommunikationsverket ska utse nämndens ordförande och vice ordförande. Till nämnden ska varje tillsynsmyndighet utnämna en ledamot och en personlig ersättare för honom eller henne. För utredningen av ett ärende som gäller påförande av påföljdsavgift svarar den tillsynsmyndighet vars tillsynsbehörighet det ärende som ska avgöras gäller, och ärendet föredras av en medlem som utsetts av denna tillsynsmyndighet. Lagförslaget innehåller dessutom bestämmelser om nämndens förtrogenhet med och sakkunskap inom dess arbetsfält samt om nämndens oberoende och opartiskhet.

Enligt grundlagsutskottet ska förvaltningsmyndigheten vid behandlingen av ett ärende iaktta garantierna för god förvaltning enligt 21 § 2 mom. i grundlagen. Dessa garantier är enligt momentet bland annat offentligheten vid handläggningen, rätten att bli hörd, rätten att få motiverade beslut och rätten att söka ändring. Garantier för god förvaltning ska enligt grundlagen tryggas genom lag. Även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen i grundlagens 8 § inte direkt gäller administrativa påföljder kan det allmänna kravet på exakthet ändå inte förbigås i ett sammanhang som detta (GrUU 34/2012 rd, s. 3, GrUU 17/2012 rd, s. 5–6 och GrUU 9/2012 rd, s. 2).

Grundlagsutskottet har i sin utlåtandepraxis ansett det vara problematiskt att ärenden i enskilda fall kan avgöras utan föredragning (GrUU 14/2018 rd, s. 18–19). Påföljdsnämnden fattar alltid beslut efter föredragning. Enligt grundlagsutskottet ska det lagstiftas exakt och tydligt om grunderna för betalningsskyldigheten och avgiftens storlek, lika väl som om rättsskyddet för den betalningsskyldige och grunderna för verkställigheten av lagen (GrUU 14/2013 rd, s. 2, GrUU 34/2012 rd, s. 3 och GrUU 17/2012 rd, s. 5). Förslagets bestämmelser om dessa omständigheter bedöms hålla en tillräcklig nivå.

Eftersom påföljdsavgifterna är betydande måste man enligt grundlagsutskottet fästa särskild uppmärksamhet vid kraven på rättssäkerhet (GrUU 14/2018 rd, s. 18). Påföljdsavgiftens belopp grundar sig enligt 39 § på en helhetsbedömning där de omständigheter som anges i paragrafen ska beaktas. I 40 § i föreskrivs om påföljdsavgiftens maximibelopp. Ändring i ett beslut om påföljdsavgift får sökas genom besvär på det sätt som föreskrivs för rättegång i förvaltningsärenden. Ett beslut om påföljdsavgift ska vara verkställbart först när det har vunnit laga kraft, vilket har bedömts trygga adekvata garantier för att rättssäkerheten blir tillbörligen tillgodosedd (GrUU 4/2004 rd, s. 7–8). Grundlagsutskottet har dessutom i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden prövning, det vill säga att avgiften inte ska påföras om de villkor som anges i bestämmelsen är uppfyllda (GrUU 49/2017 rd, s. 5, GrUU 39/2017 rd, s. 4). Detta har beaktats i förslagets 37 §, vars syfte enligt specialmotiveringen är att säkerställa att påföljdsavgift inte påförs om den antingen med stöd av de omständigheter som avses i 1 mom. 1 eller 2 punkten eller annars med stöd av någon motsvarande omständighet eller andra omständigheter är uppenbart oskälig.

Enligt *ne bis in idem*-regeln får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan har blivit slutligt frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat (GrUU 9/2012 rd, s. 3, GrUU 14/2013 rd, s. 2). Enligt Europadomstolens avgörandepraxis omfattar förbudet också administrativa påföljder av straffkaraktär (GrUU 9/2012 rd, s. 3). I propositionens lagförslag 1 har regeln beaktats i 41 § 3 mom., enligt vilket påföljdsavgift inte får påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom. Påföljdsavgift får inte heller påföras den som för samma gärning har påförts en påföljdsavgift enligt den allmänna dataskyddsförordningen.

Förslaget om en administrativ påföljdsavgift bedöms motsvara de särskilda, ovan angivna villkor som grundlagen ställer.

12.5 Delegering av lagstiftningsbehörighet

Statsrådets förordning om bestämmande av de aktörer som omfattas av tillämpningsområdet.

Enligt 3 § 3 mom. i förslaget till lag om hantering av cybersäkerhetsrisker får det genom förordning av statsrådet föreskrivas om tillämpningen av lagen på aktörer som bedriver verksamhet enligt bilaga I eller II eller som är en typ av aktör som avses i bilaga I eller II, oavsett storlek, om aktören uppfyller ett kriterium enligt samma moment.

Med stöd av 80 § 1 mom. i grundlagen kan republikens president, statsrådet och ministerierna utfärda förordningar med stöd av ett bemyndigande i grundlagen eller i någon annan lag. Genom lag ska dock utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter samt om frågor som enligt grundlagen i övrigt hör till området för lag.

En överföring av lagstiftningsbehörigheten är lagtekniskt nödvändig, eftersom det är fråga om en detaljerad definition av aktörer eller aktörstyper som oavsett storlek undantagsvis hör till tillämpningsområdet för skyldigheterna enligt lagen på grund av verksamhetens särskilda art. Med beaktande av arten av kriterierna är det dessutom sannolikt att det sker förändringar hos aktörerna när verksamhetens art eller omfattning ändras.

Genom förordning av statsrådet får det föreskrivas endast om att aktören omfattas av lagens tillämpningsområde oavsett storlek, och det får inte genom förordning föreskrivas om partiell tillämpning av lagen eller om innehållet i de rättigheter och skyldigheter som föreskrivs i lagen. Genom förordning kan tillämpningen oavsett storlek utsträckas endast till de aktörer eller aktörstyper som anges i bilagan till lagen. Genom förordning kan tillämpningen inte utsträckas till en ny sektor eller aktörstyp som annars inte omfattas av lagens tillämpningsområde. I lagen föreskrivs dessutom på motsvarande sätt som i NIS 2-direktivets förpliktande bestämmelser om tillämpningsområde om de undantagskriterier som ska uppfyllas för att en aktör ska kunna omfattas av lagens tillämpningsområde. Därför har det bedömts att förslaget motsvarar villkoren i 80 § 1 mom. i grundlagen för bemyndigande att utfärda förordning så att det genom lag föreskrivs om grunderna för individens rättigheter och skyldigheter, och att en detaljerad och teknisk bestämning av de aktörer som oavsett storlek undantagsvis ska omfattas av tillämpningsområdet kan lämnas genom förordning.

Normgivningsbemyndiganden

Enligt 80 § 2 mom. i grundlagen kan även andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska enligt grundlagen vara exakt avgränsat. Ett särskilt skäl att föreskriva om en myndighets normgivningsrätt är exempelvis en teknisk reglering av smärre detaljer (GrUU 52/2001 rd, GrUU 46/2001 rd) som inte inbegriper prövningsrätt i någon större utsträckning (GrUU 43/2000 rd). De omständigheter som ett bemyndigande att utfärda rättsnormer omfattar ska noggrant anges i lagen och bemyndigandets tillämpningsområde ska vara exakt avgränsat (RP 1/1998 rd).

Med stöd av 9 § 4 mom. i lagen om hantering av cybersäkerhetsrisker får tillsynsmyndigheten utfärda närmare tekniska föreskrifter om hanteringen av cybersäkerhetsrisker. I 9 § 4 mom. 1–6 punkten i lagförslaget specificeras de omständigheter som hänför sig till den lagstadgade riskhanteringsskyldigheten och som föreskrifter kan utfärdas om. Dessutom ingår ett bemyndigande för tillsynsmyndigheten att meddela föreskrifter i 11 § 5 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker. Enligt momentet kan tillsynsmyndigheten inom sitt ansvarsområde meddela närmare tekniska föreskrifter om de i momentets 1–3 punkter specificerade tekniska omständigheter i fråga om den rapportering av incidenter som föreskrivs i lagen. Ett tredje

bemyndigande för tillsynsmyndigheten att meddela föreskrifter finns i 43 § 3 mom. i den föreslagna lagen om hantering av cybersäkerhetsrisker. Enligt bemyndigandet får tillsynsmyndigheten meddela närmare föreskrifter om hur uppgifterna i förteckningen över aktörer ska lämnas. Förslagen är av relevans med hänsyn till 80 § 2 mom. i grundlagen. Enligt momentet kan även andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat.

Enligt grundlagens 80 § 2 mom. kan en myndighet genom lag bemyndigas att utfärda rättsnormer bara *i bestämda frågor*. Tillämpningsområdet för ett sådant bemyndigande ska dessutom vara *exakt avgränsat*. Enligt förarbetena till grundlagen (RP 1/1998 rd, s. 133) är kravet på att en myndighet ska bemyndigas att meddela föreskrifter i bestämda frågor längregående än det allmänna kravet på exakt avgränsning (även GrUU 24/2002 rd, s. 3). Grundlagens krav har beaktats i förslaget genom att de tekniska omständigheter som myndigheten med stöd av paragrafen får meddela närmare föreskrifter om specificeras och förtecknas i 9 § 4 mom. och 11 § 5 mom. I 43 § i förslaget gäller bemyndigandet att meddela föreskrifter hur uppgifter ska lämnas, vilket till sin karaktär är en teknisk och noggrant avgränsad omständighet. Bemyndigandena att meddela föreskrifter är till sin karaktär teknisk reglering och genom dem kan det inte utfärdas allmänna rättsnormer om frågor som på grund av sin betydelse ska regleras genom lag eller förordning. Grundlagsutskottet har i ett utlåtande ansett att Kommunikationsverket är en sådan myndighet som kan ges rätt att meddela föreskrifter (bl.a. GrUU 9/2004 rd, s. 8).

Bemyndigande att utfärda rättsnormer kan enligt grundlagsutskottets betänkande (GrUB 10/1998 rd, s.22/I) endast undantagsvis delegeras till en lägre myndighetsnivå än ett ministerium. I förarbetena till grundlagen (RP 1/1998 rd, s.134/I) identifieras behovet av att göra det möjligt för andra myndigheter att utfärda rättsnormer om detaljer som är mindre betydande med tanke på regleringen som helhet. Bestämmelsen i 80 § 2 mom. i grundlagen förutsätter *särskilda skäl* i anknytning till ett bemyndigande att meddela föreskrifter. Enligt grundlagspropositionen (RP 1/1998 rd, s. 134/I) kan ett särskilt skäl anses föreligga närmast när det är fråga om en sådan teknisk reglering av smärre detaljer som inte inbegriper prövningsrätt i någon större utsträckning. Grundlagsutskottet har dessutom ansett att de särskilda yrkesmässiga särdragen hos den reglerande verksamheten är sådana särskilda skäl som avses i 80 § 2 mom. i grundlagen (GrUU 17/2004 rd, s. 3, GrUU 16/2003 rd, s. 3, GrUU 24/2002 rd, s. 3). Grundlagsutskottet har inte ansett att ett bemyndigande om tekniska detaljer är problematiskt med tanke på grundlagen (GrUU 17/2004 rd, s. 3–4, GrUU 16/2003 rd, s. 3). De bemyndiganden att meddela föreskrifter som föreslås för myndigheten är av teknisk natur. Detta framgår av ordalydelsen i 9 § 4 mom., 11 § 5 mom. och 43 § 3 mom., enligt vilka tillsynsmyndigheten inom sitt behörighetsområde får meddela närmare *tekniska* föreskrifter. Förslagen anses uppfylla de särskilda villkor som beskrivs ovan.

Avsikten med bemyndigandena är att ge myndigheterna möjlighet att precisera tillämpningen av lagen genom att meddela tekniska föreskrifter om de omständigheter som anges i bestämmelserna. Bemyndigandena att meddela föreskrifter är noggrant avgränsade och gäller detaljer som är mindre betydande med tanke på regleringen som helhet. Ett bemyndigande att meddela föreskrifter om tekniska frågor gör det dessutom möjligt att beakta sektorspecifika särdrag och att samordna regleringen med de genomförandeakter eller delegerade förordningar som kommissionen antar med stöd av artiklarna 21 eller 24 i NIS 2-direktivet. De skäl för att i enlighet med förslaget bemyndiga en myndighet att utfärda föreskrifter är sådana särskilda skäl som avses i 80 § 2 mom. i grundlagen. Regeringen anser att de föreslagna bemyndigandena att utfärda föreskrifter är förenliga med 80 § 2 mom. i grundlagen.

Bemyndigandena är exakta, noggrant avgränsade och proportionella i förhållande till deras syfte och de skyddsintressen som eftersträvas. Förslagen ingriper inte i kärnområdet för de rättigheter som tryggas genom grundlagen. Den föreslagna regleringen har begränsats till den miniminivå som genomförandet av NIS 2-direktivet förutsätter och som kan anses nödvändig och proportionell med tanke på uppnåendet av de mål som ligger till grund för direktivet.

På de grunder som anges ovan anser regeringen att lagförslagen kan behandlas i vanlig lagstiftningsordning. Med anledning av förslaget om behandling av ett meddelande som innehåller ett skadligt datorprogram eller ett skadligt kommando är det dock nödvändigt att begära grundlagsutskottets utlåtande om propositionen.

Kläm

Eftersom Europaparlamentets och rådets direktiv (EU) 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) innehåller bestämmelser som enligt förslaget ska genomföras genom lag föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om hantering av cybersäkerhetsrisker

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om skyldigheter för vissa aktörer som är kritiska med tanke på samhällets funktion (*aktörer*) att hantera cybersäkerhetsrisker och rapportera om dem och om en enhet för hantering av it-säkerhetsincidenter (*CSIRT-enhet*) samt om myndigheternas samarbete för att hantera cybersäkerhetsincidenter och 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*).

2 §

Definitioner

I denna lag avses med

1) *registreringsenhet för toppdomäner* en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk,
2) *CER-direktivet* Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG,
3) *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,
4) *leverantör av DNS-tjänster* en aktör som tillhandahåller
   a) allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller
   b) auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,
5) *DORA-förordningen* 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,
6) *eIDAS-förordningen* 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,
7) *sårbarhet* en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot,
8) *leverantör av hanterade tjänster* en aktör som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av 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,
9) *kvalificerad tillhandahållare av betrodda tjänster* en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i eIDAS-förordningen,
10) *medelstor aktör* en offentlig eller privat aktör som uppfyller villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 3.4 i bilagan till rekommendationen tillämpas inte vid definieringen av en medelstor aktör,

11) *cybersäkerhet* åtgärder som behövs för att skydda kommunikationsnät och informationssystem, deras användare och andra berörda personer mot cyberhot,
12) *cyberhot* en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka kommunikationsnät och informationssystem, användare av dessa system och andra personer,
13) *tillhandahållare av betrodda tjänster* en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i eIDAS-förordningen,
14) *tillbud* en händelse som kunde ha undergrävt 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, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod av slumpmässiga skäl,
15) *molntjänst* en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser,
16) *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,
17) *incidenthantering* alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident,
18) *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 sådan incident inträffar,
19) *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,
20) *teledirektivet* Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation,
21) *leverantör av hanterade säkerhetstjänster* en leverantör av hanterade tjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker,
22) *IKT-tjänst* en IKT-tjänst enligt definitionen 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,
23) *IKT-produkt* en IKT-produkt enligt definitionen i artikel 2.12 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,
24) *tillsynsmyndighet* den tillsynsmyndighet som är behörig med stöd av 26 §,
25) *plattform för sociala nätverkstjänster* en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer,
26) *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,
27) *internetbaserad marknadsplats* en i 6 kap. 8 § 4 punkten i konsumentskyddslagen (38/1978) avsedd internetbaserad marknadsplats,
28) *kommunikationsnät och informationssystem*
a) ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i 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, eller
c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av underpunkt a och b för att de ska kunna drivas, användas, skyddas och underhållas,

29) *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 kommunikationsnät och informationssystem,
30) *den allmänna dataskyddsförordningen* 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),
31) *tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster* den som tillhandahåller kommunikationstjänster som avses i 3 § 1 mom. 37 punkten i lagen om tjänster inom elektronisk kommunikation till en grupp av användare som inte har avgränsats på förhand,
32) *tillhandahållare av allmänna elektroniska kommunikationsnät* den som tillhandahåller nättjänster som avses i 3 § 1 mom. 34 punkten i lagen om tjänster inom elektronisk kommunikation.

3 §

Aktörer

Med en aktör som omfattas av tillämpningsområdet för denna lag avses en juridisk eller fysisk person som bedriver verksamhet enligt bilaga I eller II eller är en typ av aktör som avses i bilaga I eller II och uppfyller eller överskrider definitionen av en medelstor aktör.

Med aktör avses därtill oberoende av storlek en juridisk eller fysisk person som är

a. en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,
b. en tillhandahållare av betrodda tjänster,
c. en registreringsenhet för toppdomäner,
d. en leverantör av DNS-tjänster, eller
e. en kritisk aktör enligt definitionen i CER-direktivet.

Genom förordning av statsrådet föreskrivs om tillämpningen av denna lag på sådana aktörer som bedriver verksamhet enligt bilaga I eller II eller som är en typ av aktör som avses i bilaga I eller II, oavsett storlek, om

1) aktören är den enda leverantören av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
2) en störning av den tjänst som aktören tillhandahåller har 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 medlemsstaten som är beroende av denna aktör.

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.

Bestämmelserna i 1 och 2 mom. tillämpas inte om aktören är en tillhandahållare av betrodda tjänster.

Denna lag tillämpas inte på aktörer på vilka DORA-förordningen inte tillämpas med stöd av artikel 2.4 i den förordningen.

Denna lag förpliktar inte att lämna ut sådan information vars utlämnande 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 finns från denna lag avvikande bestämmelser genom vilka en högre cybersäkerhetsnivå säkerställs, ska dessa tillämpas utöver denna lag.

Om det i en EU-förordning eller i en förordning av kommissionen som antagits med stöd av NIS 2-direktivet förutsätts sektorsspecifikt att en aktör inför åtgärder för hantering av cybersäkerhetsrisker eller anmäler betydande incidenter, och kraven har minst samma verkan som motsvarande skyldigheter som fastställs i denna lag, ska 2, 4 och 5 kap. samt 43 § i denna lag inte tillämpas på aktören i fråga om dessa skyldigheter eller tillsynen över dem.

Bestämmelser om datasäkerhet vid behandling av personuppgifter finns i den allmänna dataskyddsförordningen och dataskyddslagen (1050/2018).

6 §

Jurisdiktion och territorialitet

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

Oberoende av i vilken stat aktören är etablerad, omfattas tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster.

Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster samt tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster omfattas i fråga om de skyldigheter som avses i denna lag av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i enlighet

med artikel 26.2 i NIS 2-direktivet eller där deras utsedda företrädare i Europeiska unionen i enlighet med artikel 26.3 i NIS 2-direktivet finns. En sådan aktör som inte är etablerad i Europeiska unionen, men som tillhandahåller sina tjänster inom Europeiska unionen, ska utse en i artikel 26.3 i NIS 2-direktivet avsedd företrädare för Europeiska unionen. Om en aktör inte är etablerad i Europeiska unionen eller inte har utsett en i artikel 26.3 i NIS 2-direktivet avsedd företrädare i Europeiska unionen 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.

2 kap.

Skyldighet att hantera cybersäkerhetsrisker samt anmälan av incidenter

7 §

Skyldighet att hantera cybersäkerhetsrisker

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 säkerhets- och riskhanteringsåtgärder som är aktuella, proportionella och tillräckliga i förhållande till riskerna för de kommunikationsnät och informationssystem som används i verksamheten samt 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 riktas mot kommunikationsnät och informationssystem och deras fysiska miljö identifieras i enlighet med ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen för hantering av cybersäkerhetsrisker ska det fastställas och beskrivas åtgärder genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot risker och incidenter (nedan *hanteringsåtgärder*).

9 §

Åtgärder för hantering av cybersäkerhetsrisker

Aktörerna ska vidta proportionerliga tekniska, driftsrelaterade eller organisatoriska hanteringsåtgärder i enlighet med handlingsmodellen för hantering av cybersäkerhetsrisker för att hantera sådana risker som riktas mot säkerheten i kommunikationsnät och informationssystem och förhindra eller minimera skadliga verkningar.

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

1) riktlinjer för hantering av cybersäkerhetsrisker samt bedömning av effektiviteten i fråga om riskhanteringsåtgärderna,
2) 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 för leverantörers produkter och tjänsteleverantörers tjänster och de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem samt cybersäkerhetspraxis hos leverantörer och tjänsteleverantörer,
5) tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på säkerheten,
6) personalsäkerhet och utbildning i cybersäkerhet,
7) förfaranden för åtkomsthantering och autentisering,
8) riktlinjer och förfaranden för användning av krypteringsmetoder samt vid behov åtgärder för användning av säker elektronisk kommunikation,
9) upptäckande och hantering av incidenter i syfte att återställa och upprätthålla säkerheten och driftssäkerheten,
10) säkerhetskopiering, katastrofhantering, krishantering och annan driftskontinuitet och vid behov användning av säkrade reservkommunikationssystem i aktörens verksamhet,
11) grundläggande praxis för cyberhygien för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet, samt
12) åtgärder 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 för aktören, 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 närmare tekniska föreskrifter om

1) de delområden som ska beaktas i handlingsmodellen för hantering av cybersäkerhetsrisker och förfaranden för riskhantering och hantering av informationssäkerheten i fråga om kommunikationsnät och informationssystem,
2) förfaranden för utveckling och underhåll samt hantering av sårbarheter,
3) tillgångsförvaltning och grunderna för prioritetsklassificering av funktioner,
4) personalsäkerhet, utbildning i cybersäkerhet, upptäckande och hantering av incidenter samt driftskontinuitet,
5) metoder för åtkomsthantering, autentisering och kryptering,
6) grundläggande praxis för cyberhygien för att säkerställa grundläggande hanteringsåtgärder när det gäller säkerheten i kommunikationsnät och informationssystem,
7) hanteringsåtgärder som avser den fysiska miljön, lokalsäkerheten och nödvändiga resurser i fråga om kommunikationsnät och informationssystem.

I 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 risker och utövar tillsyn över genomförandet av den. Aktörens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

Med ledning avses aktörens styrelse, förvaltningsråd, verkställande direktör eller andra i jämförbar ställning samt en part som är verksam i uppdrag som är direkt underställda verkställande direktören, med vilket avses de högsta ledningsuppdragen hos aktören eller uppdrag där aktören de facto leds.

11 §

Incidentanmälningar till myndigheten

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

Den första anmälan ska göras inom 24 timmar från det att incidenten upptäcktes och den uppföljande anmälan inom 72 timmar från det att 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, och
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, angreppsindikatorer, och
3) eventuella uppdateringar av uppgifterna i den första anmälan.

Tillsynsmyndigheten kan inom sitt ansvarsområde meddela närmare tekniska föreskrifter om

1) när en incident som avses i 1 mom. är betydande,
2) de uppgifter som ska lämnas i den slutrapport som avses i 13 §, och
3) förfarandet för anmälan av betydande incidenter och uppgifter enligt 12–13 §.

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.

12 §

Delrapport om incident

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

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

13 §

Slutrapport om incident

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

Slutrapporten ska innehålla

1) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser,
2) den typ av hot eller grundorsak som sannolikt har utlöst incidenten,
3) tillämpade och pågående begränsande åtgärder, och
4) 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 underrättas om en betydande incident, kan tillsynsmyndigheten ålägga aktören att informera om saken eller, efter att ha hört den anmälningspliktiga, 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 incidentanmälningar om betydande incidenter, incidenter, cyberhot och tillbud också av andra aktörer än de som avses i denna lag.

Tillsynsmyndigheten ska informera den gemensamma kontaktpunkten om underrättelser enligt denna paragraf.

16 §

Mottagande av incidentanmälan

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

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

17 §

Hantering av incidentanmälningar

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

Tillsynsmyndigheten ska förse [de behöriga myndigheterna enligt CER-direktivet] med information om betydande incidenter, incidenter, cyberhot och tillbud om vilka underrättats med stöd av 11–13 och 15 § [av aktörer som identifierats som kritiska med stöd av CER-direktivet].

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

Om en betydande incident påverkar andra EU-medlemsstater eller andra sektorer, ska tillsynsmyndigheten informera den gemensamma kontaktpunkten om den betydande incidenten och sända anmälningar, rapporter och övriga uppgifter om den till den gemensamma kontaktpunkten.

Om en incident påverkar en annan medlemsstat 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 en EU-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.

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 också 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 §.

3 kap.

CSIRT-enheten

19 §

CSIRT-enheten

Vid Transport- och kommunikationsverket finns en CSIRT-enhet. CSIRT-enheten ska uppfylla kraven i artikel 11.1 i NIS 2-direktivet och dess verksamhet ska ordnas separat från den tillsynsfunktion som utförs med stöd av 25 §.

CSIRT-enheten ska

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 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 medlemmar i CSIRT-nätverket 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, och
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 i enlighet med tillgängliga resurser och på grundval av en riskbaserad metod.

CSIRT-enheten stöder sådana frivilliga arrangemang för informationsutbyte om cybersäkerhet som avses i 22 § mellan aktörer som omfattas tillämpningsområdet för denna lag, andra parter och CSIRT-enheten.

CSIRT-enheten kan producera sådana i 2 mom. 2 punkten avsedda tjänster för realtidsövervakning eller nära realtidsövervakning av kommunikationsnät och informationssystem för att säkerställa informationssäkerheten i kommunikationsnät och informationssystem samt för att 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 eller andra parter som begär det samt till sådana leverantörer av hanterade säkerhetstjänster som tillhandahåller aktörer eller andra parter en tjänst för upptäckande av kränkningar av informationssäkerheten (*servicecenter*).

Bestämmelser om de avgifter som tas ut för sådana tjänster som avses i 2 mom. 1 och 2 punkten och 20 § 4 mom. och som tillhandahållits på begäran av en aktör eller någon annan part eller om grunderna för avgifterna utfärdas genom förordning av kommunikationsministeriet.

20 §

Nätbaserad kartläggning av sårbarheter i allmänna kommunikationsnät och informationssystem

CSIRT-enheten har rätt att på ett proaktivt, icke-inkräktande sätt observera och kartlägga information i allmänt tillgängliga kommunikationsnät och informationssystem, det vill säga kommunikationsnät och informationssystem som är anslutna till ett allmänt kommunikationsnät, för att upptäcka sårbarheter, cyberhot och osäkert konfigurerade kommunikationsnät och 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 samt för att upprätthålla en lägesbild över cybersäkerheten.

Vid genomförandet av kartläggningen av sårbarheten har CSIRT-enheten rätt att via ett allmänt kommunikationsnät inhämta information om identifieringsuppgifter om teleterminalutrustning och informationssystem som är kopplade till ett allmänt kommunikationsnät samt 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 olägenhet 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.

CSIRT-enheten får använda sådan information som upptäckts vid kartläggningen av sårbarheter och som kan kopplas till föremålet för kartläggningen endast för att informera föremålet för kartläggningen om sårbarheter och risker som riktas mot kommunikationsnätet eller informationssystemet samt för att identifiera cyberhot, upprätthålla en lägesbild över cybersäkerheten och informera om sårbarheter. 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 av sårbarheter på ett sätt som avviker från 1–3 mom. för att upptäcka en sådan sårbarhet, ett sådant cyberhot eller en sådan osäker konfiguration 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 eller en riktad kartläggning av sårbarheter får innehållet i elektroniska meddelanden inte behandlas utan samtycke av en kommunikationspart. Vid en riktad kartläggning av sårbarheter som genomförs med stöd av 4 mom. har CSIRT-enheten rätt bedriva observation av och använda förmedlingsuppgifter, om det behövs för att upptäcka en sårbarhet, ett cyberhot eller en osäker konfiguration. CSIRT-enheten ska utplåna den information som den fått vid kartläggningen av sårbarheter, när informationen inte längre behövs för skötseln av de uppgifter som avses i denna paragraf.

21 §

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 rapporterna. Rapporter kan lämnas anonymt.

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

CSIRT-enheten har rätt att till den europeiska sårbarhetsdatabasen rapportera följande information om de sårbarheter som den känner till:

1) information som beskriver sårbarheten,
2) den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas,

3) tillgången till programfixar och, i avsaknad av tillgängliga programfixar, vägledning som tillhandahållits av tillsynsmyndigheten eller CSIRT-enheter riktad till användare av sårbara IKT-produkter och 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 EU-medlemsstater ska CSIRT-enheten samarbeta med CSIRT-enheterna i dessa stater inom CSIRT-nätverket.

22 §

Frivilliga arrangemang för informationsutbyte om cybersäkerhet

Mellan aktörer, CSIRT-enheten och andra parter kan upprättas frivilliga arrangemang för informationsutbyte om cybersäkerhet i syfte att förebygga och upptäcka cyberhot samt reagera på och återhämta sig från incidenter eller begränsa deras inverkan.

Mellan dem som deltar i frivilliga arrangemang för informationsutbyte om cybersäkerhet kan särskilt lämnas ut information om

1) cyberhot,
2) incidenter och tillbud,
3) sårbarheter,
4) tekniker och förfaranden,
5) angreppsindikatorer,
6) fientlig taktik,
7) specifika fientliga aktörer och
8) cybersäkerhetsvarningar.

De aktörer som deltar i arrangemang för informationsutbyte, CSIRT-enheten och andra parter får behandla information som de fått med stöd av denna paragraf endast för de ändamål som nämns i 1 mom. CSIRT-enheten kan dessutom behandla information för att upprätthålla en lägesbild över den nationella cybersäkerheten.

Utöver vad som i 319 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om utlämnande av information får CSIRT-enheten till en part 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 som enheten fått vid utförandet uppgifter enligt denna lag. En förutsättning för utlämnande av information är att den behövs för ett ändamål som nämns i 1 mom.

23 §

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

En part som använder den tjänst för upptäckande av kränkningar av informationssäkerheten som avses i 19 § 5 mom., servicecentret och CSIRT-enheten får till varandra lämna ut information som behövs för att följa upp informationssäkerheten i kommunikationsnät och informationssystem i syfte att förebygga och upptäcka cyberhot samt reagera på och återhämta sig från incidenter eller 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 part som använder tjänsten har begärt att ska behandlas i tjänsten och som parten har rätt att behandla med stöd av 272 § i lagen om tjänster inom elektronisk kommunikation.

På behandling av eventuella förmedlingsuppgifter och elektroniska meddelanden i tjänsten för upptäckande av kränkningar av informationssäkerheten vid CSIRT-enheten och servicecentret tillämpas bestämmelserna i 136, 137, 138, 145 och 272 § i lagen om tjänster inom elektronisk kommunikation. CSIRT-enheten kan dessutom använda förmedlingsuppgifter och andra uppgifter som den fått i samband med produktionen av tjänsten för att upprätthålla 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. om sekretess gäller också meddelanden och förmedlingsuppgifter som lämnats ut till CSIRT-enheten för genomförande av tjänsten för upptäckande av kränkningar av informationssäkerheten.

24 §

Utlämnande av vissa uppgifter om cyberhot och incidenter

En aktör eller någon annan part som deltar i frivilliga arrangemang för informationsutbyte om cybersäkerhet kan trots 136 § 4 i lagen om tjänster inom elektronisk kommunikation på eget initiativ till CSIRT-enheten, tillsynsmyndigheten eller någon annan part 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.

Utöver vad som föreskrivs i denna lag får CSIRT-enheten lämna ut information som den fått och inhämtat med stöd av denna lag på det sätt som föreskrivs i 319 § 2 och 3 mom. i lagen om tjänster inom elektronisk kommunikation.

Oberoende av vad som någon annanstans i lag föreskrivs om myndigheternas rätt att få sekretessbelagd information får annan information än sådan som omfattas av den obligatoriska anmälningsskyldigheten och som CSIRT-enheten fått vid utförandet av uppgifter enligt denna lag inte användas i brottsutredningar som gäller den som lämnat ut informationen eller vid administrativt eller annat beslutsfattande som gäller den som lämnat ut informationen. Ett undantag utgörs dock av en situation där CSIRT-enheten på basis av en riskbedömning för avvärjande av ett betydande cyberhot behöver underrätta tillsynsmyndigheten om en misstänkt allvarlig och uppsåtlig överträdelse av denna lag.

4 kap.

Tillsyn

25 §

Tillsynsmyndigheter

Tillsynsmyndigheter enligt denna lag är

a) Transport- och kommunikationsverket i fråga om de aktörer som avses i punkterna 1–7 i bilaga I och punkterna 1–5 i bilaga II,
b) Energimyndigheten i fråga om de aktörer som avses i punkterna 8–9 och underpunkterna a-b i punkt 10 i bilaga I,
c) Säkerhets- och kemikalieverket i fråga om de aktörer som avses i underpunkterna c-g i punkt 10 och punkterna 11–12 i bilaga I samt punkterna 6 och 11–13 i bilaga II,
d) Tillstånds- och tillsynsverket för social- och hälsovården i fråga om de aktörer som avses i punkt 13 i bilaga I,

e) Närings-, trafik- och miljöcentralen i Södra Savolax i fråga om de aktörer som avses i punkterna 14–15 i bilaga I och punkt 8 i bilaga II,
f) Livsmedelsverket i fråga om de aktörer som avses i punkt 7 i bilaga II,
g) Säkerhets- och utvecklingscentret för läkemedelsområdet i fråga om de aktörer som avses i punkterna 9–10 i bilaga II.

Tillsynsmyndigheten ska utöva tillsyn över efterlevnaden av denna lag, de föreskrifter som utfärdats med stöd av den och de rättsakter som antagits med stöd av NIS 2-direktivet i fråga om den verksamhet som avses i 1 mom.

Om tillsyn över samma aktör med stöd av 1 mom. utövas av fler än en myndighet, utövar respektive tillsynsmyndighet tillsyn över aktören endast i fråga om den verksamhet som anges i 1 mom. Tillsynsmyndigheterna ska samarbeta vid genomförandet av tillsynen.

26 §

Inriktning av tillsynen

Tillsynen inriktas på de väsentliga aktörerna.

Med väsentlig aktör avses
a) en aktör som avses i bilaga I och som överskrider definitionen av en medelstor aktör,
b) kvalificerade tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster,
c) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, vilka motsvarar eller överskrider definitionen av en medelstor aktör,
d) en aktör som med stöd av CER-direktivet har definierats som kritisk, samt
e) en aktör som definieras som väsentlig i en förordning av statsrådet som utfärdats med stöd av 3 § 2 mom.,

Tillsynsmyndigheten kan inrikta tillsynen och åtgärder enligt 29–31 § gentemot andra aktörer än väsentliga aktörer endast om det finns grundad anledning att misstänka att aktören i fråga inte har iakttagit denna lag, föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet.

Tillsynsmyndigheten kan ställa de uppgifter som föreskrivs 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
a) arten och omfattningen av den verksamhet som avses i bilaga I eller II,
b) informationssystemets eller kommunikationsnätets betydelse för den verksamhet som avses i bilaga I eller II, och
c) de omständigheter som anges i artikel 32.7 i NIS 2-direktivet,

Tillsynsmyndigheten kan lämna ett ärende utan prövning, om det är fråga om en uppenbart ogrundad begäran. Beslut om att lämna ett ärende utan prövning ska fattas utan dröjsmål.

27 §

Tillsynsmyndighetens rätt att få information

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att när den utför uppgifter enligt denna lag av aktörer som avses i denna lag få den information som är nödvändig för utförande av myndighetens uppgifter. 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 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 lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en tillsynsmyndighet enligt CER-direktivet och en CSIRT-enhet, om det är nödvändigt för skötseln av de uppgifter som föreskrivits för tillsynsmyndigheten, tillsynsmyndigheten enligt CER-direktivet eller CSIRT-enheten.

28 §

Tillsynsmyndighetens rätt till information om förmedlingsuppgifter, lokaliseringsuppgifter och elektroniska meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en aktör få förmedlingsuppgifter, lokaliseringsuppgifter eller meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för att övervaka de skyldigheter som gäller hantering av cybersäkerhetsrisker eller för att utreda betydande incidenter.

Vad som i 316 § 4 mom. och 319 § i lagen om tjänster inom elektronisk kommunikation föreskrivs om sekretess för och utlämnande och utplåning av information som Transport- och kommunikationsverket har fått och skaffat om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar tillämpas också på den information som tillsynsmyndigheten har fått och skaffat med stöd av denna paragraf.

29 §

Inspektionsrätt

Tillsynsmyndigheten har rätt att förrätta inspektioner av aktörer. Inspektionen förrättas för tillsynen över att skyldigheterna enligt denna lag eller författningar som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet fullgörs, i den omfattning det behövs. Den som förrättar inspektionen ska ha sådan utbildning och erfarenhet som behövs för inspektionen.

Tillsynsmyndigheten kan genom sitt beslut anlita en annan tillsynsmyndighet, ett bedömningsorgan för informationssäkerhet eller en utomstående expert i informationsteknik att förrätta inspektionen eller be att någon av dessa förrättar inspektionen, om detta är nödvändigt på grund av inspektionens art eller omfattning. 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 används för boende av permanent natur. Tillsynsmyndigheten, andra myndigheter som förrättar inspektion 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 förfarandet vid inspektionen tillämpas vad som i 39 § i förvaltningslagen (434/2003) föreskrivs om inspektion.

30 §

Säkerhetsrevision

Tillsynsmyndigheten har rätt att genom sitt beslut 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 vållat 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 den förutsätter 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 genom ett beslut ålägga aktören att vidta sådana rimliga och proportionella åtgärder för att utveckla hanteringen av cybersäkerhetsrisker som säkerhetsrevisionen rekommenderar.

31 §

Tillsynsbeslut, anmärkning och varning

Tillsynsmyndigheten kan genom ett beslut ålägga aktören att inom utsatt tid avhjälpa bristerna i fullgörandet av skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller rättsakter som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan 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 rättsakter som antagits med stöd av NIS2-direktivet.

Tillsynsmyndigheten kan ge aktören en anmärkning eller varning. En varning kan ges om en anmärkning inte kan anses tillräcklig med beaktande av omständigheterna i ärendet som helhet.

32 §

Begränsning av tillståndspliktig eller certifierad verksamhet och återkallande av tillstånd eller certifiering

Tillsynsmyndigheten kan temporärt begränsa verksamheten enligt ett tillstånd eller en certifiering som beviljats en väsentlig aktör eller återkalla tillståndet eller certifieringen eller, om en annan myndighet är behörig tillstånds- eller certifieringsmyndighet, lägga fram ett förslag till beslut i ärendet, om

1) en väsentlig aktör väsentligt och allvarligt har försummat att genomföra handlingsmodellen för hantering av cybersäkerhetsrisker eller de åtgärder som hanteringen av riskerna förutsätter, eller
2) en väsentlig aktör väsentligt och allvarligt underlåtit att iaktta sina övriga skyldigheter enligt denna lag, föreskrifter som utfärdats med stöd av denna lag eller rättsakter som antagits med stöd av NIS 2-direktivet.

Tillsynsmyndigheten ska innan den fattar ett beslut eller lägger fram ett förslag till beslut enligt 1 mom. ge den väsentliga aktören en anmärkning eller varning samt reservera en skälig tid för att avhjälpa bristen eller försummelsen.

En begränsning av verksamheten eller ett återkallande av tillstånd eller certifiering meddelas för viss tid som avvägs enligt hur allvarliga bristerna eller försummelserna i verksamheten är, dock högst tills behövliga åtgärder för att avhjälpa bristen eller försummelsen har vidtagits. Om bristerna eller försummelserna inte har avhjälpts inom utsatt tid, kan tillsynsmyndigheten efter utgången av tidsfristen besluta eller föreslå att beslut ska fattas om ändring av tillståndsvillkoren i syfte att begränsa verksamheten eller permanent återkalla tillståndet eller certifieringen.

33 §

Begränsning av ledningens verksamhet

Tillsynsmyndigheten kan för viss tid, högst fem år, 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 samt att sköta uppdrag som är direkt underställda verkställande direktören, med vilket avses de högsta ledningsuppdragen hos den väsentliga aktören eller uppdrag där aktören de facto leds, om personen upprepade gånger och allvarligt har brutit mot skyldigheterna i 10 §. Tillsynsmyndigheten ska innan den fattar ett beslut ge den väsentliga aktören en anmärkning eller varning samt reservera en skälig tid för att avhjälpa bristen eller försummelsen.

Med avvikelse från 1 mom. kan ledningens verksamhet inte begränsas om det är fråga om statliga myndigheter, statliga affärsverk, kommunala myndigheter, självständiga offentligrättsliga inrättningar, riksdagens ämbetsverk, republikens presidents kansli, evangelisk-lutherska kyrkan i Finland, ortodoxa kyrkan i Finland eller de två sistnämndas församlingar, kyrkliga samfälligheter och övriga organ.

34 §

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 informera dataombudsmannen om saken.

Om den tillsynsmyndighet som är behörig enligt den allmänna dataskyddsförordningen är etablerad i en annan medlemsstat, ska tillsynsmyndigheten göra en i 1 mom. avsedd anmälan till dataombudsmannen.

35 §

Vite, hot om tvångsutförande och hot om avbrytande

Tillsynsmyndigheten kan förena ett beslut som den har fattat med stöd av denna lag med vite, tvångsutförande eller hot om avbrytande, på vilka viteslagen (1113/1990) tillämpas.

36 §

Begäran om omprövning

I beslut som tillsynsmyndigheten fattat med stöd av 30–33 § får omprövning begäras. Bestämmelser om begäran om omprövning finns i förvaltningslagen.

Tillsynsmyndigheten kan i sitt beslut bestämma att beslutet ska iakttas trots ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat.

5 kap.

Påföljdsavgift

37 §

Administrativ påföljdsavgift

En administrativ påföljdsavgift kan påföras en aktör som uppsåtligen eller av grov oaktsamhet

1) försummar att fullgöra riskhanteringsskyldigheten enligt 7 §, 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) försummar att vidta de åtgärder som avses i 9 § 2 mom.,
3) försummar att lämna en incidentanmälan enligt 11 §, delrapport enligt 12 § eller slutrapport enligt 13 § till tillsynsmyndigheten,
4) försummar att lämna tillsynsmyndigheten de uppgifter som avses i 43 §.

Statliga myndigheter, statliga affärsverk, kommunala myndigheter, självständiga offentligrättsliga institutioner, 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.

38 §

Påföljdsavgiftsnämnd

Den administrativa påföljdsavgiften påförs av påföljdsavgiftsnämnden på framställning av tillsynsmyndigheten. Den administrativa påföljdsavgiften ska betalas till staten.

Ordföranden och vice ordföranden för påföljdsavgiftsnämnden utses av Transport- och kommunikationsverket. Varje tillsynsmyndighet utnämner en ledamot i nämnden och en personlig ersättare för honom eller henne. Av nämndens ledamöter och ersättare förutsätts förtrogenhet med hantering av cybersäkerhetsrisker samt NIS 2-direktivet och de skyldigheter som ställs i den reglering som genomför direktivet inom den utnämnande myndighetens tillsynsområde. Ordföranden och vice ordföranden för nämnden ska ha sådan tillräcklig juridisk sakkunskap som uppdraget förutsätter. Nämndens ledamöter utnämns 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 de uppgifter som är nödvändiga för skötseln av nämndens uppgifter.

39 §

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, anmärkningar eller varningar av tillsynsmyndigheten,
    d) förhindrande av tillsynsmyndighetens inspektion eller underlåtenhet att låta utföra en ålagd revision,
    e) lämnande av felaktiga eller vilseledande uppgifter om riskhantering eller betydande incidenter till myndigheten,
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.

40 §

Påföljdsavgiftens maximibelopp

Maximibeloppet av den administrativa påföljdsavgiften för väsentliga aktörer som avses i 26 § är 10 000 000 euro eller 2 procent av aktörens totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilken siffra som är högst.

Maximibeloppet av den administrativa påföljdsavgiften för andra än väsentliga aktörer är 7 000 000 euro eller 1,4 procent av aktörens totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilken siffra som är högst.

41 §

Avstående från och verkställighet av påföljdsavgift

Påföljdsavgift påförs inte om

1) aktören på eget initiativ vidtagit tillräckliga åtgärder för att avhjälpa överträdelsen eller försummelsen omedelbart efter att den upptäckts och utan dröjsmål underrättat tillsynsmyndigheten om den samt samarbetat med tillsynsmyndigheten, och överträdelsen eller försummelsen inte är allvarlig eller återkommande,
2) överträdelsen eller försummelsen ska anses vara ringa, eller
3) påförande av påföljdsavgift ska anses vara uppenbart oskäligt på andra grunder än de som avses i 1 eller 2 punkten.

Påföljdsavgift får inte påföras, om det har förflutit mer än fem år sedan överträdelsen eller försummelsen har skett. Om överträdelsen eller försummelsen har varit fortlöpande räknas tidsfristen från det att överträdelsen eller försummelsen har upphört.

Påföljdsavgift får inte påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som 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.

Bestämmelser om verkställigheten av påföljdsavgifter finns i lagen om verkställighet av böter (672/2002). En påföljdsavgift preskriberas när fem år har förflutit från det att det lagakraftvunna beslutet om avgiften fattades.

42 §

Sökande av ändring

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

6 kap.

Övriga bestämmelser

43 §

Förteckning över aktörer

Aktörer ska lämna tillsynsmyndigheten följande uppgifter för förande av en förteckning över aktörer:

a) aktörens namn,
b) adress, e-postadress, telefonnummer och andra aktuella kontaktuppgifter,
c) IP-adresser,
d) relevant sektor och delsektor som avses i bilaga I eller II till NIS 2-direktivet,
e) huruvida aktören är en sådan väsentlig aktör som avses i 26 §,
f) en förteckning över de EU-medlemsstater där aktören tillhandahåller tjänster som omfattas av NIS 2-direktivet, och
g) deltagande i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 22 §.

Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt tillhandahållare av internetbaserade marknadsplatser, leverantörer av sökmotorer och leverantörer av plattformar för sociala nätverkstjänster ska utöver de uppgifter som anges i 1 mom. lämna tillsynsmyndigheten följande uppgifter:

a) typ av aktör som avses i bilaga I eller II till NIS 2-direktivet,
b) adress till aktörens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i 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
c) en förteckning över de EU-medlemsstater 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 1 mom. inom två veckor och av de uppgifter som avses i 2 mom. inom tre månader från tidpunkten för ändringen. Tillsynsmyndigheten kan meddela närmare tekniska föreskrifter om hur uppgifterna ska lämnas.

Tillsynsmyndigheten för i fråga om sitt tillsynsområde en förteckning över aktörerna som innehåller de uppgifter som lämnats med stöd av 1 och 2 mom. Tillsynsmyndigheten ska till den gemensamma kontaktpunkten lämna de uppgifter ur förteckningen över aktörer som behövs för att göra de anmälningar som avses i artiklarna 3.5 och 27.4 i NIS 2-direktivet. Den gemensamma kontaktpunkten svarar för att de anmälningar som avses i artiklarna 3.5 och 27.4 i NIS 2-direktivet görs till Europeiska kommissionen, NIS-samarbetsgruppen och Europeiska unionens cybersäkerhetsbyrå.

44 §

Nationell strategi för cybersäkerhet

Statsrådet godkänner 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 godkänts. 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.

45 §

Plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser

Transport- och kommunikationsverket svarar för utarbetandet av en nationell plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser i samarbete med de tillsynsmyndigheter som avses i 25 §, polisstyrelsen, skyddspolisen, Försvarsmakten och försörjningsberedskapscentralen.

Den nationella planen för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser ska innehålla de uppgifter som avses i artikel 9.3 och 9.4 i NIS 2-direktivet. Respektive myndighet är i enlighet med sina lagstadgade uppgifter en sådan cyberkrishanteringsmyndighet som avses i artikel 9.1 i NIS 2-direktivet. Cybersäkerhetscentret vid Transport- och kommunikationsverket är samordnare vid hanteringen 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 godkänts. 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.

46 §

Myndighetssamarbete

Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska samarbeta för att fullgöra 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, den berörda myndigheten enligt Europaparlamentets och rådets förordning (EG) nr 300/2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002, den behöriga myndigheten enligt Europaparlamentets och rådets förordning (EU) 2018/1139 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91, tillsynsorganet enligt eIDAS-förordningen, den behöriga myndigheten enligt DORA-förordningen, den nationella regleringsmyndigheten enligt teledirektivet och den behöriga myndigheten enligt CER-direktivet.

Tillsynsmyndigheterna och den behöriga myndigheten enligt CER-direktivet ska regelbundet utbyta information avseende identifieringen av kritiska aktörer, om risker, cyberhot och incidenter samt icke-cyberrelaterade risker, hot och incidenter som berör aktörer som identifierats som kritiska i enlighet med CER-direktivet, samt om de åtgärder som vidtagits för att hantera sådana risker, hot och incidenter. Tillsynsmyndigheterna ska underrätta den behöriga myndigheten enligt CER-direktivet när de utövar befogenheter enligt 4 kap. gentemot en aktör som identifierats som kritisk med stöd av CER-direktivet. Tillsynsmyndigheten kan på motiverad begäran av en behörig myndighet enligt CER-direktivet rikta befogenheter enligt 4 kap. gentemot en aktör som identifierats som kritisk med stöd av CER-direktivet.

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.

Tillsynsmyndigheten och tillsynsorganen enligt eIDAS-förordningen, den behöriga myndigheten enligt DORA-förordningen och den nationella regleringsmyndigheten enligt teledirektivet ska regelbundet utbyta information om betydande incidenter och cyberhot.

47 §

Ikraftträdande

Denna lag träder i kraft den 18 oktober 2024.

Bestämmelserna i 43 § träder i kraft den 1 januari 2025.

_____

Denna lag träder i kraft den 20 .

_____

Bilaga I

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) Leverantörer av flygkontrolltjänster 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) Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster, med ansvar för trafikstyrning, med undantag för aktörer inom den offentliga förvaltningen för vilka trafikstyrning eller driften av intelligenta transportsystem är en icke väsentlig del av deras allmänna verksamhet
   b) De som tillhandahåller intelligenta transportsystem som avses i 160 § i lagen om transportservice (320/2017)
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
   b) Överföringsnätsinnehavare som avses i 3 § 1 mom. 9 punkten i naturgasmarknadslagen
   c) Naturgasleverantörer som avses i 3 § 1 mom. 14 punkten i naturgasmarknadslagen (587/2017)
   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. Operatörer av anläggningar för produktion, lagring och överföring av vätgas
13. Hälso- och sjukvård
    a) Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård
    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
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

1. Tillhandahållare av budtjänster och i 2 § 1 mom. 2 punkten i postlagen (415/2011) avsedda tillhandahållare av posttjänster
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
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 av 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 medicinska 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 punkt 13 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 §, 10 § 1 mom. 2 punkten och 18 § 1 mom. samt

fogas till 1 § ett nytt 2 mom., till 2 § nya 17–26 punkter och till lagen ett nytt 4 a kap. som följer:

1 §

Lagens syfte

— —

Genom denna lag genomförs inom den offentliga förvaltningen 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 genomförandet av NIS 2-direktivet finns dessutom i lagen om hantering av cybersäkerhetsrisker (/).

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 enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972,

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, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs i sådana system som avses i underpunkt a och b för att de 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 kommunikationsnät och informationssystem,

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

20) *cyberhot* en potentiell omständighet, händelse eller handling som 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 vålla betydande materiell eller immateriell skada,

22) *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 sådan incident inträffar,

23) *tillbud* en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod,

24) *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,

25) *betydande incident* en incident som

a) har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för myndigheten,

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

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

3 §

Lagens tillämpningsområde och begränsningar i 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).

Bestämmelserna i 4 a kap. tillämpas på de statliga ämbetsverk och inrättningar som avses i 4 § 1 mom. 1 punkten, statliga affärsverk, självständiga offentligrättsliga inrättningar som avses i 4 § 1 mom. 9 punkten samt välfärdsområden, välfärdssammanslutningar och Helsingfors stad när de sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar. Dessutom tillämpas 4 a kap. på aktörer som med stöd av [CER-lagen] har definierats som kritiska aktörer inom offentlig förvaltning. Bestämmelserna i 4 a kap. tillämpas dock inte på Försvarsmakten, Försvarsfastigheter, polisenheter som avses i polisförvaltningslagen (110/1992), Gränsbevakningsväsendet, Tullens brottsbekämpning, Åklagarmyndigheten, Finlands Bank eller sådan tjänsteproduktion i säkerhetsnätet och användning av dess tjänster som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015), nedan *säkerhetsnätslagen*. Bestämmelserna i 4 a kap. 18 h–18 l § tillämpas inte på republikens presidents kansli, verksamhet som bedrivs av justitiekanslern i statsrådet eller Folkpensionsanstalten.

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 (1054/1993) föreskrivs om informationshantering och användning av informationssystem inom Finlands evangelisk-lutherska kyrka.

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.

Vad som i 4 kap., 22–24 och 25–27 § samt 6 a kap. i denna lag föreskrivs om informationshanteringsenheter och myndigheter ska tillämpas på privatpersoner, privaträttsliga sammanslutningar och 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 § i denna lag 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.

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 2 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.

— —

18 §

Handlingar som ska säkerhetsklassificeras inom statsförvaltningen

Myndigheter vid statliga ämbetsverk, inrättningar och affärsverk samt domstolar och nämnder som har inrättats för att behandla besvärsärenden samt Suomen Erillisverkot Oy och dess helägda dotterbolag när dessa sköter uppgifter som avses i säkerhetsnätslagen ska säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckning om säkerhetsklass ska göras, om en handling eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.

— —

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 offentlig förvaltning enligt punkt 10 i bilaga I till NIS 2 -direktivet, med

undantag för välfärdsområdena och välfärdssammanslutningarna samt Helsingfors stad, vilka är viktiga aktörer.

En informationshanteringsenhet ska till Transport- och kommunikationsverket anmäla

1) informationshanteringsenhetens namn,
2) informationshanteringsenhetens adress och aktuella kontaktinformation, inklusive e-postadress och telefonnummer,
3) IP-adressintervall för informationshanteringsenheten,
4) om den är en väsentlig eller viktig aktör inom offentlig förvaltning,
5) en förteckning över övriga medlemsstater i Europeiska unionen där enheten tillhandahåller sina tjänster,
6) deltagande i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 22 § i lagen om hantering av cybersäkerhetsrisker.

Informationshanteringsenheten ska utan dröjsmål och senast inom två veckor från en ändring, anmäla alla ändringar i de uppgifter som lämnats med stöd av 1 mom.

18 b §

Skyldighet att hantera cybersäkerhetsrisker och handlingsmodell för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sin verksamhet. Syftet med hanteringen av cybersäkerhetsrisker är att skydda kommunikationsnät och informationssystem, deras användare och andra personer mot cyberhot.

Informationshanteringsenheten ska utarbeta en handlingsmodell för hantering av cybersäkerhetsrisker och hålla den uppdaterad. I handlingsmodellen identifieras de risker som riktas mot informationshanteringsenhetens kommunikationsnät och informationssystem och deras fysiska miljö i enlighet med ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen ska dessutom beskrivas målen, förfarandena och ansvaren för hantering av cybersäkerhetsrisker samt de i 18 c § avsedda tekniska, driftsrelaterade och organisatoriska åtgärder för hantering av cybersäkerhetsrisker.

Informationshanteringsenhetens 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. Informationshanteringsenhetens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

18 c §

Åtgärder för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska vidta sådana åtgärder för hantering av cybersäkerhetsrisker som är lämpliga och proportionella i förhållande till riskerna för de kommunikationsnät och informationssystem som används, kommunikationsnätets eller informationssystemets betydelse med tanke på informationshanteringsenhetens verksamhet samt de samhälleliga och ekonomiska konsekvenserna av en incident i dessa. 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.

Åtgärder för hantering av cybersäkerhetsrisker är till för att identifiera incidentrisker, förebygga, upptäcka och hantera incidenter och återhämta sig från incidenter och för att begränsa

deras inverkan. Genom åtgärder för hantering av cybersäkerhetsrisker skyddas kommunikationsnät och informationssystem och deras fysiska miljö mot cyberhot och incidenter samt minimeras incidenternas inverkan på informationshanteringsenhetens verksamhet, mottagarna av dess tjänster och övriga tjänster. Åtgärder för hantering av cybersäkerhetsrisker ska omfatta åtminstone följande åtgärdshelheter:

1) riktlinjer för hantering av cybersäkerhetsrisker samt bedömning av effektiviteten i fråga om åtgärderna för hantering av cybersäkerhetsrisker,
2) 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 för leverantörers produkter och tjänsteleverantörers tjänster och de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem samt cybersäkerhetspraxis hos leverantörer och tjänsteleverantörer,
5) tillgångsförvaltning och identifiering av funktioner som är viktiga med tanke på säkerheten,
6) personalsäkerhet och utbildning i cybersäkerhet,
7) förfaranden för åtkomsthantering och autentisering,
8) riktlinjer och förfaranden för användning av krypteringsmetoder samt vid behov åtgärder för användning av säker elektronisk kommunikation,
9) upptäckande och hantering av incidenter i syfte att upprätthålla och återställa säkerheten och driftssäkerheten,
10) säkerhetskopiering, katastrofhantering, krishantering och annan driftskontinuitet och vid behov användning av säkrade reservkommunikationssystem,
11) grundläggande praxis för cyberhygien för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet,
12) åtgärder för att skydda kommunikationsnäts och informationssystems fysiska miljö och säkerställa lokalsäkerheten samt nödvändiga resurser.

[Eventuellt bemyndigande att utfärda förordning för genomförande av artikel 21.5 led 2 samt artiklarna 24 och 25 i NIS 2-direktivet.

- kommissionens genomförandebestämmelser om riskhanteringsåtgärder
- kommissionens genomförandebestämmelser om skyldighet att använda vissa produkter som certifierats i enlighet med cybersäkerhetsakten
- användning av standarder]

18 d §

Skyldighet att anmäla betydande incidenter

Myndigheten ska utan obefogat dröjsmål, senast inom 24 timmar efter att ha fått kännedom om en betydande incident lämna Transport- och kommunikationsverket 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 den kan ha gränsöverskridande verkningar samt sannolikheten för sådana verkningar.

Myndigheten ska utan obefogat dröjsmål, senast inom 72 timmar efter att ha fått kännedom om den betydande incidenten, lämna Transport- och kommunikationsverket en uppföljande anmälan om incidenten, i vilken den information som avses i 1 mom. ska uppdateras och anges en inledande bedömning av den betydande incidentens art, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

Myndigheten ska senast en månad efter den uppföljande anmälan lämna Transport- och kommunikationsverket en slutrapport om incidenten som innehåller

1) en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser,
2) den typ av hot eller grundorsak som sannolikt har utlöst incidenten,
3) tillämpade och pågående begränsande åtgärder,
4) eventuella gränsöverskridande konsekvenser.

Om incidenten fortfarande pågår när den slutrapport som avses i 3 mom. ska lämnas in, ska en delrapport lämnas i stället för slutrapporten. Slutrapporten ska då lämnas in inom en månad från det att myndigheten har behandlat incidenten. Transport- och kommunikationsverket har rätt att om incidenten fortgår av myndigheten få ytterligare information eller en delrapport om statusuppdateringar som hänför sig till ärendet och om hur hanteringen framskrider.

[Eventuellt bemyndigande att utfärda förordning för genomförande av artikel 23.11 i NIS 2-direktivet:

- Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelse som lämnas i enlighet med punkt 1 i denna artikel (skyldighet att underrätta tillsynsmyndigheten och tjänsteanvändarna om betydande incidenter) och med artikel 30 (frivilliga) samt för underrättelser (skyldighet att informera tjänstemottagarna om betydande cyberhot) som lämnas i enlighet med punkt 2 i denna artikel.

18 e §

Mottagande av incidentanmälan

Transport- och kommunikationsverket ska utan obefogat dröjsmål och 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, anvisningar eller operativa råd om hanteringen av incidenten samt anvisningar om hur en betydande incident ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet.

18 f §

Frivillig underrättelse

En myndighet kan också underrätta Transport- och kommunikationsverket om andra än betydande incidenter samt om cyberhot och tillbud. Även andra som nämns i 3 § i denna lag, på vilka detta kapitel inte tillämpas, kan underrätta Transport- och kommunikationsverket om incidenter, cyberhot och tillbud.

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

Myndigheter och andra som nämns i 3 § kan i samband med en frivillig underrättelse lämna ut sådan information till Transport- och kommunikationsverket som Transport- och kommunikationsverket har rätt att få med stöd av 18 i § 1 och 2 mom. På utlämnande av information tillämpas också 18 i § 3 mom.

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 underrättas om en betydande incident, kan Transport- och kommunikationsverket ålägga myndigheten att informera om den betydande incidenten eller, efter att ha hört myndigheten, själv informera om saken.

18 h §

Behörig myndighet

Transport- och kommunikationsverket är inom den offentliga förvaltningen den behöriga myndighet som avses i artikel 8.1 i NIS 2 -direktivet. Transport- och kommunikationsverket ska, utöver vad som ovan i detta kapitel föreskrivs om behandlingen av incidentanmälningar, utöva tillsyn över att de skyldigheter som föreskrivs i detta kapitel och i författningar eller rättsakter som utfärdats med stöd av detta kapitel eller 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 ska när det utför sina tillsynsåtgärder och fattar ett tillsynsbeslut enligt 18 l § beakta de omständigheter som anges i artikel 32.7 i NIS 2-direktivet. Transport- och kommunikationsverket kan ställa de tillsynsuppgifter som föreskrivs i denna lag i prioritetsordning på grundval av en riskbaserad metod. Transport- och kommunikationsverket 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 författningar eller rättsakter som utfärdats med stöd av detta kapitel eller NIS 2-direktivet.

Om inte något annat föreskrivs i detta kapitel ska Transport- och kommunikationsverket 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 de övriga myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan som avses i NIS 2-direktivet samt vid utlämnandet av uppgifter till dem iaktta vad som i [6 § 4 mom., 15 § 3 mom., 17 §, 25 § 3 mom., 27 § 2 mom., 34 §, 43 § 4 mom. och 46 §] i lagen om hantering av cybersäkerhetsrisker föreskrivs om behandling av information vid tillsynsmyndigheten, om tillsynsmyndighetens samarbete med de övriga myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan som avses i NIS 2-direktivet samt om utlämnandet av information till dem. Bestämmelser om en gemensam kontaktpunkt och en CSIRT-enhet som avses i NIS 2-direktivet och om deras uppgifter, behandling av information och samarbete med de övriga myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan som avses i NIS 2 -direktivet finns i lagen om hantering av cybersäkerhetsrisker.

18 i §

Den behöriga myndighetens rätt att få information

Transport- och kommunikationsverket har när det utför uppgifter enligt detta kapitel trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en myndighet på vilken detta kapitel tillämpas få den information som är nödvändig för utförande av verkets uppgifter. Myndigheten ska lämna ut informationen utan dröjsmål, i begärd form och avgiftsfritt.

Transport- och kommunikationsverket har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en myndighet få förmedlingsuppgifter, lokaliseringsuppgifter eller meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för att övervaka att de i 18 b och 18 c § föreskrivna skyldigheter som gäller hantering av cybersäkerhetsrisker fullgörs eller för att utreda betydande incidenter. På behandlingen av denna information vid Transport- och kommunikationsverket tillämpas vad som i 316 § 4 mom. och 319 § i lagen om tjänster inom elektronisk kommunikation (917/2014) föreskrivs om sekretess för och utlämnande och utplåning av information som Transport- och kommunikationsverket har fått och skaffat om meddelanden, förmedlingsuppgifter, lokaliseringsuppgifter samt om innehållet i och existensen av konfidentiella radiosändningar

Rätten till information enligt denna paragraf förpliktar inte att till Transport- och kommunikationsverket lämna ut information om sådan tjänsteproduktion eller användning av tjänster i säkerhetsnätet som avses i säkerhetsnätslagen eller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed. En myndighet kan inom de gränser som anges i en sekretessbestämmelse som innehåller en offentlighets- eller sekretesspresumtion enligt lagen om offentlighet i myndigheternas verksamhet till Transport- och kommunikationsverket lämna ut information också om tjänsteproduktion och användning av tjänster i säkerhetsnätet samt information som har samband med försvaret och den nationella säkerheten och som är sekretessbelagd för allmänheten. Om en sådan handling eller informationen i den är säkerhetsklassificerad, fattas beslutet om utlämnande av handlingen eller informationen av den myndighet som upprättat handlingen eller den myndighet som ärendet i sin helhet hör till. Vid hantering av särskilt känsligt informationsmaterial som avses i lagen om internationella förpliktelser som gäller informationssäkerhet ska bestämmelserna i den lagen iakttas.

18 j §

Inspektionsrätt

Transport- och kommunikationsverket 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 författningar eller rättsakter som utfärdats med stöd av detta kapitel eller NIS 2-direktivet fullgörs.

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

Den som förrättar inspektionen har för förrättande av inspektionen rätt att få tillträde till andra utrymmen än sådana som används för boende av permanent natur och till det kommunikationsnät eller informationssystem som inspektionen gäller samt rätt att trots sekretessbestämmelserna få granska den information och de handlingar, maskinvaror och programvaror som behövs för inspektionsuppdraget, utföra behövliga tester och mätningar samt granska de säkerhetsarrangemang som myndigheten har genomfört. På förfarandet vid inspektionen tillämpas vad som i 39 § i förvaltningslagen föreskrivs om inspektion.

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.

18 k §

Tilldelande av biträdande uppgift till godkänt bedömningsorgan samt att låta utföra bedömning

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

Transport- och kommunikationsverket kan för tillsynen ålägga en myndighet att låta ett godkänt bedömningsorgan 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 vållat 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 godkänt bedömningsorgan och som förrättar inspektion eller utför bedömning tillämpas vad som i 18 j § 2–4 mom. föreskrivs om inspektionsförrättarens erfarenhet och utbildning samt inspektionsförrättarens rättigheter. På den som är anställd vid ett godkänt bedömningsorgan tillämpas bestämmelserna om straffrättsligt tjänsteansvar för tjänstemän när han eller hon sköter uppgifter som avses i denna paragraf, med undantag för bestämmelserna om avsättningspåföljd. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

18 l §

Påföljder

Transport- och kommunikationsverket kan genom sitt beslut ålägga en myndighet att inom utsatt tid avhjälpa bristerna i fullgörandet av skyldigheterna enligt detta kapitel eller författningar eller rättsakter som utfärdats med stöd av detta kapitel eller NIS 2-direktivet. Transport- och kommunikationsverket kan ålägga myndigheten att offentliggöra dessa brister eller andra omständigheter som har samband med överträdelser av de nämnda bestämmelserna.

Transport- och kommunikationsverket kan ge myndigheten en anmärkning eller varning. En varning kan ges om en anmärkning inte kan anses tillräcklig med beaktande av omständigheterna i ärendet som helhet.

Transport- och kommunikationsverket kan förena ett beslut som avses i 1 mom. med vite. Bestämmelser om vite finns i viteslagen (1113/1990).

18 m §

Sökande av ändring

Omprövning av ett beslut som Transport- och kommunikationsverket fattat med stöd av detta kapitel får begäras. Bestämmelser om omprövningsförfarandet finns i 7 a kap. i förvaltningslagen.

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

Denna lag träder i kraft den [18] [oktober] 2024.

Den anmälan som avses i 18 a § 2 mom. ska göras senast den 31 december 2024.

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) 1 kap. 2 § 2 mom. och 29 kap. 247 a §, sådana de lyder, 1 kap. 2 § 2 mom. i lag 1207/2020 och 29 kap. 247 a § i lag 281/2018, och

ändras 21 kap. 165 § 1 mom., 167 och 170 §, 33 kap. 275 §, 38 kap. 308 § 3 mom., 39 kap. 313 § 2 mom. 2 punkten, 40 kap. 318 § 4 mom., sådana de lyder, 21 kap. 165 § 1 mom. och 170 §, 38 kap. 308 § 3 mom. samt 39 kap. 313 § 2 mom. 2 punkten i lag 1003/2018, 21 kap. 167 § i lagarna 1003/2018 och 1207/2020 samt 33 kap. 275 § och 40 kap. 318 § 4 mom. i lag 1207/2020, samt

fogas till 21 kap. 165 § ett nytt 4 mom. och till 29 kap. 247 § 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:

a) registrarens namn, FO-nummer eller, om sådant saknas, annan identifieringsuppgift samt den e-postadress som ska användas för hörande och delgivning,
b) adress och aktuell kontaktinformation till registrarens huvudkontor och andra lagliga verksamhetsställen i 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,
c) registrarens IP-adressintervall,
d) en förteckning över de EU-medlemsstater där registraren tillhandahåller tjänster, och
e) andra uppgifter som behövs för tillsynen.

Transport- och kommunikationsverket ska utan dröjsmål informeras om ändringar i de uppgifter som registraren har anmält. Om verksamheten läggs ned ska Transport- och kommunikationsverket och kunderna informeras om detta minst två veckor i förväg. Om Transport- och kommunikationsverket med stöd av 171 § 2 mom. har meddelat ett förbudsbeslut ska kunderna utan dröjsmål informeras om detta.

Transport- och kommunikationsverket får meddela närmare föreskrifter om hur anmälan ska göras och om innehållet i den.

Transport- och kommunikationsverket ska lämna den gemensamma kontaktpunkt som avses i 18 § i lagen om hantering av cybersäkerhetsrisker (/) 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 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 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 med rätta begär åtkomst till registreringsuppgifter utan obefogat dröjsmål och senast inom 72 timmar efter mottagandet av en laglig och vederbörligen 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 riktlinjer och förfaranden, om informationssäkerheten i registrarens verksamhet, 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 en leverantör av DNS-tjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt att anmäla avvikelser finns i lagen om hantering av cybersäkerhetsrisker (/).

— —

247 §

Skyldighet att sörja för informationssäkerheten vid kommunikationsförmedling och tillhandahållande av mervärdestjänster

— —

När det gäller att sörja för informationssäkerheten tillämpas dessutom vad som i lagen om hantering av cybersäkerhetsrisker (/) föreskrivs i fråga om en sådan kommunikationsförmedlare och leverantör 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 lagen om hantering av cybersäkerhetsrisker 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

— —

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, Organet för europeiska regleringsmyndigheter för elektronisk kommunikation och för tillsynsmyndigheterna 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 NIS 2-direktivet, om det är nödvändigt med tanke på övervakningen av nät- och informat-

ionssäkerheten, 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.

— —

_____

Denna lag träder i kraft den 20 .

_____

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 §.

_____

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 §.

_____

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) 18 kap. 161 §, sådan den lyder i lag 1256/2020, samt

ändras 15 kap. 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 lagen om hantering av cybersäkerhetsrisker (/).

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 (/) 18 a §.

_____

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 §.

_____

Denna lag träder i kraft den 20 . _____

9.

Lag

om ändring av lagen om behandling av kunduppgifter inom social- och hälsovården

I enlighet med riksdagens beslut
upphävs i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) 90 § 4 mom. samt
ändras 2 § 3 mom. och 90 § 2 och 3 mom. som följer:

2 §

Tillämpningsområde och förhållande till annan lagstiftning

— —

Genom denna lag utfärdas 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 lagen om hantering av cybersäkerhetsrisker (/) 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

— —

Bestämmelser om skyldighet för tjänstetillhandahållare inom hälso- och sjukvården att anmäla störningar i informationssäkerheten finns i 11–14 § i lagen om hantering av cybersäkerhetsrisker. En tjänstetillhandahållare inom socialvården, 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 socialservice kan äventyras avsevärt. Institutet för hälsa och välfärd får meddela närmare föreskrifter om när en sådan 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 inom socialvården, 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.

———

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 och 26 a §, 27 § 3 mom., 28, 29, 50–53, 53 a, 54–57, 57 a, 58 och 59 §.

— —

———

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 §.

_____

Denna lag träder i kraft den 20 .

_____

12.

Lag

om ändring av 1 § i lagen om Energimyndigheten

I enlighet med riksdagens beslut

fogas till 1 § 2 mom. i lagen om Energimyndigheten (870/2013), sådant det lyder delvis ändrat i lagarna 634/2020, 804/2020, 606/2021 och 500/2023, en ny 21 punkt som följer:

1 §

Uppgifter

— —

Energimyndigheten sköter de uppgifter som myndigheten har enligt

— —

21) lagen om hantering av cybersäkerhetsrisker (/),

— —

_____

Denna lag träder i kraft den 20 .

_____

13.

Lag

om ändring av 28 § i lagen om tillsyn över el- och naturgasmarknaden

I enlighet med riksdagens beslut
ändras i lagen om tillsyn över el- och naturgasmarknaden (590/2013) 28 § 1 mom. 1 punkten, sådan den lyder i lag 1002/2018, som följer:

28 §

Energimyndighetens rätt att lämna ut uppgifter till andra myndigheter

— —
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 föreskrivs:

1 §

Genom denna lag upphävs i lagen om vattentjänster (119/2001) 35 § 2 mom. 3 punkten.

_____

Denna lag träder i kraft den 20 . _____

Helsingfors den 20 .

Statsminister

Förnamn Efternamn

...minister Förnamn Efternamn

Välj mål.
Välj mål.