U 17/2026 rd

Statsrådets skrivelse till riksdagen om förslag till Europaparlamentets och rådets cybersäkerhetsakt (CSA2) och direktiv om ändring av NIS 2-direktivet

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen kommissionens förslag av den 20 januari 2026 till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå Enisa, europeiska ramen för cybersäkerhetscertifiering och säkerheten i leveranskedjor för informations- och kommunikationsteknik samt till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2055 (NIS 2) för att förenkla och harmonisera åtgärderna [med cybersäkerhetsakt 2, nedan *CSA2*].

Helsingfors den 12 mars 2026

Kommunikationsminister Lulu Ranne

Överinspektör Eevi Vuorinen

KOMMUNIKATIONSMINISTERIET | PROMEMORIA | EU/385/2026 EU/388/2026

12.3.2026

FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS CYBERSÄKERHETSAKT (CSA2) OCH DIREKTIV OM ÄNDRING AV NIS 2-DIREKTIVET

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen kommissionens förslag av den 20 januari 2026 till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå Enisa, europeiska ramen för cybersäkerhetscertifiering och säkerheten i leveranskedjor för informations- och kommunikationsteknik samt förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2055 (NIS 2) för att förenkla och harmonisera åtgärderna [med cybersäkerhetsakt 2, nedan *CSA2*].

1 Bakgrund

Europeiska kommissionen gav den 20 januari 2026 ett förslag (COM(2026) 11 final) till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå Enisa, europeiska ramen för cybersäkerhetscertifiering och säkerheten i IKT-leveranskedjor samt om upphävande av förordning (EU) 2019/881 (CSA2-förslaget). Genom CSA2-förslaget upphävs Europaparlamentets och rådets förordning (EU) 2019/881 om Europeiska unionens cybersäkerhetsbyrå Enisa och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten, CSA) som trädde i kraft 2019. Enligt gällande CSA ska kommissionen senast den 28 juni 2024, och därefter vart femte år, utvärdera effekterna av och ändamålsenligheten och effektiviteten hos Enisas arbete samt dess arbetsmetoder, det eventuella behovet av att ändra Enisas mandat samt de finansiella följderna av sådana ändringar. Det har dessutom varit meningen att utvärderingen ska bedöma effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer i unionen och förbättra den inre marknadens funktion (ordningar för cybersäkerhetscertifiering).

I samband med översynen av CSA observerades att Enisas uppgifter och resurser inte motsvarade det faktiska behovet av exempelvis funktioner som stöder medlemsstaterna och organisationerna. I fråga om den europeiska ramen för cybersäkerhetscertifiering visade översynen att utnyttjandet av ramverket inte på behövligt sätt förhindrade en fragmentering av den inre marknaden och att processerna i anslutning till den ansågs ineffektiva. Vid tidpunkten för publiceringen av CSA2 användes endast en ordning för cybersäkerhetscertifiering (*EU Cybersecurity Certification Scheme on Common Criteria*) och fyra var i beredningsskedet.

Bakgrunden till CSA2-förslaget är en ständig förändring av hotbilden inom cyberområdet som innebär att Europa dagligen utsätts för cyber- och hybridhot som riktar sig mot kritiska tjänster och demokratiska institutioner. Både i EU:s strategi för en beredskapsunion och i strategin för den inre säkerheten (*ProtectEU*) är cybersäkerheten i centrum för EU:s resiliens. Även i EU:s meddelande om en europeisk strategi för ekonomisk säkerhet betonas att skydd av känslig information och förebyggande av störningar i kritisk infrastruktur är viktiga mål för säkerheten. För att svara på växande och föränderliga hot mot cybersäkerheten och cyberattacker har Europeiska kommissionen föreslagit en ny cybersäkerhetsakt som stärker cybersäkerheten och förmågan att agera. Bakgrunden till förslaget har dessutom varit ett behov av att harmonisera och förenkla de metoder som medlemsstaterna använder för att reagera på störningar och hot mot cybersäkerheten.

År 2019 genomfördes en bedömning av säkerhetsriskerna med 5G-näten inom EU. I riskbedömningarna identifierade medlemsstaterna både tekniska och strategiska risker. En samordnad riskbedömning på EU-nivå genomfördes i en 5G-underarbetsgrupp till NIS-samarbetsgruppen (*Network and Information Security Cooperation Group*) i ett samarbete mellan medlemsstaterna, kommissionen och EU:s cybersäkerhetsbyrå (nedan Enisa). År 2020 utarbetade medlemsstaterna i samma samarbetsstruktur och utifrån riskbedömningen gemensamma 5G-rekommendationer som NIS-samarbetsgruppen godkände i januari 2020. Syftet med rekommendationerna är att hantera de strategiska och tekniska risker i 5G-näten som identifierats i anslutning till riskbedömningen. Medlemsstaterna har delvis genomfört rekommendationerna genom olika lösningar. Kommissionen har försökt främja genomförandet av 5G-rekommendationerna i medlemsstaterna, i synnerhet i fråga om den strategiska rekommendationen som gäller hanteringen av risker i anslutning till högriskleverantörer. Den 15 juni 2023 utfärdade kommissionen ett meddelande om läget i fråga om genomförandet av 5G-verktygslådan och betonade de risker som vissa leverantörer av utrustning till mobilnäten medför för unionens säkerhet samt uppmanade medlemsstaterna att vidta åtgärder för att hantera riskerna. I EU:s strategi för den inre säkerheten och strategin för en beredskapsunion ses stärkandet av leveranskedjorna för informations- och kommunikationsteknik (IKT) som ett viktigt mål.

För att stärka säkerheten i IKT-leveranskedjorna har det beretts rekommendationer i EU om IKT-leveranskedjorna (IKT-verktygslådan eller *ICT Toolbox*) som följer strukturen i verktygslådan för 5G-säkerhet (5G-verktygslådan eller *5G Toolbox*). Rekommendationerna som gäller IKT-leveranskedjorna har beretts i en underarbetsgrupp till NIS-samarbetsgruppen som utvärderar säkerheten i leveranskedjorna i samarbete med medlemsstaterna, kommissionen och EU:s cybersäkerhetsbyrå Enisa. Rekommendationerna gäller huvudsakligen medlemsstaterna. Rekommendationerna som gäller IKT-leveranskedjorna hänför sig också till artikel 22 i NIS 2-direktivet, eftersom de skapar en ram för att utföra samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor i enlighet med artikeln. Även om rekommendationerna huvudsakligen gäller medlemsstaterna kan även till exempel entiteter som omfattas av NIS 2-direktivet utnyttja dem i samband med bedömning av riskerna för IKT-leveranskedjorna och för att bedöma nödvändiga åtgärder. Rekommendationerna godkändes och publicerades i början av 2026.

Samtidigt som CSA2-förslaget lade kommissionen fram förslag (COM(2026) 13 final) till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2055 (NIS 2) för att förenkla och harmonisera det med CSA2-förslaget (förslag till ändring av NIS 2). Eftersom förslaget till ändring av NIS 2 är nära kopplat till CSA2-förslaget behandlas förslagen i samma skrivelse. Det föreslås att NIS 2-direktivets tillämpningsområde utvidgas till att omfatta leverantörer av undervattensinfrastruktur, entiteter inom energi- och kemiindustrin och leverantörer av europeiska e-identitetsplånböcker och digitala företagsplånböcker.

2 Förslagets syfte

Det finns två huvudsyften med reformen av cybersäkerhetsakten: att höja cybersäkerhetens kapacitet och resiliens samt att förebygga splittring av den inre marknaden. Syftet är för det första att stärka förvaltningen av cybersäkerheten inom EU och att säkerställa att behöriga organ, myndigheter och andra intressenter har bättre förutsättningar att förebygga, upptäcka och bekämpa cybersäkerhetshot på ett samordnat och effektivt sätt. Vidare är målet med översynen av cybersäkerhetsakten att stödja utvecklingen, genomförandet och införandet av gemensamma cybersäkerhetsverktyg såsom certifieringsordningar i unionen, samt att erbjuda harmoniserade metoder för att bygga upp förtroende och interoperabilitet mellan medlemsstaterna. Förslaget syftar till att utveckla den europeiska ramen för cybersäkerhetscertifiering, hitta lösningar på de

komplicerade och fragmenterade processerna i anslutning till cybersäkerheten och ingripa i de ökande säkerhetsriskerna i anslutning till IKT-leveranskedjorna. Målet är att harmonisera de icke-tekniska åtgärderna för hantering av cybersäkerhetsrisker i anslutning till IKT-leveranskedjorna inom EU, inklusive kommunikationsnäten, i syfte att säkerställa att den inre marknaden fungerar, stödja den tekniska suveräniteten och stärka nivån på EU:s gemensamma cybersäkerhet och resiliens. Det är fråga om skyldigheter på miniminivå. Medlemsstaterna ska ha möjlighet att ställa nationella åtgärder som går längre än skyldigheterna i förslaget och som är i linje med unionsrätten.

Enligt kommissionen är målen i direktivet om ändring av NIS 2 -direktivet en del av genomförandet av målen med översynen av cybersäkerhetsakten. Målet med den riktade ändringen i direktivet om ändring av NIS 2-direktivet är att förenkla överensstämmelsen med kraven i NIS 2-direktivet och att genomföra det mer konsekvent. Detta omfattar preciseringar av NIS 2-direktivets tillämpningsområde, definitioner, anmälan om utpressningsprogram och kontroll av entiteter som tillhandahåller gränsöverskridande tjänster. Målet är dessutom att förenkla regleringen och sänka de kostnader som regleringen innebär för entiteterna.

3 Förslagets huvudsakliga innehåll

3.1 Huvudsakligt innehåll i förslaget till cybersäkerhetsakt (CSA2)

3.1.1 EU:s cybersäkerhetsbyrå Enisas mandat och uppgifter

I förslaget till förordning föreslås att EU:s cybersäkerhetsbyrå Enisas uppgifter förtydligas och uppdateras så att de motsvarar hotbilden inom cybersäkerhet. I framtiden kommer syftet med Enisas verksamhet att vara att stärka EU:s och medlemsländernas cybersäkerhet, cyberresiliens och förtroende. Byrån ska fungera som central rådgivare och ett expertcentrum för cybersäkerhet i hela unionen. Enisas uppgift ska bland annat vara att stödja medlemsstaterna och EU-organen i utvecklingen och verkställandet av EU-lagstiftningen och politiken i anslutning till cybersäkerhet, stärka cybersäkerhetsberedskapen och resiliensen i hela EU, främja det operativa samarbetet och informationsutbytet, delta i utvecklingen och upprätthållandet av EU:s ordning för cybersäkerhetscertifiering samt främja kompetensen och utbildningen inom cybersäkerhet.

Enisas uppgifter

I förslaget till förordning är Enisas arbetsfält indelat i stöd för verkställande av unionens lagstiftning och politik, operativt samarbete, cybersäkerhetscertifiering och standardisering samt verkställande av akademin för cyberkompetens.

I fråga om stöd för verkställande av lagstiftning är förslaget att Enisa bland annat ska kunna ge medlemsländer och organisationer tekniska anvisningar, lämna rapporter, ge råd och dela bästa praxis samt stödja informationsutbytet mellan myndigheterna. Det skulle främja spridningen av information om cybersäkerhet inom och mellan olika sektorer, i synnerhet inom de sektorer som omfattas av NIS 2-direktivet. På kommissionens begäran ska Enisa också kunna ge riktat tekniskt stöd till medlemsländerna till exempel inom riskhantering och bedömning av cyberkapacitet. I förhållande till de tidigare uppgifterna föreslås Enisa få nya övergripande uppgifter i anslutning till uppbyggnaden av cybersäkerhetskapaciteten inklusive väldigt detaljerade uppgifter, såsom att stödja organisationer när de ska ordna cyberövningar. I enlighet med NIS 2-direktivet kan Enisa stödja medlemsländerna i utvecklingen av enheter för hantering av it-säkerhetsincidenter (*Computer Security Incident Response Team, CSIRT*) och i beredningen av strategier för cybersäkerhet.

Det föreslås att Enisas mandat i fråga om operativa cybersäkerhetsuppgifter ska utvidgas i betydande grad. I fortsättningen skulle Enisa i synnerhet via CSIRT-nätverket bestående av medlemsländernas CSIRT-enheter och Europeiska kontaktnätverket för cyberkriser (*European Cyber Crisis Liaison Organisation Network*, *EU-CyCLONe)* stödja medlemsländerna genom att på deras begäran erbjuda expertbedömningar och stöd vid cyberhot, analysera sårbarheter och bistå i hanteringen av storskaliga cyberkriser på EU-nivå och i samordningen av informationsutbytet. I förslaget föreslås dessutom preciseringar i de säkra medier som Enisa använder.

Det föreslås även preciseringar i Enisas skapande av en lägesbild. I fortsättningen skulle Enisa bland annat framställa tidiga varningar om cyberhot, analysera hot och risker, komma med tekniska analyser och producera mer omfattande rapporter om hotlandskapet. Enisa skulle också kunna stödja medlemsländerna i samband med att de ordnar cybersäkerhetsövningar.

En ny förmåga som Enisa dessutom skulle få i uppgift är att utveckla en gemensam förmåga för hela EU att hantera sårbarheter i informationssystemen. Enisa ska upprätthålla en europeisk sårbarhetsdatabas som upprättas med stöd av NIS 2-direktivet och som samlar information om kända IKT-sårbarheter och stöder medlemsländer och intressenter i arbetet med sårbarheter.

I fråga om cybersäkerhetscertifiering ska Enisa även i fortsättningen utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering. I fortsättningen ska Enisa även upprätthålla godkända certifieringsordningar och bereda eventuella mindre ändringar som gäller dem och främja ibruktagandet av godkända ordningar. Enisa ska även följa upp och vid behov delta i arbetet med att standardisera cybersäkerheten på EU-nivå och internationellt och främja införandet av europeiska och internationella cybersäkerhetsstandarder.

I förslaget föreslås ett fjärde delområde i form av en starkare roll för Enisa i stärkandet av cybersäkerhetskompetensen och genomförandet av EU-akademin för cyberkompetens (*Cybersecurity Skills Academy* COM(2023) 207 final). Förslaget fastställer att Enisa ska utarbeta och upprätthålla en europeisk kompetensram för cybersäkerhet (*European Cybersecurity Skills Framework ECSF*) som fastställer de roller som ingår i cybersäkerhetsexperternas uppgifter och de färdigheter och kompetenskrav som hör samman med dessa. Enisa bör ha ett nära samarbete med medlemsländerna när byrån bereder ramen. I framtiden kan separat auktoriserade kompetensverifierare på basis av kompetensramen bevilja europeiska kompetensintyg till yrkespersoner inom cybersäkerhet. Enisa kan även samla in avgifter av auktoriserade kompetensverifierare. Det skulle vara frivilligt för medlemsländer och yrkespersoner inom cybersäkerhet att använda sig av kompetensramen.

Innehåll som rör Enisas förvaltning

Förslaget innehåller bestämmelser om Enisas verksamhet som gäller budgetering, personalfrågor och ledning av byrån. Byråns administrativa struktur ska i fortsättningen bestå av en direktion, en styrelse, en generaldirektör, en vice generaldirektör, en rådgivande grupp samt en besvärsnämnd. Vice generaldirektören och besvärsnämnden är nya strukturer. Däremot skulle nätverket av nationella kontaktpersoner avskaffas.

Enisas direktion ska även i fortsättningen fastställa de allmänna riktlinjerna för byråns verksamhet och utse en generaldirektör. Generaldirektören ansvarar för den dagliga ledningen av byrån och rapporterar till direktionen. Styrelsen bereder direktionens beslut. Den rådgivande gruppen ska vara ett sakkunnigorgan med representanter från den privata sektorn, konsumentorganisationerna och andra centrala intressenter. I detta avseende motsvarar huvuddragen i förslaget byråns nuvarande verksamhet.

Ett nytt förslag i fråga om beslutsfattandet i Enisas direktion är att kommissionen i fortsättningen ska ha vetorätt i beslut som gäller budget- och personalfrågor i direktionen. I fortsättningen ska dessutom medlemsländerna i första hand som sin representant i direktionen utse direktören för den nationella behöriga myndigheten enligt NIS 2-direktivet eller någon annan representant på hög nivå från myndigheten i fråga. Direktionen kan också besluta att inrätta en ny uppgift som vice generaldirektör för byrån. Vice generaldirektören ska ha i uppgift att stödja generaldirektören i arbetet med att leda byrån och sköta uppgifter samt fungera som ställföreträdare för generaldirektören.

I förslaget föreslås också att en oberoende besvärsnämnd ska inrättas, vilket byrån inte har haft tidigare. Besvärsnämnden ska kunna behandla besvär som gäller auktoriserade tjänsteleverantörers ansökningar om verifiering av kompetens. Enisa ska även i fortsättningen kunna samla in avgifter av auktoriserade kompetensverifierare för ansökningar om verifiering av kompetens inom cybersäkerhetsfärdigheter, av organ för bedömning av överensstämmelse med kraven när de deltar i beviljandet av europeiska cybersäkerhetscertifikat samt av offentliga myndigheter eller privata entiteter för testning av verktyg. Avgifterna ska täcka kostnaderna för denna verksamhet.

De ändringar i byråns verksamhetsfält som ingår i förslaget skulle även förutsätta en betydande ökning av Enisas resurser och personalantal. Medlemsländerna ska i fortsättningen utse två nationella experter som fungerar som deras kontaktpersoner (*liaison officer*) vid byrån. Lönekostnaderna för dessa experter ska i första hand täckas av medlemsländerna. Enisa ska fritt kunna utnyttja de nationella experterna i olika uppgifter. Tjänsteföreskrifterna och anställningsvillkoren som gäller EU:s tjänstemän ska inte gälla de nationella experterna.

3.1.2 Europeisk ram för cybersäkerhetscertifiering

Syften, tillämpningsområde och processer

I förslaget till förordning föreslås reformer i regleringen av den europeiska cybersäkerhetscertifieringen. Med ett EU-omfattande cybersäkerhetscertifikat går det att påvisa att föremålet för certifieringen uppfyller de tekniska cybersäkerhetskrav som fastställts i en lämplig certifieringsordning. Förordningen ska även i fortsättningen innehålla bestämmelser om utveckling och användning av europeiska cybersäkerhetscertifikat, men den ska inte innehålla certifieringsskyldigheter. I regel ska det alltså vara frivilligt att ansöka om och utnyttja europeiska cybersäkerhetscertifikat, om inte något annat bestäms särskilt. Dessutom ska det europeiska cybersäkerhetscertifikatet och försäkran om överensstämmelse erkännas automatiskt i alla medlemsstater.

Genom förslaget förnyas ramen för europeisk cybersäkerhetscertifiering, med stöd av vilken ordningarna för cybersäkerhetscertifiering bedömer om IKT-produkter, IKT-tjänster, IKT-processer och säkerhetstjänster uppfyller cybersäkerhetskraven. Dessutom gör förslaget det möjligt att göra en bedömning av organisationers arbete på cyberområdet (*cyber posture*) och utnyttja certifieringen för att påvisa överensstämmelse med kraven i Europeiska unionens lagstiftning. I förslaget framförs det att bedömningsåtgärderna (*evaluation activities*) i ordningarna för cybersäkerhetscertifiering vid bedömningen av överensstämmelse med kraven ska överensstämma med tillämpliga EU-rättsakter, vilket leder till presumtion om överensstämmelse (*presumption of conformity*). Om vissa bedömningsåtgärder inte hade fastställts i unionsrätten, skulle certifieringsordningen kunna användas för att precisera kriterierna. Enligt förslaget ska bedömningen av överensstämmelse med kraven i regel göras av en tredje part.

I och med förslaget ökar verksamhetens transparens och olika entiteters delaktighet. Kommissionen ska med stöd från Enisa minst en gång om året ordna ett möte om cybersäkerhetscertifiering (*European Cybersecurity Certification Assembly*), till vilket medlemmar av europeiska gruppen för cybersäkerhetscertifiering (*ECCG*), experter från medlemsstaterna och unionens organisationer samt relevanta intressenter bjuds in. Dessutom ska kommissionen upprätthålla och uppdatera en webbplats där europeiska ordningar för cybersäkerhetscertifiering som ska utvecklas samt strategiska prioriteringar för harmonisering av säkerhetskraven för informations- och kommunikationstekniska produkter, tjänster och processer samt arbete på cyberområdet och EU-lagstiftning görs tillgängliga. Enisa ska också upprätthålla en webbplats där europeiska ordningar för cybersäkerhetscertifiering, avgifter för underhåll av dem, beviljade europeiska cybersäkerhetscertifikat och försäkran om överensstämmelse med kraven, sakkunnigbedömningar, tekniska specifikationer och relevant tilläggsinformation publiceras.

Enligt förslaget ska kommissionen kunna be Enisa bereda ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer samt säkerhetstjänster och arbete på cyberområdet. Enisa ska upprätta en ordning för cybersäkerhetscertifiering inom 12 månader efter kommissionens begäran. När certifieringsordningen bereds bör Enisa ha ett nära samarbete med europeiska gruppen för cybersäkerhetscertifiering och involvera behöriga myndigheter i medlemsstaterna.

Dessutom föreslås det i förslaget att varje ordning för cybersäkerhetscertifiering ska ha en underhållsstrategi (*maintenance strategy*) och tillhörande underhållsmetoder. Enligt förslaget ska Enisa upprätthålla europeiska ordningar för cybersäkerhetcertifiering i samarbete med kommissionen, europeiska gruppen för cybersäkerhetscertifiering och medlemsstaterna. Enligt förslaget ska Enisa bedöma effekterna av och effektiviteten hos en ordning för cybersäkerhetcertifiering minst vart fjärde år efter att den har tagits i bruk. Dessutom kan Enisa utveckla tekniska specifikationer för framtida europeiska ordningar för cybersäkerhetscertifiering eller upprätthållandet av dem.

Innehåll i europeiska ordningar för cybersäkerhetscertifiering

Förslaget innehåller säkerhetsmål för den europeiska ordningen för cybersäkerhetscertifiering till exempel i fråga om komponenter, sårbarheter, incidenthantering och interna processer. I förslaget fastställs dessutom minimikrav för den europeiska ordningen för cybersäkerhetscertifiering, till exempel en beskrivning av ordningens föremål, tillämpningsområde och funktionssätt; en redogörelse för certifieringsordningens syfte; en underhållsstrategi; cybersäkerhetskrav, bedömningskriterier och metoder. Utöver detta föreslås minimiregler och villkor som styr ramen för cybersäkerhetscertifiering bland annat i fråga om uppföljning av överensstämmelse med kraven, påförande av påföljder och konfidentiell behandling av information.

Enligt förslaget kan det i den europeiska ordningen för cybersäkerhetscertifiering ställas en eller flera assuransnivåer för IKT-produkter, IKT-tjänster och IKT-processer samt säkerhetstjänster och arbete på cyberområdet. Assuransnivåerna ”grundläggande”, ”betydande” eller ”hög” ska överensstämma med riskerna i anslutning till produkterna, tjänsterna och processerna samt säkerhetstjänstens användningsändamål, verksamhetens art och omständigheterna. I förslaget föreslås miniminivåer för assuransnivåerna och närmare krav ska fastställs i certifieringsordningarna. Den europeiska ordningen för cybersäkerhetscertifiering kan göra det möjligt med självbedömning av överensstämmelse när det är fråga om ett ”grundläggande” certifikat.

Förvaltning av den europeiska ramen för cybersäkerhetscertifiering

Enligt kommissionens förslag skulle certifiering av IKT-produkter, IKT-tjänster och IKT-processer samt leverantörer av säkerhetstjänster och arbete på cyberområdet skapa presumtion om överensstämmelse med kraven i fråga om certifieringsordningens tillämpningsområde. Organen för bedömning av överensstämmelse ska bevilja cybersäkerhetscertifikat i enlighet med kraven i den aktuella ordningen för cybersäkerhetcertifiering. Bilaga 1 till förslaget ska innehålla definitioner av de krav som ställs på organen för bedömning av överensstämmelse bland annat i fråga om deras opartiskhet. I ordningen för cybersäkerhetscertifiering går det att förutsätta att certifikat endast kan beviljas av en ackrediterad nationell myndighet för cybersäkerhetscertifiering eller ett ackrediterat offentligt organ.

Enligt förslaget ska de nationella ordningarna för cybersäkerhetscertifiering, som gäller områdena för de europeiska ordningarna för cybersäkerhetscertifiering och tillämpningsområdet för dem, upphöra i och med förslaget om fastställande av en europeisk ordning för cybersäkerhetscertifiering. Medlemsstaterna ska inte få skapa nya nationella ordningar för cybersäkerhetscertifiering om det redan finns en europeisk ordning för cybersäkerhetscertifiering inom ämnesområdet och tillämpningsområdet i fråga. Dessutom kan tredjelandscertifikat erkännas som likvärdiga med det europeiska cybersäkerhetscertifikatet om kraven på certifikaten överensstämmer.

Enligt kommissionens förslag ska varje medlemsstat utse en eller flera nationella myndigheter för cybersäkerhetscertifiering. Alternativet är att på begäran utse en eller flera myndigheter för cybersäkerhetscertifiering i en annan medlemsstat till att ansvara för tillsynsuppgifterna i den medlemsstat som framför begäran.

De nationella myndigheterna för cybersäkerhetscertifiering bör övervaka och anmäla organ för bedömning av överensstämmelse med kraven; delta i bland annat Europeiska gruppen för cybersäkerhetscertifiering; övervaka och följa genomförandet och efterlevnaden av de europeiska ordningarna för cybersäkerhetcertifiering; behandla klagomål som gäller cybersäkerhetcertifikat samt ge årliga rapporter till kommissionen, Enisa och Europeiska gruppen för cybersäkerhetscertifiering. Dessutom föreslås befogenheter för nationella myndigheter för cybersäkerhetscertifiering till exempel i fråga om rätten att få information, revisioner (*audits*) och påförande av påföljder. Enligt förslaget ska de nationella myndigheterna för cybersäkerhetscertifiering vara en del av de inbördes granskningar som medlemsstaterna genomför, där myndigheternas allmänna, övervakande och verkställande verksamhet och förfaranden ska bedömas. Inbördes granskning genomförs minst vart femte år av två andra nationella myndigheter för cybersäkerhetscertifiering.

Enligt kommissionens förslag ska Europeiska gruppen för cybersäkerhetscertifiering (*ECCG*) bestå av representanter för nationella myndigheter för cybersäkerhetscertifiering eller andra relevanta nationella myndigheter. Europeiska gruppen för cybersäkerhetscertifiering ska bistå kommissionen vid implementeringen och tillämpningen av normerna i ramen för cybersäkerhetscertifiering samt vid beredningen av begäran som har med europeiska ordningar för cybersäkerhetscertifiering att göra. Vid sidan av andra uppgifter ska Europeiska gruppen för cybersäkerhetscertifiering bistå Enisa med att bereda ett förslag till certifieringsordningar och fastställa tekniska specifikationer för sådana samt samarbeta med kommissionen och Enisa i frågor som gäller upprätthållandet av certifieringsordningarna.

Rättsskydd och påföljder

Enligt kommissionens förslag har fysiska och juridiska personer rätt att lämna in besvär till den som utfärdar det europeiska cybersäkerhetscertifikatet. Den som söker ändring ska ha rätt att få information om hur besväret framskrider, om beslutet och om rätten att söka ändring i domstol.

Enligt förslaget ska medlemsstaterna ställa påföljder för brott mot skyldigheterna i anslutning till ramen för cybersäkerhetscertifiering och den europeiska cybersäkerhetscertifieringen samt vidta nödvändiga åtgärder för att genomföra dem. Medlemsstaterna ska snarast möjligt underrätta kommissionen om dessa regler och förfaranden.

3.1.3 Säkerheten i IKT-leveranskedjorna

Förslaget innehåller skyldigheter som gäller hanteringen av icke-tekniska risker i IKT-leveranskedjorna inom EU. Genom förslaget skapas ett säkerhetssystem för betrodda IKT-leveranskedjor (*security mechanism/framework*) som hanterar icke-tekniska risker inom sektorerna i bilagorna I och II till NIS 2-direktivet (2022/2555). Kommissionen kan genom en genomförandeakt definiera kritiska IKT-tillgångar i kritiska IKT-leveranskedjor. Den kan utifrån riskbedömningarna som nämns i förslaget genom genomförandeakter föreslå ändamålsenliga och proportionerliga riskhanteringsåtgärder som gäller sektorerna i bilagorna I och II till NIS 2-direktivet.

Bedömning av säkerhetsrisker, identifiering av kritiska IKT-tillgångar och riskhanteringsåtgärder

Enligt förslaget kan kommissionen eller en grupp som består av minst tre medlemsstater be NIS-samarbetsgruppen (*NIS Cooperation Group*) som inrättats med stöd av artikel 14 i NIS 2-direktivet (2022/2555) att göra en riskbedömning av IKT-leveranskedjan i enlighet med artikel 22 i NIS 2-direktivet. Riskbedömningen bör beakta kritiska IKT-tillgångar i den granskade IKT-leveranskedjan och centrala hotfaktorer, risker och sårbarheter i anslutning till dem. Utifrån riskbedömningen bör riskscenarier utarbetas och åtgärder föreslås för att hantera de risker som identifierats i bedömningen. Riskbedömningen ska göras inom sex månader från begäran om upprättande eller inom kortare tid än så på kommissionens begäran och om NIS-samarbetsgruppen har kommit överens om det.

Om kommissionen har tillräckliga skäl att misstänka att det finns ett betydande cyberhot i IKT-leveranskedjan som påverkar unionens säkerhet och förutsätter åtgärder för att trygga den inre marknadens funktion, kan kommissionen utan dröjsmål konsultera medlemsstaterna om nödvändiga riskhanteringsåtgärder enligt förslaget samt göra en riskbedömning där kommissionen beaktar observationer från medlemsstaternas konsultation.

Om riskbedömningen ovan visar på betydande cybersäkerhetsrisker i IKT-leveranskedjan, kan kommissionen genom en genomförandeakt definiera kritiska IKT-tillgångar (*key ICT-assets)* som entiteter inom sektorerna i bilagorna I och II till NIS 2-direktivet använder för att producera sina produkter eller tjänster. När kommissionen bedömer kritiska IKT-tillgångar ska den beakta olika faktorer, såsom om IKT-tillgångarna har centrala och kritiska funktioner, eventuella incidenter, eventuella beroenden och resultaten av riskbedömningen som ingår i förslaget.

Enligt förslaget kan kommissionen genom en genomförandeakt förbjuda entiteter som avses i bilagorna I och II till NIS 2-direktivet att använda, installera eller integrera IKT-komponenter från högriskleverantörer eller komponenter som innehåller IKT-komponenter i identifierade kritiska IKT-tillgångar. Dessa genomförandeakter skulle fastställa lämpliga övergångsperioder under vilka kommissionen skulle offentliggöra en förteckning över högriskleverantörer. I

genomförandeakterna fastställs dessutom övergångstider för byte av förbjudna IKT-komponenter.

Kommissionen kan genom genomförandeakter utifrån en riskbedömning ställa en eller flera riskhanteringsskyldigheter i IKT-leveranskedjorna och i synnerhet i kritiska IKT-tillgångar för vissa entiteter inom sektorerna i bilagorna I och II till NIS 2-direktivet. Till dessa åtgärder hör skyldigheten att göra IKT-leveranskedjorna transparenta för den behöriga tillsynsmyndigheten, begränsningarna i överföringen av data till ett tredjeland eller behandlingen av data i ett tredjeland, tekniska åtgärder som en utomstående part skulle auditera, begränsningar i anslutning till den operativa verksamheten och avtalsförhållandena samt åtgärder i anslutning till diversifieringen av leveranskedjan. Innan dessa riskhanteringsåtgärder anvisas ska kommissionen bedöma eventuella risker och beroenden. För att säkerställa att den inre marknaden fungerar kan kommissionen även i exceptionella situationer förbjuda entiteter inom sektorerna i bilagorna I och II till NIS 2-direktivet att anlita sådana leverantörer som medför en betydande icke-teknisk cybersäkerhetsrisk för minst tre medlemsstater.

Säkerheten i de elektroniska kommunikationsnätens IKT-leveranskedjor

I förslaget föreslås motsvarande riskhanteringsskyldigheter för kommunikationsnätens IKT-leveranskedjor för att hantera icke-tekniska risker. I förslaget fästs dock särskild uppmärksamhet vid kommunikationsnäten (artiklarna 110–111). I bilaga II till förslaget presenteras kommunikationsnätens kritiska IKT-tillgångar för mobilnät, fasta kommunikationsnät och satellitkommunikationsnät. Kommissionen kan genom en delegerad akt uppdatera förteckningen i fråga så att den motsvarar den tekniska utvecklingen. Enligt förslaget ska IKT-komponenterna hos högriskleverantörer i mobilnäten bytas ut senast inom 36 månader från det att kommissionen har publicerat en förteckning över högriskleverantörer för dessa typer av kommunikationsnät. Kommissionen kan utfärda genomförandeakter där den preciserar övergångstiderna för att byta ut IKT-komponenter när det gäller fasta kommunikationsnät och satellitkommunikationsnät. Enligt förslaget ska leverantörer av ovan nämnda kommunikationsnät inte använda, installera eller integrera IKT-komponenter från högriskleverantörer eller komponenter som innehåller IKT-komponenter i de kritiska IKT-tillgångar som anges i bilaga II till förslaget till förordning.

Utpekande av tredjeländer som orsakar cybersäkerhetsbekymmer

I förslaget till förordning föreslås att kommissionen ska kunna utse tredjeländer som orsakar cybersäkerhetsbekymmer (*third countries posing cybersecurity concerns*) utifrån ovan nämnda riskbedömningar eller utifrån andra källor, såsom ett uttalande från unionen eller en medlemsstat. Kommissionen ska bedöma en sådan risk som orsakas av ett tredjeland med beaktande av de omständigheter som anges i artikel 100.1 a–e.

Om kommissionen i sin bedömning konstaterar att ett tredjeland skulle orsaka en allvarlig och strukturell icke-teknisk risk i IKT-leveranskedjorna, kan den genom en genomförandeakt utse det till ett tredjeland som orsakar cybersäkerhetsbekymmer i IKT-leveranskedjorna.

Identifiering av högriskleverantörer i tredjeländer som orsakar cybersäkerhetsbekymmer och begränsningar gällande dem

Enligt förslaget kan kommissionen genom en genomförandeakt upprätta en förteckning över högriskleverantörer som kommissionen kan utfärda de föreslagna begränsningarna om genom genomförandeakter. För att utfärda begränsningar ska kommissionen först utreda leverantörerna i IKT-leveranskedjan och göra en preliminär bedömning av sådana leverantörer som kan vara

baserade i ett tredjeland som orsakar cybersäkerhetsbekymmer eller som kan besittas av ett sådant land eller av en entitet eller medborgare som är baserad i landet i fråga. Kommissionen ska bedöma leverantörernas etableringsort, ägarförhållande och förvaltningssystem. Kommissionen ska ha rätt att begära information av leverantörerna för att kunna göra bedömningen. Om en leverantör inte lämnar de uppgifter som krävs för bedömningen inom utsatt tid, kan kommissionen på basis av detta besluta att leverantören är baserad i ett tredjeland som orsakar cybersäkerhetsbekymmer eller att den besitts av ett sådant tredjeland eller en entitet eller medborgare i ett sådant land. Kommissionen ska höra leverantören som är föremål för granskning i processen och gå igenom de preliminära observationerna med denne. Kommissionen kan även be den behöriga tillsynsmyndigheten att göra motsvarande bedömning och myndigheten ska meddela kommissionen om en leverantör bör läggas till i förteckningen över högriskleverantörer. Kommissionen ska regelbundet uppdatera förteckningen över högriskleverantörer.

Kommissionen kan bevilja undantag från begränsningar som riktats mot en högriskleverantör om en sådan leverantör bevisligen kan påvisa effektiva riskhanteringsmetoder för att hantera icke-tekniska risker och garantera att det tredjeland som orsakar cybersäkerhetsbekymmer inte har en negativ inverkan på den aktuella leverantörens leverans av IKT-komponenter. Kommissionen kan vid behov ställa närmare villkor för detta genom genomförandeakter. Kommissionen ska höra en leverantör som ansökt om undantag i processen och meddela ett beslut i ärendet inom nio månader från ansökan om undantag. Den kan ställa en tidsfrist för giltigheten för det beviljade undantaget och en tidsfrist för genomförandet av de riskhanteringsåtgärder som är villkor för undantaget. Kommissionen ska föra ett offentligt tillgängligt register över beslut i vilka den har beviljat undantag. Kommissionen kan ta ut avgifter för ansökningar om undantag och lämna närmare uppgifter om avgifterna genom genomförandeakter.

De behöriga tillsynsmyndigheternas tillsynsuppgifter

Medlemsstaterna ska utse behöriga myndigheter enligt artikel 8 i NIS 2-direktivet till tillsynsmyndigheter för de skyldigheter som gäller IKT-leveranskedjorna i förslaget till förordning. Tillsynsåtgärderna i detta förslag till förordning gäller entiteterna i bilagorna I och II till NIS 2-direktivet. I artikel 114 i förslaget innehåller bestämmelser om de behöriga tillsynsmyndigheternas tillsynsuppgifter. De behöriga myndigheterna ska ha rätt att begära nödvändiga uppgifter, genomföra tillsynsåtgärder och vidta proportionerliga och effektiva korrigerande eller restriktiva åtgärder för att säkerställa att förordningen följs. Tillsynsåtgärderna ska vara effektiva, proportionerliga och konsekventa. Innan tillsynsåtgärder genomförs ska de behöriga tillsynsmyndigheterna underrätta den entitet som är föremål för tillsynsåtgärderna om sina eventuella observationer. Entiteten ska ha möjlighet att bemöta dessa observationer. Tillsynsmyndigheterna ska i sina tillsynsuppgifter iaktta principerna om konfidentialitet samt affärs- och yrkeshemligheten.

För att sköta sina tillsynsuppgifter enligt förslaget till förordning ska de behöriga tillsynsmyndigheterna vara strukturellt och funktionellt självständiga och fria från yttre inflytande. De ska inte få anvisningar av en annan myndighet eller en privat entitet. Kommissionen ska inrätta ett samarbetsnätverk för dessa tillsynsmyndigheter för att främja det nödvändiga samarbetet och informationsutbytet samt för att stödja processen med att identifiera högriskleverantörer.

Om en entitet som omfattas av bilagorna I eller II till NIS 2-direktivet tillhandahåller tjänster i flera medlemsstater eller om dess kritiska IKT-tillgångar finns i flera medlemsstater, ska de behöriga tillsynsmyndigheterna samarbeta med varandra och med kommissionen för att

säkerställa en effektiv och enhetlig tillämpning av förordningen. Förslaget innehåller även bestämmelser om jurisdiktion att sköta tillsynsuppgifter som entiteterna i bilagorna I och II till NIS 2-direktivet ska omfattas av för att rikta in tillsynsuppgifterna som ingår i detta författningsförslag.

Påföljder

I förslaget föreslås att medlemsstaterna ska fastställa påföljdsavgifter (*penalties*) för brott mot skyldigheterna i förslaget till förordning. Påföljdsavgifterna ska vara effektiva, proportionerliga och avskräckande, och de kan fastställas utöver åtgärderna i artikel 114.3 a–c i förslaget till förordning. Enligt förslaget kan en påföljdsavgift som motsvarar högst 1 procent av föregående års globala omsättning påföras för brott mot artikel 103.2 a. För brott mot artikel 103.2 b–g i förslaget till förordning kan en påföljdsavgift som motsvarar högst 2 procent påföras och för brott mot artikel 103.1 och artikel 111 en påföljdsavgift som motsvarar högst 7 procent.

3.1.4 Slutbestämmelser

I förslaget föreslås att kommissionen senast xx.yy.zzzz och därefter vart femte år ska utvärdera Enisas resultat i förhållande till dess syften, uppdrag, uppgifter, förvaltning och läge; genomslaget och effektiviteten hos EU:s enskilda system för verifiering av cybersäkerhetskompetens och mervärdet som EU ger; konsekvenserna, effekten och effektiviteten för informations- och kommunikationstekniska produkter, tjänster och processer samt säkerhetstjänster i förhållande till de uppställda målen och säkerhetsnivåerna; säkerheten i leveranskedjorna för informations- och kommunikationsteknik och de genomförda åtgärderna.

3.2 Direktivet om ändring av NIS 2-direktivet

Genom direktivet föreslås riktade ändringar i NIS 2-direktivet (EU) 2022/2555. Syftet med de riktade ändringarna är att förtydliga och precisera direktivets tillämpningsområde, främja ett enhetligt genomförande i medlemsstaterna, underlätta påvisande av överensstämmelse med kraven samt minska de kostnader som regleringen medför för entiteterna. De föreslagna ändringarna gäller direktivets tillämpningsområde, klassificeringen av entiteter som väsentliga och viktiga, kommissionens genomförandeakter om riskhantering och rapportering av betydande incidenter, anmälan av uppgifter om utpressningsprogram, Enisas uppgift som stöd för medlemsstaternas tillsyn samt utnyttjandet av den europeiska cybersäkerhetscertifieringen för att påvisa överensstämmelse med kraven på riskhantering.

Det föreslås att nya typer av entiteter som erbjuder europeiska digitala identitetsplånböcker och europeiska företagsplånböcker ska läggas till i direktivets tillämpningsområde. Det föreslås dessutom att tillämpningsområdet ska omfatta nya typer av entiteter som äger, förvaltar eller använder strategisk infrastruktur med dubbla användningsområden. Dessa entiteter ska oberoende av storlek vara väsentliga entiteter i direktivets tillämpningsområde. Till direktivets tillämpningsområde föreslås dessutom en ny typ av entitet i form av operatörer av undervattensinfrastruktur, om de är medelstora eller större. Det föreslås att mikroföretag och små företag som tillhandahåller DNS-tjänster, elproducenter med en produktionskapacitet på mindre än 1 MW och hälso- och sjukvårdsproducenter som endast tillhandahåller långvarig vård ska strykas från direktivets tillämpningsområde. Dessutom föreslås vissa preciseringar i begrepp som definierar tillämpningsområdet i fråga om vätgasoperatörer, operatörer av intelligenta transportsystem samt den kemiska industrin. I artikel 26 i direktivet föreslås dessutom vissa preciseringar av medlemsstaternas jurisdiktion i fråga om flygbolag och entiteter som är etablerade i tredjeländer. Dessutom föreslås vissa preciseringar i artiklarna 27 och 3 i

direktivet som gäller den förteckning över entiteter som upprätthålls av Enisa samt entiteternas skyldighet att anmäla sina uppgifter till tillsynsmyndigheten.

Kommissionen föreslår att storleksgränsen som tillämpas vid fastställandet av en väsentlig entitet ska höjas. De väsentliga entiteter som avses i direktivet ska i fortsättningen vara entiteter som bedriver sådan verksamhet som avses i bilaga I till direktivet och som överskrider storleksgränsen för små midcapföretag. På definitionen av små midcapföretag tillämpas kommissionens rekommendation (EU) 2025/1099. Enligt 2 punkten i bilagan till rekommendationen utgörs kategorin små midcapföretag av företag som sysselsätter färre än 750 personer och vars omsättning inte överstiger 150 miljoner euro årligen eller vars balansomslutning inte överstiger 129 miljoner euro årligen. Den storleksgräns som för närvarande tillämpas grundar sig på kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag, och som motsvarande storleksgräns har det tillämpats en överstigning av gränsvärdena för en företagskategori som utgörs av företag som sysselsätter färre än 250 personer och vars årsomsättning inte överstiger 50 miljoner euro eller vars balansomslutning inte överstiger 43 miljoner euro per år.

Kommissionen föreslår en ändring i fråga om strategins innehållskrav, med stöd av vilken medlemsstaterna i fortsättningen i de nationella cybersäkerhetsstrategierna bland annat ska godkänna politik som gäller införande av kvantresistent kryptering (*post-quantum cryptography, PQC*).

Kommissionen kan nu utfärda genomförandeakter som preciserar åtgärderna i anslutning till kravet på riskhantering. Kommissionen kan i fortsättningen utfärda genomförandeakter om riskhantering som är fullständigt harmoniserande och, i den mån sådana har utfärdats, får medlemsstaterna inte kräva riskhanteringsåtgärder som avviker från dessa. Förslaget är ett undantag till NIS 2-direktivets karaktär som minimiharmoniserande bestämmelse och utvidgar i praktiken den genomförandebehörighet som delegerats till kommissionen i fråga om riskhantering.

Enligt förslaget bör kommissionen genom en genomförandeakt som gäller rapportering av betydande incidenter förutsätta att en entitet anmäler om den har upptäckt en attack genom utpressningsprogram, vilken sektor som varit föremål för attacken och åtgärderna för att hantera den. Även om förslaget inte grundar sig på någon ny skyldighet att utfärda en genomförandeakt, lämpar det sig som ett nytt innehållsmässigt krav för genomförandeakter som gäller rapportering av en betydande incident. Enligt förslaget ska medlemsstaterna dessutom kräva att entiteterna om en betydande incident beror på ett utpressningsprogram rapporterar om de har tagit emot ett krav på lösensumma, av vem de har tagit emot kravet på lösensumma samt uppgifter om betalning och mottagare av lösensummorna.

Enligt förslaget ska Enisa göra en analys av gränsöverskridande cybersäkerhetsrisker med särskilt fokus på incidenternas gränsöverskridande konsekvenser. Utifrån denna bedömning kan Enisa ge medlemsstaternas tillsynsmyndigheter anvisningar eller rekommendationer samt på begäran av en medlemsstats tillsynsmyndighet delta i tillsynsåtgärderna eller i bedömningen av om en entitets riskhanteringsåtgärder är tillräckliga. För att stödja tillsynen förutsätts att medlemsstaterna lämnar uppgifter till Enisa om tillsynen och föremålen för den. Dessutom föreslår kommissionen att Enisa läggs till som medlem i CSIRT-nätverket.

Enligt förslaget kan medlemsstaterna kräva att entiteter skaffar certifiering enligt den europeiska ordningen för cybersäkerhetscertifiering för att påvisa att riskhanteringen överensstämmer med kraven. Om en entitet har skaffat lämplig certifiering ska medlemsstaterna anse att den

certifierade entiteten uppfyller skyldigheterna i fråga om riskhantering. Dessutom får tillsynen inte rikta regelbundna säkerhetsrevisioner eller säkerhetskontroller mot en certifierad entitet.

Enligt förslaget ska medlemsstaterna införliva direktivet om ändring av NIS 2-direktivet i den nationella lagstiftningen inom 12 månader efter att det har trätt i kraft.

4 Rättslig grund, subsidiaritetsprincipen och proportionalitetsprincipen

4.1 Rättslig grund

Den rättsliga grunden för CSA2-förslaget och direktivet om ändring av NIS 2-direktivet är artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som gör det möjligt att utfärda åtgärder som gäller genomförandet av den inre marknaden och dess funktion. Rättsakter som utfärdas med stöd av artikel 114 i EUF-fördraget antas i vanlig lagstiftningsordning. Rådet fattar sitt beslut med kvalificerad majoritet.

Enligt kommissionen syftar förslaget till att undvika fragmentering av den inre marknaden.

Kommissionen fäster uppmärksamhet vid att förordning (EU) 2019/881 om Enisa och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (CSA) antogs med stöd av artikel 114 i EUF-fördraget.

Enligt kommissionen kan splittringen av den nationella lagstiftningen, i synnerhet när det gäller icke-tekniska risker, leda till att den inre marknaden fragmenteras i fråga om säkerheten i IKT-leveranskedjorna. Avvikande nationella tillvägagångssätt kan öka sårbarheten i vissa medlemsstater och föranleda gränsöverskridande återverkningar, vilket skulle försämra hela Europeiska unionens resiliens och trovärdighet i fråga om cybersäkerheten. Av dessa orsaker anser kommissionen att artikel 114 i EUF-fördraget förblir en lämplig rättslig grund för översynen av CSA. Statsrådet anser att den rättsliga grunden är lämplig.

I fråga om direktivet om ändring av NIS 2-direktivet motiveras tillämpningen av artikel 114 i EUF-fördraget med att det direktiv som föreslås bli ändrat har utfärdats på samma rättsliga grund. Statsrådet anser att den rättsliga grunden är lämplig.

4.2 Proportionalitets- och subsidiaritetsprinciperna

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 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, vare sig på central nivå eller på regional och lokal nivå, och därför, på grund av den planerade åtgärdens omfattning eller verkningar, bättre kan uppnås på unionsnivå.

Kommissionen anser att uppfyllandet av subsidiaritetsprincipen godkändes redan när den gällande cybersäkerhetsakten antogs. Kommissionen anser att det fortfarande är av avgörande vikt att ingripa på unionsnivå, eftersom hoten mot cybersäkerheten och de utmaningar som är förknippade med dem är gränsöverskridande. De fragmenterade nationella lösningarna har inte visat sig vara tillräckliga för att uppnå förtroende och samordning på marknaden. En omprövning av lagstiftningen behövs för att säkerställa ett konsekvent genomförande av den och för att stödja medlemsstaterna i en allt mer komplex reglerings- och hotmiljö. Vidare anser kommissionen att de föreslagna åtgärderna inte överskrider vad som är nödvändigt för att uppnå

målen i förslaget och att de inte hindrar medlemsstaterna från att vidta egna åtgärder i frågor som gäller den nationella säkerheten. Kommissionen anser följaktligen att verksamheten är förenlig med subsidiaritets- och proportionalitetsprinciperna.

När det gäller Europeiska unionens cybersäkerhetsbyrå Enisa innehåller förslaget några nya uppgifter som syftar till att stödja medlemsstaterna i åtgärder där det har uppdagats brister med tanke på hanteringen av cybersäkerheten. Enligt kommissionens bedömning avviker förslaget inte från den tidigare cybersäkerhetsakten vad subsidiariteten beträffar. Statsrådet stöder i huvudsak kommissionens bedömning av subsidiariteten och proportionalitetsprincipen i fråga om Enisas mandat. Under förhandlingarna ska det dock göras en bedömning av förhållandet mellan Enisas uppgifter och medlemsländernas cybersäkerhetsuppgifter och åtgärdernas komplementaritet säkerställas. Dessutom ska det säkerställas att medlemsländerna har tillräcklig möjlighet att delta i beslutsfattandet som gäller Enisas verksamhet. I fråga om Enisas nya uppgifter i anslutning till cybersäkerhetskompetens som föreslagits har kommissionen inte presenterat någon mer ingående bedömning av hur subsidiaritets- och proportionalitetsprinciperna uppfylls i fråga om åtgärderna. Under behandlingen ber statsrådet kommissionen om ytterligare upplysningar om hur dessa åtgärder påverkar medlemsländerna.

Kommissionen har tidigare strävat efter att harmonisera åtgärderna för säkerheten i kommunikationsnäten med EU:s 5G-rekommendationer. Medlemsstaterna har under de senaste åren genomfört dessa rekommendationer med hjälp av olika nationella lösningar, vilket har lett till en fragmentering av åtgärderna inom unionen. Kommissionen anser i sitt förslag att fragmenteringen av nationella åtgärder som påverkar icke-tekniska riskfaktorer försämrar den inre marknadens funktion i fråga om cybersäkerheten i IKT-leveranskedjorna. Kommissionen anser att medlemsstaternas olika strategier skulle kunna leda till en ökad sårbarhet i vissa medlemsstater, och detta kan återspeglas i hela unionen. Kommissionen anser att säkerheten i IKT-leveranskedjorna är gränsöverskridande. På grund av IKT-leveranskedjornas gränsöverskridande karaktär anser kommissionen att olika nationella lösningar skulle försämra rättssäkerheten på den inre marknaden. Kommissionen anser att identifieringen av tredjeländer som orsakar cybersäkerhetsbekymmer och säkerheten i IKT-leveranskedjorna bäst kan säkerställas genom minimiåtgärder på unionsnivå i enlighet med förslaget. Enligt förslaget är bestämmelserna om IKT-leveranskedjorna minimiskyldigheter som inte begränsar medlemsstaternas möjlighet att vidta nationella åtgärder som går längre än dessa, i synnerhet i fråga om den nationella säkerheten, där medlemsstaterna har exklusiv befogenhet enligt artikel 4.2 i EUF-fördraget.

Medlemsstaterna kan inte ensamma effektivt garantera säkerheten i IKT-leveranskedjorna när de är gränsöverskridande till sin karaktär och när underleverantörskedjorna består av flera nivåer. Statsrådets preliminära uppfattning är att de bestämmelser i förslaget som gäller IKT-leveranskedjor är förenliga med proportionalitets- och subsidiaritetsprinciperna och att kommissionens motiveringar är korrekta. Under förhandlingarna är det dock viktigt att försäkra sig om att åtgärderna i förslaget främjar den inre marknadens funktion och unionens mer omfattande strategiska mål och att de genom harmoniserade åtgärder ökar unionens rättssäkerhet och inte leder till plötsliga, oförutsedda eller svåra förändringar i medlemsstaterna. Vid förhandlingarna är det dessutom viktigt att se till att medlemsstaterna även i fortsättningen kan lägga fram nationella åtgärder som går längre än skyldigheterna i förslaget och att artikel 4.2 i EUF-fördraget iakttas.

Kommissionen bedömer att direktivet om ändring av NIS 2-direktivet uppfyller subsidiaritets- och proportionalitetsprincipernas krav. När det gäller subsidiaritetsprincipen motiveras förslaget med att det direktiv som är föremål för ändringar har konstaterats vara förenligt med subsidiaritetsprincipen. Dessutom förtydligar och förbättrar ändringarna lagstiftningsramens

funktion. I fråga om proportionalitetsprincipen anser kommissionen att förslagen står i rätt proportion till deras målsättningar, särskilt med beaktande av att det bland annat handlar om att ingripa i de behov av att utveckla regleringen som framförs av medlemsstaterna och intressenterna.

Statsrådet stöder i huvudsak kommissionens bedömning att direktivet om ändring av NIS 2-direktivet uppfyller subsidiaritets- och proportionalitetsprincipernas krav. Under förhandlingarna ska det dock med tanke på dessa principer göras en noggrannare bedömning av kommissionens förslag om att den ska kunna utfärda fullständigt harmoniserande genomförandeakter om riskhanteringsåtgärder inom cybersäkerhet.

4.3 Delegering av befogenheter samt uppgifter som föreslås för kommissionen

Den föreslagna cybersäkerhetsakten (CSA2) och direktivet om ändring av NIS 2-direktivet innehåller en delegering av genomförandebefogenheter till kommissionen.

Enligt förslaget till förordning kan kommissionen utfärda genomförandeakter som fastställer detaljerade regler för fastställandet av de avgifter som Enisa tar, till exempel när det gäller avgiftsbeloppen och villkoren för dem.

Enligt förslaget ska kommissionen kunna utfärda genomförandeakter som stärker den europeiska ordningen för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer samt leverantörer av säkerhetstjänster och arbete på cyberområdet. Dessutom kan kommissionen utfärda genomförandeakter som stärker gemensamma principer och modellbestämmelser för elementen i de europeiska ordningarna för cybersäkerhetscertifiering. Kommissionen ska ha befogenhet att utfärda genomförandeakter som fastställer en minst femårig plan för inbördes granskning.

Kommissionen kan utfärda genomförandeakter för att utifrån en riskbedömning kunna utse ett tredjeland till ett land som orsakar cybersäkerhetsbekymmer (*country posing cybersecurity concerns*) för IKT-leveranskedjorna. Kommissionen kan genom en genomförandeakt sammanställa en förteckning över högriskleverantörer som omfattas av begränsningarna som ingår i förslaget. Kommissionen kan genom en genomförandeakt närmare definiera villkoren för att en högriskleverantör ska kunna beviljas undantag från begränsningarna. Kommissionen kan utfärda genomförandeakter för att definiera de kritiska IKT-tillgångar som entiteterna i bilagorna I och II till NIS 2-direktivet använder för att tillhandahålla sina produkter eller tjänster. Kommissionen kan utfärda genomförandeakter för att förbjuda entiteter som avses i bilagorna I och II till NIS 2-direktivet att använda, installera eller integrera IKT-komponenter från högriskleverantörer eller komponenter som innehåller IKT-komponenter i identifierade kritiska IKT-tillgångar. Kommissionen skulle fastställa lämpliga övergångsperioder genom genomförandeakterna. Genom genomförandeakter kan kommissionen föreslå riskhanteringsåtgärder för IKT-leveranskedjor och centrala IKT-tillgångar för vissa entiteter i bilagorna I och II till NIS 2-direktivet. Kommissionen kan beakta storleken på dessa entiteter när genomförandeakterna utarbetas. Genomförandeakterna skulle även gälla EU:s institutioner, organ och byråer.

Enligt förslaget till direktiv om ändring av NIS 2-direktivet kan kommissionen utfärda genomförandeakter om tekniska och metodologiska krav på riskhantering samt sektorsspecifika krav. Enligt förslaget ska de genomförandeakter som kommissionen utfärdar vara fullständigt harmoniserande. Dessutom föreslås det att den befogenhet som delegeras till kommissionen att utfärda genomförandeakter om rapportering av betydande incidenter ska utvidgas genom

ändringsdirektivet så att kommissionen i genomförandeakterna ska förutsätta att entiteter rapporterar uppgifter om attacker genom utpressningsprogram.

5 Förslagets konsekvenser

5.1 Ekonomiska konsekvenser

Enligt kommissionens bedömning skulle en utvidgning av Europeiska unionens cybersäkerhetsbyrå Enisas verksamhetsfält under granskningsperioden kunna leda till besparingar på 14,6 miljarder euro för företag som är verksamma inom unionen. Därtill skulle möjligheten att på ett snabbare och effektivare sätt bekämpa cyberhot och effekterna av dem kunna medföra besparingar på cirka 3,7–4,4 miljarder euro på unionsnivå.

Förslaget innebär att Enisas omkostnader ökar avsevärt. Under åren 2028–2034 skulle Enisas omkostnader i genomsnitt uppgå till 50 miljoner euro årligen. År 2025 uppgick omkostnaderna till cirka 26 miljoner euro och antalet anställda motsvarade cirka 131 årsverken. Fram till 2031 föreslås Enisas personalstyrka växa till cirka 260 årsverken. Förslaget påverkar också omkostnaderna vid Transport- och kommunikationsverket Traficom eller en annan utsändande nationell myndighet. Den föreslagna skyldigheten att utse två nationella experter som medlemsstaterna bekostar skulle medföra en kostnad på cirka 200 000 euro per år.

Europeiska kommissionen föreslås också få tilläggsresurser motsvarande sammanlagt 50 årsverken för skötseln av de uppgifter som ingår i förslaget. Tilläggsresurserna ska användas för att sköta uppgifter i anslutning till det operativa samarbetet, den europeiska kompetensramen för cybersäkerhet (ECSF), certifieringar samt riskbedömningar som har med IKT-leveranskedjor att göra.

Enligt kommissionens bedömning är kostnadskalkylen för certifieringsramen när det gäller medlemsstaternas personalkonsekvenser cirka 2–10 årsverken beroende på de ordningar för cybersäkerhetscertifiering som bereds och den befintliga personalen eller en eventuell utökning av den. Kommissionen uppskattar att certifiering av arbete på cyberområdet skulle kosta ett företag omkring 30 000 euro per certifiering. Enligt kommissionens beräkningar skulle utarbetandet, upprätthållandet och beviljandet av certifieringsordningar i framtiden helt eller delvis finansieras med de avgifter som Enisa tar. Ändringen i den avgiftsbelagda verksamheten sker stegvis.

Kommissionen har uppskattat att de årliga kostnaderna för att byta ut vissa delar från högriskleverantörer under en treårsperiod skulle uppgå till 3,4–4,3 miljarder euro för mobilnätsoperatörer. Samtidigt skulle investeringarna i betrodda leverantörer årligen öka till högst 2 miljarder euro per år. Förslaget kan påverka medlemsstaternas eventuella ersättningsskyldighet. Kommissionen har varken i sitt förslag till förordning eller i sin konsekvensbedömning om förslaget gjort en bedömning på EU-nivå om ersättningsarrangemangen eller ersättningsmöjligheterna i samband med att högriskleverantörers IKT-komponenter byts ut. Kommissionen har inte gjort någon närmare bedömning av eventuella kostnader för andra sektorer som omfattas av NIS 2-direktivet och skyldigheterna som gäller IKT-leveranskedjor. Konsekvenserna beror också på när begränsningen av användningen av nätutrustningen träder i kraft.

Förslagen i direktivet om ändring av NIS 2-direktivet kan ha ekonomiska konsekvenser för entiteter som omfattas av direktivets tillämpningsområde, vilka i Finland utgörs av aktörer och myndigheter som omfattas av tillämpningsområdet för cybersäkerhetslagen eller 4 a kap. i lagen om informationshantering inom den offentliga förvaltningen. Genom ändringarna eftersträvas

bland annat sänkta kostnader för dem som iakttar regleringen och påvisar överensstämmelse med kraven. En del av förslagen, exempelvis bestämmelsen om rapportering av uppgifter om utpressningsprogram, kan i sig även leda till att kostnaderna som iakttagande av regleringen innebär ökar. De ekonomiska konsekvensernas belopp varierar från entitet till entitet. Konsekvenserna skulle vara mest kännbara för entiteter som inte har omfattats av direktivets tillämpningsområde tidigare.

5.2 Konsekvenser för den nationella lagstiftningen

De nationella bestämmelser som kompletterar bestämmelserna i cybersäkerhetsakten om den europeiska ramen för cybersäkerhetscertifiering ingår numera i lagen om tjänster inom elektronisk kommunikation (917/2014). Regeringens proposition RP 179/2025 rd är under behandling i riksdagen. Den innehåller förslag till komplettering av de nationella bestämmelserna om cybersäkerhetscertifieringar och en överföring av dem från lagen om tjänster inom elektronisk kommunikation till en ny lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering. Reformen av cybersäkerhetsakten torde förutsätta en utvärdering och ändring av de nationella bestämmelser som kompletterar cybersäkerhetscertifieringen.

De bestämmelser om IKT-leveranskedjor som föreslås i förslaget förutsätter åtminstone en granskning av bestämmelserna i lagen om tjänster inom elektronisk kommunikation. Förslagen kan även föranleda ändringar i cybersäkerhetslagen (124/2025). Förslaget kan också förutsätta en granskning av upphandlingslagen i fråga om de skyldigheter som gäller offentliga IKT-upphandlingar. I fråga om den nationella lagstiftningen bör det säkerställas att regleringen överensstämmer med bestämmelserna om IKT-leveranskedjor i förslaget till förordning så att den nationella lagstiftningen inte överlappar eller strider mot unionsrätten.

Ändringarna i NIS 2-direktivet torde kräva ändringar i cybersäkerhetslagen (124/2025) och lagen om informationshantering inom den offentliga förvaltningen (906/2019). Ändringarna kan även medföra andra konsekvenser för den nationella lagstiftningen.

Förslagen som gäller Europeiska unionens cybersäkerhetsbyrå Enisa har inte identifierats ha några avsevärda konsekvenser för den nationella lagstiftningen. Förslagen kan medföra ett behov av att bedöma bestämmelserna om informationsutbyte och samarbete mellan myndigheter.

5.3 Konsekvenser för myndigheternas verksamhet

Förslaget kan ha konsekvenser för myndighetsverksamheten, i synnerhet för Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom. Enisas större roll i det operativa samarbetet skulle påverka verksamheten i hela unionens etablerade cybersäkerhetsnätverk (t.ex. CSIRT-nätverket och EU-CyCLONe) och det informationsutbyte som sker inom dem. Att Enisa får en starkare roll i skapandet av en lägesbild kan i viss mån på längre sikt minska behovet av att skapa lägesbildsprodukter nationellt. Förslaget kan dock även belasta myndigheterna om det leder till ökad rapportering och informationsdelning från myndigheterna till Enisa.

Reformerna av den europeiska ramen för cybersäkerhetscertifiering påverkar de nationella behöriga myndigheternas uppgifter och befogenheter. I förslaget fastställs uppgifter och krav för nationella myndigheter för cybersäkerhetscertifiering och organ för bedömning av överensstämmelse med kraven. I Finland finns det än så länge inga organ för bedömning av överensstämmelse med kraven enligt cybersäkerhetsakten. Enligt förslaget ska medlemsstaterna

se till att de nationella myndigheterna för cybersäkerhetscertifiering har tillräckliga resurser för att sköta sina uppgifter och befogenheter.

Utifrån bestämmelserna om säkerheten i IKT-leveranskedjorna föreslås de nationella behöriga myndigheterna få nya tillsynsuppgifter (*supervisory*) och verkställighetsuppgifter (*enforcement*) i fråga om entiteterna i bilagorna I och II till NIS 2-direktivet (2022/2555). Enligt förslaget ska de behöriga myndigheterna i strukturellt och funktionellt hänseende vara helt opartiska och fria från all yttre påverkan. De ska inte söka eller ta emot anvisningar från någon annan myndighet eller privat aktör. Enligt förslaget ska medlemsstaterna säkerställa att de behöriga myndigheterna har tillräckliga befogenheter, tillräckliga resurser och den sakkunskap som krävs för att sköta sina uppgifter effektivt.

Förslagen som ingår i direktivet om ändring av NIS 2-direktivet har konsekvenser för myndigheterna som övervakar den nationella genomförande lagstiftningen, det vill säga cybersäkerhetslagen och 4 a kap. i lagen om informationshantering inom den offentliga förvaltningen. Förslagen som gäller tillämpningsområdet och storleksgränsen för en väsentlig entitet påverkar tillämpningsområdet och antalet entiteter som omfattas av tillsynen.

Det ansenliga antal genomförandeakter som ingår i förslaget medför konsekvenser för de ministerier inom vars ansvarsområde delegerade akter bereds i kommittéförfaranden.

5.4 Andra konsekvenser

Genom förslaget att komplettera Enisas verksamhet kan cybersäkerheten stärkas i hela unionen. Förslaget stärker i synnerhet verksamheten i nätverken för samarbete och informationsutbyte inom cybersäkerhet på EU-nivå som skapats i och med NIS 2-direktivet (CSIRT-nätverket och EU-CyCLONe) när det gäller att observera cyberhot, reagera på hot och återhämta sig från cyberstörningar. Förslaget förtydligar verksamheten i dessa nätverk i samband med cyberincidenter samt Enisas roll i sådana situationer. Genom förslaget går det även att förebygga cybersäkerhetsincidenter tack vare en bättre, mer omfattande och mer aktuell lägesbild. Förslaget skulle sannolikt påverka i synnerhet utvecklingen av cybersäkerheten i mindre digitalt mogna länder, eftersom Enisa i fortsättningen tydligare skulle erbjuda exempelvis stöd för övningar och återhämtning från störningar. Bättre lägesbildsprodukter och ett effektivare samarbete på unionsnivå kan även stödja företag som är verksamma inom EU med att förbereda sig för cyberhot och reagera på dem, och därigenom minska sannolikheten för allvarliga och omfattande cyberstörningar.

Förslaget om Enisas roll i upprätthållandet av en europeisk sårbarhetsdatabas och hanteringen av sårbarheter stärker unionens strategiska autonomi och oberoende av utomstående tjänsteleverantörer.

I förslaget ingår endast en partiell bedömning av hur den europeiska kompetensramen för cybersäkerhet och de kompetensintyg som beviljas utifrån den påverkar arbetsmarknaden eller ökar antalet experter inom cybersäkerhet. Enligt kommissionens bedömning kan förslaget öka antalet europeiska kompetensverifierare och förbättra de europeiska företagens förståelse för olika kompetensbehov inom cybersäkerhet. Däremot har det inte gjorts någon separat bedömning av förslagets konsekvenser för antalet cybersäkerhetsexperter eller deras nivå.

Bestämmelserna om säkerheten i IKT-leveranskedjorna kan även ha olika handelspolitiska och utrikespolitiska konsekvenser.

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

Kommissionen bedömer att Enisas mandat skulle främja cybersäkerheten inom hela ekonomiska samarbetsområdet och i samhället generellt samt förbättra personers integritet och skyddet av personuppgifter. Förslaget stöder också utbildning och övning i cybersäkerhet, eftersom det skulle förtydliga Enisas roll i utvecklingen av kapaciteten hos dem som arbetar med cybersäkerhet.

I fråga om den europeiska ramen för cybersäkerhetscertifiering konstaterar kommissionen att den skulle öka allmänhetens och företagens förtroende för lösningar inom informations- och kommunikationsteknik, särskilt när en kritisk sektor skulle kunna påvisa en hög nivå av cybersäkerhet med hjälp av certifieringen. Dessutom konstaterar kommissionen att förtroendet för skyddet av känsliga uppgifter kunde bli större genom att harmonisera rapporteringen av fall av utpressningsprogram och främja en övergång till kvantresistent kryptering.

Enligt kommissionens bedömning har bestämmelsen om säkerheten i IKT-leveranskedjorna som ingår i förslaget en viss inverkan på skyddet av de grundläggande fri- och rättigheterna, eftersom de begränsar påverkan som kommer från länder utanför EU. Åtgärderna enligt förslaget kan enligt kommissionen således öka förtroendet, säkerheten och integritetsskyddet i olika former av teknik och digitala lösningar.

Förslaget kan ha positiva konsekvenser för skyddet av de grundläggande fri- och rättigheterna, såsom skyddet för privatlivet enligt 10 § i grundlagen och skyddet av konfidentiell kommunikation. Förslaget gäller sektorer som är kritiska för samhället och som i sin verksamhet i stor omfattning behandlar olika slags uppgifter, inklusive personuppgifter, och förmedlar konfidentiell kommunikation. Enligt förslaget kan högriskleverantörer i länder som orsakar cybersäkerhetsbekymmer orsaka olika risker i IKT-leveranskedjorna, till exempel att uppgifter läcker till sådana länder. Genom de åtgärder som föreslås strävar kommissionen efter att förebygga den här typen av risker.

Kommissionen har innan förslaget lämnades först försökt främja de mål som presenteras i förslaget, i synnerhet i fråga om att trygga säkerheten i 5G-kommunikationsnäten med hjälp av EU:s 5G-rekommendationer som publicerades 2020. Kommissionen har bedömt att medlemsstaternas olika lösningar inte har varit tillräckliga för att trygga säkerheten i 5G-kommunikationsnäten på det sätt som avses i EU:s 5G-rekommendationer, och föreslår delvis av den anledningen de åtgärder som föreslås i förslaget.

Den föreslagna regleringen är betydelsefull med tanke på egendomsskyddet som tryggas i 15 § i grundlagen, eftersom det aktuella förslaget kan förbjuda entiteter som omfattas av NIS 2-direktivet att i någon form använda, installera och integrera IKT-komponenter från högriskleverantörer i de produkter och tjänster som entiteten använder och erbjuder i unionen. Vidare är den föreslagna bestämmelsen betydelsefull med tanke på näringsfriheten som tryggas i 18 § i grundlagen, eftersom det genom förslaget går att ställa begränsningar för högriskleverantörers verksamhet på den inre marknaden.

Grunden för att ingripa i ovan nämnda grundläggande fri- och rättigheter är enligt förslaget att trygga störningsfri verksamhet i IKT-leveranskedjorna inom unionen och att hantera icke-tekniska risker i anslutning till IKT-leveranskedjorna. Enligt förslaget kan störningar i IKT-leveranskedjorna ha en negativ inverkan på den inre marknadens funktion, orsaka ekonomiska förluster, undergräva användarnas förtroende för tjänster och produkter samt orsaka allvarlig skada för europeiska ekonomiska samarbetsområdet och medlemsstaternas verksamhet.

Enligt artikel 52.1 i EU:s stadga om de grundläggande rättigheterna ska varje begränsning i utövandet av rättigheter och friheter vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Enligt förslaget ska ett eventuellt förbud mot att använda IKT-komponenter från högriskleverantörer föregås av olika åtgärder som ökar proportionaliteten. Först ska medlemsstaterna och kommissionen utarbeta en gemensam riskbedömning av de risker som riktas mot IKT-leveranskedjan, centrala fientliga aktörer och sårbarheter som riktas mot de kritiska IKT-tillgångar som identifierats i bedömningarna. Om det i en sådan riskbedömning eller utifrån ett uttalande av en medlemsstat finns bevis på att ett tredjeland skulle medföra en allvarlig och strukturell icke-teknisk risk för IKT-leveranskedjorna, ska kommissionen utifrån detta göra en separat bedömning utifrån kriterierna i förslaget. I bedömningen ska kommissionen beakta vilken inverkan eventuella begränsningar har på verksamheten i de sektorer som omfattas av NIS2-direktivet och tillgången på alternativa leverantörer som kunde ersätta högriskleverantörernas IKT-komponenter.

I samband med att kommissionen utarbetar genomförandeakter ska den höra medlemsstaterna i granskningsförfarandet. Dessutom går kommissionen igenom sina preliminära observationer med den entitet som är föremål för högriskbedömningen och ger entiteten möjlighet att bli hörd. En entitet som är baserad i eller som kontrolleras från ett tredjeland som orsakar cybersäkerhetsbekymmer kan ansöka om undantag från begränsningarna för högriskleverantörer på de villkor som nämns i förslaget. En entitet som finns med i förteckningen över högriskleverantörer kan be kommissionen göra en ny bedömning om entiteten lämnar in bevis på ändringar.

Grundlagsutskottet har i sina tidigare utlåtanden konstaterat att grundlagen inte skyddar egendom mot alla användningsbegränsningar, och att ägarens rättigheter kan begränsas genom en lag som uppfyller de allmänna förutsättningar som krävs av en lag som begränsar de grundläggande fri- och rättigheterna (GrUB 25/1994 rd). Enligt grundlagsutskottets utlåtandepraxis (10/2007 rd) har lagstiftaren större marginaler vid begränsning av egendomsskyddet när regleringsobjektet har särdrag, såsom teknisk komplexitet och en internationell verksamhetsmiljö, skyldigheterna gäller börsbolag eller juridiska personer med betydande förmögenhetsmassa och det är fråga om reglering på EU-nivå som ovan nämnda företag ska förbereda sig på. Enligt Europeiska unionens domstols rättspraxis (C-292/97) går det dessutom att begränsa användningen av grundläggande fri- och rättigheter, förutsatt att dessa begränsningar faktiskt motsvarar det allmänna intresse som eftersträvas av gemenskapen (unionen) och att de inte utgör ett oproportionerligt och orimligt ingripande i förhållande till det eftersträvade målet som äventyrar kärnan i de grundläggande fri- och rättigheterna. Enligt 15 § 2 mom. i grundlagen bestäms expropriation av egendom för allmänt behov mot full ersättning genom lag. Åtgärder enligt förslaget som förbjuder entiteter som hör till de sektorer som omfattas av NIS 2-direktivet att använda IKT-komponenter från högriskleverantörer kan ha betydelse för sådan expropriation som avses i 15 § 2 mom. i grundlagen. Grundlagsutskottet har i sin utlåtandepraxis (35/2020 rd) ansett att tillämpningsområdet för bestämmelsen ovan inte begränsar sig enbart till situationer där äganderätten övergår från ett subjekt till ett annat. Enligt grundlagsutskottet kan en begränsning av användningen av egendom vara så betydande att den till sina faktiska verkningar kan jämställas med expropriation, och då måste bedömas med avseende på 15 § 2 mom. i grundlagen. Reglering som ingriper i egendomsskyddet bedöms med tanke på de allmänna förutsättningarna för att begränsa de grundläggande fri- och rättigheterna,

såsom godtagbarheten för regleringens syfte och regleringens proportionalitet (GrUU 31/2006 rd).

Kommissionens förslag kan bedömas ha betydelse för offentlighetsprincipen enligt 12 § 2 mom. i grundlagen och för utlämnandet av sekretessbelagda uppgifter. Ett sådant utlämnande av uppgifter som avses i förordningen kan förutsätta att sekretessbelagda uppgifter lämnas ut till Enisa, EU-kommissionen och andra medlemsländer. Kommissionen har inte gjort någon närmare bedömning av betydelsen av sekretessbelagda uppgifter och informationsutbyte.

Grundlagsutskottet har i sina tidigare utlåtanden fäst uppmärksamhet vid bland annat vad och vem rätten att få information gäller och hur rätten är kopplad till nödvändighetskriteriet. Myndigheternas rätt att få information och möjlighet att lämna ut information kan enligt utskottet gälla "behövliga uppgifter" för ett visst syfte, om lagen innehåller en uttömmande förteckning över innehållet i uppgifterna. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att "uppgifterna är nödvändiga" för ett visst syfte (t.ex. GrUU 13/2023 rd och GrUU 92/2022). Utskottet har dock ansett att grundlagen inte tillåter en generös och ospecificerad rätt att få uppgifter, inte ens om den är förenad med nödvändighetskriteriet (t.ex. 96/2022 rd). Vid bedömningen av exaktheten hos och innehållet i bestämmelserna om utlämnande av uppgifter har särskild betydelse fästs vid arten av de uppgifter som lämnas ut som känsliga uppgifter (t.ex. GrUU 96/2022).

Statsrådet stöder i huvudsak kommissionens åsikter. Förslaget kan främja skydd av personuppgifter som tryggas genom artikel 8 i stadgan om de grundläggande rättigheterna och i 10 § i grundlagen. Statsrådet anser att förslaget gynnar den offentliga sektorn, men å andra sidan ökar enskilda personers förtroende för cybersäkerhetens verksamhetsfält och skyddet av personuppgifter. I den fortsatta beredningen fäster statsrådet uppmärksamhet vid 12 § i grundlagen och vid att bestämmelserna om informationsutbyte är exakt och noggrant avgränsade. Bestämmelserna behöver eventuellt kompletteras i detta avseende.

7 Ålands ställning

Reformen av cybersäkerhetsakten och direktivet om ändring av NIS 2-direktivet innehåller bestämmelser om åtgärder i anslutning till cybersäkerhet som skulle förenkla, effektivisera och förtydliga samarbetet mellan medlemsstaterna och unionens organ och skapa en mer enhetlig marknad inom cybersäkerhet. Fördelningen av lagstiftningsbehörigheten mellan riket och landskapet följer självstyrelselagen för Åland (1144/1991, nedan självstyrelselagen). Självstyrelselagen innehåller inga separata bestämmelser om fördelningen av lagstiftningsbehörigheten i fråga om cybersäkerhet eller informationssäkerhet. Därmed ska frågan bedömas i enlighet med de övriga grunderna för fördelningen av behörigheten mellan landskapet och riket som ingår i självstyrelselagen.

Enligt 27 § i självstyrelselagen har riket lagstiftningsbehörighet i fråga om bland annat statsmyndigheternas organisation och verksamhet, standardisering, televerksamhet samt andra än i paragrafen särskilt nämnda privaträttsliga angelägenheter, om de inte direkt hänför sig till ett rättsområde som enligt självstyrelselagen hör till landskapets lagstiftningsbehörighet. Enligt 18 § i självstyrelselagen har landskapet lagstiftningsbehörighet i fråga om bland annat landskapsregeringen och under denna lydande myndigheter och inrättningar, hälso- och sjukvård med vissa undantag samt näringsverksamhet med vissa undantag.

Statsrådet anser att förslagen fördelas delvis på rikets lagstiftningsbehörighet och delvis på landskapets. I fråga om förslaget till cybersäkerhetsakt hör förslaget i huvudsak till rikets lagstiftningsbehörighet. I fråga om de förslag i cybersäkerhetsakten som gäller säkerheten i

IKT-leveranskedjorna samt i fråga om förslagen om ändring av NIS 2-direktivet fördelas lagstiftningsbehörigheten mellan riket och landskapet till de delar förslagen gäller de sektorer där landskapet har lagstiftningsbehörighet med stöd av självstyrelselagen.

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

Kommissionen lade fram förslaget till förordning den 20 januari 2026.

Behandlingen av förslaget inleddes i rådets övergripande arbetsgrupp för cyberfrågor den 26 januari 2026. Behandlingen av förslaget i Europaparlamentet har ännu inte inletts.

9 Nationell behandling av förslaget

U-skrivelsen har beretts som tjänsteuppdrag vid kommunikationsministeriet.

Den behandlas i finansutskottet den 12 mars 2026. Utkastet till U-skrivelse har behandlats i sektionen för kommunikation och sektionen för hybridhot den 13–16 februari 2026. Dessutom ordnades samrådsmöten om förslaget för myndigheter och den privata sektorn den 4 februari 2026.

10 Statsrådets ståndpunkt

Cybersäkerhetsakten (CSA2)

Statsrådet anser att cybersäkerhet är en viktig del av tryggandet av störningsfri verksamhet och samhällsstabilitet på EU:s inre marknad samt medborgarnas integritet. Statsrådet understöder EU-lagstiftningens mål att stärka förvaltningen av cybersäkerheten samt att behöriga organ, myndigheter och andra intressenter ska ha bättre förutsättningar att förebygga, upptäcka och bekämpa cybersäkerhetshot på ett samordnat och effektivt sätt.

Statsrådet förhåller sig positivt till en övergripande översyn av Europeiska unionens cybersäkerhetsbyrå Enisas mandat med beaktande av den förändrade hotbilden och unionens lagstiftning om cybersäkerhet. Statsrådet anser att Enisas verksamhet ska vara effektiv, prioriterad och transparent. Enisas verksamhet och uppgifter bör i första hand komplettera de cybersäkerhetsuppgifter som medlemsländernas myndigheter har.

Statsrådet förhåller sig positivt till att Enisas verksamhet utvidgas till att omfatta stöd av operativt samarbete och skapande av en lägesbild, dock med beaktande av att medlemsländerna och deras myndigheter har det primära ansvaret för myndighetsuppgifter som säkerställer cybersäkerheten och stöder samhällsaktörer. Statsrådet förhåller sig avvaktande till informationsutbyte som kan ha negativa konsekvenser för den nationella säkerheten. Statsrådet förhåller sig dock positivt till en intensifiering av Enisas samarbete med partnerländer och internationella organisationer, såsom Nato.

Statsrådet anser att det är särskilt viktigt att utvidga Enisas uppgifter till tjänster som har att göra med hantering av sårbarheter i informationssystem. Genom att stärka unionens egen förmåga att hantera sårbarheter i informationssystem stärks unionens strategiska autonomi.

Statsrådet anser att det är viktigt att medlemsländerna och kommissionen även i fortsättningen har en jämlik ställning i beslutsfattandet som har med Enisas verksamhet att göra.

Medlemsländerna ska själva kunna fatta beslut om de representanter som utnämns till byråns organ och om de sakkunniga som sänds till byrån.

Statsrådet anser att det är viktigt att den här förordningen inte förebådar finansieringen av den kommande budgetramen (2028–2034). Det tas separat ställning till dimensioneringen av finansieringen för kommande period som en del av förhandlingarna om budgetramen som helhet.

Statsrådet betonar att förvaltningsutgifterna och antalet anställda vid EU:s institutioner och byråer ska hållas på en rimlig nivå. I den fortsatta beredningen ber statsrådet om preciseringar av de avgifter som Enisa tar och av finansieringen av verksamheten.

Statsrådet förhåller sig avvaktande till utvecklingen av en mer ingående reglering i anslutning till cybersäkerhetskompetens. Statsrådet anser att det är viktigt att se till att åtgärderna i fråga om kompetens är frivilliga och resursneutrala för medlemsstaterna.

Statsrådet stöder allmänt reformen, effektiveringen och förtydligandet av den europeiska ramen för cybersäkerhetscertifiering. Statsrådet förhåller sig i princip positivt till att arbetet på cyberområdet och presumtionen om överensstämmelse med kraven i EU-lagstiftningen inkluderas i tillämpningsområdet för certifieringsordningar. Vidare understöder statsrådet att strategin och åtgärderna för upprätthållande av europeiska ordningar för cybersäkerhetscertifiering läggs till som en del av certifieringsramen. Statsrådet anser att det är viktigt att medlemsstaterna har möjlighet att delta i processerna inom den europeiska ramen för cybersäkerhetscertifiering. Dessutom anser statsrådet att certifieringarna i princip ska förbli frivilliga.

Statsrådet understöder att EU utifrån förslaget söker gemensamma lösningar för IKT-leveranskedjor som stärker säkerheten, främjar den inre marknadens funktion och EU:s tekniska suveränitet. Åtgärderna ska vara förutsägbara och kontrollerade samt grunda sig på ändamålsenligt hörande och konsekvensbedömning. Statsrådet anser att åtgärderna som presenteras i förslaget även ska vara proportionerliga och riskbaserade. Statsrådet anser att det är viktigt att medlemsstaterna även i fortsättningen kan ställa nationella skyldigheter och åtgärder som går längre än förslaget till förordning, i synnerhet för att trygga säkerheten i kommunikationsnäten. Statsrådet stöder förslagets mål och anser samtidigt att det är viktigt att gränserna mellan unionens och medlemsstaternas befogenheter förblir tydliga, i synnerhet i frågor som gäller den nationella säkerheten. Statsrådet framhäver även medlemsstaternas centrala roll i riskbedömningen av IKT-leveranskedjorna.

Statsrådet förutsätter att de befogenheter som delegeras till kommissionen är noga avgränsade, proportionerliga, ändamålsenliga och motiverade.

Finlands ståndpunkter till meddelandet från kommissionen och den höga representanten om att stärka EU:s ekonomiska säkerhet framgår av utredningen E 3/2026 rd. Utredningen innehåller skrivningar som är relevanta med tanke på det aktuella förslaget. Utredningen innehåller en anteckning, som är grundläggande ur förslagets synvinkel, på internationellt samarbete för att minska skadliga beroenden:

För att minska skadliga beroenden måste EU avancera snabbt i handelsförhandlingar och partnerskap till exempel i leverans- och värdekedjor för kritiska råvaror, industri, energi och kritisk teknik. EU borde undersöka fördelarna och möjligheterna med att skapa standarsbaserade marknader och investera i regleringssamarbete med partners från tredjeländer.

EU måste göra omfattande användning av unionens existerande instrument även i samarbete med tredjeländer för att bryta skadliga beroenden.

Därtill framgår Finlands ståndpunkter till meddelandet från kommissionen om kompetensunionen av utredningen E 56/2025 rd, där följande skrivning beaktas när det gäller det aktuella förslaget:

Finland anser att det är viktigt att kommissionens förslag grundar sig på tillräckligt omfattande konsekvensbedömningar. Finland betonar att det är viktigt att planera åtgärder på EU-nivå så att de är kostnadseffektiva, inte ökar den administrativa bördan, beaktar medlemsländernas olika utbildningssystem och arbetskraftspolitiska prioriteringar och utnyttjar befintliga strukturer i så stor utsträckning som möjligt.

Direktivet om ändring av NIS 2-direktivet

Statsrådet understöder ändringsförslagens mål att förenkla regleringen och göra den smidigare samt minska de administrativa kostnaderna som regleringen medför. Statsrådet förhåller sig positivt till ändringsförslag som främjar dessa mål och samtidigt tryggar en hög nivå av cybersäkerhet.

Statsrådet anser att det är nödvändigt att förhandlingarna omfattar en närmare bedömning av förslagets konsekvenser för de kostnader som regleringen orsakar för entiteterna och för målen i förslaget.

Statsrådet förhåller sig positivt till ändringsförslagen som gäller direktivets tillämpningsområde och till förslaget att höja storleksgränsen för centrala entiteter. Statsrådet anser det vara nödvändigt att precisera tillämpningsområdet i synnerhet i fråga om småskaliga elproducenter och kemiindustrin. Statsrådet anser att det är nödvändigt att i förhandlingarna göra en mer detaljerad bedömning av kommissionens förslag att inkludera ägare och operatörer av strategisk infrastruktur med dubbla användningsområden i direktivets tillämpningsområde, i synnerhet med tanke på försvaret och den nationella säkerheten.

Statsrådet anser att det är viktigt att kraven i NIS 2-direktivet är proportionerliga och riskbaserade. Statsrådet förhåller sig preliminärt avvaktande till förslaget om kommissionens behörighet när det gäller fullständig harmonisering av riskhanteringsåtgärder genom genomförandeakter. Statsrådet anser att det är ändamålsenligt att medlemsstaterna har ett tillräckligt nationellt spelrum för att ställa krav på riskhanteringen.

Statsrådet anser att det i princip är bra att certifieringar enligt de europeiska ordningarna för cybersäkerhetscertifiering kan utnyttjas för att påvisa att kraven som NIS 2-direktivet ställer uppfylls.

Statsrådet förhåller sig positivt till förslaget om Enisas uppgift att göra bedömningar av gränsöverskridande cybersäkerhetsrisker. Statsrådet anser dock att det är viktigt att Enisas befogenheter att stödja tillsynsmyndigheterna och få information om dem grundar sig på samtycke av medlemsstatens myndighet.

Statsrådet förhåller sig preliminärt avvaktande till förslaget om nya skyldigheter i anslutning till anmälan av uppgifter om utpressningsprogram samt till förslaget om utvidgning av den befogenhet som delegeras till kommissionen i fråga om anmälan av uppgifter om utpressningsprogram. Statsrådet anser till denna del att det är nödvändigt att i förhandlingarna

närmare bedöma hur förslaget påverkar de kostnader och den administrativa börda som regleringen innebär för entiteterna.