RP 27/2025 rd

Regeringens proposition till riksdagen med förslag till lagar om ändring av cybersäkerhetslagen och 3 § i lagen om informationshantering inom den offentliga förvaltningen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att cybersäkerhetslagen och lagen om informationshantering inom den offentliga förvaltningen ändras.

Genom propositionen utvidgas tillämpningsområdet för cybersäkerhetslagen och lagen om informationshantering inom den offentliga förvaltningen till att gälla sådana sammanslutningar som identifieras som kritiska med tanke på samhällets funktion enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Genom propositionen kompletteras det nationella genomförandet av Europaparlamentets och rådets direktiv om kritiska entiteters motståndskraft och av cybersäkerhetsdirektivet.

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

Lagen avses träda i kraft samtidigt som den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Informations- och kommunikationsteknik och därmed anslutna tjänster är en viktig del av det moderna samhället och dess kritiska infrastruktur. Avancerade informations- och kommunikationstekniska lösningar möjliggör nya innovationer, verksamhetssätt och tjänster i samhället. Samtidigt är allt fler tjänster och funktioner i allt högre grad beroende av att kommunikationsnäten och informationssystemen fungerar på ett pålitligt sätt. Cybersäkerheten i kommunikationsnät och informationssystem är föremål för många olika risker som om de realiseras orsakar störningar och skador som en följd av olika orsakssammanhang. När störningar eller skador uppstår kan detta vara en följd av en ouppsåtlig skada eller en uppsåtlig, olaglig gärning med varierande bakgrundsmotiv.

Finland är som ett informationssamhälle beroende av fungerande kommunikationsnät och informationssystem och således också sårbart för störningar i dem. Med tanke på den övergripande säkerheten i samhället är det viktigt att öka graden av cybersäkerhet i kommunikationsnät och informationssystem. Störningar anslutna till cybersäkerhet kan få betydande ekonomiska följder för såväl samhället som enskilda medborgare, företag och andra sammanslutningar. Med tanke på tjänsternas funktion kan sådana störningar vara särskilt skadliga som får som följd att tjänsterna eller uppgifter i dem inte är tillgängliga för användarna. Den ekonomiska skada som en störning orsakar kan vara en följd av till exempel skadad egendom, avbrott i företags affärsverksamhet eller utgifter för skydd mot skador. Med tanke på samhällets funktion är det viktigt att sörja för cybersäkerheten i sådana informationssystem och kommunikationsnät som används för att producera tjänster och bedriva verksamhet som är en del av samhällets kritiska infrastruktur.

Beredningen av propositionen har föranletts av Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, nedan *CER-direktivet*, samt Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), nedan *NIS 2-direktivet*.

Det nationella genomförandet av CER-direktivet beskrivs i regeringens proposition RP 205/2024 rd till riksdagen med förslag till lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft och till vissa andra lagar. Behandlingen av den regeringspropositionen pågår i riksdagen. Det har föreslagits att det för genomförandet av CER-direktivet ska stiftas en ny lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Kritiska entiteter enligt CER-direktivet ska med stöd av lagen identifieras i Finland i enlighet med den tidsplan som CER-direktivet förutsätter före sommaren 2026.

NIS 2-direktivet förutsätter att på entiteter som identifieras som kritiska entiteter enligt CER-direktivet tillämpas, oavsett deras storlek, skyldigheterna som gäller cybersäkerhet enligt NIS 2-direktivet. Bestämmelser om cybersäkerhetsskyldigheterna enligt NIS 2-direktivet finns i cybersäkerhetslagen (124/2025) och i 4 a kap. i lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan *informationshanteringslagen*). Eftersom cybersäkerhetslagens tillämpningsområde är omfattande, omfattas största delen av de aktörer (i direktiven ”entiteter”, men i de föreslagna lagarna ”aktörer”) som identifieras som kritiska också

sedan tidigare av tillämpningsområdet för de skyldigheter som gäller cybersäkerhet. På motsvarande sätt omfattar även informationshanteringslagens tillämpningsområde största delen av de aktörer inom sektorn för offentlig förvaltning som identifieras som kritiska, eftersom tillämpningsområdet för 4 a kap. som gäller cybersäkerhetsskyldigheterna inom sektorn för offentlig förvaltning i princip är mer omfattande än sektorn för offentlig förvaltning i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Genomförandet av direktiven behöver dock kompletteras så att skyldigheterna som gäller cybersäkerhet tillämpas på aktörer som identifieras som kritiska aktörer enligt CER-direktivet också när en kritisk aktör inte sedan tidigare omfattas av tillämpningsområdet för cybersäkerhetslagen eller i fråga om sektorn för offentlig förvaltning tillämpningsområdet för 4 a kap. i informationshanteringslagen.

I avsnitt 10 i regeringens proposition RP 205/2024 rd konstateras det att statsrådet separat bereder en proposition med förslag till sådana tekniska lagstiftningsändringar som behövs för att skyldigheterna enligt den föreslagna cybersäkerhetslagen (RP 57/2024 rd) ska kunna tillämpas på de kritiska aktörer som identifieras enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft, på det sätt som NIS 2-direktivet och CER-direktivet förutsätter. I denna proposition är det fråga om de lagstiftningsändringar som det hänvisas till.

NIS 2-direktivet har genomförts nationellt genom cybersäkerhetslagen (124/2025). I fråga om sektorn för offentlig förvaltning har NIS 2-direktivet dessutom genomförts genom ändringar av informationshanteringslagen (125/2025).

1.2 Beredning

Regeringens proposition har beretts som tjänsteuppdrag vid kommunikationsministeriet i samarbete med inrikesministeriet och finansministeriet.

Beredningen av NIS 2-direktivet och det nationella genomförandet av det beskrivs i avsnitt 1.2 i regeringens proposition RP 57/2024 rd.

Beredningen av CER-direktivet och det nationella genomförandet av det beskrivs i avsnitt 1.2 i regeringens proposition RP 205/2024 rd.

2 EU-rättsaktens målsättning och huvudsakliga innehåll

I detta avsnitt beskrivs de viktigaste punkter i direktivens innehåll som hänför sig till de föreslagna ändringarna i cybersäkerhetslagen och informationshanteringslagen. NIS 2-direktivets målsättning och huvudsakliga innehåll beskrivs till övriga delar i avsnitt 2 i regeringens proposition RP 57/2024 rd och CER-direktivets målsättning och huvudsakliga innehåll i avsnitt 2 i regeringens proposition RP 205/2024 rd.

Tillämpning av NIS 2-direktivet på entiteter som identifieras enligt CER-direktivet

NIS 2-direktivet innehåller bestämmelser om åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Syftet med CER-direktivet är att säkerställa att den inre marknaden fungerar i fråga om kritiska tjänster inom tillämpningsområdet för direktivet och att stärka motståndskraften hos tjänster som är nödvändiga för Europeiska unionen samt att upprätthålla samhällets vitala och ekonomiska funktioner genom att fastställa vissa kritiska sektorer som tillhandahåller sådana tjänster. Målet med NIS 2-direktivet är att höja både EU:s gemensamma och medlemsstaternas nationella

cybersäkerhetsnivå i fråga om sektorer och typer av entiteter som är väsentliga och viktiga med tanke på samhällets funktion. Syftet med CER-direktivet är att stärka kritiska entiteters motståndskraft på den inre marknaden.

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

Med stöd av artikel 2.3 i NIS 2-direktivet är direktivet oavsett entiteternas storlek tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER-direktivet. Genom CER-direktivet åläggs kritiska entiteter andra skyldigheter än sådana som gäller cybersäkerhet i fråga om riskhantering och rapportering av incidenter. Till de delar som gäller cybersäkerhet ska på kritiska entiteter tillämpas de skyldigheter enligt NIS 2-direktivet som gäller riskhantering och rapportering av incidenter.

I artikel 6 i CER-direktivet föreskrivs det om identifiering av kritiska entiteter. Medlemsstaterna ska senast den 17 juli 2026 identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i bilagan till CER-direktivet. I artikel 6.2 föreskrivs det om de kriterier som hänsyn ska tas till vid identifieringen. Artikel 6.3 innehåller bestämmelser om medlemsstaternas skyldighet att upprätta en förteckning över kritiska entiteter och att säkerställa att de kritiska entiteterna underrättas om att de har identifierats som kritiska entiteter. Medlemsstaterna ska också informera dessa kritiska entiteter om deras skyldigheter. Enligt artikel 6.4 ska medlemsstaterna säkerställa att deras behöriga myndigheter enligt CER-direktivet underrättar de behöriga myndigheterna enligt NIS 2-direktivet om identiteten på de kritiska entiteter som de har identifierat enligt denna artikel inom en månad från den identifieringen. Medlemsstaterna ska enligt artikel 6.5 vid behov och minst vart fjärde år uppdatera förteckningen över kritiska entiteter. Kommissionen ska i samarbete med medlemsstaterna utarbeta rekommendationer och icke-bindande riktlinjer för att stödja medlemsstaterna i arbetet med att identifiera kritiska entiteter.

Väsentliga entiteter

Entiteter som identifierats som kritiska entiteter enligt CER-direktivet ska enligt artikel 3.1 f i NIS 2-direktivet med avseende på tillämpningen av NIS 2-direktivet anses vara väsentliga entiteter.

Skillnaden mellan väsentliga och viktiga entiteter är av betydelse med tanke på bestämmelserna om tillsyn och administrativa sanktioner i NIS 2-direktivet. I fråga om väsentliga entiteter ska tillsynen omfatta förhandstillsyn och efterhandstillsyn, men i fråga om viktiga entiteter räcker det enligt direktivet med endast tillsyn i efterhand. Direktivet förutsätter även vissa tillsynsbefogenheter som gäller väsentliga entiteter och som inte förutsätts i fråga om viktiga entiteter. I direktivet fastställs dessutom sanktionsavgiftens lägsta tillåtna maximibelopp för väsentliga entiteter till en högre nivå än i fråga om viktiga entiteter. På det sätt som konstateras ovan förutsätter NIS 2-direktivet att kritiska entiteter ska anses vara väsentliga entiteter. Bestämmelser om tillsynsåtgärder i fråga om väsentliga entiteter finns i artikel 32 i NIS 2-direktivet och bestämmelser om nivån på administrativa sanktionsavgifter i artikel 34.

Incidentanmälningar

I artikel 23 i NIS 2-direktivet föreskrivs det om entiteters skyldighet att underrätta den behöriga myndigheten och enheten för hantering av it-säkerhetsincidenter, det vill säga CSIRT-enheten

enligt NIS 2-direktivet, om betydande incidenter. Artikel 30 i NIS 2-direktivet innehåller bestämmelser om annan underrättelse än den som entiteterna är förpliktade till.

Enligt artikel 23.10 i NIS 2-direktivet ska CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna förse de behöriga myndigheterna enligt CER-direktivet med information om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med artikel 23.1 och artikel 30 i NIS 2-direktivet av entiteter som identifierats som kritiska i enlighet med CER-direktivet.

Samarbete mellan tillsynsmyndigheterna

I artikel 13 i NIS 2-direktivet föreskrivs det om myndighetssamarbete på nationell nivå inom tillsynen enligt NIS 2-direktivet. I artiklarna 13.4 och 13.5 föreskrivs det om samarbetet mellan tillsynsmyndigheterna enligt NIS 2-direktivet och CER-direktivet. I artikel 13.4 förutsätts det att medlemsstaterna främjar bland annat myndighetsarbetet med brottsbekämpande myndigheter, dataskyddsmyndigheter, civila luftfartsmyndigheter, tillsynsmyndigheten enligt Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen) och tillsynsmyndigheten enligt Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (nedan DORA-förordningen). Enligt artikel 13.5 ska medlemsstaterna säkerställa att deras behöriga myndigheter enligt NIS 2-direktivet och deras behöriga myndigheter enligt CER-direktivet regelbundet samarbetar och utbyter information avseende identifieringen av kritiska entiteter, om risker, cyberhot och incidenter samt icke-cyberrelaterade risker, hot och incidenter som berör väsentliga entiteter som identifierats som kritiska, samt om de åtgärder som vidtagits till följd av sådana risker, hot och incidenter.

I artikel 32 i NIS 2-direktivet föreskrivs det om tillsyn över väsentliga entiteter. Artikel 32.9 förutsätter att medlemsstaternas behöriga myndigheter enligt NIS 2-direktivet informerar de relevanta behöriga myndigheterna inom samma medlemsstat i enlighet med CER-direktivet när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en entitet som identifierats som en kritisk entitet i enlighet med CER-direktivet efterlever NIS 2-direktivet. I artikeln sägs det även att när så är lämpligt får behöriga myndigheter enligt CER-direktivet begära att behöriga myndigheter enligt NIS 2-direktivet utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en kritisk entitet.

Nationellt handlingsutrymme

NIS 2-direktivet och CER-direktivet är till sin karaktär minimiharmoniserande. Direktiven hindrar inte medlemsstaterna från att behålla nationella bestämmelser som säkerställer en högre cybersäkerhetsnivå eller en högre grad av motståndskraft för kritiska entiteter, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

NIS 2-direktivet och CER-direktivet innehåller inget nationellt handlingsutrymme som gäller tillämpningen av de skyldigheter enligt NIS 2-direktivet som gäller hantering av cybersäkerhetsrisker och rapportering av betydande incidenter på entiteter som identifierats som kritiska i enlighet med CER-direktivet eller när dessa entiteter betraktas som väsentliga entiteter som avses i NIS 2-direktivet. Det nationella handlingsutrymme som är centralt med tanke på

propositionen hänför sig till hur tillsynen över efterlevnaden av bestämmelserna och de därmed anslutna myndighetsuppgifterna ska ordnas i Finland.

Till övriga delar beskrivs det nationella handlingsutrymmet i fråga om NIS 2-direktivet i avsnitt 2 i regeringens proposition RP 57/2024 rd och i fråga om CER-direktivet i avsnitt 2 i regeringens proposition RP 205/2024 rd.

3 Nuläge och bedömning av nuläget

I Finland har det inte identifierats kritiska aktörer enligt CER-direktivet. Kritiska aktörer ska identifieras i enlighet med CER-direktivet första gången senast i juli 2026. Identifieringen av kritiska aktörer ska göras enligt den föreslagna CER-genomförandelagen, det vill säga den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Regeringens proposition RP 205/2024 rd som gäller lagen behandlas i riksdagen.

NIS 2-direktivet har genomförts genom den nya cybersäkerhetslagen och till den del som gäller den offentliga förvaltningen genom informationshanteringslagen. Cybersäkerhetslagen och ändringarna i informationshanteringslagen har trätt i kraft den 8 april 2025 (RP 57/2024 rd; RSv 15/2025 rd). I cybersäkerhetslagen föreskrivs det om skyldigheterna enligt NIS 2-direktivet för andra aktörer än aktörer inom sektorn för offentlig förvaltning. Cybersäkerhetslagens tillämpningsområde omfattar nästan alla sektorer från vilka kritiska aktörer ska identifieras i enlighet med CER-direktivets tillämpningsområde.

Följande aktörer kan identifieras som kritiska enligt CER-direktivet, även om de i nuläget inte nämns i bilagorna I eller II som anger cybersäkerhetslagens tillämpningsområde:

- Vägtrafik, kollektivtrafik (kollektivtrafikföretag enligt definitionen i artikel 2 d i Europaparlamentets och rådets förordning (EG) nr 1370/2007)

- Hälso- och sjukvård, entiteter med tillstånd att bedriva partihandel (entiteter med tillstånd att bedriva partihandel i den mening som avses i artikel 79 i direktiv 2001/83/EG)

Med stöd av CER-direktivet kan som kritiska aktörer identifieras också aktörer som underskrider den storleksgräns för medelstora företag som gäller cybersäkerhetslagens tillämpningsområde, det vill säga är små företag eller mikroföretag.

I cybersäkerhetslagen och i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har tillsynsmyndighetens uppgifter fördelats sektorsvis på i huvudsak samma myndigheter. Således övervakas skyldigheterna enligt CER-direktivet och NIS 2-direktivet av i huvudsak samma myndigheter inom olika sektorer. Eftersom det dock finns flera tillsynsmyndigheter och det undantagsvis är möjligt att skyldigheterna inte i alla situationer övervakas av samma myndigheter för samma aktörer, behöver det föreskrivas om samarbete och informationsutbyte mellan tillsynsmyndigheterna på det sätt som NIS 2-direktivet och CER-direktivet förutsätter.

Inom sektorn för offentlig förvaltning tillämpas NIS 2-direktivet på aktörer inom offentlig förvaltning på central och regional nivå, medan aktörerna inom offentlig förvaltning på lokal nivå däremot omfattas av det nationella handlingsutrymmet. CER-direktivet tillämpas endast på aktörer inom den offentliga förvaltningen på central nivå. I direktiven fastställs i stort sett samstämmigt på vilka entiteter inom sektorn för offentlig förvaltning bestämmelserna inte

tillämpas. Således är det osannolikt att en aktör inom sektorn för offentlig förvaltning som bestämmelserna om cybersäkerhet i 4 a kap. i informationshanteringslagen inte tillämpas på identifieras som en kritisk aktör med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Detta är dock möjligt, eftersom tillämpningen av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har fastställts på ett i lagtekniskt hänseende delvis annat sätt i den lagen än det sätt på vilket tillämpningen av informationshanteringslagens 4 a kap. som gäller genomförandet av NIS 2-direktivet har fastställts i 3 § i den lagen. I CER-genomförandelagen definieras till exempel inte till alla delar entydigt på lagnivå de aktörer inom den offentliga förvaltningen inom området för den nationella säkerheten, den allmänna säkerheten, försvaret och laglighetsövervakningen som bestämmelserna inte tillämpas på.

Eftersom CER-direktivet och NIS 2-direktivet förutsätter att skyldigheterna enligt NIS 2-direktivet ska tillämpas på entiteter som identifieras som kritiska, behöver det för komplettering av genomförandet av direktiven föreslås ändringar i lagstiftningen genom vilka skyldigheterna enligt cybersäkerhetslagen ska tillämpas på kritiska aktörer som identifierats i enlighet med CER-direktivet också när aktören inte annars omfattas av cybersäkerhetslagens tillämpningsområde, det vill säga är ett småföretag eller mikroföretag eller en aktör som bedriver kollektivtrafik eller partihandel med läkemedel. Av ovan beskrivna skäl behöver också de bestämmelser om tillämpningsområdet för 4 a kap. i informationshanteringslagen som finns i 3 § kompletteras med en bestämmelse som gäller tillämpningen av kapitlet på kritiska aktörer. För att komplettera genomförandet behöver det dessutom föreslås ändringar i lagstiftningen genom vilka en kritisk aktör som har identifierats i enlighet med CER-direktivet betraktas som en väsentlig aktör också när aktören inte annars uppfyller definitionen av väsentlig aktör i cybersäkerhetslagen. Det behöver även göras ändringar i cybersäkerhetslagen vad gäller samordningen av tillsynen och myndighetssamarbetet på det sätt som direktiven förutsätter. Enligt 18 a § i informationshanteringslagen är en aktör inom den offentliga förvaltningen på central nivå (på vilken CER-direktivet tillämpas inom sektorn för offentlig förvaltning) en kritisk aktör. Således behöver definitionen av väsentliga och viktiga aktörer i informationshanteringslagen inte ändras.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

Syftet med propositionen är att komplettera det nationella genomförandet av NIS 2-direktivet och CER-direktivet i fråga om tillämpningen av de skyldigheter som gäller cybersäkerhet på kritiska aktörer. Målet för propositionen är att genomföra de lagstiftningsändringar som behövs för att skyldigheterna som gäller cybersäkerheten enligt cybersäkerhetslagen och informationshanteringslagen ska kunna tillämpas på de kritiska aktörer som identifieras enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Ett viktigt förslag i propositionen är att cybersäkerhetslagen och informationshanteringslagen ska kompletteras så att skyldigheterna enligt dem när det gäller cybersäkerhetsrelaterad riskhantering och rapportering av betydande incidenter också ska tillämpas på sammanslutningar som ska identifieras som kritiska aktörer enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. En aktör som har identifierats som kritisk är en väsentlig aktör som avses i cybersäkerhetslagen. I propositionen ingår dessutom lagstiftningstekniska förslag bland annat om tillsynsmyndigheternas behörighet och samarbete samt om en övergångsperiod för tillämpningen av skyldigheterna efter det att en aktör har identifierats som kritisk.

Förslagen motsvarar den miniminivå som NIS 2-direktivet och CER-direktivet förutsätter i fråga om nivån på de skyldigheter som gäller cybersäkerhet och tillsynen över dem för kritiska aktörer.

4.2 De huvudsakliga konsekvenserna

Konsekvenser för myndigheterna

Att företag eller sammanslutningar identifieras som kritiska enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft kan utöka antalet aktörer som omfattas av cybersäkerhetslagens tillämpningsområde samt i synnerhet antalet väsentliga aktörer som omfattas av förhandstillsynen. Propositionen medför således en liten ökning av uppgiftsmängden för tillsynsmyndigheterna enligt cybersäkerhetslagen samt av CSIRT-enhetens uppgiftsmängd, vilket föranleds av de nya aktörer som omfattas av lagens tillämpningsområde och att sådana aktörer betraktas som väsentliga aktörer som inte annars uppfyller tröskeln för en väsentlig aktör. Den förutsägbara ökningen av myndigheternas uppgiftsmängd i förhållande till de nuvarande uppgifterna enligt cybersäkerhetslagen beror på i vilken omfattning företag eller sammanslutningar i framtiden identifieras som kritiska aktörer enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Ökningen av uppgiftsmängden bedöms vara liten med beaktande av antalet aktörer som sedan tidigare omfattas av cybersäkerhetslagens tillämpningsområde.

Konsekvenserna för aktörerna inom den offentliga förvaltningen som föremål för riskhanterings- och rapporteringsskyldigheterna behandlas i regeringens proposition RP 57/2024 rd i slutet av avsnitt 4.4.1 samt konsekvenserna av ändringarna i informationshanteringen i avsnitt 4.4.2. I regeringens proposition RP 57/2024 rd (s. 118) sägs det att *”Fullgörandet av skyldigheterna kommer inte i regel att medföra betydande kostnader för de myndigheter som är föremål för dem. Ett undantag kan utgöras av aktörer inom den offentliga förvaltningen som förvaltar informationssystem som utnyttjas av flera myndigheter eller används i stor utsträckning. Dessutom kan propositionen ha indirekta konsekvenser för den dataskyddsnivå som krävs av de nya informationssystemen. Kostnaderna som uppstår när bestämmelserna iakttas ska täckas med anslag enligt rambeslutet för statsfinanserna och statsbudgeten.”* Såsom konstateras ovan i avsnitt 3 är det osannolikt att en aktör inom sektorn för offentlig förvaltning som bestämmelserna om cybersäkerhet i 4 a kap. i informationshanteringslagen inte tillämpas på sedan tidigare identifieras som en kritisk aktör med stöd av CER-genomförandelagen.

Konsekvenser för företagen

Propositionen har inga direkta ekonomiska konsekvenser för andra företag eller sammanslutningar än för dem som i framtiden identifieras som kritiska aktörer enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Propositionens konsekvenser för företag och sammanslutningar som i framtiden identifieras som kritiska aktörer enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft beror i avsevärd grad på om företaget eller sammanslutningen sedan tidigare har omfattats av tillämpningsområdet för skyldigheterna enligt cybersäkerhetslagen. Konsekvenserna beror dessutom i betydande grad på hur och i vilken omfattning ett företag eller en sammanslutning tidigare har genomfört riskhantering i

fråga om cybersäkerhet och i vilken utsträckning kommunikationsnät och informationssystem används i dess verksamhet.

Om företag eller sammanslutningar innan de identifieras som kritiska omfattas av cybersäkerhetslagens tillämpningsområde och är i 27 § 2 mom. i den lagen avsedda väsentliga aktörer, har propositionen inga direkta ekonomiska konsekvenser för dem.

Om företag eller sammanslutningar innan de identifieras som kritiska omfattas av cybersäkerhetslagens tillämpningsområde, men inte är i 27 § 2 mom. i den lagen avsedda väsentliga aktörer, har propositionen små ekonomiska konsekvenser för dem. Efter det att ett företag har identifierats som en kritisk aktör betraktas det som en väsentlig aktör.

För de företag och sammanslutningar som till följd av att de identifieras som kritiska blir nya organisationer som omfattas av cybersäkerhetslagens tillämpningsområde har propositionen ekonomiska konsekvenser. Konsekvenserna beror dessutom i betydande grad på hur och i vilken omfattning ett företag eller en sammanslutning tidigare har genomfört riskhantering i fråga om cybersäkerhet och i vilken utsträckning kommunikationsnät och informationssystem används i dess verksamhet.

Nya organisationer som omfattas av cybersäkerhetslagens tillämpningsområde kan vara företag eller sammanslutningar som har identifierats som kritiska och som till sin storlek är små företag eller mikroföretag, eller som bedriver sådan verksamhet som inte nämns i bilagorna till NIS 2-direktivet, men som nämns i bilagorna till CER-direktivet. Små företag eller mikroföretag är enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG företag som sysselsätter färre än 50 personer och vars omsättning eller balansomslutning inte överstiger 10 miljoner euro per år. De sektorer som nämns i bilagorna till CER-direktivet och som inte nämns i bilagorna till NIS 2-direktivet är kollektivtrafik och läkemedelspartiaffärer.

Eftersom cybersäkerhetslagens tillämpningsområde sedan tidigare i stor utsträckning omfattar medelstora och större företag som bedriver sådan verksamhet som avses i bilagorna till CER-direktivet, bedöms det att den grupp företag eller sammanslutningar som propositionen har mer än små ekonomiska konsekvenser för blir begränsad.

Propositionens konsekvenser beror i betydande grad på i vilken omfattning kritiska aktörer och i synnerhet små företag eller mikroföretag eller aktörer som bedriver kollektivtrafik eller läkemedelspartihandel identifieras enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Dessutom beror konsekvenserna i betydande grad på hur de kritiska aktörerna tidigare har genomfört riskhanteringen i fråga om cybersäkerhet.

Propositionen orsakar ekonomiska kostnader för företag i synnerhet om de på grund av kraven i lagstiftningen blir tvungna att satsa på informationssäkerheten i sina informationsnät på ett nytt sätt. Kostnadernas storlek beror på utgångsnivån för informationssäkerheten i ett företags informationssystem. Kostnadernas storlek beror också på riskhanteringsåtgärdernas art och omfattning när det bedöms huruvida de står i rätt proportion till de förutsebara riskerna och verksamhetens art. Kostnader orsakas till exempel av investeringar för att höja informationssäkerhetsnivån samt till exempel av kontroller för att verifiera informationssäkerhetsnivån. De mest betydande ekonomiska konsekvenserna av att en aktör identifieras som kritisk gäller små företag och mikroföretag, som annars på grund av sin storlek inte omfattas av cybersäkerhetslagens tillämpningsområde. Genomförandet av riskhanteringen och hanteringen av incidenter i enlighet med den miniminivå som NIS 2-direktivet förutsätter

kan för små företag eller mikroföretag som har identifierats som kritiska medföra kostnader som är väsentliga med tanke på omsättningen och antalet anställda.

Beloppet av de kostnader som propositionen orsakar påverkas av nivån på den riskhantering i fråga om cybersäkerhet som sedan tidigare genomförts i ett företag, verksamhetens art och omfattning samt antalet kommunikationsnät och informationssystem som används i verksamheten och deras art. Ju större och mer omfattande företagets verksamhet är, desto större är kostnaderna för riskhanteringen. De företagsspecifika skillnaderna i IT- och cybersäkerhetskostnaderna är betydande och står i väsentlig proportion till företagets verksamhet. Allmänt taget utgör IT-kostnaderna i genomsnitt cirka 4–5 procent av ett företags omsättning. Variationsbredden är 1,5–5 procent beroende på aktörens storlek, cybermognad och sektor. Det är svårt att särskilja enbart kostnaderna som hänför sig till cybersäkerhet eller cyberriskhantering från ett företags övriga it- eller riskhanteringskostnader. Det kan riktgivande bedömas att ett företag som omfattas av cybersäkerhetslagens tillämpningsområde orsakas kostnader för riskhantering i fråga om cybersäkerhet på den miniminivå som lagen förutsätter till ett belopp av cirka 0,2–0,8 procent av den årliga omsättningen, om jämförelsepunkten är en situation där företaget överhuvudtaget inte vidtar riskhanteringsåtgärder inom cybersäkerheten sedan tidigare. Bedömningarna är förenade med betydande osäkerhet i fråga om de företagsspecifika skillnaderna.

De behövliga ekonomiska satsningarna på informationssäkerheten i de enskilda kritiska företagens system är dock med beaktande av det nuvarande säkerhetsläget synnerligen motiverade och behövliga för samhället. Satsningarna är också till fördel för företagen själva, eftersom de ökar ett företags kunders förtroende för företagets tjänster. En förbättring av cybersäkerhetsnivån har positiva konsekvenser både för företagens förutsättningar för affärsverksamhet och för samhällsekonomin och samhällets kristålighet.

Konsekvenser för informationssamhället och säkerheten

Propositionen har positiva konsekvenser för utvecklingen av informationssamhället, eftersom propositionen främjar ibruktagandet av informationssäkra tjänster och praxis och därmed skapar efterfrågan på sådana tjänster och på experter inom cybersäkerhet. En förbättrad cybersäkerhetsnivå minskar störningarna i användningen av tjänsterna och främjar det allmänna förtroendet för digitala tjänster.

Propositionen bedöms ha positiva konsekvenser för medborgarnas säkerhet i och med att den främjar en störningsfri verksamhet i samhället. Propositionen främjar förmågan hos aktörer som är kritiska med tanke på samhällets funktion att tåla cyberstörningar, vilket förbättrar medborgarnas säkerhet i synnerhet när det inom en sektor eller tjänst är fråga om funktioner som påverkar medborgarnas säkerhet och som hänför sig till infrastruktur som är kritisk med tanke på samhällets funktion. Genom propositionen stärks även samhällets allmänna kristålighet och den nationella säkerheten till denna del. Dessutom kan det att synliga cyberstörningar blir vanligare inverka negativt på medborgarnas upplevelse av säkerhet i samhället, och att förhindra detta i fråga om kritiska aktörer är syftet med propositionen.

5 Alternativa handlingsvägar

Tillämpningen av miniminivån på skyldigheterna enligt NIS 2-direktivet på aktörer som identifieras som kritiska enligt CER-direktivet är inte förenad med nationellt handlingsutrymme.

Ett lagstiftningstekniskt alternativ till de föreslagna ändringarna är att bestämmelser om skyldigheterna enligt NIS 2-direktivet för kritiska aktörer tas in i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft i stället för i cybersäkerhetslagen. För en sådan sammanslutning som inte sedan tidigare omfattas av cybersäkerhetslagens tillämpningsområde, men som enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft identifieras som en kritisk aktör, kan alternativet förtydliga bestämmelserna, eftersom alla skyldigheter som identifieringen av sammanslutningen som kritisk medför för den då finns i den lagen. Vid beredningen av propositionen har det dock bedömts att största delen av de aktörer som identifieras som kritiska aktörer omfattas av cybersäkerhetslagens tillämpningsområde också före de identifieras som kritiska, eftersom cybersäkerhetslagens tillämpningsområde är omfattande och de bilagor till CER-direktivet och NIS 2-direktivet som anger tillämpningsområdena så gott som motsvarar varandra. Det är också osannolikt att en aktör inom sektorn för offentlig förvaltning som bestämmelserna om cybersäkerhet i 4 a kap. i informationshanteringslagen inte tillämpas på identifieras som en kritisk aktör med stöd av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Därför, och även i övrigt med beaktande av direktivens inbördes samband, är det viktigt att lagstiftningstekniskt välja det tillvägagångssätt som bäst säkerställer att förhållandet mellan bestämmelserna i cybersäkerhetslagen, informationshanteringslagen och den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft är tydligt och att skyldigheterna kan tillämpas som komplement till varandra i sammanslutningar som omfattas av båda författningarnas tillämpningsområde. Det tydligaste alternativet med tanke på lagstiftningshelheten och det alternativ som bäst undviker överlappande bestämmelser har bedömts vara att på det föreslagna sättet komplettera cybersäkerhetslagen och informationshanteringslagen så att de ska tillämpas på aktörer som identifieras som kritiska också när aktören inte annars omfattas av lagens tillämpningsområde, men har identifierats som kritisk enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

6 Remissvar

Regeringens proposition var på remiss den 24 januari–10 februari 2025.

Remisstiden har varit kortare än vanligt på grund av brådskan med att komplettera genomförandet av NIS 2-direktivet och CER-direktivet. Tidsfristen för godkännande av den nationella lagstiftningen om genomförande av direktiven löpte ut den 17 oktober 2024. Dessutom har de föreslagna lagändringarna till centrala delar varit på remiss i utkastet till regeringens proposition om genomförande av NIS 2-direktivet (begäran om utlåtande VN/18157/2023, material finns i utlåtandetjänsten på adressen www.utlåtande.fi).

Utlåtande om regeringens proposition lämnades av 26 aktörer, varav 23 inom utsatt tid. Utlåtanden lämnades inom utsatt tid av Finlands näringsliv rf, Energimyndigheten, Finanssiala ry, Finansinspektionen, Cyber Industri Finland, HSL Helsingin seudun liikenne JHL ry, Centralhandelskammaren, Transport- och kommunikationsverket, Lääketeollisuus ry, jord- och skogsbruksministeriet, Puolustus- ja Ilmailuteollisuus PIA ry, Finlands Fackförbunds Centralorganisation FFC rf, Tillstånds- och tillsynsverket för social- och hälsovården, social- och hälsovårdsministeriet, Suomen Taksiliitto r.y., Företagarna i Finland rf, Strålsäkerhetscentralen, Teknologiateollisuus ry, Terveysteknologia ry, dataombudsmannens byrå, Säkerhets- och kemikalieverket och finansministeriet. Också en privatperson lämnade ett utlåtande. Utlåtanden lämnades efter utsatt tid av Livsmedelsverket, inrikesministeriet och Finlands Kommunförbund rf. Fyra av dem som lämnat utlåtande hade inga kommentarer om

lagförslaget. Dessutom konstaterade Finansinspektionen och justitieministeriet att de inte hade några kommentarer om propositionen.

Det ansågs i utlåtandena att propositionen allmänt taget kan understödas. Utlåtandena innehöll kommentarer om sådant som gäller genomförandet av CER-direktivet, såsom identifieringen av kritiska aktörer och organiseringen av de myndighetsuppgifter som avses i CER-direktivet. Regeringens proposition innehåller inga förslag till dessa delar. På identifieringen av kritiska aktörer ska tillämpas vad som föreskrivs i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (RP 205/2024). Utlåtandena innehöll också vissa kommentarer om kriterierna för cybersäkerhetslagens tillämpningsområde, vilka inte föreslås bli ändrade genom propositionen.

De som lämnat utlåtande ansåg att de föreslagna ändringarna allmänt taget är behövliga och tillräckliga för att komplettera genomförandet av direktiven. De som lämnat utlåtande förhöll sig positivt till att kritiska aktörer omfattas av cybersäkerhetsskyldigheterna enligt NIS 2-direktivet och förstod att det utgör en del av den miniminivå som NIS 2-direktivet och CER-direktivet förutsätter för kraven på kritiska aktörer. Vissa intresseorganisationer påpekade att de bestämmelser som träder i kraft kan vara delvis överlappande med de redan gällande sektorspecifika bestämmelserna.

Flera av dem som lämnat utlåtande uttryckte oro över huruvida resurserna för myndighetsuppgifterna är tillräckliga. I utlåtandena uttrycktes oro över huruvida myndigheterna kan fullgöra de tillsynsskyldigheter som nu åläggs dem samt ge aktörerna råd om de skyldigheter som de nya bestämmelserna medför utan nya anslag. Energimyndigheten konstaterade att den inte på behörigt sätt kan genomföra ändringarna enligt de lagförslag som föreslås och som är under behandling med nuvarande och under de närmaste åren till och med minskande anslagen. Enligt jord- och skogsbruksministeriet kan det faktum att tillsynsmyndigheterna inte har anvisats separata permanenta resurser för tillsynen över de aktörer som omfattas av lagförslagens tillämpningsområde medföra utmaningar. De nya kostnader som regeringens proposition medför för myndigheterna påverkas i betydande grad av i vilken omfattning kritiska aktörer i framtiden identifieras enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Vissa intresseorganisationer anser att det skulle vara bra att noggrannare bedöma antalet företag som kommer att omfattas av bestämmelserna samt kostnadseffekterna också för företagen.

Inrikesministeriet föreslog att vad gäller identifiering av en kritisk aktör ska hänvisningen till den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft ändras från 10 § till 13 §. Enligt inrikesministeriets utlåtande gäller 13 § beslutsfattande om kritiska aktörer. Det fattas enligt inrikesministeriet i praktiken ett förvaltningsbeslut i ärendet, varefter aktören betraktas som en kritisk aktör enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Med anledning av utlåtandet har hänvisningen till den nämnda lagen preciserats i 3 § i lagförslag 1 vad gäller identifieringen av en kritisk aktör.

Finansministeriet identifierade i sitt utlåtande vissa ändringsbehov också i informationshanteringslagen. Genom informationshanteringslagen genomförs NIS 2-direktivet inom den i punkt 10 i bilaga I till NIS 2-direktivet avsedda sektorn för offentlig förvaltning. Med anledning av finansministeriets utlåtande har det till propositionen fogats ett lagförslag om ändring av 3 § i informationshanteringslagen.

Strålsäkerhetscentralen påpekade att den redan i nuläget övervakar kärnkraftverkens cybersäkerhet och att det i och med de föreslagna ändringarna kommer att finnas en annan

tillsynsmyndighet vid sidan av den. Strålsäkerhetscentralen ansåg att det är viktigt att den nämns som tillsynsmyndighet enligt 26 § i cybersäkerhetslagen. I propositionen föreslås inga ändringar i uppgiftsfördelningen mellan tillsynsmyndigheterna enligt cybersäkerhetslagen.

Vissa intresseorganisationer ansåg att den föreslagna övergångsperiod på en månad för tillämpningen av skyldigheterna efter det att en aktör identifierats som kritisk är för snäv. Energimyndigheten och Säkerhets- och utvecklingscentret för läkemedelsområdet ansåg att den föreslagna tidsfristen är lyckad. I utlåtandena föreslogs dessutom vissa mindre och tekniska ändringar i lagförslagen.

De utlåtanden om det nationella genomförandet av NIS 2-direktivet och CER-direktivet som lämnades i samband med beredningen av RP 57/2024 rd och RP 205/2024 rd har också utnyttjats vid beredningen av regeringens proposition.

7 Specialmotivering

7.1 Cybersäkerhetslagen

3 §. *Aktörer.* Det föreslås att till den förteckning över aktörer på vilka lagen tillämpas oavsett storlek som finns i *2 mom.* fogas en ny 5 punkt. Enligt den nya 5 punkten avses med en kritisk aktör en aktör som med stöd av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har identifierats som kritisk aktör. Kritiska aktörer är alltså kritiska aktörer som har identifierats i enlighet med CER-direktivet. Kritiska aktörer är sådana aktörer som avses i cybersäkerhetslagen oavsett deras storlek eller arten av den verksamhet som de bedriver. Avgörande med tanke på huruvida definitionen uppfylls är endast det att aktören med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har identifierats som kritisk. Till följd av den nya punkten gäller skyldigheterna enligt cybersäkerhetslagen de kritiska aktörer som har identifierats med stöd av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft också när en aktör inte i övrigt uppfyller definitionen av aktör enligt 1 mom. Momentet ändras inte till övriga delar.

Kritiska aktörer enligt den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har inte identifierats. Med stöd av övergångsbestämmelsen i 30 § i det nämnda lagförslaget ska beslut om identifiering av kritiska aktörer fattas första gången senast den 17 juli 2026.

På kritiska aktörer som identifieras inom sektorn för offentlig förvaltning tillämpas cybersäkerhetsskyldigheterna enligt 4 a kap. i informationshanteringslagen.

Genom den nya punkten genomförs artikel 2.3 i NIS 2-direktivet.

4 §. *Avgränsning av tillämpningsområdet.* I *6 mom.* föreskrivs det om en avgränsning av cybersäkerhetslagens tillämpningsområde som gäller kommuner. Det föreslås att momentet ändras så att cybersäkerhetslagen ska tillämpas på en kommun också när kommunen eller en del av dess verksamhet har identifierats som en kritisk aktör med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Tillägget är lagstiftningstekniskt och behövs för tillämpningen av cybersäkerhetslagen när någon annan verksamhet i kommunen än sådan som avses i bilagorna till cybersäkerhetslagen eller en kommun i sin helhet identifieras som en kritisk aktör.

Tillägget behövs för genomförandet av artikel 2.3 i NIS 2-direktivet i dessa situationer.

17 §. *Hantering av incidentanmälningar.* Det föreslås att till paragrafen fogas ett nytt *6 mom.* med stöd av vilket tillsynsmyndigheten ska informera den myndighet som enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft är behörig att utöva tillsyn om betydande incidenter, cyberhot och tillbud som avses i cybersäkerhetslagen och som de kritiska aktörer som har identifierats med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har informerat tillsynsmyndigheten om med stöd av 11–13 eller 15 § i cybersäkerhetslagen. Tillägget är lagstiftningstekniskt och blir tillämpligt endast om den myndighet som utövar tillsyn över en kritisk aktör inte är densamma i fråga om cybersäkerhetslagen och i fråga om lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Genom det nya momentet genomförs artikel 23.10 i NIS 2-direktivet.

Begreppen incident och cyberhot definieras i 2 § i cybersäkerhetslagen. Med tillbud avses på motsvarande sätt som i definitionen i artikel 6.5 i NIS 2-direktivet en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som av någon slumpmässig orsak inte uppstod.

26 §. *Tillsynsmyndigheter.* Det föreslås att till paragrafen fogas ett nytt *3 mom.* i vilket det föreskrivs om den tillsynsmyndighet som avses i cybersäkerhetslagen om en aktör som har identifierats som kritisk inte bedriver verksamhet enligt bilaga I eller II till cybersäkerhetslagen. När det gäller en kritisk aktör som enligt den föreslagna 3 § 2 mom. 5 punkten omfattas av tillämpningsområdet för skyldigheterna kan det i undantagsfall också vara fråga om en annan aktör än en aktör som bedriver verksamhet enligt bilaga I eller II till cybersäkerhetslagen, varför bestämmelsen är behövlig.

Huvudregeln är att tillsynsmyndigheten enligt cybersäkerhetslagen även i fråga om kritiska aktörer bestäms i enlighet med paragrafens 1 mom. Om aktören dock inte bedriver verksamhet enligt bilaga I eller II och dess tillsynsmyndighet således inte kan bestämmas med stöd av 1 mom. utövas tillsynen enligt cybersäkerhetslagen av samma myndighet som är behörig att utöva tillsyn över aktören när det gäller skyldigheterna enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Bestämmelser om tillsynsmyndigheter finns i 19 § i den lagen.

27 §. *Inriktning av tillsynen.* Det föreslås att till *2 mom.* fogas en ny 5 punkt enligt vilken också de kritiska aktörer som har identifierats med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft ska vara sådana väsentliga aktörer som avses i cybersäkerhetslagen och NIS 2-direktivet. Momentet ska inte ändras till övriga delar.

Genom den nya punkten genomförs artikel 3.1 f i NIS 2-direktivet.

28 §. *Rätt att få information.* Det föreslås att *4 mom.* ändras så att i momentet tas in de tillsynsmyndigheter som avses i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft som myndigheter som en tillsynsmyndighet enligt cybersäkerhetslagen har rätt att lämna ut information till när de förutsättningar som anges i momentet uppfylls. En förutsättning för utlämnande av information är att utlämnandet är nödvändigt för en uppgift som i cybersäkerhetslagen eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft föreskrivits för myndigheten. Utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden

eller integritetsskyddet mer än vad som är nödvändigt. Bestämmelsen behövs för samarbetet mellan tillsynsmyndigheterna och en CSIRT-enhet i samband med myndigheternas skötsel av sina uppgifter enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft och cybersäkerhetslagen.

45 §. *Myndighetssamarbete.* Det föreslås att *2 mom.* ändras så att de myndigheter som omfattas av samarbetsskyldigheten ska inbegripa också en tillsynsmyndighet som avses i 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Dessutom görs en teknisk ändring i den ordningsföljd i vilken myndigheterna räknas upp i momentet.

Det föreslås att till paragrafen fogas ett nytt *5 mom.* med en specialbestämmelse om samarbetet mellan tillsynsmyndigheten och den behöriga tillsynsmyndigheten enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Enligt det föreslagna 5 mom. ska de tillsynsmyndigheter som avses i cybersäkerhetslagen regelbundet utbyta information om identifieringen av kritiska aktörer samt om risker, cyberhot och incidenter samt om icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska aktörer, samt om de åtgärder som vidtagits för att hantera sådana risker, hot och incidenter. Förutsättningen motsvarar artikel 13.5 i NIS 2-direktivet.

Den myndighet som utövar tillsyn över kritiska aktörer med stöd av cybersäkerhetslagen ska underrätta tillsynsmyndigheten enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft när tillsyn och befogenheter enligt 4 kap. i cybersäkerhetslagen utövas gentemot en kritisk aktör. Underrättelsen möjliggör samarbete och samordning mellan myndigheterna vid tillsyn som riktas mot kritiska aktörer. Dessutom kan tillsynsmyndigheten på begäran av tillsynsmyndigheten enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft rikta befogenheter enligt 4 kap. mot en kritisk aktör. Tillsynsmyndigheterna är i huvudsak desamma enligt båda lagarna, men bestämmelserna är av betydelse särskilt på grund av samarbetet mellan myndigheterna samt i sådana situationer där en aktör undantagsvis övervakas av olika myndigheter i fråga om skyldigheterna. När samma myndighet utövar tillsyn över en kritisk aktör i fråga om båda lagarna behöver myndigheten inte underrätta sig själv om utövandet av sina befogenheter eller rikta en begäran om utövande av befogenheter till sig själv. Bestämmelserna motsvarar artikel 32.9 i NIS 2-direktivet.

Genom de föreslagna ändringarna genomförs artiklarna 13.4 och 13.5 i NIS 2-direktivet delvis samt artikel 32.9 i NIS 2-direktivet.

Ikraftträdande- och övergångsbestämmelser. I slutet på lagen föreslås ikraftträdande- och övergångsbestämmelser.

7.2 Lagen om informationshantering inom den offentliga förvaltningen

3 §. *Lagens tillämpningsområde och begränsningar i det.* Det föreslås att det till 3 § i informationshanteringslagen fogas ett nytt 7 mom., enligt vilket 4 a kap. med avvikelse från 3 mom. ska tillämpas på en myndighet som avses i 4 § 1 mom. 1 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan *offentlighetslagen*), om myndigheten identifierats som en kritisk aktör inom sektorn för offentlig förvaltning med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Det nya 7 mom. behövs för genomförandet av artikel 2.3 i NIS 2-direktivet inom den i direktivet avsedda sektorn för offentlig förvaltning. Sektorn för offentlig förvaltning definieras i 1 § 2 mom. i informationshanteringslagen.

Inom sektorn för offentlig förvaltning tillämpas NIS 2-direktivet och därmed också 4 a kap. i informationshanteringslagen på aktörer inom den offentliga förvaltningen på central och regional nivå. På regional nivå omfattar tillämpningsområdet för 4 a kap. i informationshanteringslagen välfärdsområden och välfärdssammanslutningar samt Helsingfors stad när den sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar. CER-direktivet och således den i regeringens proposition RP 205/2024 rd föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft tillämpas endast på aktörer inom den offentliga förvaltningen på central nivå. I den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft definieras aktörer inom sektorn för offentlig förvaltning på central nivå med en materiell hänvisning till 4 § 1 mom. 1 punkten i offentlighetslagen (statliga förvaltningsmyndigheter samt övriga statliga ämbetsverk och inrättningar). Definitionen är snävare än 3 § i informationshanteringslagen, enligt vilken aktörer inom den offentliga förvaltningen på central nivå också är statens affärsverk och självständiga offentligrättsliga inrättningar med de undantag som anges i 3 § 3 mom. i informationshanteringslagen.

I NIS 2-direktivet och CER-direktivet och därmed också i informationshanteringslagen och den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft finns i stort sett samstämmiga definitioner av vilka aktörer inom sektorn för offentlig förvaltning bestämmelserna inte tillämpas på. Det är således osannolikt att som kritisk aktör definieras en aktör inom sektorn för offentlig förvaltning som bestämmelserna om cybersäkerhet i 4 a kap. i informationshanteringslagen inte tillämpas på. Till exempel en kommunal myndighet kan inte bli definierad som en kritisk aktör inom sektorn för offentlig förvaltning. Inte heller ett välfärdsområde eller en välfärdssammanslutning kan definieras som en kritisk aktör inom sektorn för offentlig förvaltning. Således kan 4 a kap. i informationshanteringslagen inte tillämpas på andra kommuner än Helsingfors stad och ett välfärdsområde eller en välfärdssammanslutning kan inte bli en väsentlig aktör inom sektorn för offentlig förvaltning. Den definitionen som finns i 18 a § i informationshanteringslagen och som gäller väsentliga och viktiga aktörer inom den offentliga förvaltningen behöver därför inte ändras.

I teorin är det dock möjligt att en sådan statlig myndighet definieras som en kritisk aktör på vilken 4 a kap. i informationshanteringslagen inte tillämpas. Detta beror på att i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft har tillämpningen inom sektorn för offentlig förvaltning fastställts på ett lagtekniskt delvis annat sätt än det sätt på vilket tillämpningen av 4 a kap. i informationshanteringslagen fastställs i 3 § i den lagen. I den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft fastställs till exempel på lagnivå inte uttömmande de aktörer inom offentlig förvaltning som är verksamma inom området för den nationella säkerheten, den allmänna säkerheten, försvaret eller brottsbekämpningen och räknas som statliga myndigheter och som bestämmelserna inte tillämpas på.

I 2 § i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft finns bestämmelser om avgränsning av tillämpningsområdet. De myndigheter som avses i 1 mom. i den paragrafen kan således inte identifieras som kritiska med stöd av lagen. Med stöd av 2 § 1 mom. i den föreslagna CER-lagen tillämpas lagen inte på republikens presidents kansli, riksdagen, riksdagens justitieombudsman, justitiekanslern i

statsrådet, Finlands Bank eller domstolarna. Lagen tillämpas inte heller på myndighetsverksamhet inom området för försvaret, den nationella säkerheten och den allmänna ordningen och säkerheten, eller på förebyggande av brott, brottsutredning, förande av brott till åtalsprövning eller väckande av åtal. Dessa myndigheter kan således inte identifieras som kritiska med stöd av den föreslagna CER-lagen och de kan inte heller komma att omfattas av tillämpningsområdet för 4 a kap. i informationshanteringslagen trots det föreslagna undantaget.

Ikraftträdande- och övergångsbestämmelser. I slutet på lagen föreslås ikraftträdande- och övergångsbestämmelser.

8 Ikraftträdande

Lagarna avses träda i kraft samtidigt som den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Bestämmelserna i 2 kap. och 41 § i cybersäkerhetslagen ska tillämpas på en kritisk aktör som avses i den föreslagna 3 § 2 mom. 5 punkten en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. I fråga om de skyldigheter enligt 7–9 § som gäller riskhantering är övergångsperioden dock nio månader, vilket motsvarar den med stöd av 30 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft fastställda övergångsperioden för en riskbedömning som görs av en kritisk aktör. Övergångsperioden på en månad ska således tillämpas på skyldigheterna enligt cybersäkerhetslagen att lämna uppgifter till tillsynsmyndigheten för förteckningen över aktörer och att anmäla betydande incidenter. Tidsfristerna ska beräknas från det att aktören har fått del av beslutet.

Bestämmelserna i 4 a kap. i informationshanteringslagen ska tillämpas på en kritisk aktör som avses i det föreslagna 3 § 7 mom. en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. På motsvarande sätt som i ikraftträdandebestämmelserna i cybersäkerhetslagen ska en kritisk aktör dock anpassa sin verksamhet till bestämmelserna om riskhantering i 18 b och 18 c § i informationshanteringslagen först inom nio månader. Tidsfristerna ska beräknas från det att aktören har fått del av beslutet.

9 Verkställighet och uppföljning

Kommunikationsministeriet följer upp verkställigheten och tillämpningen av cybersäkerhetslagen.

Finansministeriet följer upp konsekvenserna av de bestämmelser om genomförande av NIS 2-direktivet inom sektorn för offentlig förvaltning som föreslås i informationshanteringslagen och bedömer ändamålsenligheten i tillämpningsområdet för skyldigheterna samt fullgörandet av skyldigheterna och tillsynen över att de fullgörs.

Enligt artikel 25 i CER-direktivet ska kommissionen regelbundet se över hur direktivet fungerar och rapportera resultaten till Europaparlamentet och rådet. Rapporten ska framför allt bedöma mervärdet av direktivet, dess effekt när det gäller att säkerställa kritiska entiteters motståndskraft och huruvida bilagan till direktivet bör ändras. Den första rapporten ska lämnas senast den 17 juni 2029.

Enligt artikel 40 i NIS 2-direktivet ska kommissionen senast den 17 oktober 2027 och därefter var 36:e månad se över hur direktivet fungerar och rapportera resultatet till Europaparlamentet

och rådet. Rapporten ska särskilt bedöma relevansen av de berörda enheternas storlek och sektorer, delsektorer och typer när det gäller den entitet som avses i bilagorna I och II till NIS 2-direktivet för ekonomins och samhällets funktion när det gäller cybersäkerhet.

10 Förhållande till andra propositioner

Regeringens proposition har samband med regeringens proposition till riksdagen med förslag till lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft och till vissa andra lagar (RP 205/2024 rd) som gäller genomförandet av CER-direktivet och som behandlas i riksdagen. Avsikten är att regeringspropositionerna i den mån det är möjligt ska behandlas samtidigt i riksdagen. De föreslagna lagstiftningsändringarna föreslås träda i kraft samtidigt som den genom regeringens proposition RP 205/2024 rd föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

I avsnitt 10 i regeringens proposition RP 205/2024 rd konstateras det att statsrådet separat bereder en proposition med förslag till sådana tekniska lagstiftningsändringar som behövs för att skyldigheterna enligt den föreslagna cybersäkerhetslagen (RP 57/2024 rd) ska kunna tillämpas på de kritiska aktörer som identifieras enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft, på det sätt som NIS 2-direktivet och CER-direktivet förutsätter. I denna proposition är det fråga om dessa lagstiftningsändringar.

11 Förhållande till grundlagen samt lagstiftningsordning

Propositionen har samband med tillämpningen av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Förhållandet till grundlagen vad gäller det nämnda lagförslaget och förfarandet för identifiering av en kritisk aktör bedöms i avsnitt 11 i regeringens proposition RP 205/2024 rd. Till följd av propositionen gäller skyldigheterna och tillsynsbefogenheterna enligt cybersäkerhetslagen aktörer som identifieras som kritiska. Förhållandet till grundlagen vad gäller befogenheterna och skyldigheterna enligt cybersäkerhetslagen bedöms i avsnitt 12 i regeringens proposition RP 57/2024 rd.

En kritisk aktör är enligt cybersäkerhetslagen skyldig att vidta åtgärder för att hantera risker som hänför sig till cybersäkerheten, att underrätta tillsynsmyndigheten om betydande incidenter samt att anmäla uppgifter enligt bestämmelsen om förteckningen över aktörer till tillsynsmyndigheten och att uppdatera förteckningen. De föreslagna skyldigheterna medför kostnader för de kritiska aktörerna. De föreslagna bestämmelserna är av betydelse med tanke på näringsfriheten, som tryggas i 18 § i grundlagen.

I fråga om anmälningsskyldigheten har grundlagsutskottet i utlåtandet GrUU 54/2002 rd konstaterat att bestämmelser om anmälningsskyldighet inte utgör ett problem ur näringsfrihetssynpunkt, i synnerhet inte då myndigheten inte förväntas fatta några beslut med anledning av anmälan. Den föreslagna anmälningsskyldigheten gäller en situation av det slag som beskrivs ovan. Även om underlåtelse att göra en anmälan enligt cybersäkerhetslagen inte i sig medför ett förbud mot att tillhandahålla tjänster eller bedriva verksamhet, ska underlåtelse att göra anmälan åläggas en administrativ påföljd och tillsynsmyndigheten ska ha befogenhet att bestämma att försummelsen ska rättas till med stöd av vite eller hot om avbrytande eller i sista hand genom utövande av andra befogenheter enligt cybersäkerhetslagen. Grundlagsutskottet har i sin utlåtandepraxis ansett att skyldigheten att göra en anmälan om verksamhet till tillsynsmyndigheten och att lämna den uppgifter i en situation där underlåtelse att göra en anmälan har negativa följder, ofta kan jämställas med tillståndsplikt och således

innebär ett ingripande i näringsfriheten (GrUU 45/2001 rd). När det gäller anmälningsskyldigheten är det dock fråga om en skyldighet som ingriper i näringsfriheten på ett lindrigare sätt än tillståndsplikt. Grundlagsutskottet har inte ansett att anmälningsskyldigheten är problematisk med tanke på näringsfriheten, om försummelse att göra anmälan inte har förenats med förbud mot att bedriva näringsverksamhet (GrUU 16/2009 rd) eller myndigheten inte förväntas fatta några beslut med anledning av anmälan (GrUU 54/2002 rd). När det gäller anmälningsskyldigheterna enligt cybersäkerhetslagen är det som helhet betraktat fråga om inskränkningar i näringsfriheten och förslaget ska uppfylla de allmänna kraven på en lag som begränsar de grundläggande fri- och rättigheterna, såsom kraven på godtagbarhet, exakthet och noggrann avgränsning (GrUU 58/2014 rd, s. 5, GrUU 19/2009 rd, s. 2). Enligt grundlagsutskottet ska det finnas godtagbara och tungt vägande skäl att begränsa näringsfriheten (GrUU 15/2008 rd, s. 2).

I förslaget är det fråga om genomförandet av de delar av NIS 2-direktivet som är förpliktande och inte innehåller nationellt handlingsutrymme. Syftet med propositionen är att stärka cybersäkerhetsnivån i fråga om de typer av aktörer som är väsentliga och viktiga med tanke på samhällets funktion. Förslaget syftar till att förbättra nivån på den riskhantering som gäller cybersäkerheten hos aktörerna inom samhällets kritiska infrastruktur och på så sätt trygga kontinuiteten i de tjänster som är kritiska med tanke på samhällets funktion. Förslaget bedöms ha ett vägande och godtagbart skäl med tanke på den begränsning av näringsfriheten som anmälningsskyldigheten medför. Dessutom uppfyller bestämmelserna de allmänna kraven på att en begränsning av de grundläggande fri- och rättigheterna ska vara noggrant avgränsad och exakt, och förslaget bedöms inte strida mot näringsfriheten, som tryggas i 18 § 1 mom. i grundlagen, på ett sätt som hindrar att propositionen behandlas i vanlig lagstiftningsordning.

Grundlagsutskottet har i utlåtande GrUU 62/2024 rd bedömt tillämpningen av bestämmelserna i 4 a kap. i informationshanteringslagen på riksdagens ämbetsverk och dess förhållande till riksdagens konstitutionella ställning och till 2 § i grundlagen. Grundlagsutskottet ansåg att det i fråga om riksdagens kansli och riksdagens övriga ämbetsverk inte är förenligt med riksdagens ställning som högsta statsorgan att 4 a kap. i informationshanteringslagen och dess bestämmelser om tillsyn ska tillämpas som sådana på riksdagens kansli eller riksdagens övriga ämbetsverk. Med anledning av den ändring som föreslås i informationshanteringslagen genom denna proposition kan tillämpningsområdet för 4 a kap. i informationshanteringslagen omfatta endast sådana myndigheter som identifieras som kritiska inom sektorn för offentlig förvaltning med stöd av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Enligt 1 § 3 mom. i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft avses med sektorn för offentlig förvaltning de myndigheter som avses i 4 § 1 mom. 1 punkten i offentlighetslagen. De myndigheter som avses i 4 § 1 mom. 1 punkten i offentlighetslagen är statliga förvaltningsmyndigheter samt övriga statliga ämbetsverk och inrättningar. Sektorn för offentlig förvaltning omfattar således inte riksdagens ämbetsverk och inrättningar som avses i 4 § 1 mom. 6 punkten i offentlighetslagen. Dessutom innehåller 2 § i den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft en allmän avgränsning av tillämpningsområdet enligt vilken lagen inte tillämpas på republikens presidents kansli, riksdagen, riksdagens justitieombudsman, justitiekanslern i statsrådet, Finlands Bank eller domstolarna. Således kan riksdagens kansli eller riksdagens övriga ämbetsverk inte bli identifierade som kritiska aktörer inom sektorn för offentlig förvaltning med stöd av den föreslagna lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft och kan därmed inte heller omfattas av tillämpningsområdet för 4 a kap. i informationshanteringslagen trots den ändring som föreslås i denna proposition. Riksdagens ämbetsverks konstitutionella ställning bedöms på så sätt inte utgöra något hinder för att propositionen behandlas i vanlig lagstiftningsordning.

På de grunder som anges ovan kan lagförslagen behandlas i vanlig lagstiftningsordning.

Kläm

Eftersom NIS 2-direktivet och CER-direktivet innehåller bestämmelser som föreslås bli genomförda genom lag, föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av cybersäkerhetslagen

I enlighet med riksdagens beslut

ändras i cybersäkerhetslagen (124/2025) 3 § 2 mom., 4 § 6 mom., 27 § 2 mom., 28 § 4 mom. och 45 § 2 mom. samt

fogas till 17 § ett nytt 6 mom., till 26 § ett nytt 3 mom. och till 45 § ett nytt 5 mom. som följer:

3 §

Aktörer

— —

Denna lag tillämpas också på en aktör som oavsett storlek är

1) en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,

2) en tillhandahållare av betrodda tjänster,

3) den som förvaltar ett toppdomänregister,

4) en leverantör av DNS-tjänster, eller

5) en kritisk aktör som med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (/) har identifierats som kritisk aktör inom någon annan sektor än sektorn för offentlig förvaltning (*kritisk aktör*).

— —

4 §

Avgränsning av tillämpningsområdet

— —

Denna lag tillämpas på en i kommunallagen (410/2015) avsedd kommun endast i fråga om verksamhet enligt bilaga I eller II samt till den del kommunen fungerar som en kritisk aktör.

— —

17 §

Hantering av incidentanmälningar

— —

Om en anmälan, rapport eller underrättelse som avses i 11–13 eller 15 § görs av en kritisk aktör, ska tillsynsmyndigheten informera den myndighet som enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och stärkande av samhällets motståndskraft är behörig att utöva tillsyn över den kritiska aktören om anmälan, rapporten eller underrättelsen.

26 §

Tillsynsmyndigheter

— —

Om en kritisk aktör inte bedriver verksamhet enligt bilaga I eller II, bestäms tillsynsmyndigheten enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

27 §

Inriktning av tillsynen

— —

Med väsentlig aktör avses

1) en i bilaga I avsedd aktör som överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag,

2) kvalificerade tillhandahållare av betrodda tjänster, de som förvaltar ett toppdomänregister samt leverantörer av DNS-tjänster,

3) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster som uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag,

4) en aktör som avses i 3 § 3 mom., samt

5) en kritisk aktör.

— —

28 §

Rätt att få information

— —

Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en CSIRT-enhet och en tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft, om det är nödvändigt för en uppgift som i denna lag eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft föreskrivits för myndigheten. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt.

— —

45 §

Myndighetssamarbete

— —

Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska vid behov samarbeta med polisen eller någon annan förundersökningsmyndighet, dataombudsmannen, Finansinspektionen och med en tillsynsmyndighet som avses i 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft samt med Transport- och kommunikationsverket i fråga om de uppgifter verket har enligt luftfartslagen (864/2014), lagen om tjänster inom elektronisk kommunikation och eIDAS-förordningen.

— —

Tillsynsmyndigheterna och de tillsynsmyndigheter som avses i 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft ska regelbundet utbyta information om identifieringen av kritiska aktörer samt om risker, cyberhot och incidenter samt om icke-cyberrelaterade risker, hot och incidenter som påverkar aktörer som identifierats som kritiska, samt om de åtgärder som vidtagits för att hantera sådana risker, hot och incidenter. Tillsynsmyndigheten ska underrätta den behöriga tillsynsmyndigheten enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft när befogenheter enligt 4 kap. i denna lag utövas gentemot en kritisk aktör. Tillsynsmyndigheten kan rikta tillsyn mot en kritisk aktör på begäran av en behörig tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

———

Denna lag träder i kraft den 20 .

Denna lag och 10–18 och 41 § i den lag som ändras genom denna lag tillämpas på en kritisk aktör en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. Bestämmelserna i 7–9 § i den lag som ändras genom denna lag tillämpas dock på en kritisk aktör först nio månader efter det att aktören har fått del av det beslut genom vilket den identifierats som kritisk aktör.

———

2.

Lag

om ändring av 3 § i lagen om informationshantering inom den offentliga förvaltningen

I enlighet med riksdagens beslut

fogas till 3 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019), sådan den lyder i lag 125/2025 ett nytt 7 mom. som följer:

3 §

Lagens tillämpningsområde och begränsningar i det

— —

Med avvikelse från vad som föreskrivs i 3 mom. tillämpas 4 a kap. på en myndighet som avses i 4 § 1 mom. 1 punkten i lagen om offentlighet i myndigheternas verksamhet, om den identifierats som en kritisk aktör inom sektorn för offentlig förvaltning med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (/).

———

Denna lag träder i kraft den 20 .

Bestämmelserna i 4 a kap. i den lag som ändras genom denna lag tillämpas på en kritisk aktör en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. En kritisk aktör ska anpassa sin verksamhet till 18 a och 18 b § i den lag som ändras genom denna lag inom nio månader från det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör.

———

Helsingfors den 10 april 2025

Statsminister

Petteri Orpo

Kommunikationsminister Lulu Ranne

Bilaga
Parallelltext

1.

Lag

om ändring av cybersäkerhetslagen

I enlighet med riksdagens beslut
ändras i cybersäkerhetslagen (124/2025) 3 § 2 mom., 4 § 6 mom., 27 § 2 mom., 28 § 4 mom. och 45 § 2 mom. samt
fogas till 17 § ett nytt 6 mom., till 26 § ett nytt 3 mom. och till 45 § ett nytt 5 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Aktörer	*Aktörer*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Denna lag tillämpas också på en aktör som oavsett storlek är 1) en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, 2) en tillhandahållare av betrodda tjänster, 3) den som förvaltar ett toppdomänregister, *eller* 4) en leverantör av DNS-tjänster.	Denna lag tillämpas också på en aktör som oavsett storlek är 1) en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, 2) en tillhandahållare av betrodda tjänster, 3) den som förvaltar ett toppdomänregister, 4) en leverantör av DNS-tjänster, *eller* *5) en kritisk aktör som med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (/) har identifierats som kritisk aktör inom någon annan sektor än sektorn för offentlig förvaltning (kritisk aktör).*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4 §	4 §
Avgränsning av tillämpningsområdet	*Avgränsning av tillämpningsområdet*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Denna lag tillämpas på en i kommunallagen (410/2015) avsedd kommun endast i fråga om verksamhet enligt bilaga I eller II.	Denna lag tillämpas på en i kommunallagen (410/2015) avsedd kommun endast i fråga om verksamhet enligt bilaga I eller II *samt till den del kommunen fungerar som en kritisk aktör.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
17 §	17 §
Hantering av incidentanmälningar	*Hantering av incidentanmälningar*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
(fogas)	*Om en anmälan, rapport eller underrättelse som avses i 11–13 eller 15 § görs av en kritisk aktör, ska tillsynsmyndigheten informera den myndighet som enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och stärkande av samhällets motståndskraft är behörig att utöva tillsyn över den kritiska aktören om anmälan, rapporten eller underrättelsen.*
26 §	26 §
Tillsynsmyndigheter	*Tillsynsmyndigheter*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
(fogas)	*Om en kritisk aktör inte bedriver verksamhet enligt bilaga I eller II, bestäms tillsynsmyndigheten enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.*
27 §	27 §
Inriktning av tillsynen	*Inriktning av tillsynen*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
Med väsentlig aktör avses 1) en i bilaga I avsedd aktör som överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag, 2) kvalificerade tillhandahållare av betrodda tjänster, de som förvaltar ett toppdomänregister samt leverantörer av DNS-tjänster, 3) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster som uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om	Med väsentlig aktör avses 1) en i bilaga I avsedd aktör som överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag, 2) kvalificerade tillhandahållare av betrodda tjänster, de som förvaltar ett toppdomänregister samt leverantörer av DNS-tjänster, 3) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster som uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om

Gällande lydelse	*Föreslagen lydelse*
definitionen av mikroföretag samt små och medelstora företag, samt 4) en aktör som avses i 3 § 3 mom.	definitionen av mikroföretag samt små och medelstora företag, 4) en aktör som avses i 3 § 3 mom., *samt* *5) en kritisk aktör.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
28 §	28 §
Rätt att få information	*Rätt att få information*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet *samt* en CSIRT-enhet, om det är nödvändigt för en uppgift som i denna lag föreskrivits för myndigheten. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än vad som är nödvändigt.	Tillsynsmyndigheten har trots sekretessbestämmelserna, skyldigheten att iaktta sekretess enligt 2 mom. och andra begränsningar som gäller utlämnande av information rätt att lämna ut handlingar som den fått eller utarbetat i samband med skötseln av sina uppgifter enligt denna lag samt att röja sekretessbelagd information för en annan tillsynsmyndighet, en CSIRT-enhet *och en tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft,* om det är nödvändigt för en uppgift som i denna lag *eller i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft* föreskrivits för myndigheten. Utnyttjandet av rätten att få information eller utlämnandet av information får inte begränsa skyddet av förtroliga meddelanden eller integritetsskyddet mer än vad som är nödvändigt.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
45 §	45 §
Myndighetssamarbete	*Myndighetssamarbete*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska vid behov samarbeta med polisen eller någon annan förundersökningsmyndighet, dataombudsmannen, Transport- och kommunikationsverket i fråga om de uppgifter verket har enligt luftfartslagen (864/2014), lagen om tjänster inom elektronisk kommunikation och eIDAS-förordningen samt med Finansinspektionen.	Tillsynsmyndigheterna, CSIRT-enheten och den gemensamma kontaktpunkten ska vid behov samarbeta med polisen eller någon annan förundersökningsmyndighet, dataombudsmannen, Finansinspektionen *och med en tillsynsmyndighet som avses i 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft samt med* Transport- och kommunikationsverket i fråga om de uppgifter verket har enligt luftfartslagen (864/2014), lagen om tjänster inom

Gällande lydelse	*Föreslagen lydelse*
	elektronisk kommunikation och eIDAS-förordningen.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(fogas)	*Tillsynsmyndigheterna och de tillsynsmyndigheter som avses i 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft ska regelbundet utbyta information om identifieringen av kritiska aktörer samt om risker, cyberhot och incidenter samt om icke-cyberrelaterade risker, hot och incidenter som påverkar aktörer som identifierats som kritiska, samt om de åtgärder som vidtagits för att hantera sådana risker, hot och incidenter. Tillsynsmyndigheten ska underrätta den behöriga tillsynsmyndigheten enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft när befogenheter enligt 4 kap. i denna lag utövas gentemot en kritisk aktör. Tillsynsmyndigheten kan rikta tillsyn mot en kritisk aktör på begäran av en behörig tillsynsmyndighet enligt 19 § i lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.*
	Denna lag träder i kraft den 20 .
	Denna lag och 10–18 och 41 § i den lag som ändras genom denna lag tillämpas på en kritisk aktör en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. Bestämmelserna i 7–9 § i den lag som ändras genom denna lag tillämpas dock på en kritisk aktör först nio månader efter det att aktören har fått del av det beslut genom vilket den identifierats som kritisk aktör.

2.

Lag

om ändring av 3 § i lagen om informationshantering inom den offentliga förvaltningen

I enlighet med riksdagens beslut

fogas till 3 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019), sådan den lyder i lag 125/2025 ett nytt 7 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Lagens tillämpningsområde och begränsningar i det	*Lagens tillämpningsområde och begränsningar i det*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(fogas)	*Med avvikelse från vad som föreskrivs i 3 mom. tillämpas 4 a kap. på en myndighet som avses i 4 § 1 mom. 1 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999), om den identifierats som en kritisk aktör inom sektorn för offentlig förvaltning med stöd av lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (/).*
	Denna lag träder i kraft den 20 .
	Bestämmelserna i 4 a kap. i den lag som ändras genom denna lag tillämpas på en kritisk aktör en månad efter det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör. En kritisk aktör ska anpassa sin verksamhet till 18 a och 18 b § i den lag som ändras genom denna lag inom nio månader från det att aktören har fått del av det beslut genom vilket den identifierats som en kritisk aktör.