U 9/2021 rd

Statsrådets skrivelse till riksdagen om kommissionens förslag till Europaparlamentets och rådets direktiv (COM(2020) 823 final) om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och, om upphävande av direktiv 2016/1148 (direktivet om säkerhet i nätverks- och informationssystem)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska kommissionens förslag av den 16 december 2020 till Europaparlamentets och rådets direktiv (COM(2020) 823 final) om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och, om upphävande av direktiv 2016/1148 (direktivet om säkerhet i nätverks- och informationssystem) samt en promemoria om förslaget.

Helsingfors den 11 februari 2021

Kommunikationsminister Timo Harakka

Specialsakkunnig Marième Korhonen

KOMMUNIKATIONSMINISTERIET | PROMEMORIA | EU/2020/0359

11.2.2021

KOMMISSIONENS FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV OM ÅTGÄRDER FÖR EN HÖG GEMENSAM CYBERSÄKERHETSNIVÅ I HELA UNIONEN OCH, OM UPPHÄVANDE AV DIREKTIV 2016/1148 (DIREKTIVET OM SÄKERHET I NÄTVERKS- OCH INFORMATIONSSYSTEM)

1 Bakgrund

Den 16 december 2020 lade kommissionen fram ett förslag till Europaparlamentets och rådets direktiv (COM(2020) 823 final) om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148.

Förslaget bygger på det första EU-omfattande rättsinstrumentet, direktivet om säkerhet i nätverks- och informationssystem (EU) 2016/1148 (nedan benämnt *NIS-direktivet*), som syftade till att höja den gemensamma cybersäkerhetsnivån i EU. I Finland införlivades NIS-direktivet i den sektorspecifika lagstiftningen genom att bestämmelser om skyldigheten för viktiga tillhandahållare av tjänster att hantera riskerna i fråga om kommunikationsnät och informationssystem infördes i informationssamhällsbalken (i dag: lagen om tjänster inom elektronisk kommunikation), luftfartslagen, järnvägslagen, lagen om fartygstrafikservice, lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, lagen om transportservice, elmarknadslagen, naturgasmarknadslagen och lagen om vattentjänster. I de nationella lagar som gäller för viktiga tillhandahållare av tjänster inom de övriga kritiska sektorer som avses i NIS-direktivet låg dataskyddsbestämmelserna på samma nivå som i det första NIS-direktivet eller så var de mer noggrannare och behövde inte ändras.

År 2020 såg kommissionen över NIS-direktivet och analyserade medlemsstaternas erfarenheter av tillämpningen av direktivet. Dessutom ordnade kommissionen ett offentligt samråd om direktivet under 2020. Finland svarade för sin del på det offentliga samrådet utifrån riktlinjerna för föregripande inflytande (E 107/2020 rd).

2 Förslagets syfte

I förslaget av den 16 december 2020 konstaterar kommissionen att den digitala utvecklingen, som har påskyndats av covid-19-pandemin, i samhällen har förändrat den nuvarande miljön väsentligt och medfört nya utmaningar som kräver innovativa lösningar. Antalet cyberattacker har ökat och attackerna har varit allt mer avancerade. Cybersäkerhetsincidenter gör det svårare för den inre marknaden att fungera, orsakar ekonomiska förluster och undergräver användarnas förtroende för unionens ekonomiska och sociala sektorer. Enligt kommissionen ska förslaget till ett nytt direktiv reformera det befintliga regelverket genom att ta hänsyn till förändringarna på den inre marknaden. Förslaget är en del av kommissionens prioriteringar att främja ett Europa rustat för den digitala tidsåldern.

Syftet med förslaget är att genom att fastställa riskhanteringsåtgärder i händelse av cybersäkerhetsincidenter höja både EU:s gemensamma cybersäkerhetsnivå och medlemsstaternas nationella cybersäkerhetsnivå för de sektorer och entiteter som anses vara kritiska. Förslaget ska harmonisera identifieringen av entiteter på EU-nivå och därmed minska medlemsstaternas admi-

nistrativa börda. Dessutom ska förslaget harmonisera cybersäkerhets- och rapporteringsskyldigheterna och utvidga tillämpningsområdet till att omfatta nya sektorer och entiteter. Tillsynsmyndigheterna ska fortfarande ha sina befintliga uppgifter, men också tilldelas nya tillsynsuppgifter, bland annat tillsyn över de entiteter som har lagts till i tillämpningsområdet.

3 Förslagets huvudsakliga innehåll

3.1 Identifiering av väsentliga entiteter

Enligt det första NIS-direktivet var medlemsstaterna ansvariga för att identifiera väsentliga tjänsteleverantörer. Enligt kommissionen ledde den tidigare metoden till mycket varierande tillvägagångssätt vid identifieringen av väsentliga tjänsteleverantörer i medlemsstaterna. Därför ska det nya förslaget syfta till att genom att avskaffa den separata identifieringsprocessen lösa detta problem som kommissionen har identifierat.

Enligt det nya förslaget till direktiv ska medlemsstaterna inte längre behöva identifiera väsentliga entiteter på nationell nivå, eftersom kriterierna ska harmoniseras i hela EU så att alla stora och medelstora entiteter inom de kritiska sektorerna i alla medlemsstater ska omfattas av regleringen. Medlemsstaterna behöver inte skicka förteckningar över sådana entiteter till kommissionen, utan Enisa ska framöver föra ett EU-omfattande register över väsentliga tjänsteleverantörer och tillsynsmyndigheter i medlemsstaterna.

Små företag och mikroföretag ska i princip undantas från den föreslagna regleringen. I vissa situationer ska medlemsstaterna dock även kunna identifiera väsentliga små entiteter och mikroentiteter, om de tjänster som dessa tillhandahåller kan anses vara viktiga för kontinuiteten i samhällets funktioner. I samarbete med den samarbetsgrupp som inrättats genom NIS-direktivet (nedan benämnd *NIS-samarbetsgruppen*) ska kommissionen offentliggöra riktlinjer för tillämpningen av kriterierna för identifiering av sådana entiteter. Medlemsstaterna bör förse kommissionen med förteckningar över identifierade små entiteter och mikroentiteter.

3.2 Kategorisering av entiteter

Enligt förslaget ska entiteter kategoriseras som väsentliga (*essential*) och viktiga (*important*) beroende på hur kritisk en entitet är och hur beroende entiteten är av andra sektorer och entiteter och tvärtom. Samma riskhanterings- och rapporteringsskyldigheter ska gälla för entiteter i både kategorierna. Tillsyns- och sanktionssystemen ska dock vara strängare för väsentliga entiteter än för viktiga entiteter. I det tidigare direktivet fanns det inga skillnader mellan kritiska entiteter.

3.3 Utvidgning av tillämpningsområdet

Enligt förslaget ska tillämpningsområdet för direktivet utvidgas till att bland de väsentliga sektorerna även inom energisektorn omfatta producenter av väte respektive fjärrvärme och fjärrkyla. När det gäller hälso- och sjukvården ska tillämpningsområdet utvidgas till att omfatta EU-referenslaboratorier, forsknings- och utvecklingsentiteter inom läkemedelsbranschen och tillverkare av läkemedel och medicintekniska produkter. Dessutom ska tillämpningsområdet gälla för avloppsrening och entiteter inom rymdsektorn som nya tillägg. En ny sektor bland de väsentliga sektorerna är även den offentliga förvaltningen, såsom entiteter inom centralförvaltningen och regionala förvaltningsorgan definierade på NUTS 1- och NUTS 2-nomenklaturnivåerna i bilaga I till förordning (EU) nr 1059/2003. Enligt bilagorna II och III till förordning (EU) 1059/2003 ska nomenklaturnivåerna i Finland beröra statsförvaltningen och de riksomfattande ämbetsverk och inrättningar som lyder under statsförvaltningen samt landskap och kommuner.

Enligt artikel 4.23 i förslaget ska offentliga förvaltningsentiteter som bedriver verksamhet på områdena allmän säkerhet, brottsbekämpning, försvar eller nationell säkerhet undantas från tillämpningsområdet. Enligt artikel 2.3 i förslaget till direktiv påverkar dessutom direktivet inte medlemsstaternas befogenheter när det gäller att upprätthålla allmän säkerhet, försvar och nationell säkerhet.

Entiteter som erbjuder digitala infrastrukturtjänster ska höra till väsentliga entiteter. Till dessa ska det som nya entiteter läggas till leverantörer av datacentraltjänster, leverantörer av nätverk för innehållsleverans, tillhandahållare av betrodda tjänster, tillhandahållare av allmänna elektroniska kommunikationsnät och kommunikationstjänster samt leverantörer av molntjänster.

I kategorin *viktiga entiteter* ska tillämpningsområdet utvidgas till att omfatta entiteter i följande sektorer: post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier samt produktion och distribution av livsmedel. Ett mer omfattande sektorstillägg till kategorin *viktiga entiteter* är produktionsprocesser (*manufacturing*) som ska omfatta tillverkning av medicintekniska produkter, tillverkning av datorer, elektronik och optik, tillverkning av elektriska anordningar, tillverkning av andra maskiner och produkter samt tillverkning av fordon, egentliga släpvagnar och påhängsvagnar. Dessutom ska leverantörer av sociala nätverkstjänster, e-marknadsplatser och sökmotorer online läggas till som viktiga entiteter bland digitala tjänsteleverantörer.

3.4 Utveckling av cybersäkerhetskapaciteten i EU och på nationell nivå i medlemsstaterna

På EU-nivå innefattar förslaget åtgärder för att förbättra den gemensamma lägesbilden, det nära samarbetet och informationsutbytet för att utveckla EU:s resiliens i fråga om cybersäkerhet. På medlemsstatsnivå innefattar förslaget åtgärder för att höja kapaciteten i syfte att säkerställa en hög cybersäkerhetsnivå.

Det första NIS-direktivet utgjorde ett underlag för utveckling av cybersäkerhetskapaciteten genom att kräva att medlemsstaterna skulle utarbeta nationella informationssäkerhetsstrategier och att leverantörer av samhällsviktiga tjänster skulle uppfylla sina förpliktelser som gäller informationssäkerhet. Dessutom tilldelade direktivet tillsynsmyndigheterna nya uppgifter för att utöva tillsyn över viktiga entiteter och stärka samarbetet både på nationell nivå och inom EU. Utifrån direktivet om säkerhet i nätverks- och informationssystem utarbetade Finland en nationell strategi för informationssäkerhet och fastställde nät- och informationssäkerhetsskyldigheter för entiteter som hade identifierats som viktiga.

Enligt kommissionens nya förslag bör medlemsstaterna utarbeta nationella cybersäkerhetsstrategier i enlighet med artikel 5 och stärka tillsynsmyndigheternas tillsynsuppgifter. Dessutom bör entiteterna införa de riskhanteringsåtgärder som föreslås i förslaget.

3.5 Identifiering av sårbarheter

Som ett nytt element fastställer förslaget i enlighet med artikel 6 rutiner för att identifiera sårbarheter. Enligt artikeln ska en CSIRT-enhet (*Computer Security Incident Response Teams*) fungera som samordnare. Enligt förslaget bör entiteternas sårbarheter rapporteras till CSIRT-enheten för att sårbarheterna ska kunna avhjälpas. För att medlemsstaterna ska kunna identifiera sårbarheter bör de granska och fastställa behövliga riktlinjer. Europeiska unionens byrå för nät- och informationssäkerhet (nedan benämnd *Enisa*) bör samla in och föra ett register över upptäckta sårbarheter för att kunna säkerställa transparensen och uppdatera lägesbilden.

3.6 Beredskap för storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser

Enligt artikel 7 i förslaget bör medlemsstaterna ta fram riktlinjer för att hantera storskaliga cybersäkerhetsrisker.

Medlemsstaterna bör fastställa en eller flera tillsynsmyndigheter som ska ansvara för den operativa ledningen vid storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser. Medlemsstaterna bör se till att tillsynsmyndigheterna har tillräckliga resurser för att utföra dessa uppgifter. Varje medlemsstat bör identifiera den kapacitet, de resurser och de processer som kan inledas och införas i sådana situationer som avses i förslaget.

Kommissionen bör informeras om de tillsynsmyndigheter som har utsetts för att utföra de nämnda uppgifterna och om antagandet av riktlinjerna inom tre månader efter att riktlinjerna tagits fram.

3.7 Utveckling av riskhanteringsåtgärder

Enligt artiklarna 17 och 18 i förslaget bör riskhanteringsåtgärderna omfatta åtgärder för att identifiera risker för potentiella störningar, identifiera och hantera potentiella störningar samt minska konsekvenserna av störningarna. Enligt förslaget bör dessa åtgärder omfatta riskanalyser och säkerhetsåtgärder i informationssystem, hantering av störningar (förebyggande, identifiering och hantering av störningar), driftskontinuitet och krishantering, cybersäkerhet i produktionskedjor, cybersäkerhet vid köp av nät- och informationssystem samt utveckling och underhåll av systemen. Dessutom ska riskhanteringsåtgärderna omfatta hantering och identifiering av sårbarheter, riktlinjer och processer, såsom testning och revision, för att bedöma effektiviteten i riskhanteringsåtgärderna avseende cybersäkerhet, samt användning av kryptografi och kryptering.

Enligt förslaget bör särskilt totalsträckskrypteringen utvecklas, utnyttjas och efter behov vara obligatorisk för att främja säkerheten hos leverantörer av kommunikationsnät. Enligt förslaget ska en balanserad lösning hittas mellan de brottsbekämpande myndigheternas uppgifter och en effektiv användning av kryptering.

I förslaget föreslår kommissionen att riskhanteringsskyldigheterna avseende cybersäkerhet ska stå i proportion till de risker som bedöms för varje entitet. När det gäller att skydda nät- och informationssystem bör riskhanteringsåtgärder och rapporteringsskyldigheter införas oberoende av om åtgärderna för att underhålla systemen har lagts ut på entreprenad eller inte. Enligt artikel 17 ska entiteternas ledningsorgan godkänna de riskhanteringsåtgärder som fastställs i artikel 18, övervaka att åtgärderna genomförs och stå till svars om de inte fullgör sina skyldigheter. Förslaget ska utvidga riskhanteringsåtgärderna till att även omfatta entiternas produktionskedjor. I samarbete med relevanta nationella myndigheter, kommissionen och Enisa bör NIS-samarbetsgruppen i enlighet med artikel 19 utvärdera potentiella hot mot och sårbarheter i kritiska IKT-tjänster, IKT-produkter och IKT-system i produktionskedjor.

Enligt artikel 3 i förslaget kan medlemsstaterna, utöver de skyldigheter som anges i förslaget, införa bestämmelser som garanterar en hög nationell cybersäkerhetsnivå.

3.8 Rapporteringsskyldigheter

Enligt artikel 20 fastställer förslaget en tvåstegsrapportering i syfte att säkerställa ett snabbt informationsutbyte och en mer djupgående rapportering. Entiteter bör för första gången rappor-

tera till tillsynsmyndigheten inom 24 timmar efter att entiteten har fått kännedom om en betydande störning eller ett hot om it-incident. Efter detta bör entiteten lämna in en slutrapport till tillsynsmyndigheten inom en månad efter störningen. Dessutom ger artikel 27 i förslaget entiteter som inte omfattas av tillämpningsområdet för förslaget till direktiv möjlighet att rapportera störningar på frivillig basis.

3.9 Tillsynsmyndigheternas uppgifter

Enligt artikel 28 i förslaget ska medlemsstaterna se till att tillsynsmyndigheterna utövar en effektiv tillsyn och vidtar de åtgärder som krävs för att försäkra sig om att entiterna uppfyller de fastställda skyldigheterna. Förslaget föreslår förhands- och efterhandstillsyn över väsentliga entiteter och endast efterhandstillsyn över viktiga entiteter. Tillsynsmyndigheterna ska ha ett nära samarbete med dataskyddsmyndigheterna när de behandlar säkerhetsöverträdelser som berör personuppgifter.

I förslaget föreslås ett stort antal mer specifika uppgifter för tillsynsmyndigheterna. Uppgifterna omfattar kontroller på plats hos entiteter och fjärrövervakning. Dessutom omfattar uppgifterna slumpmässiga granskningar, regelbundna revisioner, riktade säkerhetsrevisioner utgående från riskbedömningar eller riskbaserad information, säkerhetsskanningar, begäran om information för utvärdering av entiteters cybersäkerhetsåtgärder, tillgång till information som behövs för att utföra tillsynsuppgifter och begäran om bevis för att entiteter har genomfört cybersäkerhetsåtgärder.

Medlemsstaterna bör se till att tillsynsmyndigheterna har möjlighet att varna entiteter för överträdelse av de skyldigheter som anges i förslaget till direktiv, att utfärda bestämmelser för att åtgärda brister efter överträdelsen, att utfärda bestämmelser om att entiteter ska ge relevanta organisationer och personer information om eventuella skyddsåtgärder om entiteten utsätts för cybersäkerhetshot, och att påföra eller begära att få påföra administrativa sanktionsavgifter beroende på cybersäkerhetsincident. Om en entitet inte följer tillsynsmyndighetens föreskrifter, har tillsynsmyndigheten möjlighet att på viss tid meddela verksamhetsförbud till entiteten och personer i ledande ställning.

Dessutom föreslår förslaget administrativa sanktionsavgifter för överträdelse av skyldigheter. Nivån på en sådan sanktionsavgift ska bero på entitetens kategori, störningens eller krisens omfattning och den skada som orsakats. Enligt kommissionen kan den högsta sanktionen enligt artikel 31 uppgå till minst 10 000 000 euro eller upp till två procent av entitetens årliga omsättning, beroende på vilken av sanktionerna som är det högsta straffet för entiteten. Enligt artikel 31.6 i förslaget får varje medlemsstat på nationell nivå överväga huruvida sanktionsavgifter påförs offentliga förvaltningsentiteter. Enligt artikel 33.1 ska medlemsstaterna även fastställa regler om sanktioner för överträdelse av bestämmelser i detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas.

3.10 Utveckling av samarbetet och informationsutbyte på nationell nivå och i EU

Enligt artikel 26 i förslaget ska entiteter utbyta information för att stärka samarbetet. Enligt artikel 11 i förslaget ska dessutom samarbete bedrivas mellan en nationell kontaktpunkt, en CSIRT-enhet och tillsynsmyndigheter så att målen för förslaget kan uppnås. Samarbete bör även bedrivas med andra tillsynsmyndigheter som avses i sektorspecifika lagar, särskilt med de tillsynsmyndigheter som avses i förslaget till förordning om digital operativ motståndskraft för finanssektorn och förslaget till direktiv om skydd av fysiska kritiska infrastrukturer.

Förslaget fortsätter även de samarbetsmekanismer som tidigare fastställts utifrån NIS-direktivet, och kommer att precisera samarbetsuppgifterna och målen. Enligt artikel 12 ska NIS-samarbetsgruppen ha till uppgift att kartlägga nationella erfarenheter och lösningar, diskutera erfarenheter av genomförandet och potentiella utmaningar och ta fram rekommendationer för införande av bestämmelserna.

Dessutom fortsätter förslaget de uppgifter som genom NIS-direktivet har tilldelats CSIRT-enheterna och CSIRT-nätverkets verksamhet och samarbete i enlighet med direktivet.

I enlighet med artikel 14 ska förslaget inrätta nätverket CyCLONe (Cyber Crises Liaison Organisation Network), som består av EU:s medlemsstater, i händelse av storskaliga cybersäkerhetskriser. Nätverket ska ha till uppgift att stödja samordnings- och ledningsuppgifter på operativ nivå inför cybersäkerhetsincidenter och cybersäkerhetskriser. Som ett nytt element föreslår kommissionen även att den i enlighet med artikel 16 i samarbete med Enisa ska ordna en sakkunniggranskning inom 18 månader efter att det uppdaterade direktivet har trätt i kraft.

3.11 Certifiering och standardisering

Enligt artikel 21 i förslaget får medlemsstaterna med stöd av artikel 49 i cybersäkerhetsakten (2019/881) kräva att entiteter ska certifiera vissa IKT-produkter, IKT-tjänster och IKT-processer utifrån europeiska ordningar för cybersäkerhetscertifiering. Dessutom kan kommissionen be Enisa utarbeta en alternativ certifieringsordning, om en lämplig certifieringsordning inte finns tillgänglig för detta ändamål.

Såsom i det första NIS-direktivet bör medlemsstaterna också enligt detta förslag uppmuntras att utnyttja de nät- och informationssystemstandarder som antagits av EU och på internationell nivå.

3.12 Delegerade akter och genomförandeakter

Enligt förslaget ska kommissionen ges befogenhet att i enlighet med artikel 36 anta delegerade akter om de riskhanteringsåtgärder som avses i förslaget. Dessutom ska kommissionen ges befogenhet att anta delegerade akter som specificerar vilka väsentliga entiteter certifiering ska avkrävas och vilken ordning för cybersäkerhetscertifiering kravet utgår från. Enligt förslaget kan kommissionen anta genomförandeakter som rör tekniska och metodologiska preciseringar av riskhanteringsåtgärder och, när det gäller rapportering av störningar, formatet och förfarandet för uppgiftsöverföringen. Kommissionen ska biträdas av en sådan kommitté med företrädare för medlemsstaterna som avses i förordning (EU) (182/2011).

4 Förslagets rättsliga grund och förhållande till proportionalitets- och subsidiaritetsprincipen

Förslagets rättsliga grund är artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Artikeln handlar om åtgärder i syfte att upprätta den inre marknaden och säkerställa dess funktion, och målet för artikeln är tillnärmning av medlemsstaternas bestämmelser.

Enligt kommissionens bedömning ska förslaget undanröja hinder och stärka den inre marknadens funktion för sådana väsentliga och viktiga entiteter som avses i förslaget, genom att det harmoniserar gemensamma riskhanteringsskyldigheter och rapporteringsskyldigheter. Det fragmenterade nuläget för den nivå som ansvarar för både lagstiftningen och tillsynen i EU respektive på nationell nivå utgör hinder för den inre marknadens funktion, eftersom entiteterna möter olika, och eventuellt överlappande, krav i de gränsöverskridande verksamheterna.

Kommissionen anser att förslaget är förenligt med subsidiaritetsprincipen. Enligt kommissionen är en EU-omfattande resiliens inom cybersäkerhet inte möjlig, om målet endast ska nås på nationell eller regional nivå. Det första NIS-direktivet tillgodosåg detta behov genom att det tog fram ett gemensamt regelverk för att höja nät- och informationssäkerhetsnivån både i EU och på nationell nivå i medlemsstaterna. I dag är EU:s ekonomi alltmer beroende av nät- och informationssystem. De sektorer och tjänster som omfattas av NIS-direktivet är alltmer sammanlänkade. Enligt kommissionen är målen med förslaget motiverade, eftersom cybersäkerhetsriskerna och cybersäkerhetsincidenterna har gränsöverskridande karaktär. Dessutom anser kommissionen att EU genom gemensamma åtgärder har potential för att stärka effektiva och samordnade nationella åtgärder. Enligt kommissionen har samordnade gemensamma åtgärder också en positiv inverkan på skyddet av de grundläggande rättigheterna och särskilt skyddet för personuppgifter och integritetsskyddet.

Kommissionen anser att förslaget är förenligt med proportionalitetsprincipen. I förslaget anser kommissionen att de bestämmelser som föreslås står i rätt proportion till målen. De föreslagna cybersäkerhets- och rapporteringsskyldigheterna har beaktat medlemsstaternas önskemål och behov av att förbättra det befintliga regelverket. Förslaget tar hänsyn till de befintliga åtgärderna och riktlinjerna i medlemsstaterna. En högre cybersäkerhetsnivå som ska uppnås genom bestämmelserna i förslaget står i rätt proportion till de ökade riskerna, inklusive risker som har gränsöverskridande karaktär. De föreslagna åtgärderna tillgodoser entiteternas intressen på allmän nivå genom att de säkerställer driftskontinuiteten och kvaliteten på de tjänster som tillhandahålls av entiteterna. Kommissionen anser att de kostnader som uppstår på grund av förslaget är lägre än de kostnader som uppstår vid störningar som orsakar betydande samhälleliga och ekonomiska förluster. Dessutom stödde resultaten av det offentliga samrådet om NIS-direktivet en översyn av direktivet.

4.1 Val av rättsligt instrument

Enligt kommissionen kommer förslaget att harmonisera skyldigheter och regler mellan medlemsstaterna. Samtidigt skapar förslaget flexibilitet för medlemsstaterna att ta hänsyn till nationella skillnader. I enlighet med nationell lagstiftning kan medlemsstaterna utöver de entiteter som anges i direktivet identifiera väsentliga respektive viktiga entiteter som överskrider utgångsnivån i förslaget. Därför valde kommissionen som rättsligt instrument ett direktiv som enligt kommissionen å ena sidan möjliggör riktade förbättringar av harmoniseringen av cybersäkerhetsskyldigheterna och å andra sidan skapar nationell flexibilitet.

Statsrådet anser att förslagens rättsliga grunder är sakenliga. Statsrådet anser att förslagen ligger i linje med subsidiaritets- och proportionalitetsprinciperna. Medan behandlingen framskrider är det viktigt att kontrollera att de bestämmelser som presenteras i förslaget är förenliga med den föreslagna rättsliga grunden.

5 Förslagets konsekvenser

5.1 Kommissionens konsekvensbedömning

I konsekvensbedömningen identifierade kommissionen att företagens nuvarande cyberresiliens är för låg. Tjänsteleverantörerna har inte vidtagit tillräckliga åtgärder för att förbättra informationssäkerheten. När det gäller cybersäkerhet finns det dessutom brister i hanteringen av den gemensamma lägesbilden och cybersäkerhetskriserna. Kommissionen anser att till exempel en del stora sjukhus i medlemsstaterna kan ha utelämnats från tillämpningsområdet för NIS-direktivet. Enligt kommissionen har specificeringen av tillämpningsområdet och identifieringen av

väsentliga tjänsteleverantörer i det tidigare regelverket inte lyckats. De regler som föreslås i förslaget ska ses över 54 månader efter att direktivet har trätt i kraft.

Förslaget minskar fragmenteringen av den inre marknaden och jämnar ut entiteternas verksamhetsförutsättningar. Enligt kommissionen gör den föreslagna regleringen cybersäkerhetsresiliensen i EU mer enhetlig, vilket till sist leder till ekonomiska besparingar för både företag och samhälle. Kommissionen anger att det uppdaterade regelverket kan göra det möjligt att uppnå kostnadsbesparingar på hela 11,3 miljarder euro, dvs. ett belopp som kan orsakas av eventuella cybersäkerhetsincidenter och cybersäkerhetsattacker. Enskilda störningr och avvärjningsåtgärder kan medföra extra kostnader, till exempel i en situation där verksamheten måste avbrytas.

Till följd av den föreslagna regleringen kommer medelstora företags kostnader att öka under de första åren då regelverket införs. Samtidigt bidrar en utökning av säkerhetsskyldigheterna för dessa entiteter till deras cybersäkerhetskapacitet och till att förbättra hanteringen av IKT-risker.

Enligt kommissionen kan cybersäkerhetsincidenter och cybersäkerhetsattacker även medföra kostnader för medlemsstater i form av budgetutgifter och för medborgare i form av inkomstbortfall till följd av störningar i ekonomin. Kommissionens konsekvensbedömning innehåller inga bedömningar av konsekvenserna för myndigheterna.

Enligt kommissionen tilldelar förslaget Enisa ytterligare uppgifter utöver de befintliga uppgifterna. Dessa uppgifter ska omfatta följande: inrätta och föra ett sårbarhetsregister, vara sekretariat för CyCLONe-nätverket, offentliggöra en årlig rapport om cybersäkerhetsläget i EU, stödja i sakkunniggranskningen, samla in uppgifter om cybersäkerhetsincidenter från alla medlemsstater och tillhandahålla tekniskt stöd samt inrätta och föra ett register över entiteter som tillhandahåller gränsöverskridande tjänster. För att dessa uppgifter ska kunna utföras behövs mer personalresurser.

5.2 Konsekvenser för EU:s budget

Enligt kommissionen är förslaget förenligt med den nuvarande fleråriga budgetramen (2021–2027). Kommissionen har för avsikt att ur programmet för ett digitalt Europa täcka de ytterligare personalkostnader som uppstår för Enisa till följd av det ökade antalet uppgifter som föreslås i förslaget.

5.3 Nationell konsekvensbedömning

5.3.1 Konsekvenser för den nationella lagstiftningen

Rättsaktstypen av förslaget är ett direktiv som bör införlivas i den nationella lagstiftningen.

I Finland införlivades det första NIS-direktivet i den sektorspecifika lagstiftningen genom att bestämmelser om skyldigheten för viktiga tillhandahållare av tjänster att hantera riskerna i fråga om kommunikationsnät och informationssystem infördes i informationssamhällsbalken (i dag: lagen om tjänster inom elektronisk kommunikation), luftfartslagen, järnvägslagen, lagen om fartygstrafikservice, lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, lagen om transportservice, elmarknadslagen, naturgasmarknadslagen och lagen om vattentjänster. De nationella lagarna för finanssektorn och hälso- och sjukvården ändrades inte eftersom de redan ansågs uppfylla kraven i det första NIS-direktivet.

De regler som föreslås i förslaget kräver åtminstone en översyn av ovannämnda sektorsspecifika lagar och införande av de bestämmelser som föreslås i förslaget. Dessutom krävs en översyn av

annan relevant sektorspecifik lagstiftning samt införande av de föreslagna bestämmelserna, särskilt på grund av utvidgningen av tillämpningsområdet. Lagstiftningen om offentlig förvaltning bör också granskas. I anslutning till införandet av direktivet bör man, för att kunna säkerställa en enhetlig reglering, även göra en granskning av de cybersäkerhetsskyldigheter som redan i övrigt har fastställts eller ska fastställas. Den allmänna lagstiftningen om behandling av personuppgifter innehåller även informationssäkerhetskrav som ska tillämpas i alla informationssystem där personuppgifter behandlas.

Förslaget kommer att påverka bestämmelserna om sanktioner. Det behövs dock ännu en närmare granskning av förhållandet mellan artiklarna 31–33 i förslaget till direktiv. Det verkar som om särskilt tillämpningsområdet för den föreslagna artikeln 33 delvis är överlappande med bestämmelserna om administrativa sanktionsavgifter, men att det i större utsträckning omfattar skyldigheter som bygger på direktivet. Nya lagstadgade skyldigheter kommer att följa av bestämmelserna om administrativa sanktionsavgifter. Deras konsekvenser bör utvärderas noggrant under förhandlingarna. Trots att förslaget till direktiv innefattar ett visst nationellt handlingsutrymme, finns det skäl att i fråga om administrativa sanktionsavgifter kontrollera att de är förenliga med bestämmelserna om andra sanktioner.

5.3.2 Konsekvenser för myndigheternas verksamhet

Till följd av införandet av det första NIS-direktivet i Finland har de sektorspecifika tillsynsmyndigheterna ansvarat för tillsynen över de skyldigheter som fastställs i direktivet. I Finland är dessa tillsynsmyndigheter Transport- och kommunikationsverket, Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) och närings-, trafik- och miljöcentralerna. Redan före NIS-direktivet hade Transport- och kommunikationsverket omfattande lagstadgade uppgifter för att reagera på säkerhetsöverträdelser och utreda överträdelser. Därför ansågs Transport- och kommunikationsverket vara en lämplig nationell kontaktpunkt och CSIRT-enhet.

I det föreliggande förslaget föreslås precisering och utökning av de nationella tillsynsmyndigheternas uppgifter. En utvidgning av tillämpningsområdet utökar tillsynsmyndigheternas uppgifter och sannolikt antalet tillsynsmyndigheter. Artikel 11 i förslaget till direktiv innefattar skyldigheter för myndigheterna att samarbeta. Dessa skyldigheter kommer att påverka verksamheten för alla myndigheter som avses i artikeln. Artikel 28 i förslaget innefattar även en uttrycklig skyldighet för myndigheterna att ha samarbete med dataskyddsmyndigheter när de behandlar incidenter som medför personuppgiftsincidenter. Detta kommer att påverka dataombudsmannens verksamhet. Resurskonsekvenserna och eventuella andra konsekvenser av förslaget till direktiv bör utvärderas närmare när förslaget behandlas.

Under den fortsatta behandlingen av förslaget till direktiv är det bra att närmare utvärdera vilka myndigheter som ska kunna omfattas av nya krav till följd av direktivet och till vilka delar. Enligt förslaget till direktiv ges medlemsstaterna utrymme för skönsmässig bedömning av huruvida administrativa sanktionsavgifter ska påföras offentliga förvaltningsentiteter.

Enligt förslaget till direktiv ska myndigheterna, i stället för den nuvarande efterhandstillsynen, i förväg på eget initiativ övervaka att entiteterna uppfyller sina informationssäkerhetsförpliktelser. En effektiv övervakning av regleringen kräver en betydande ökning av resurserna för sektorsspecifika tillsynsmyndigheter och en ökning av informationssäkerhetskompetensen. Förslaget till direktiv innehåller också bestämmelser om administrativa sanktionsavgifter och utnyttjande av befogenheter att påföra administrativa sanktionsavgifter. Samarbete som har samband med det ovannämnda kan medföra åtminstone administrativa bördor för den behöriga tillsyns-

myndigheten och dataskyddsmyndigheten. Dessutom kan de föreslagna bestämmelserna om administrativa sanktionsavgifter innebära en ny ärendegrupp för förvaltningsdomstolar. Enligt en preliminär bedömning kommer dock en eventuell ökning i arbetsmängden att vara den mest betydande konsekvensen för förvaltningsdomstolarna. Dessutom kan Rättsregistercentralen i viss mån få konsekvenser, eftersom centralen i egenskap av personuppgiftsansvarig ansvarar för justitieförvaltningens riksomfattande informationssystem och verkställandet av administrativa påföljdsavgifter. Konsekvenserna av bestämmelserna om administrativa sanktionsavgifter bör utvärderas närmare när förslaget till direktiv behandlas.

5.3.3 Ekonomiska konsekvenser

Enligt kommissionen kommer den föreslagna regleringen att medföra ekonomiska kostnader för de entiteter som omfattas av tillämpningsområdet. Enligt kommissionens beräkning ökar entiteternas IKT-kostnader med 22 procent under de första åren då regelverket införs. Kostnaderna har dock beräknats öka med tolv procent för de entiteter som redan omfattas av det första NIS-direktivet. Enligt kommissionen leder dock de beräknade extra kostnaderna till ett proportionellt kostnads-nyttoförhållande, eftersom antalet cybersäkerhetsincidenter samtidigt minskar. Enligt kommissionens beräkning uppgår kostnaderna för störningarna till totalt 118 miljarder euro under en period på tio år. Dessutom anser kommissionen att förslaget bidrar till att minska de ökade kostnaderna för hantering av enskilda cybersäkerhetsincidenter och cybersäkerhetskriser på medlemsstatsnivå.

Bedömningen av de ekonomiska konsekvenserna påverkas bland annat av entiteternas allmänna mognadsnivå inom cybersäkerhet och kapacitet, som i nuläget varierar mellan sektorer och entiteter. Dessutom kan ekonomiska konsekvenser föranledas av behovet av att samtidigt beakta skyddet av personuppgifter, inbegripet dataskyddskompetensen. Kraven i EU:s dataskyddsförordning blir tillämpliga till den del personuppgifter behandlas i system som omfattas av tillämpningsområdet för direktivet och personuppgifter utbyts utifrån den implementerande lagstiftningen gällande direktivet.

I början kommer en utvidgning av tillämpningsområdet att medföra extra kostnader för de sektorer och entiteter som har lagts till i tillämpningsområdet, såsom offentliga förvaltningsentiteter inom statsförvaltningen, landskapen och kommunerna. De extra kostnaderna kan till exempel beaktas i kundavgifter.

De närmare konsekvenserna för myndigheternas ekonomiska behov och behov av personalresurser kan inte bedömas förrän i anslutning till genomförandet av de föreslagna bestämmelserna, men de verkar ändå öka väsentligt. Utöver ovannämnda konsekvenser för myndigheterna kan förslaget till direktiv medföra andra kostnadseffekter på tillsynsmyndigheten och andra myndigheter.

5.3.4 Konsekvenser för informationssamhället

På samma sätt som det första NIS-direktivet ska den föreslagna regleringen öka transparensen när det är fråga om cybersäkerhetsincidenter, risker för cybersäkerhetsincidenter, beredskap för risker och inverkan av riskerna på olika entiteter i samhället. Den föreslagna regleringen kommer att stärka samarbetet mellan olika myndigheter och informationsutbytet både på nationell nivå och mellan medlemsstaterna. Genomförandet av reglerna främjar förtroendet för de entiteter som är väsentliga för kontinuiteten i samhällets funktioner. Den föreslagna regleringen kommer att förbättra samhällets kapacitet att bereda sig och hantera cybersäkerhetshot hos de entiteter som är relevanta och kritiska för samhället.

5.3.5 Miljökonsekvenser

Enligt kommissionens bedömning kommer en höjning av cybersäkerhetsnivån att bidra till att förebygga miljörisker och miljöskador inför cyberincidenter eller cyberkriser. Detta är särskilt viktigt för energisektorn, vattenförsörjningen och transportsektorn. Genom att stärka cybersäkerhetskapaciteten bidrar förslaget till ett bättre utnyttjande av den senaste generationens IKT-infrastrukturer och IKT-tjänster, som med tanke på miljön är mer hållbara. Detta leder i sin tur till ett minskat antal cybersäkerhetsincidenter, och de resurser som frigörs från incidenthanteringen kan riktas till hållbara investeringar.

6 Förslagets förhållande till grundlagen och till de grundläggande fri- och rättigheterna och de mänskliga rättigheterna

Enligt förslaget har EU åtagit sig att garantera en hög nivå på skyddet av de grundläggande fri- och rättigheterna. Alla frivilliga arrangemang för informationsutbyte mellan entiteter som stöds av detta förslag bör ske konfidentiellt och i enlighet med EU:s gemensamma bestämmelser om behandling av uppgifter, särskilt den allmänna dataskyddsförordningen (EU) 2016/679. Av dataskyddsförordningen följer även direkt tillämpliga skyldigheter för de näringsidkare och myndigheter som avses i förslaget till direktiv, nämligen skyldigheter som gäller informationssäkerhet i behandling av personuppgifter. Vissa krav som ingår i förslaget till direktiv kan samtidigt förbättra det skydd av personuppgifter som avses i dataskyddsförordningen.

Skyddet för privatlivet och skyddet för förtrolig kommunikation garanteras i 10 § i Finlands grundlag. Denna grundläggande rättighet förutsätter att staten avstår från att kränka privatlivets helgd, men å andra sidan ska den vidta aktiva åtgärder för att skydda privatlivet mot kränkningar av andra individer. Personuppgifter är en väsentlig del av skyddet för privatlivet. Den föreslagna regleringen är relevant för att skydda privatlivet och kommunikationen.

Dessutom är den föreslagna regleringen relevant för den näringsfrihet som tryggas genom 18 § i grundlagen, eftersom det föreliggande förslaget ålägger näringsidkare olika skyldigheter som stärker cybersäkerheten som en del av bedrivandet av näringsverksamhet. Förslaget ger myndigheten behörighet att avbryta en näringsidkares verksamhet, om olika cybersäkerhetsförpliktelser inte har fullgjorts. Begränsning av näringsfriheten bör vara proportionell i förhållande till målet.

Bestämmelserna i artikel 18 i förslaget till direktiv ålägger näringsidkare skyldighet att vid behov investera i en sådan teknik som gör att de cybersäkerhetskrav som ställs i direktivet uppfylls. Bestämmelserna är å sin sida relevanta för det egendomsskydd som fastställs i 15 § i grundlagen. Artikel 29 i förslaget till direktiv innehåller bestämmelser om myndigheternas inspektionsbefogenheter. Under behandlingen ska uppmärksamhet ägnas åt potentiella konsekvenser av artikel 29 för hemfriden, som skyddas genom 10 § i grundlagen. Dessutom är det viktigt att bedöma hur de administrativa sanktionsavgifter och andra sanktioner som föreslås i artiklarna 31–33 eventuellt påverkar det rättsskydd som fastställs i 21 § i grundlagen.

7 Direktivförslagets förhållande till annan lagstiftning och initiativ

7.1 Sektorspecifik lagstiftning och säkerställande av enhetlighet

Enligt förslaget bidrar den sektorsspecifika lagstiftningen till att säkerställa en hög cybersäkerhetsnivå med beaktande av särdragen hos varje sektor. Om EU:s sektorspecifika regelverk kräver att en väsentlig eller viktig entitet ska införa riskhanteringsåtgärder avseende cybersäkerhet eller rapportera om störningar eller betydande cybersäkerhetshot och om dessa villkor har

samma verkan som de skyldigheter som fastställs i detta förslag, ska sektorspecifika bestämmelser (*lex specialis*) bli tillämpliga. Enligt förslaget kan kommissionen ge vägledning i införande av särskilda regler.

Enligt kommissionen ska förslaget inte begränsa införandet av ytterligare regler per sektor. Genom ytterligare regler är det möjligt att utveckla riskhanteringsåtgärderna och störningsanmälningarna i fråga om cybersäkerhet.

Kommissionen anser att den föreslagna regleringen är förenlig med andra antagna utkast till akt, såsom förslaget till förordning om digital operativ motståndskraft för finanssektorn och förslaget till direktiv om skydd av fysiska kritiska infrastrukturer. Dessutom anser kommissionen att förslaget är förenligt med den allmänna dataskyddsförordningen, den europeiska kodexen för elektronisk kommunikation och förordningen om elektronisk identifiering och betrodda tjänster.

Förslaget är också en viktig del av EU:s nya strategi för cybersäkerhet och dess mål.

8 Ålands behörighet

Enligt 18 § självstyrelselagen för Åland (1144/1991) har landskapet lagstiftningsbehörighet i fråga om landskapsregeringen och under denna lydande myndigheter och inrättningar samt, med vissa begränsningar, näringsverksamhet. Enligt 27 § har riket i sin tur lagstiftningsbehörighet i fråga om handelssjöfart, luftfart, standardisering, statsmyndigheternas organisation och verksamhet samt televerksamhet.

9 Behandling av förslaget i Europeiska unionens institutioner och de övriga medlemsstaternas ståndpunkter

För behandlingen av förslaget ansvarar rådets övergripande arbetsgrupp för cyberfrågor. Förslaget behandlas för första gången i arbetsgruppen den 12 januari 2021. Före detta behandlades förslaget som en del av behandlingen av cyberstrategin den 17 december 2020. Dessutom kommer förslaget på grund av den horisontella karaktären sannolikt också att behandlas i andra relevanta arbetsgrupper.

De övriga medlemsstaternas ståndpunkter är ännu inte kända.

10 Nationell behandling av förslaget

Statsrådets skrivelse har beretts vid kommunikationsministeriet.

Kommissionens förslag behandlades på ett möte för EU-sektionen Kommunikation (EU 19) den 12 januari 2021.

Förslaget och utkastet till skrivelse om förslaget behandlades i ett skriftligt förfarande inom sektionerna Kommunikation (EU 19), Transport (EU 22), Rättsliga och inrikes frågor (EU 7), Konkurrenskraft (EU 8), Finansiella tjänster och kapitalrörelser (EU 10), Energi och Euratom (EU 21), Hälsa (EU 33) och Jordbruk och livsmedel (EU 18) mellan den 15 och den 21 januari 2021 och inom sektionen Miljö (EU 23) mellan den 20 och den 22 januari 2021.

Förslaget behandlades i EU-ministerutskottet den 5 februari 2021

11 Statsrådets ståndpunkt

Statsrådet stöder målet för kommissionens förslag om att bättre svara mot den förändrade cybermiljön och vidareutveckla EU:s gemensamma cybersäkerhetsnivå. Enligt statsrådet är det viktigt med förslagets positiva konsekvenser som höjer cybersäkerhets- och dataskyddsnivån.

Det är viktigt att EU har ett tydligt regelverk för cybersäkerhet, eftersom många störningar och deras konsekvenser kan skrida över medlemsstaternas gränser. Därför är det naturligt att cybersäkerhetskraven för väsentliga och viktiga entiteter i samhället bygger på ett gemensamt regleringsinstrument. Statsrådet anser att regelverket om cybersäkerhet bör vara förenligt med annan sektorspecifik respektive relevant lagstiftning.

Enligt statsrådet är det särskilt viktigt att de nya skyldigheter och krav som hänför sig till nät- och informationssäkerhet ska vara proportionella och riskbaserade i förhållande till storleken och verksamheten för sådana entiteter som omfattas av tillämpningsområdet, med beaktande av särdragen i de olika sektorerna.

En kategorisering av entiteter kan stödjas, om den gör det möjligt att ställa effektiva och proportionerliga krav på sådana entiteter som omfattas av tillämpningsområdet för direktivet. Genom kategorisering bör en orimligt stor administrativ börda, särskilt för små entiteter och mikroentiteter, undvikas.

Statsrådet välkomnar i princip en utvidgning av tillämpningsområdet och registret över entitetstyper eftersom de berörda entiteterna, såsom kommunerna inom den offentliga sektorn, är kritiska med tanke på kontinuiteten i samhällets funktioner. Enligt statsrådet är det bra att direktivet inte påverkar medlemsstaternas befogenheter när det gäller att upprätthålla allmän säkerhet, försvar och nationell säkerhet. Dessutom anser statsrådet att det är bra att offentliga förvaltningsentiteter som bedriver verksamhet på områdena allmän säkerhet, brottsbekämpning, försvar eller nationell säkerhet, enligt förslaget, undantas från tillämpningsområdet.

Enligt statsrådet är det bra att kommissionen i förslaget identifierar vikten av nationella cybersäkerhetsstrategier. Statsrådet välkomnar utarbetandet av strategier för att identifiera sårbarheter och bereda sig på storskaliga cybersäkerhetsincidenter. Statsrådet anser att det är bra att ställa upp säkerhetsskyldigheter som en del av riskhanteringsåtgärderna i enlighet med vad som föreslås i förslaget. Dessutom stöder statsrådet en effektivisering av rapporteringen genom de rapporteringsskyldigheter som föreslås. Statsrådet stöder att kommissionen i förslaget till direktiv även behandlar betydelsen och säkerheten i produktionskedjor.

Statsrådet anser att de preciserade uppgifter som föreslagits för tillsynsmyndigheterna och utökningen av uppgifterna i princip är motiverade. Under förhandlingarna är det bra att granska huruvida uppgifterna är förenliga med kraven i grundlagen. Riktlinjer för nationell resursfördelning kommer som normalt att införas genom förfaranden för budgeten och planen för de offentliga finanserna.

Statsrådet stöder att medlemsstaterna även i framtiden samarbetar intensivt och utbyter information om cybersäkerheten. Det är bra att även framöver intensifiera samarbetet på nationell nivå, både på frivillig basis och genom de skyldigheter som föreslås i förslaget. Statsrådet stöder särskilt ett mer effektivt informationsutbyte på frivillig basis. Enligt statsrådet är det motiverat att direktivet föreslår en möjlighet för brottsbekämpande myndigheter att få information om cybersäkerhetsincidenter som har koppling till brottslig verksamhet.

Enligt statsrådet är det viktigt att medlemsstaterna trots förslaget fortfarande har ett tillräckligt nationellt handlingsutrymme så att de också kan införa sådana nationella åtgärder som säker-

ställer en hög cybersäkerhetsnivå. När det gäller myndigheternas befogenheter och bestämmelserna om sanktioner ska det i beredningen siktas på en lösning där hela sanktionssystemet är välfungerande, sådant att det kan samordnas och beaktar det nationella handlingsutrymmet överlag.

Statsrådet anser också att de befogenheter som delegeras till kommissionen bör vara avgränsade, proportionella, ändamålsenliga och välmotiverade.

Statsrådet anser att förslaget till direktiv i huvudsak motsvarar slutsatserna i interimsrapporten från arbetsgruppen för att förbättra det nationella föregripande påverkansarbetet samt informationssäkerheten och dataskyddet.