U 20/2023 rd

Statsrådets skrivelse till riksdagen om kommissionens förslag till Europaparlamentets och rådets förordningar (cybersolidaritetsakten och ändring av cybersäkerhetsakten)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska kommissionens förslag av den 18 april 2023 till Europaparlamentets och rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och till Europaparlamentets och rådets förordning om ändring av förordning (EU) 2019/881 vad gäller hanterade säkerhetstjänster samt en promemoria om förslaget.

Helsingfors den 6 juli 2023

Kommunikationsminister Lulu Ranne

Specialsakkunning Emma Hokkanen

KOMMUNIKATIONSMINISTERIET | PROMEMORIA | EU/688/2023

6.7.2023

KOMMISSIONENS FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNINGAR (CYBERSOLIDARITETSAKTEN OCH ÄNDRING AV CYBERSÄKERHETSAKTEN)

1 Bakgrund

Den 18 april 2023 lade Europeiska kommissionen fram ett förslag (COM(2023) 209 final) till Europaparlamentets och rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter (cybersolidaritetsakt). Förutom ny lagstiftning föreslås det också ändringar i förordning (EU) 2021/694 (programmet för ett digitalt Europa). Bakgrunden till förslaget är utvecklingen inom cybersäkerheten, där antalet cyberattacker har ökat och användningen av digital teknik i samhällena ökar exponeringen för cybersäkerhetsincidenter och deras potentiella gränsöverskridande konsekvenser. Hotet om en eventuell storskalig incident som skulle orsaka betydande störningar och skador på kritisk infrastruktur kräver ökad beredskap och samarbete på alla nivåer i EU:s cybersäkerhetsekosystem. EU har bidragit till den digitala omställningen genom finansiering från programmet för ett digitalt Europa. Ett av programmets fem specifika mål är cybersäkerhet och förtroende.

Den 18 april 2023 lade kommissionen också fram ett förslag (COM (2023) 208 final) till Europaparlamentets och rådets förordning om ändring av förordning (EU) 2019/881 vad gäller hanterade säkerhetstjänster (ändring av cybersäkerhetsakten). Förslaget kompletterar förslaget till cybersolidaritetsakt, där det föreslås att tjänsteleverantörer för cybersäkerhetsreserven ska väljas ut med beaktande av certifieringar från betrodda leverantörer.

Enligt preliminära uppgifter ska förslagen till ändring av cybersäkerhetsakten behandlas parallellt med förslaget till cybersolidaritetsakt.

2 Förslagets syfte

Det allmänna syftet med cybersolidaritetsakten är att stärka EU:s gemensamma förmåga att upptäcka cybersäkerhetsincidenter samt situationsmedvetenheten om och förmågan att hantera dessa. Det andra syftet är att stärka kritiska aktörers beredskap i hela EU och stärka solidariteten genom att utveckla en gemensam insatskapacitet mot betydande eller omfattande cybersäkerhetsincidenter, bl.a. genom stöd till tredjeländer för hantering av cybersäkerhetsincidenter. Syftet är också att främja europeisk teknisk suveränitet på cybersäkerhetsområdet. Vidare är syftet att förbättra kriståligheten och främja en effektiv hantering av cybersäkerhetsincidenter genom att skapa en mekanism för utvärdering av betydande eller storskaliga incidenter och erfarenheter av hanteringen av dem.

Genom de föreslagna ändringarna av cybersäkerhetsakten läggs leverantörer av hanterade säkerhetstjänster (*managed security services provider*) till cybersäkerhetsaktens tillämpningsområde. I rådets slutsatser från våren 2022 uppmanas unionen att förbättra den övergripande cybersäkerhetsnivån, t.ex. genom att underlätta nyetablering av leverantörer av hanterade säkerhetstjänster, och betonade att främjande av framväxten av sådana leverantörer bör vara en prioritering för EU:s industripolitik på cybersäkerhetsområdet. Enligt motiveringen till förslaget

anser kommissionen att certifiering av leverantörer av hanterade säkerhetstjänster kan vara ett effektivt sätt att öka förtroendet för dessa tjänsters kvalitet och på så sätt underlätta framväxten av en tillförlitlig bransch för cybersäkerhetstjänster i Europa. De föreslagna ändringar i cybersäkerhetsakten som gäller leverantörer av hanterade säkerhetstjänster avser betrodda leverantörer (*trusted providers*) enligt artikel 16 i förslaget till cybersolidaritetsakt.

Kommissionen påpekar att vissa medlemsstater redan har infört certifieringssystem för leverantörer av hanterade säkerhetstjänster. Förslaget om certifieringssystem för dessa tjänster syftar till att förhindra en fragmentering av tjänsterna i medlemsstaterna.

3 Förslagets huvudsakliga innehåll

3.1 Det huvudsakliga innehållet i förslaget till cybersolidaritetsakt

Det föreslås att det inrättas en europeisk infrastruktur av säkerhetscentrum (Security Operations Center, SOC) som ska utgöra den europeiska cyberskölden (European Cyber Shield) i syfte att förbättra och förstärka unionens gemensamma kapacitet för upptäckt och situationsmedvetenhet.

Vidare föreslås det att det inrättas en cybersäkerhetsreserv som består av en cyberkrismekanism med tjänster från betrodda privata leverantörer för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter.

Det föreslås också att en mekanism för granskning av cybersäkerhetsincidenter ska inrättas för granskning och analys av vissa betydande eller storskaliga incidenter. Den europeiska cyberskölden, cyberkrismekanismen och cybersäkerhetsreserven ska stödjas genom finansiering från programmet för ett digitalt Europa, som kommer att ändras genom denna rättsakt för att inrätta åtgärderna i förslaget.

3.1.1 Allmänna bestämmelser

Enligt kommissionens förslag kommer förordningen att stärka unionens kapacitet att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter.

Förslaget begränsar inte medlemsstaternas primära ansvar för nationell säkerhet, allmän säkerhet och förebyggande, utredning, upptäckt och lagföring av brott.

3.1.2 Inrättande av en europeisk cybersköld

Med stöd av förslaget inrättas en europeisk infrastruktur av säkerhetscentrum (den europeiska cyberskölden) för att utveckla kapacitet att upptäcka, analysera och behandla data om cyberhot och cyberincidenter i unionen. Skölden ska bestå av nationella säkerhetscentrum (SOC) och konsortier av gränsöverskridande säkerhetscentrum. Cybersköldens kapacitet ska byggas upp med stöd från programmet för ett digitalt Europa och dess tredje specifika mål (cybersäkerhet och förtroende).

Den europeiska cyberskölden ska föra samman och dela data om cyberhot och cyberincidenter från olika källor via konsortier av gränsöverskridande säkerhetscentrum, producera högkvalitativ och agerbar underrättelseinformation om cyberhot genom användning av förstklassiga verk-

tyg såsom artificiell intelligens och dataanalysteknik. Dessutom ska skölden påskynda upptäckten av cyberhot och tillhandahålla tjänster för cybersäkerhetssamfundet i EU, inbegripet att bidra till utvecklingen av avancerade AI-verktyg och dataanalysverktyg.

För att delta i den europeiska cyberskölden bör varje medlemsstat utse minst en offentlig myndighet som ska fungera som nationellt säkerhetscentrum. Det nationella säkerhetscentrumet ska ha kapacitet att fungera som kontaktpunkt mot andra offentliga och privata organisationer på nationell nivå för insamling och analys av information om cyberhot. Det ska också ha kapacitet att delta i ett gränsöverskridande konsortium bestående av nationella säkerhetscentrum. Det nationella säkerhetscentrumet ska utnyttja avancerad teknik som kan upptäcka och analysera data om cyberhot och cybersäkerhetsincidenter. Det nationella säkerhetscentrumet kan delta i gemensam upphandling tillsammans med Europeiska kompetenscentrumet för cybersäkerhet (ECCC), genom vilken ovannämnda verktyg kan förvärvas med 50 procents finansiellt bidrag från kommissionen. Nationella säkerhetscentrum som representerar minst tre medlemsstater får gemensamt inrätta ett konsortium av gränsöverskridande säkerhetscentrum. Även dessa konsortier kan få finansiellt bidrag på mellan 50 och 75 procent för gemensam upphandling och driftskostnader som möjliggör tillgång till avancerade verktyg för upptäckt och analys. Innan ett upphandlingsförfarande inleds ska ECCC och konsortiet ingå ett värd- och användningsavtal som anger villkoren för användningen av verktygen.

En förutsättning för nationella säkerhetscentrums deltagande i gemensamma upphandlingar är att de förbinder sig att delta i ett konsortium av gränsöverskridande säkerhetscentrum inom två år från den dag då verktygen och infrastrukturerna förvärvas eller då de erhåller bidragsfinansiering, beroende på vad som inträffar först.

Utöver avtalet mellan ECCC och konsortiet ska konsortiemedlemmarna ingå ett ömsesidigt avtal som anger och fastställer de interna arrangemangen för genomförandet av värd- och användningsavtalet. I det ömsesidiga konsortieavtalet ska deltagarna åta sig att dela en betydande mängd information inom konsortiet, bl.a. om cyberhot, tillbud, sårbarheter, fientliga aktörer, varningar och konfiguration av verktyg för att upptäcka cyberattacker, när utbytet av sådan information syftar till att förebygga, upptäcka, reagera på eller återhämta sig från cyberincidenter. Alternativt ska medlemmarna åta sig att dela sådan information när utbytet av information förbättrar cybersäkerheten, t.ex. genom att begränsa eller förhindra spridning av hot, stödja en rad defensiva förmågor, avhjälpa eller delge information om sårbarheter.

I det ömsesidiga avtalet bör konsortiemedlemmarna ange villkoren för detta informationsutbyte mellan medlemmarna. Avtalet ska också fastställa en styrningsram som ger alla parter incitament att utbyta information samt mål för bidrag till utvecklingen av avancerade AI-verktyg och dataanalysverktyg.

Gränsöverskridande säkerhetscentrum ska ingå samarbetsavtal med varandra, och specificera principer för informationsutbyte mellan de gränsöverskridande plattformarna. När gränsöverskridande säkerhetscentrum får information om en potentiell eller pågående storskalig cybersäkerhetsincident ska de ge relevant information till EU-CyCLONe, CSIRT-nätverket och kommissionen, med beaktande av deras krishanteringsuppdrag enligt NIS2-direktivet. CSIRT-nätverket (*Computer Security Incident Response Teams*) och EU-CyCLONe (*European Cyber Crisis Liaison Organisation Network*) är EU-omfattande befintliga nätverk för samarbete och informationsutbyte på cybersäkerhetsområdet. Finland deltar i båda nätverkens verksamhet.

Kommissionen får genom genomförandeakter fastställa förfaranden för den information som ska lämnas till EU-CyCLONe och CSIRT-nätverket samt till kommissionen, kraven på interoperabilitet för gränsöverskridande säkerhetscentrum och de tekniska kraven på säkerhet för säkerhetscentrum.

3.1.3 Inrättande av en cyberkrismekanism och en cybersäkerhetsreserv

Det föreslås att en cyberkrismekanism (Cyber Emergency Mechanism) ska inrättas.

Genom mekanismen genomförs beredskapsåtgärder, åtgärder för hantering av betydande och storskaliga cyberincidenter samt ömsesidiga stödåtgärder som utgörs av stöd från de nationella myndigheterna i en medlemsstat till en annan medlemsstat, särskilt genom CSIRT-nätverket i enlighet med artikel 11.3 f i NIS2-direktivet.

Som en del av cyberkrismekanismen kan också samordnad beredskapstestning utföras. För att genomföra beredskapstester ska kommissionen i förteckningen i bilaga I till NIS2-direktivet fastställa vilka sektorer som kan bli föremål för samordnade beredskapstester. Innehållet i beredskapstesterna, vem som ska genomföra dem eller andra förfaranden beskrivs inte närmare i förslaget. Enligt förslaget ska NIS-samarbetsgruppen i samarbete med kommissionen, Europeiska unionens cybersäkerhetsbyrå Enisa och den höga representanten ta fram gemensamma riskscenarier och metoder för de samordnade testerna.

Det föreslås också att en EU-cybersäkerhetsreserv ska inrättas som en del av cyberkrismekanismen. Reserven ska bestå av betrodda leverantörer (*trusted providers)* och tillhandahålla stöd för att hantera eller återhämta sig från betydande eller storskaliga cybersäkerhetsincidenter på begäran av medlemsstaterna. Entiteter som är verksamma inom kritiska eller högkritiska sektorer i medlemsstaterna samt unionens institutioner, byråer och organ kan få tillgång till reservens tjänster för att hantera betydande eller storskaliga cyberincidenter som drabbar en organisation, i syfte att få stöd för att hantera eller återhämta sig från sådana incidenter. Begäran om tjänster kan lämnas in av medlemsstaternas myndigheter för hantering av cyberkriser enligt NIS2-direktivet och CSIRT-enheter. Begäran om stöd ska lämnas till kommissionen och Enisa via den gemensamma kontaktpunkt som avses i NIS2-direktivet. För att få stöd från EU-cybersäkerhetsreserven ska de som begär stöd också vidta åtgärder för att begränsa konsekvenserna av den incident som begäran avser.

Begäran till reserven ska innehålla ändamålsenlig information om den påverkade entiteten och incidentens potentiella konsekvenser samt den planerade användningen av det begärda stödet, inbegripet en angivelse av de uppskattade behoven, information om de åtgärder som vidtagits för att begränsa incidenten och information om andra former av stöd som är tillgängliga för den berörda enheten, inbegripet avtalsarrangemang för förebyggande av incidenter samt försäkringsavtal som skulle kunna täcka sådana typer av incidenter. Enisa ska i samarbete med kommissionen och NIS-samarbetsgruppen utarbeta en mall för inlämning av begäranden om stöd. Medlemsstaterna ska informera CSIRT-nätverket och vid behov EU-CyCLONe om sina begäranden.

Kommissionen ska med stöd från Enisa bedöma begäranden om stöd från EU-cybersäkerhetsreserven och ett svar på begäran ska sändas utan dröjsmål. Begäran om stöd kan prioriteras med tanke på cybersäkerhetsincidentens allvarlighetsgrad, de potentiella konsekvenserna för påverkade medlemsstater eller berörda användare, incidentens potentiella gränsöverskridande karaktär och den påverkade entiteten, med prioritering av de väsentliga entiteter som avses i NIS2-direktivet.

Kommissionen ska ha ansvaret för genomförandet av reserven. Kommissionen ska fastställa prioriteringar för reserven, övervaka dess genomförande och säkerställa eventuella förbindelser med andra stödåtgärder inom ramen för denna förordning samt andra unionsåtgärder och unionsprogram. Kommissionen får också helt eller delvis anförtro driften och förvaltningen av EU-cybersäkerhetsreserven åt Enisa. För att stödja kommissionen i inrättandet av EU-cybersäkerhetsreserven ska Enisa utarbeta en kartläggning av vilka tjänster som behövs.

Inom en månad från det att stödåtgärden avslutats ska tjänsternas användare förse kommissionen och Enisa med en sammanfattning om den tjänst som tillhandahållits, de resultat som uppnåtts och lärdomar som dragits. Kommissionen ska regelbundet rapportera till NIS-samarbetsgruppen om användningen och resultaten av stödet. Kommissionen får genom genomförandeakter precisera hur tjänsterna inom EU-cybersäkerhetsreserven ska organiseras och vilka tjänster reserven ska tillhandahålla.

I förslaget beaktas att om cybersäkerhetsincidenter utgör eller resulterar i katastrofer enligt definitionen i beslutet om EU:s civilskyddsmekanism ska det stöd som ges ta hänsyn till förfaranden inom ramen för civilskyddsmekanismen.

Det föreslås också att cyberkrismekanismen ska komplettera det bistånd som ges inom ramen för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken, däribland genom snabbinsatsteam för cybersäkerhet (Cyber Rapid Response Teams). Snabbinsatsteamen för cybersäkerhet bygger på medlemsstaternas frivilliga insatser. Endast en del av medlemsstaterna, främst försvarsförvaltningen, deltar i verksamheten. Finland medverkar som observatörsmedlem. Dessutom kan det stöd som tillhandahålls genom mekanismen mellan medlemsstaterna utgöra stöd i enlighet med artikel 42.7 i fördraget om Europeiska unionen. Stöd inom ramen för cyberkrismekanismen får även vara ett led i unionens och medlemsstaternas gemensamma insatser i situationer som avses i artikel 222 i fördraget om Europeiska unionens funktionssätt.

I arrangemangen för inrättandet av EU-cybersäkerhetsreserven ställs vissa krav på upphandlingsförfarandena. I upphandlingarna ska det t.ex. säkerställas att EU-cybersäkerhetsreserven omfattar tjänster som kan användas i alla medlemsstater, med beaktande av i synnerhet nationella krav för tillhandahållandet av sådana tjänster, inbegripet certifiering. Upphandlingarna ska också säkerställa skyddet av unionens och dess medlemsstaters väsentliga säkerhetsintressen och säkerställa att reserven tillför ett mervärde genom att bidra till de mål som fastställs i artikel 3 i förordningen om ett digitalt Europa.

Vid upphandlingen av tjänster för EU-cybersäkerhetsreserven ska den upphandlande myndigheten beakta leverantörens yrkesmässiga integritet och kompetens, leverantörens tillräckliga erfarenhet av att leverera liknande tjänster till relevanta nationella myndigheter eller entiteter som är verksamma i kritiska eller högkritiska sektorer, förmågan att tillhandahålla tjänsten inom en kort tidsram och på det lokala språket i den medlemsstat där den kan tillhandahålla tjänsten. Leverantören ska också ha lämplig teknisk utrustning för att tillhandahålla tjänsten.

När det gäller säkerhetskraven ska leverantören ha en lämplig säkerhetsprövning, åtminstone för personal som är avsedd för utförandet av tjänsterna och en relevant säkerhetsnivå för sina it-system samt tillräckliga åtgärder för att skydda uppgifterna och säkerställa säkerheten vid utförandet av tjänsten. I förslaget anges också att leverantören ska vara certifierad i enlighet med cybersäkerhetsakten (EU) 2019/881 när det finns ett EU-certifieringssystem för dessa leverantörer av hanterade säkerhetstjänster.

Tredjeländer och deras behöriga myndigheter, såsom CSIRT-enheter och myndigheter för cyberkrishantering, kan också begära stöd från EU-cybersäkerhetsreserven, om detta uttryckligen föreskrivs i associeringsavtal som ingåtts om deras deltagande i programmet för ett digitalt Europa. Innan tredjeländer får stöd ska de förse kommissionen och den höga representanten med information om bl.a. sin cyberresiliens och riskhanteringskapacitet samt information om nationella åtgärder som vidtagits som förberedelse inför betydande eller storskaliga cybersäkerhetsincidenter.

3.1.4 Mekanism för granskning av cybersäkerhetsincidenter

Enligt förslaget ska Enisa på begäran av kommissionen, EU-CyCLONe eller CSIRT-nätverket granska och analysera hot, sårbarheter och begränsningsåtgärder med avseende på en viss betydande eller storskalig cybersäkerhetsincident. Som ett resultat av granskningen ska Enisa lämna en incidentgranskningsrapport till CSIRT-nätverket, EU-CyCLONe och kommissionen. Granskningsrapporten ska stödja dessa aktörer särskilt när det gäller att utföra de uppgifter som åläggs dem i NIS2-direktivet. När så är relevant ska kommissionen dela rapporten med den höga representanten.

Vid utarbetandet av incidentgranskningsrapporten ska Enisa samarbeta med alla relevanta intressenter, inbegripet företrädare för medlemsstaterna, kommissionen, andra berörda EU-institutioner, EU-organ och EU-byråer, leverantörer av hanterade säkerhetstjänster och användare av cybersäkerhetstjänster. När så är lämpligt ska Enisa också samarbeta med aktörer som påverkas av betydande eller storskaliga cybersäkerhetsincidenter. Enisa får också samråda med andra intressenter som ett led i granskningen.

Enisas granskningsrapport ska granska och analysera cybersäkerhetsincidenten, dess orsaker, sårbarheter och lärdomar från incidenten. Konfidentiella uppgifter ska skyddas i enlighet med unionsrätten eller nationell rätt. När så är lämpligt ska rapporten omfatta rekommendationer för att förbättra unionens säkerhetsstatus. När så är möjligt ska en del av rapporten göras tillgänglig för allmänheten. Denna version får endast innehålla offentlig information.

3.1.5 Slutbestämmelser

I slutbestämmelserna föreslås ändringar av regelverket för programmet för ett digitalt Europa (EU) 2021/694. Förslaget innebär att artikel 6 kompletteras, så att den europeiska cyberskölden och cyberkrismekanismen blir en del av programmet för ett digitalt Europa. Dessutom ska artikeln ändras så att ansvaret för genomförandet av åtgärder inom specifikt mål 3 (cybersäkerhet och förtroende) främst ligger hos Europeiska kompetenscentrumet för cybersäkerhet (ECCC), medan ansvaret för genomförandet av cybersäkerhetsreserven ligger hos kommissionen och Enisa.

Det föreslås ändringar av finansieringsramen i artikel 9 så att det vägledande beloppet för specifikt mål 2 (artificiell intelligens) minskas med 285 000 000 euro, för specifikt mål 3 (cybersäkerhet och förtroende) minskas med 20 000 000 euro och för specifikt mål 4 (avancerade digitala färdigheter) minskas med 95 000 000 euro.

Förslaget innehåller också preciseringar för användningen av överskott från specifikt mål 3 under det kommande året och för att göra det möjligt för Enisa och kommissionen att agera som förvärvande parter när det gäller cyberreserven. När det gäller ansökningsförfarandena ska artikel 14 ändras så att bidrag kan beviljas utan utlysning till nationella säkerhetscentrum och gränsöverskridande säkerhetscentrum enligt solidaritetsinitiativet och för användning av tjänster inom ramen för krismekanismen.

Kommissionen ska utvärdera förordningen fyra år efter den dag då den börjar tillämpas. Förordningen föreslås träda i kraft den tjugonde dagen efter det att den har offentliggjorts i Europeiska unionens officiella tidning.

3.2 Förslaget till ändring av cybersäkerhetsakten

Förslaget till ändring av cybersäkerhetsakten innehåller ett antal tekniska ändringar så att leverantörer av hanterade säkerhetstjänster omfattas av cybersäkerhetsakten (EU) 2019/881 och skyldigheterna i den. Förslaget innehåller också en ny artikel som anger säkerhetsmålen för den europeiska ordningen för cybersäkerhetscertifiering med avseende på leverantörer av hanterade säkerhetstjänster.

Enligt förslaget ska certifieringsramen bl.a. säkerställa att leverantörer av hanterade säkerhetstjänster har den kompetens och expertis som krävs samt en mycket hög nivå av teknisk kunskap och kompetens på det relevanta området. Det ska också säkerställas att säkerhetstjänster hela tiden tillhandahålls med hög kvalitet, att information som behandlas i samband med tillhandahållandet av tjänster skyddas mot oavsiktlig, otillåten eller obehörig åtkomst och att personer, program eller maskiner som tillhandahåller tjänsterna endast har åtkomst till de data, tjänster eller funktioner som omfattas av deras åtkomsträttigheter.

Det ska också säkerställas att de IKT-produkter, IKT-tjänster och IKT-processer och den IKT-utrustning som leverantörer av hanterade säkerhetstjänster använder för att tillhandahålla sina tjänster är säkra i sitt grundutförande och genom sin konstruktion, att de inte innehåller publikt kända sårbarheter och att de är korrekt uppdaterade när det gäller säkerhetsuppdateringar.

4 Förslagets rättsliga grund och förhållande till proportionalitets- och subsidiaritetsprinciperna

4.1 Rättslig grund

Den rättsliga grunden för förslaget till cybersolidaritetsakt är artiklarna 173.3 och 322.1 a i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Förslaget behandlas enligt det ordinarie lagstiftningsförfarandet där Europaparlamentet och rådet tillsammans antar förordningen. I rådet krävs omröstning med kvalificerad majoritet. Kommissionens förslag till ändring av cybersäkerhetsakten grundar sig på artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

Syftet med åtgärder som grundar sig på artikel 173 i EUF-fördraget bör vara att säkerställa att det finns nödvändiga förutsättningar för unionsindustrins konkurrensförmåga. Enligt artikeln ska denna verksamhet särskilt syfta till att påskynda industrins anpassning till strukturförändringar, främja en miljö som är gynnsam för initiativ och för utveckling av företag inom hela unionen, särskilt i fråga om små och medelstora företag, främja en miljö som är gynnsam för samarbete mellan företag och främja ett bättre utnyttjande av de industriella möjligheter som skapas genom politiken inom sektorerna för innovation, forskning och teknisk utveckling.

Artikel 173.3 i EUF-fördraget möjliggör särskilda åtgärder som syftar till att stödja de insatser som görs i medlemsstaterna för att uppnå dessa mål, men de får inte omfatta någon harmonisering av medlemsstaternas lagar och andra författningar.

Enligt artikel 2.2. i förslaget till förordning har förslaget tre syften:

- Stärka den gemensamma upptäcktsförmågan och situationsmedvetenheten i unionen när det gäller cyberhot och cyberincidenter och därigenom göra det möjligt att stärka konkurrenskraften för unionens industri- och tjänstesektorer i hela den digitala ekonomin och bidra till unionens tekniska suveränitet på cybersäkerhetsområdet.

- Förbättra beredskapen hos entiteter som är verksamma inom kritiska och högkritiska sektorer i hela unionen och stärka solidariteten genom att utveckla gemensam insatskapacitet mot betydande eller storskaliga cybersäkerhetsincidenter, bl.a. genom att göra unionsstöd för hantering av cybersäkerhetsincidenter tillgängligt för tredjeländer som deltar i programmet för ett digitalt Europa.

- Öka unionens resiliens och bidra till effektiva insatser genom att granska och analysera betydande eller storskaliga incidenter för att bl.a. dra lärdomar och, när så är lämpligt, utfärda rekommendationer.

Statsrådet konstaterar att den rättsliga grunden för artikel 173.3 i EUF-fördraget är starkt kopplad till främjandet av företagens verksamhetsförutsättningar. EU-domstolen har erinrat om att denna artikel ingår i den tredje delen av EUF-fördraget som rör unionens inre politik och inre åtgärder, där den återfinns under industrirubriken i avdelning XVII (mål C- 733/19, Royaume des Pays-Bas c. Conseil de l'Union européenne et Parlament européen, punkt 73). Statsrådet konstaterar att i synnerhet den europeiska cyberskölden (som består av alla nationella säkerhetscentrum och gränsöverskridande säkerhetscentrum) och mekanismen för granskning av cybersäkerhetsincidenter (som utförs av Europeiska cybersäkerhetsbyrån Enisa) inte har någon direkt inverkan på företagens operativa kapacitet. Domstolen har dock tolkat den tidigare artikel 130 i EG-fördraget som en möjlig rättslig grund för att genomföra de mål som anges i artikel 130.1 [nuvarande artikel 173.1) i fördraget, trots att den avser den offentliga sektorn (mål C-42/97, Europaparlamentet mot rådet, punkt 60). Statsrådet anser att det är oklart hur dessa helheter i slutändan kommer att tjäna syftet med artikeln, eftersom det främst är medlemsstaterna eller unionens institutioner som gynnas av åtgärderna och deras inverkan på cybersäkerhetssektorn är indirekt (jfr mål C-42/97, Europaparlamentet mot rådet, punkterna 40 och 44). Statsrådet anser också att bestämmelserna om de nationella säkerhetscentrumen kan leda till en verklig tillnärmning av medlemsstaternas lagstiftning, vilket inte är möjligt på grundval av den rättsliga grunden. Den föreslagna cyberkrismekanismen skulle däremot bidra till att förbättra förutsättningarna för företagsverksamhet i den förändrade cybersäkerhetsmiljön. När cybersäkerhetsreserven inrättas måste man dock ta hänsyn till att en åtgärd enligt den rättsliga grunden inte kan medföra att konkurrensen snedvrids.

Förslaget till cybersolidaritetsakt bygger också på artikel 322.1 a i EUF-fördraget. Förutom ny lagstiftning föreslås det också ändringar i förordning (EU) 2021/694 (programmet för ett digitalt Europa). Den rättsliga grunden för programmet för ett digitalt Europa är artiklarna 172 och 173.3 i EUF-fördraget. Enligt kommissionens motiveringspromemoria bör dock cybersolidaritetsakten också grunda sig på artikel 322.1 i EUF-fördraget, eftersom de föreslagna ändringarna i programmet för ett digitalt Europa innebär ett undantag från principen om ettårighet i förordning (EU, Euratom) 2018/1046 12 (budgetförordningen) när det gäller åtagande- och betalningsbemyndiganden. En rättslig grund för budgetförordningen är artikel 322.1 i EUF-fördraget. Enligt artikel 322.1 a i EUF-fördraget ska Europaparlamentet och rådet genom förordningar, i enlighet med det ordinarie lagstiftningsförfarandet och efter att ha hört revisionsrätten, anta finansiella regler som särskilt ska ange närmare bestämmelser om budgetens uppställning och genomförande och om redovisning och revision.

EU-domstolen har sedan länge ansett att unionslagstiftaren i den mån det är möjligt bör sträva efter att alltid använda en enda rättslig grund. Att använda två eller flera parallella rättsliga

grunder är en exceptionell lösning. Detta är enligt domstolen möjligt när det rör sig om en åtgärd med flera målsättningar eller flera beståndsdelar, vilka är oskiljaktigt förbundna med varandra, utan att den ena är underordnad eller indirekt i förhållande till den andra. Enligt statsrådets bedömning är det nu fråga om en sådan situation. Förslaget har inte ett enda huvudsakligt syfte eller en enda avgörande faktor, utan består av två sinsemellan olika beståndsdelar där den del som gäller finansieringen kan särskiljas från det övriga innehållet. Dessutom krävs det alltid att de rättsliga grunderna är kompatibla med varandra för att flera rättsliga grunder ska kunna användas. Även detta villkor är uppfyllt, eftersom beslutsförfarandet är detsamma i de båda rättsliga grunderna.

Därför anser statsrådet i fråga om den föreslagna cybersolidaritetsakten att

- artikel 173.3 i EUF-fördraget inte verkar vara en lämplig rättslig grund för den europeiska cyberskölden eller mekanismen för granskning av cybersäkerhetsincidenter, om inte regleringens koppling till industrin och tillnärmningen av lagstiftningen tydliggörs

- artikel 173.3 i EUF-fördraget verkar vara en lämplig rättslig grund för cyberkrismekanismen

- artikel 322 i EUF-fördraget verkar vara en lämplig rättslig grund för att göra undantag från principen om ettårighet

- det verkar motiverat att använda två rättsliga grunder.

Den rättsliga grunden för den föreslagna ändringen av cybersäkerhetsakten är artikel 114 i EUF-fördraget. För att genomföra den inre marknaden ska parlamentet och rådet enligt artikeln vidta åtgärder för tillnärmning av medlemsstaternas lagar, förordningar och administrativa beslut.

Enligt artikel 114 i EUF-fördraget ska rådet anta förslaget med kvalificerad majoritet tillsammans med Europaparlamentet i enlighet med det ordinarie lagstiftningsförfarandet. EU-domstolen har sedan länge ansett att en rättsakt kan antas på grundval av artikel 114 i EUF-fördraget endast om det av rättsakten ”objektivt framgår att den syftar till att förbättra villkoren för upprättandet av den inre marknaden och dess funktion”. Om detta villkor är uppfyllt ger artikel 114 i EUF-fördraget unionslagstiftaren ett stort utrymme för egen bedömning när det gäller valet av behövliga tillnärmnings- och harmoniseringsåtgärder.

Kommissionen anser att förslaget, liksom när det gäller den ändrade cybersäkerhetsakten, syftar till att undvika en fragmentering av den inre marknaden, särskilt genom att möjliggöra införandet av europeiska ordningar för cybersäkerhetscertifiering av förvaltade säkerhetstjänster. Medlemsstaterna har redan börjat införa nationella certifieringssystem för förvaltade säkerhetstjänster. Det finns därför en påtaglig risk för en fragmentering av den inre marknaden för sådana tjänster, vilket detta förslag syftar till att förhindra.

Statsrådet konstaterar att den föreslagna rättsliga grunden är densamma som för den ursprungliga cybersäkerhetsakten. Statsrådet kan instämma i kommissionens motivering till förslaget och dess syfte att förbättra den inre marknaden och dess funktion. Statsrådet anser därför att artikel 114 i EUF-fördraget verkar vara den lämpliga rättsliga grunden för den föreslagna ändringen av cybersäkerhetsakten.

4.2 Subsidiaritets- och proportionalitetsprincipen

Enligt artikel 5 om subsidiaritets- och proportionalitetsprinciperna i fördraget om Europeiska unionen får unionen anta akter endast när det är nödvändigt och i den utsträckning det är nödvändigt. Enligt subsidiaritetsprincipen i artikel 5.3 i fördraget om Europeiska unionen ska unionen på de områden där den inte har exklusiv befogenhet vidta en åtgärd endast om och i den mån som målen för den planerade åtgärden inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, och därför, på grund av den planerade åtgärdens omfattning eller verkningar, bättre kan uppnås på unionsnivå.

Kommissionen anser att förslaget till cybersolidaritetsakt är förenligt med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). På grund av cybersäkerhetshotens gränsöverskridande karaktär är målen i förslaget inte effektivt genomförbara genom medlemsstaternas nationella lagstiftning. Kommissionen anser att stöd genom olika mekanismer kompletterar de nationella kapaciteterna utan att överlappa befintliga åtgärder för att upptäcka, förbereda sig inför och hantera cyberhot.

Kommissionen anser att åtgärderna i förslaget till cybersolidaritetsakt inte påverkar medlemsstaternas ansvar för nationell säkerhet, allmän säkerhet och förebyggande, utredning, upptäckt och lagföring av brott. Kommissionen anser att åtgärderna inte heller påverkar de rättsliga skyldigheterna för entiteter som är verksamma i kritiska och högkritiska sektorer att anta cybersäkerhetsåtgärder i enlighet med NIS 2-direktivet, utan att de kompletterar dessa åtgärder genom att förbättra upptäckten av hot.

Statsrådet anser utifrån tillgängliga uppgifter att förslaget i huvudsak är förenligt med subsidiaritetsprincipen, även om bedömningen försvåras av avsaknaden av en konsekvensanalys. Det finns ett tydligt behov av att främja samarbete och informationsutbyte mellan medlemsstaterna på EU-nivå, vilket man också har gjort tidigare, t.ex. inom samarbetsgruppen enligt NIS2-direktivet, CSIRT-nätverket och EU-CyCLONe samt genom Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (förordning (EU) 2021/887). Finland har redan relativt avancerade metoder och samarbets- och förtroendenätverk som skapats under en lång tid och som kommer att vidareutvecklas i och med CSIRT- och CyCLONe-nätverken enligt definitionen i NIS2-direktivet. Det kan dock bedömas att det föreslagna nätverket av säkerhetscentrum kan ge viss nytta även för Finland, även om Finland inte nödvändigtvis får den största nyttan av förslaget.

Statsrådet påpekar dock att den nationella säkerheten med stöd av artikel 4.2 i EU-fördraget förblir varje medlemsstats eget ansvar. Enligt den föreslagna artikel 1.3 påverkar förordningen inte medlemsstaternas *primära* ansvar för nationell säkerhet. Statsrådet anser att man med tanke på inriktningen av åtgärderna i förslaget till cybersolidaritetsakt, vilka på många sätt är kopplade till frågor som rör nationell säkerhet, i den fortsatta beredningen måste ta hänsyn till i synnerhet förslagets förhållande till den nationella säkerheten, som uteslutande är en fråga för varje medlemsstat.

För det andra påpekar statsrådet att det – utöver de begränsningar som rör den rättsliga grunden – inte är förenligt med subsidiaritetsprincipen att begränsa medlemsstaternas administrativa autonomi genom att ange att det nationella säkerhetscentrumet uttryckligen ska vara ett offentligrättsligt organ (artiklarna 2.1.2 och 4.1).

Kommissionen anser att den föreslagna ändringen av cybersäkerhetsakten är förenlig med subsidiaritetsprincipen, eftersom införandet av europeiska ordningar för cybersäkerhetscertifiering av förvaltade säkerhetstjänster endast kan uppnås genom åtgärder på unionsnivå för att undvika

en fragmentering av den inre marknaden. Dessutom kommer leverantörer av förvaltade säkerhetstjänster som berörs av den föreslagna ändringen, liksom deras största potentiella kunder, enligt kommissionen att vara verksamma i hela unionen. Statsrådet kan omfatta kommissionens motiveringar om förslagets överensstämmelse med subsidiaritetsprincipen.

Enligt proportionalitetsprincipen i artikel 5.4 i fördraget om Europeiska unionen ska unionens åtgärder till innehåll och form inte gå utöver vad som är nödvändigt för att nå målen i fördragen. För att iaktta proportionalitetsprincipen måste lagstiftaren därför, när det finns flera olika alternativ, välja det alternativ genom vilket målet kan nås effektivt med de lindrigaste konsekvenserna. Enligt kommissionens bedömning går de föreslagna åtgärderna i cybersolidaritetsakten inte utöver vad som är nödvändigt för att uppnå målen med förslaget. Förslaget påverkar inte medlemsstaternas skyldigheter i fråga om nationell säkerhet och inte heller de skyldigheter som åligger aktörer som omfattas av NIS2-direktivet. De föreslagna åtgärderna kommer att komplettera och stödja inrättandet av infrastruktur för upptäckt och analys av hot.

Statsrådet anser att förslaget inte till alla delar är helt förenligt med proportionalitetsprincipen. Generellt bör det noteras att de finansiella instrumenten inte bör skapa felaktiga incitament för medlemsstaterna att inte utveckla egen cybersäkerhetskapacitet.

Statsrådet anser att i synnerhet den föreslagna regleringen om den europeiska cyberskölden inte uppfyller kraven enligt proportionalitetsprincipen. Förslaget tar inte tillräcklig hänsyn till befintliga samarbetsstrukturer och skapar nya administrativa strukturer utöver dessa. Det är särskilt viktigt att beakta CSIRT-nätverket, som fastställs i EU:s direktiv 2016/1148 om nät- och informationssäkerhet och som redan har uppgifter som rör övervakning av cyberhot, sårbarheter och incidenter. Dessutom kommer CSIRT-nätverkets uppgifter att preciseras och utvidgas i det nya NIS2-direktivet. Det är också värt att notera att de föreslagna säkerhetscentrumen med stor sannolikhet skulle vara desamma som de nationella CSIRT-enheterna.

När det gäller informationsutbyte inom nätverket av säkerhetscentrum har man identifierat en risk för att förslaget de facto kan komma att strida mot sina mål. Informationsutbyte om cybersäkerhet har av tradition byggt på ömsesidigt förtroende mellan aktörerna. Förslaget anger inte tillräckligt specifikt vilken typ och nivå av informationsutbyte det egentligen handlar om, hur informationen rör sig mellan de olika nätverken av säkerhetscentrum, vilken typ an information det är fråga om och hur den kan lämnas ut, t.ex. till den privata sektorn, varvid det är möjligt att informationsutbytet minskar i stället för att öka. Det är dock svårt att göra en adekvat bedömning av fakta på grund av avsaknaden av en konsekvensanalys, och särskild uppmärksamhet måste ägnas åt detta under förhandlingarna.

När det gäller cybersäkerhetsakten anser kommissionen att det föreslagna initiativet står i proportion till målet, eftersom de föreslagna ändringarna i cybersäkerhetsakten ska anpassa tillämpningsområdet för ramverket för cybersäkerhetscertifiering genom att inkludera ”förvaltade säkerhetstjänster”, definiera dessa tjänster i enlighet med NIS 2-direktivet och ändra säkerhetsmålen för den europeiska cybersäkerhetscertifieringen för att ta hänsyn till ”förvaltade säkerhetstjänster”. Statsrådet kan instämma i kommissionens motivering till förslagets överensstämmelse med proportionalitetsprincipen.

4.3 Delegering av befogenheter samt föreslagna uppgifter för kommissionen

Den föreslagna cybersolidaritetsakten innebär att kommissionen tilldelas genomförandebefogenheter. Kommissionen ges befogenhet att anta genomförandeakter i enlighet med det granskningsförfarande som avses i artikel 21 för att

- specificera villkoren för interoperabiliteten mellan gränsöverskridande säkerhetscentrum (artikel 6.3)

- fastställa förfarandena för informationsutbyte mellan gränsöverskridande säkerhetscentrum och unionsentiteter om en potentiell eller pågående storskalig cybersäkerhetsincident (artikel 7.2)

- ange tekniska krav för att säkerställa en hög nivå av dataskydd och fysiskt skydd för infrastrukturen och för att skydda unionens säkerhetsintressen vid utbyte av information med entiteter som inte är offentliga organ i medlemsstaterna (artikel 8.3)

- fastställa vilken typ av och hur många insatstjänster som behövs för EU-cybersäkerhetsreserven (artikel 12.8)

- ytterligare specificera de närmare arrangemangen för tilldelning av stödtjänsterna från EU-cybersäkerhetsreserven (artikel 13.7).

Statsrådet anser att den föreslagna delegeringen av befogenheter i huvudsak är lämplig. Det praktiska genomförandet av informationsutbytet är förenat med tekniska frågor som behöver harmoniseras. Genomförandebefogenheterna bör dock förtydligas ytterligare för att de tydligare ska hänvisa till teknisk interoperabilitet, till skillnad från den interoperabilitet som uppstår genom funktionell eller administrativ enhetlighet. Medlemsstaternas administrativa autonomi är en av utgångspunkterna för unionsrätten och förordningens rättsliga grund gör det inte möjligt att tillnärma medlemsstaternas lagstiftning. Den information som utbyts kan inte heller omfattas av enbart reglering på lägre nivå än lag om det är fråga om annan än offentlig information, eftersom statsrådet anser att det då är fråga om regleringens väsentliga innehåll (se också avsnittet om grundlagen nedan). Statsrådet anser också att det vore lämpligt att åtminstone i någon mån definiera olika typer av incidenthanteringstjänster i den föreslagna förordningen, eftersom det kan vara fråga om regleringens väsentliga innehåll. De tjänster som tillhandahålls kan nämligen indirekt påverka vilken egen kapacitet och vilka åtgärder som medlemsstaterna själva väljer att finansiera.

Enligt förslaget tilldelas kommissionen också vissa uppgifter. Kommissionen ska utse de sektorer eller delsektorer från vilka entiteter kan bli föremål för samordnad beredskapstestning (artikel 11.1). Kommissionen ska också fastställa EU-cybersäkerhetsreservens prioriteringar och utveckling och övervaka dess genomförande (artikel 12.5). Förslaget till förordning anger dock inte hur detta ska gå till. Kommissionen ska bedöma begäran om stöd från EU-cybersäkerhetsreserven (artikel 14.1). Statsrådet anser att ansvaret för att hantera begäran om stöd från cybersäkerhetsreserven borde ligga hos Europeiska cybersäkerhetsbyrån Enisa och inte kommissionen. Statsrådet anser att medlemsstaterna bör involveras i bedömningen av inriktningen av beredskapstesterna och prioriteringarna för cybersäkerhetsreserven.

5 Förslagets konsekvenser

Kommissionen har inte gjort någon konsekvensbedömning av förslaget till cybersolidaritetsakt. Kommissionen motiverar avsaknaden av en konsekvensanalys med att förslaget är brådskande. Enligt kommissionen kommer förslaget inte att medföra några betydande administrativa eller miljömässiga konsekvenser utöver vad som anges i konsekvensbedömningen av förordningen om programmet för ett digitalt Europa. När det gäller beredskapstester och incidenthanteringstjänster (cyberkrismekanismen) har kommissionen i förslaget tagit fasta på lärdomarna från genomförandet av det pilotprojekt som Enisa inledde 2022.

Förslagets nationella konsekvenser är svåra att bedöma i avsaknad av en konsekvensanalys från kommissionens sida. Konsekvenserna för Finland och finländska aktörer bedöms närmare när behandlingen framskrider.

5.1 Ekonomiska konsekvenser

Förslaget har direkta konsekvenser för statsfinanserna och företag och indirekta konsekvenser för företag och hushåll. Enligt kommissionens bedömning kommer förslaget att öka anslaget till det specifika målet för cybersäkerhet i programmet för ett digitalt Europa med 100 miljoner euro genom en omfördelning av programmets anslag från andra specifika mål. Förändringar i finansieringen från programmet kan undergräva uppnåendet av programmets övriga mål (t.ex. artificiell intelligens och digitala färdigheter). Ytterligare information om finansieringsmekanismerna i förslaget krävs innan en tillräcklig bedömning av de nationella ekonomiska konsekvenserna av förslaget kan göras. I upphandlingen av den cybersköld som ingår i förslaget ingår en nationellt finansiellt bidrag på 25–50 procent av den totala kostnaden.

Förslaget kommer att få statsfinansiella konsekvenser i och med de ökade myndighetsuppgifterna. Konsekvenserna preciseras i konsekvensbedömningarna inför den nationella genomförandefasen.

Förslaget förutsätter att ett nationellt säkerhetscentrum utses. Detta kan kräva lagstiftningsändringar och en omvärdering av anslagen för de nationella myndigheternas uppgifter och verksamhet på grund av ytterligare resursbehov.

Anslutning till ett konsortium av gränsöverskridande säkerhetscentrum skulle påverka den nuvarande nationella upphandlingen av cyberlägesbildstjänster och potentiellt medföra besparingar på längre sikt.

Cybersäkerhetsreserven kan skapa nya affärsmöjligheter i unionen för betrodda cybersäkerhetsföretag som uppfyller kriterierna för leverantörer när det gäller att tillhandahålla incidenthanteringstjänster. Kravet på att tillhandahålla tjänster på mållandets språk kan å ena sidan minska antalet tillgängliga leverantörer i Finland och å andra sidan försämra affärsmöjligheterna för finländska företag inom informationssäkerhetsbranschen i andra medlemsstater. Det skulle också vara möjligt för finländska företag inom vissa sektorer att få hjälp från cybersäkerhetsreserven om villkoren är uppfyllda, vilket kan anses vara positivt för företagens verksamhet.

Under arbetsgruppsbehandlingen ber Finland kommissionen om ytterligare utredningar av konsekvenserna.

5.2 Konsekvenser för myndigheternas verksamhet

Verksamheten inom det föreslagna konsortiet av gränsöverskridande säkerhetscentrum överlappar delvis de befintliga mekanismerna för informationsutbyte och situationsmedvetenhet. Ett välfungerande informationsutbyte inom konsortiet av gränsöverskridande säkerhetscentrum skulle kunna förbättra vissa myndigheters insamling av cyberlägesbildsuppgifter i Finland. Nätverkens verksamhet bygger dock på de deltagande ländernas aktivitet. I takt med att antalet internationella nätverk ökar måste man kunna prioritera de viktigaste nätverken i förhållande till befintliga resurser.

Förslaget kräver också att den nationella myndigheten för hantering av cyberkriser eller en CSIRT-enhet ska fungera som kontaktpunkt för ansökan om cybersäkerhetsreservens tjänster.

Den gemensamma kontaktpunkten i Finland skulle vara Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom.

Beredskapstestningen av kritiska sektorer inom ramen för cyberkrismekanismen kan förbättra cybersäkerheten på nationell nivå och EU-nivå genom att man på förhand kan identifiera brister i företagens cyberskydd.

5.3 Konsekvenser av de föreslagna ändringarna av cybersäkerhetsakten

När det gäller de föreslagna ändringarna av cybersäkerhetsakten har kommissionen inte genomfört någon konsekvensbedömning på grund av förslagets begränsade omfattning.

De föreslagna ändringar i cybersäkerhetsakten som gäller ramen för certifiering av hanterade säkerhetstjänster skulle kunna harmonisera de kvalitets- och säkerhetskrav som ställs på cybersäkerhetsföretag som är verksamma i unionen. Detta skulle kunna öka de europeiska cybersäkerhetsföretagens konkurrenskraft i förhållande till företag utanför unionen och förbättra kvaliteten och tillförlitligheten deras tjänster. Certifieringsramen skulle dock kunna öka den administrativa och ekonomiska bördan för små och medelstora företag och försämra deras affärsmöjligheter.

De föreslagna ändringarna av cybersäkerhetsförordningen medför inte några konsekvenser för den nationella lagstiftningen eller direkta konsekvenser för statsfinanserna.

6 Förslagets förhållande till grundlagen samt till de grundläggande och mänskliga rättigheterna

Genom att öka säkerheten för digital information kommer förslaget enligt kommissionen att bidra till att skydda rätten till frihet och säkerhet enligt artikel 6 i EU:s stadga om de grundläggande rättigheterna och rätten till respekt för privatlivet och familjelivet enligt artikel 7 i EU:s stadga om de grundläggande rättigheterna. Genom att skydda företag från ekonomiskt skadliga cyberattacker kommer förslaget enligt kommissionen också att bidra till näringsfriheten enligt artikel 16 i EU:s stadga om de grundläggande rättigheterna och rätten till egendom enligt artikel 17 i EU:s stadga om de grundläggande rättigheterna. Genom att skydda den kritiska infrastrukturens integritet vid cyberattacker kommer förslaget enligt kommissionen också att bidra till rätten till hälsovård enligt artikel 35 i EU:s stadga om de grundläggande rättigheterna och rätten till tillgång till tjänster av allmänt ekonomiskt intresse enligt artikel 36 i EU:s stadga om de grundläggande rättigheterna.

Statsrådet kan instämma i kommissionens uppfattning, även om de konsekvenser som kommissionen nämner i huvudsak är indirekta. Förslaget kan också indirekt bidra till skyddet för personuppgifter enligt artikel 8 i stadgan om de grundläggande rättigheterna och 10 § i grundlagen genom att förebygga it-säkerhetsincidenter. Enligt statsrådets uppfattning kommer förslaget främst att gynna organ inom den offentliga sektorn. Förebyggande av it-säkerhetsincidenter har därmed ett samband med handlingsoffentligheten och sekretessen enligt grundlagens 12 § 2 mom. och genomförandet av de krav i fråga om god förvaltning och rättsskydd som föreskrivs i grundlagens 21 §.

Trots detta konstaterar statsrådet att en del av bestämmelserna i den föreslagna cybersolidaritetsakten måste granskas närmare mot bakgrund av grundlagen och grundlagsutskottets praxis.

Lagbundenhet och överföring av offentliga förvaltningsuppgifter (GrL 2 och 124 §)

Den föreslagna europeiska cybersköldens bygger på de nationella säkerhetscentrumen (artikel 3.1). Varje medlemsstat ska utse minst ett säkerhetscentrum. Det nationella säkerhetscentrumet ska vara ett offentligrättsligt organ. Det ska fungera som ”referenspunkt och gränssnitt mot andra offentliga och privata organisationer på nationell nivå för insamling och analys av information om cybersäkerhetshot och cybersäkerhetsincidenter och ska bidra till ett gränsöverskridande säkerhetscentrum” och ”ska vara utrustat med förstklassig teknik som klarar att upptäcka, aggregera och analysera data av relevans för cybersäkerhetshot och cybersäkerhetsincidenter”. Artiklarna 2.1.2 och 4.1

Enligt 124 § i grundlagen kan offentliga förvaltningsuppgifter 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. Statsrådet konstaterar att det på cybersäkerhetssidan utöver myndigheter finns privata aktörer som samlar in och analyserar information om cyberhot och cyberhändelser. Enligt statsrådet kan dock det faktum att det nationella säkerhetscentrumet ska fungera som en slags knutpunkt göra uppgiften till en offentlig förvaltningsuppgift (jfr 3 § i lagen om Transport- och kommunikationsverket, där en av cybersäkerhetscentrets uppgifter är att upprätthålla en lägesbild över den nationella cybersäkerheten och inom sitt verksamhetsområde stödja samhällets allmänna beredskap för störningssituationer och undantagsförhållanden under normala förhållanden). Utifrån kommissionens förslag kan man inte heller helt utesluta att uppdraget innebär betydande utövning av offentlig makt. De föreslagna gränsöverskridande säkerhetscentrumen och den europeiska cybersköldens, vilka består av nationella säkerhetscentrum, inbegriper nämligen ett omfattande informationsutbyte (artiklarna 3.2, 6 och 7.1), och exempelvis sekretessbelagd information enligt 24 § 1 mom. 3, 7, 9 och 20 punkten i offentlighetslagen, personuppgifter eller förmedlingsuppgifter om elektronisk kommunikation enligt lagen om tjänster inom elektronisk kommunikation undantas inte från informationsutbytet (i fråga om personuppgifter, se skäl 22 och i fråga om sekretessbelagd information se skäl 23). Vidare fäster statsrådet uppmärksamhet vid att ett av målen med de gränsöverskridande säkerhetscentrumen är att ”stödja produktionen av högkvalitativ underrättelseinformation” (artikel 2.1.1). Därför anser statsrådet att förslaget inte är problemfritt med tanke på 124 § i grundlagen, utan att det måste preciseras i detta avseende.

Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag. I all offentlig verksamhet ska lag noggrant iakttas.

Statsrådet konstaterar att den europeiska cybersköldens verksamhet i hög grad verkar bygga på överenskommelser mellan såväl medlemsstaterna som mellan medlemsstaternas konsortier och unionsorganen. Statsrådet noterar att ett gränsöverskridande säkerhetscentrum beskrivs som ”en flerlandsplattform ... inom en samordnad nätverksstruktur” (artikel 2.1.1). De gränsöverskridande säkerhetscentrumen baseras på ett avtal (värdkonsortium) som ingåtts mellan de nationella säkerhetscentrumen (artiklarna 2, 1, 3, 5 och 6). Gränsöverskridande säkerhetscentrum ska ha en juridisk företrädare, som tydligen också vara en juridisk person (artikel 5.4) och ingå samarbetsavtal med andra gränsöverskridande säkerhetscentrum (artikel 6.4) samt värd- och användningsavtal om de verktyg och infrastrukturer som ska upphandlas tillsammans med Europeiska kompetenscentrumet för cybersäkerhet (artikel 5.2). Gränsöverskridande säkerhetscentrum och nationella säkerhetscentrum ska, direkt med stöd av förordningen, utgöra den europeiska cyberskölden (artikel 3.1).

Statsrådet anser att strukturen är förhållandevis komplex. Om det på det sätt som beskrivs ovan är fråga om en myndighetsuppgift, anser statsrådet att strukturen inte utan problem kan samord-

nas med den lagbundna myndighetsverksamheten. Grundlagsutskottet har ansett att ett samarbetsavtal mellan myndigheterna måste bedömas med avseende på 2 § 3 mom. i grundlagen. Grundlagsutskottet har t.ex. ansett det olämpligt i statsförfattningsrättsligt hänseende att en myndighets kompetens till den del det är fråga om utövning av offentlig makt gentemot enskilda grundar sig på ett avtal mellan myndigheter. (GrUU 19/2005 rd s. 8/I). Ett eventuellt utbyte av konfidentiell information mellan myndigheter kan inte heller grunda sig på ett avtal, vilket behandlas närmare nedan.

Det nationella säkerhetscentrumet får ingå ett gemensamt upphandlingsavtal med Europeiska kompetenscentrumet för cybersäkerhet. Detta kräver ett värd- och användningsavtal för de verktyg och den infrastruktur som ska upphandlas. (Artikel 4.2) För tydlighetens skull konstaterar statsrådet att ett förvaltningsavtal som hänför sig till en upphandling i sig inte är problematiskt med avseende på grundlagen, så länge de ovan nämnda kraven enligt 2 § 3 mom. i grundlagen beaktas.

Det finns också skäl att bedöma användningen av den föreslagna EU-cybersäkerhetsreserven mot grundlagens 124 §. Användningen av reserven verkar vara obligatorisk för myndigheternas insatser mot betydande eller storskaliga incidenter som riktar sig mot dem eller när de bistår entiteter i kritiska sektorer med insatser (artikel 12.4).

Skydd för privatlivet, skydd av personuppgifter, dataskydd vid elektronisk kommunikation samt offentlighetsprincipen (GrL 10 och 12 §)

Enligt 10 § 1 och 2 mom. i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden är okränkbar. Enligt 10 § 4 mom. i grundlagen kan dock vissa nödvändiga begränsningar i meddelandehemligheten föreskrivas genom lag.

Enligt 12 § 2 mom. i grundlagen är handlingar och upptagningar som innehas av myndigheterna offentliga om inte offentligheten av tvingande skäl särskilt har begränsats genom lag. Var och en har rätt att ta del av offentliga handlingar och upptagningar.

För det första påpekar statsrådet att uppgifter som en myndighet samlar in, begär eller som lämnas till den är myndighetshandlingar. Offentligheten och sekretessen för dem bestäms enligt offentlighetslagstiftningen. Förordningens förhållande till den nationella offentlighetslagstiftningen, inklusive sekretess, är oklart. Förordningen innehåller endast generella hänvisningar till exempelvis konfidentialitet och säkerhet (skäl 23, artiklarna 8.1 och 18.3).

För det andra påpekar statsrådet, såsom redan konstaterats ovan, att den europeiska cybersköldden och det gränsöverskridande säkerhetscentrumet inbegriper ett omfattande informationsutbyte och att t.ex. sekretessbelagd information, personuppgifter eller förmedlingsuppgifter om elektronisk kommunikation enligt 24 § 1 mom. 3, 7 och 20 punkten i offentlighetslagen inte är undantagna från informationsutbytet. Informationsutbyte inom ramen för den europeiska cyberskölden definieras inte närmare (artikel 3.2 a). Däremot ska värdkonsortiets medlemmar utbyta ”relevant information” sinsemellan, och syftet med utbytet definieras i förordningen. (Artikel 6.1) På samma sätt ska ”relevant information” om potentiella eller pågående storskaliga cybersäkerhetsincidenter ges till vissa EU-organ (artikel 7.1).

Grundlagsutskottet har särskilt påpekat att det bör finnas exakta och noga avgränsade bestämmelser om att det är tillåtet att behandla känsliga uppgifter bara om det är absolut nödvändigt,

och bestämmelserna om behandling av känsliga uppgifter måste vara detaljerade och omfattande, inom de ramar som dataskyddsförordningen tillåter (se t.ex. GrUU 4/2021 rd, 4 punkten). Grundlagsutskottet har analyserat bestämmelserna om myndigheternas rätt att trots tystnadsplikten få och lämna ut information med avseende på skyddet för privatlivet och för personuppgifter i 10 § 1 mom. i grundlagen, och då fäst vikt bl.a. vid vad och vem rätten att få information gäller och hur rätten är kopplad till nödvändighetskriteriet. Myndigheternas rätt att få uppgifter och möjlighet att lämna ut uppgifter har kunnat gälla ”behövliga uppgifter” för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om informationsinnehållen däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på ”att informationen är nödvändig” för ett visst ändamål. I sina analyser av exakthet och innehåll har grundlagsutskottet lagt särskild vikt vid huruvida de uppgifter som lämnas ut är av känslig art. Om de föreslagna bestämmelserna om överlåtelse av uppgifter har gällt också känsliga uppgifter, har det för vanlig lagstiftningsordning krävts att bestämmelserna preciseras så att de följer grundlagsutskottets ovan återgivna praxis för bestämmelser som rör rätten att få och att lämna ut myndighetsuppgifter trots sekretess. Samtidigt har utskottet inte ansett att mycket vaga och ospecificerade rättigheter att få uppgifter är möjliga ur grundlagssynvinkel ens i sådana fall där de är knutna till nödvändighetskriteriet (se t.ex. GrUU 4/2021 rd, 10 punkten och de utlåtanden som nämns där).

Statsrådet anser att bestämmelserna i förordningen bör preciseras för att förtydliga dess förhållande till offentlighetsprincipen. Dessutom bör det klargöras i vilken utsträckning förordningen förpliktar till informationsutbyte och om informationsutbytet omfattar utbyte av sekretessbelagda uppgifter enligt offentlighetslagen, utbyte av personuppgifter eller utbyte av uppgifter om innehållet i eller förmedlingsuppgifter om kommunikation. Statsrådet anser att de konstitutionella villkoren för informationsutbytet måste beaktas bättre i förslaget. Statsrådet anser också att förslaget behöver preciseras så att t.ex. datainnehåll som ska utbytas, skyddsåtgärder, användningsändamål och förstöring av uppgifter inte ska vara beroende av samarbetsavtal (artikel 6.4) eller kommissionens genomförandeakter (artiklarna 6.3, 7.2 och 8.3), utan att dessa endast ska gälla tekniska aspekter.

Det finns också skäl att bedöma användningen av den föreslagna EU-cybersäkerhetsreserven med hänsyn till ovannämnda aspekter. Användningen av cyberreserven innebär lämnande av uppgifter (artiklarna 12.4, 12.5 och 14.6).

Egendomsskydd och näringsfrihet (GrL 15 och 18 §)

Enligt 15 § i grundlagen är vars och ens egendom tryggad.

Enligt grundlagens 18 § 1 mom. har var och en rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt.

Den föreslagna cyberkrismekanismen omfattar samordnad beredskapstestning inom kritiska sektorer (artikel 11). Om testningen är avsedd att vara obligatorisk medför den enligt statsrådets uppfattning kostnader för aktörerna. Då bör den föreslagna regleringen preciseras för att uppfylla kraven på exakthet och noggrann avgränsning när det gäller begränsning av egendomsskyddet.

EU-cybersäkerhetsreserven ska bestå av incidenthanteringstjänster från betrodda leverantörer som valts ut i enlighet med fastställda kriterier (artikel 12.1). Cybersäkerhetsreserven ska tydligen inrättas genom ett upphandlingsförfarande (artikel 16.1). Medlemsstaterna och unionsorganen får av allt att döma anlita leverantörer i reserven endast för insatser eller stöd till insatser till följd av betydande eller storskaliga incidenter som påverkar entiteter som är verksamma

inom kritiska eller högkritiska sektorer (artikel 12.4). Detta innebär att endast vissa aktörer får tillhandahålla dessa tjänster till myndigheter och unionsorgan. I och för finns det en godtagbar orsak till begränsningen av näringsfriheten, dvs. målet att säkerställa förmågan att hantera allvarliga cybersäkerhetsincidenter genom högkvalitativa externa tjänster. Även användningen av ett upphandlingsförfarande för att välja ut aktörerna – förutsatt att förfarandet är öppet och rättvist – minskar graden av begränsning. Statsrådet anser dock att den föreslagna regleringen delvis bör förtydligas och vid behov preciseras (se t.ex. GrUU 60/2001 rd, s. 4/II). Detta gäller t.ex. om förfarandet är jämförbart med tillstånds- eller anmälningsplikt (se GrUU 69/2014 rd, s. 2/II), om behörighetskraven har angetts tillräckligt noggrant (jfr GrUU 8/2005 rd, s. 3) och om det är fråga om bunden prövning eller ändamålsenlighetsprövning (se GrUU 69/2014 rd, s. 2/II).

Statsrådet konstaterar att certifieringstvång för leverantörer (16.2 j) medför kostnader för leverantörerna och därmed utgör en begränsning av deras egendomsskydd. Statsrådet anser dock att detta kan motiveras med samma godtagbara skäl som ovannämnda begränsning av näringsfriheten. Kraven för att få certifiering måste dock bedömas ytterligare för att man ska kunna säkerställa att kraven är proportionerliga.

Övrigt

Den rättsliga grunden och delegeringen av befogenheter behandlas i avsnitten ovan. Dessa är EU-rättsliga frågor. Grundlagsutskottet har dock ansett det viktigt att unionslagstiftningen i första hand utvecklas inom ramen för fördragen (se t.ex. GrUU 31/2022 rd, punkt 8). Grundlagsutskottet har också fäst uppmärksamhet vid delegering av befogenheter (se t.ex. GrUU 37/2021 rd, punkt 42).

7 Ålands behörighet

I cybersolidaritetsakten föreslås bestämmelser om samarbetet mellan medlemsstater och unionsorgan på cybersäkerhetsområdet och tillgången till stöd från aktörer som ingår i cyberreserven. De föreslagna ändringarna av cybersäkerhetsakten innebär att även leverantörer av hanterade säkerhetstjänster omfattas av skyldigheterna i förordningen och möjliggör skapandet av ett gemensamt certifieringssystem för dem. Cybersäkerhet nämns inte uttryckligen i självstyrelselagen. Frågan ska därför bedömas enligt kriterierna för behörighetsfördelningen mellan landskapet och riket som anger vad som hör till landskapet och vad som hör till riket. Enligt 27 § i självstyrelselagen för Åland (1144/1991) har riket lagstiftningsbefogenhet i fråga om statsmyndigheternas organisation och verksamhet (3 punkten) och televerksamhet (40 punkten). Enligt 18 § i självstyrelselagen har landskapet däremot lagstiftningsbehörighet i frågor som rör landskapsregeringen och under denna lydande myndigheter och inrättningar (1 punkten). I samband med lagstiftningskontrollen har det ansetts att offentligheten för handlingar som innehas av myndigheter och skyddet av personuppgifter som innehas av dessa är frågor som hör till landskapets lagstiftningsbehörighet.

Statsrådet anser att den föreslagna regleringen hör till rikets lagstiftningsbehörighet. De frågor som ingår i förslaget har samband med televerksamhet och statliga myndigheters befogenheter (Cybersäkerhetscentret vid Transport- och kommunikationsverket). Så som beskrivs ovan är cybersolidaritetsaktens förhållande till offentlighets- och dataskyddsregleringen oklart. Enligt statsrådets uppfattning påverkar regleringen dock inte landskapets myndigheters informationshantering till denna del, eftersom de inte deltar i samarbetet annat än genom att eventuellt få hjälp från cybersäkerhetsreserven. Statsrådet konstaterar för tydlighetens skull att den föreslagna cybersolidaritetsakten inte ändrar myndigheternas skyldighet att förbereda sig på cyberhot och därmed inte ändrar de skyldigheter som gäller informationshanteringen vid landskapets myndigheter.

8 Behandlingen av förslaget i Europeiska unionens institutioner och de övriga medlemsstaternas ståndpunkter

Kommissionen lade fram förslaget till förordning den 18 april 2023.

Behandlingen av förslaget inleddes i rådets övergripande arbetsgrupp för cyberfrågor den 26 april 2023. Behandlingen av förslaget i Europaparlamentet har ännu inte inletts.

9 Nationell behandling av förslaget

U-skrivelsen har beretts vid kommunikationsministeriet i samarbete med statsrådets kansli, finansministeriet, justitieministeriet, arbets- och näringsministeriet, utrikesministeriet, inrikesministeriet, försvarsministeriet samt Transport- och kommunikationsverket och Försvarsmakten.

Ett utkast till U-skrivelse har behandlats i sektionen för kommunikation (EU-19) 29.5.2023–2.6.2023 och sektionen för hybridhot och krisberedskap (EU-13) 29.5.2023–2.6.2023. Dessutom hölls samråd om förslaget med myndigheterna den 3 maj 2023 och med den privata sektorn den 8 maj 2023.

10 Statsrådets ståndpunkt

10.1 Förslaget till cybersolidaritetsakt

Statsrådet anser att cybersäkerhet är avgörande för att EU:s inre marknad ska fungera utan störningar och för att säkerställa social stabilitet och medborgarnas integritet. Statsrådet understöder målen för det föreslagna cybersolidaritetsinitiativet, men konstaterar att ytterligare information behövs om initiativets uppskattade konsekvenser och kostnader.

När det gäller cyberhot betonar statsrådet vikten av en enhetlig strategi, informationsutbyte och en gemensam lägesbild samt krisberedskap i unionen för att hantera cybersäkerhetsutmaningarna. Statsrådet anser att det ligger i Finlands intresse att stärka cybersäkerheten också genom EU:s gemensamma åtgärder och att söka och utnyttja synergier mellan nationella åtgärder och unionsåtgärder. Statsrådet anser att en övergripande utveckling av EU:s krisresiliens är central.

Statsrådet understöder åtgärder som främjar informationsutbyte om cybersäkerhetsincidenter mellan medlemsstaterna. Statsrådet konstaterar dock att man vid inrättandet av nya lägesbilds- och informationsutbytesfunktioner bör undvika överlappningar med befintliga funktioner. Statsrådet anser att ytterligare information behövs både om informationsutbytet mellan de nationella säkerhetscentrumen och konsortierna av gränsöverskridande säkerhetscentrum och om delegeringen av befogenheter till kommissionen.

När det gäller cyberkrismekanismen välkomnar statsrådet de samordnade åtgärderna för att stärka beredskapen för cyberincidenter i kritiska sektorer. Statsrådet anser att det är särskilt viktigt att främja kritiska aktörers fysiska och digitala resiliens och beredskap i EU. När det gäller cybersäkerhetsreserven understöder statsrådet åtgärder som kan bromsa eller förhindra spridning av betydande eller storskaliga cybersäkerhetsincidenter. Med beaktande av proportionalitetsprincipen anser statsrådet att det är viktigt att de finansiella instrumenten inte skapar incitament som försvagar medlemsstaternas benägenhet att utveckla egen cybersäkerhetskapacitet.

På grund av cyberhotens gränsöverskridande karaktär ställer sig statsrådet positivt till att utöka cybersäkerhetsreservens tjänster till att även omfatta tredjeländer. Statsrådet anser det viktigt att cyberkrismekanismen och cybersäkerhetsreserven främjar affärsmöjligheterna på den inre marknaden för finländska företag inom cybersäkerhetsbranschen.

Statsrådet ställer sig i princip positivt till den föreslagna mekanismen för granskning av cyberincidenter, men ytterligare information behövs om dess funktion samt om utlämnande av information och informationsutbyte inom mekanismen. Statsrådet ställer sig avvaktande till informationsutbyte som kan få negativa konsekvenser för den nationella säkerheten.

Statsrådet ser programmet för ett digitalt Europa som EU:s väsentliga åtagande att stödja den digitala omställningen. I synnerhet kommer satsningar på strategiska projekt såsom artificiell intelligens och cybersäkerhet att stödja EU:s tillväxt och konkurrenskraft. När det gäller ändringar av finansieringen av programmet för ett digitalt Europa betonar statsrådet behovet av att ytterligare analysera vilka konsekvenser en eventuell omfördelning av de finansiella instrumenten får för deras ursprungliga syften.

Statsrådet har reservationer mot den föreslagna ändringen av programmet för ett digitalt Europa, som i fråga om outnyttjade åtagande- och betalningsbemyndiganden innebär ett undantag från principen om ettårighet, enligt vilken outnyttjade anslag ska förfalla vid utgången av budgetåret (se U 78/2022 rd om omarbetning av budgetförordningen). Det förfarande som kommissionen föreslår är särskilt exceptionellt med tanke på att medlen ska användas automatiskt och inte diskretionärt under de kommande budgetåren.

Statsrådet anser att de operativa uppgifterna inom cybersäkerhet på unionsnivå fortfarande bör skötas av Europeiska cybersäkerhetsbyrån Enisa i första hand. Statsrådet anser att Enisa i sin verksamhet bör undvika överlappningar med de nationella myndigheternas verksamhet. Statsrådet anser det viktigt att man vid granskningen av de tilläggsuppgifter som föreslås för cybersäkerhetsmyndigheterna strävar efter att tygla den extra administrativa bördan son förslaget medför.

Statsrådet anser att förslagets koppling till industrin och tillnärmningen av lagstiftningen bör preciseras med hänsyn till den rättsliga grunden för förslaget. Statsrådet anser att man vid den fortsatta beredningen särskilt bör bedöma förslagets förhållande till den nationella säkerheten, som uteslutande är varje medlemsstats ansvar.

När det gäller subsidiaritetsprincipen påpekar statsrådet att utnämningen av ett nationellt säkerhetscentrum inte bör begränsa medlemsstaternas administrativa autonomi.

10.2 Föreslagna ändringar i cybersäkerhetsakten

Statsrådet anser det viktigt att förslaget syftar till att stärka informationssäkerheten i hela EU och förbättra tillgången till cybersäkra tjänster på den inre marknaden.

Statsrådet anser det viktigt att standardiserings- och certifieringsverksamheten för cybersäkra produkter och tjänster gynnar finländska företag, men inte orsakar dem en extra administrativ börda som hämmar deras konkurrenskraft. Målen för den föreslagna ramen för certifiering av

betrodda leverantörer kan anses värda att stödjas i den mån som regleringen syftar till att öka förtroendet för den digitala inre marknaden, minska företagens kostnader för certifiering och förbättra kvaliteten och säkerheten i cybersäkerhetstjänster. De föreslagna metodernas och förfarandenas effektivitet i förhållande till det eftersträvade målet måste dock bedömas noggrant. Statsrådet anser det viktigt att certifieringen av betrodda leverantörer främjar affärsmöjligheterna på den inre marknaden för finländska företag inom cybersäkerhetsbranschen.