Regeringskansliet
Faktapromemoria 2022/23:FPM87

Cybersolidaritetsinitiativet

2022/23:FPM87

Försvarsdepartementet

2023-05-23

Dokumentbeteckning

COM (2023) 207
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')

COM (2023) 208
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services

COM (2023) 209
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

Sammanfattning

Kommissionen presenterade den 18 april 2023 det så kallade Cybersolidaritetsinitiativet som består av ett gemensamt meddelande om en cybersäkerhetskompetensakademi, förslag till ändringar i EU:s Cybersäkerhetsakt samt en ny förordning benämnd Cybersolidaritetsakten.

I meddelandet ”Minska kompetensgapet gällande cybersäkerhet för att stärka EU:s konkurrenskraft, tillväxt och motståndskraft” (’Cybersäkerhetskompetensakademin’) föreslår kommissionen att en Cybersäkerhetskompetensakademi inrättas. Syftet med akademin är att samla cybersäkerhetsutbildningar, fortbildningsmöjligheter och

kompetenscertifiering samt finansieringsmöjligheter och andra åtgärder som främjar cybersäkerhetskompetensförsörjningen inom unionen på en samlad mötesplattform. Inrättandet av akademin föreslås stödjas med 10 miljoner euro från programmet för ett digitalt Europa (DIGITAL).

Kommissionens förslag till ändringar i förordning (EU) 2019/881 (Cybersäkerhetsakten) innebär att leverantörer av cybersäkerhetstjänster (så kallade *managed security services*) ska kunna certifieras enligt ramverket för cybersäkerhetscertifiering.

Kommissionens förslag till en ny förordning benämnd ’Cybersolidaritetsakten’ syftar till att storskaliga cyberattacker, som kan vara svåra att hantera för enskilda medlemsstater, ska kunna hanteras genom ömsesidigt stöd och solidaritet mellan medlemsstaterna. Förordningsförslaget innefattar tre åtgärder som syftar till att stärka solidariteten och kapaciteten inom unionen när det kommer till att upptäcka, stärka beredskapen mot, svara på samt bedöma och utvärdera cybersäkerhetshot och incidenter:

- Utbyggnad av en pan-europeisk infrastruktur av säkerhetsoperationscenter (SOC) och en ’cybersköld’ för att stärka den gemensamma förmågan att detektera och upprätta lägesbilder (’European Cyber Shield’).
- Inrättande av en ’cyber-nödmekanism’ (’Cyber Emergency Mechanism’) för att stödja medlemsstaterna i att stärka beredskapen för, svara på samt skyndsamt återhämta sig från betydande och storskaliga cybersäkerhetsincidenter.
- Etablering av en incidentutvärderingsmekanism (’European Cybersecurity Incident Review Mechanism’) för att utvärdera betydande eller storskaliga cybersäkerhetsincidenter.

’Cyberskölden’ och ’cyber-nödmekanismen’ föreslås få finansiering från DIGITAL. Förordningsförslaget innebär därmed även en ändring i förordning (EU) 2021/694 om inrättande av programmet för ett digitalt Europa (DIGITAL).

Regeringen välkomnar initiativ som utgår från medlemsstaternas behov, som bidrar till en stärkt och effektiv EU-samverkan på cybersäkerhetsområdet och som bidrar till en höjd cybersäkerhet. Det är viktigt att EU:s förslag på området inte innebär onödig duplicering av initiativ som görs inom ramen för andra organisationer, exempelvis inom Nato-samarbetet. EU:s och Nato:s åtgärder bör ses som komplement till varandra. Regeringen anser vidare att det är viktigt att varje medlemsstats eget ansvar för nationell säkerhet säkerställs och genomgående beaktas i förordningsförslagen.

Förslaget kommer troligen att behandlas under Sveriges EU-ordförandeskap den 1 januari till och med den 30 juni 2023.

1 Förslaget

1.1 Ärendets bakgrund

Den 18 april 2023 presenterade kommissionen ett gemensamt meddelande, ett förslag till ändring i förordning 2019/881 samt ett förslag till en ny förordning (Cybersolidaritetsakten). Dessa instrument benämns tillsammans som ’Cybersolidaritetsinitiativet’.

Kommissionen har de senaste åren tagit flera initiativ för att stärka cybersäkerheten i EU. Cybersolidaritetsinitiativet ska ses mot bakgrund av tidigare EU-initiativ på cyberområdet, och mot bakgrund av det försämrade säkerhetspolitiska läget innefattande Rysslands fullskaliga invasion av Ukraina som föregicks, och fortsatt understöds, av fientliga cyberoperationer.

I det gemensamma meddelandet om EU:s cyberförsvarspolicy som antogs av kommissionen den 10 november 2022 angavs att kommissionen skulle presentera förslag till initiativ som syftar till att stärka EU:s gemensamma beredskap samt svarsåtgärder för att bättre kunna bemöta och hantera cybersäkerhetshot och incidenter. Kommissionen åtog sig även att undersöka förutsättningarna för en certifieringsordning på EU-nivå för cybersäkerhetsindustrin och privata företag. I meddelandet föreslogs dessutom en gradvis etablering av en europeisk cyberreserv (’EU Cybersecurity reserve’) bestående av betrodda leverantörer och deras tjänster, samt testning av kritiska entiteter. Cyberreserven föreslogs kunna aktiveras vid större cybersäkerhetsincidenter. Cyberreserven föreslogs bestå av ”betrodda leverantörer” i enlighet med Cybersolidaritetsakten. Med betrodda leverantörer avses leverantörer av cybersäkerhetstjänster som föreslås kunna certifieras enligt de nu föreslagna ändringarna i Cybersäkerhetsakten.

1.2 Förslagets innehåll

Kommissionen motiverar Cybersolidaritetsinitiativet med att det råder brist på cybersäkerhetskompetens inom unionen och att samverkan mellan medlemsstaterna behöver stärkas för att bättre kunna möta de utmaningar som unionen står inför på cybersäkerhetsområdet.

Meddelandet om en europeisk cybersäkerhetskompetensakademi

Meddelandet föreslår att det ska inrättas en virtuell Cybersäkerhetskompetensakademi (i det följande benämnd ’akademin’). Det övergripande målet med akademin är att inom EU öka antalet professionellt verksamma inom cybersäkerhetsområdet. Akademin syftar till att sammanföra existerande initiativ som rör cybersäkerhetskompetens och att göra dessa tillgängliga på en samlad mötesplattform för att på så sätt erbjuda en gemensam ingångspunkt. Akademin föreslås inriktas på kompetenshöjning av yrkesverksamma inom cybersäkerhetsområdet.

Akademin syftar till att: i) främja kunskapsgenerering genom utbildning och träning, ii) öka synligheten för tillgängliga finansieringsmöjligheter, iii) uppmana intressenter att agera, och iv) definiera indikatorer för att bevaka marknadens utveckling på cybersäkerhetsområdet.

Akademin föreslås utformas som ett europeiskt digitalt infrastrukturs-konsortium (*European Digital Infrastructure Consortium – EDIC*). Medlemsstater som är intresserade av att ingå i konsortiet ombeds att komma in med en intresseanmälan till kommissionen senast den 30 maj 2023. EU:s cybersäkerhetsbyrå (Enisa) föreslås bidra till inrättandet av akademin, i synnerhet avseende hjälp med cybersäkerhetsutbildning och träning. Europeiska kompetenscentret för cybersäkerhet (ECCC) föreslås att, i linje med dess strategiska agenda, stötta inrättandet av akademin.

Ändringar i förordning 2019/881 (EU:s cybersäkerhetsakt – ’Cybersäkerhetsakten’)

Ändringarna syftar till att göra det möjligt för leverantörer av cybersäkerhetstjänster (så kallade *managed security services*) att bli certifierade i enlighet med cybersäkerhetsakten. Vissa länder i EU utfärdar redan idag liknande certifikat på nationell nivå. De föreslagna ändringarna i cybersäkerhetsakten syftar bland annat till att komma till rätta med en fragmentisering av kravspecifikationer på den inre marknaden för dessa leverantörer.

I cybersäkerhetsakten finns redan bestämmelser om certifiering av IKT-produkter, IKT-tjänster och IKT-processer (Informations-och kommunikationsteknik). I ändringsförslagen till cybersäkerhetsakten föreslås att certifiering ska kunna ske även av leverantörer av cybersäkerhetstjänster. De cybersäkerhetstjänster som avses kan exempelvis omfatta områden som incidenthantering, penetrationstester, säkerhetsrevisioner och rådgivning.

Enligt förslaget till ändring av cybersäkerhetsakten ska certifiering av leverantörer av cybersäkerhetstjänster syfta till att säkerställa att:

i) leverantören av cybersäkerhetstjänsten har hög nivå av teknisk kompetens, tillräcklig erfarenhet samt professionell integritet,
ii) leverantören av cybersäkerhetstjänsten har interna processer för att säkerställa hög kvalitet i utförandet,
iii) leverantören av cybersäkerhetstjänsten har kompetens att hantera datalagring, databearbetning och dataöverföring och i de processerna kan skydda sig mot oavsiktlig eller icke-auktoriserad tillgång till eller förlust av data,
iv) leverantören av cybersäkerhetstjänsten kan återskapa data, service och funktioner i händelse av incident,
v) leverantören av cybersäkerhetstjänsten tillser att enbart auktoriserade personer, programvaror eller maskiner får tillgång till den data som auktoriseringen avser,
vi) leverantören av cybersäkerhetstjänsten kan analysera och utvärdera vilka data, tjänster eller funktioner som har tillgängliggjorts, när detta skett och av vem,
vii) cybersäkerhetstjänsterna (och i förekommande fall hårdvaran) som tillhandahålls av leverantören är säkra i sin utformning och inte innehåller sårbarheter samt är uppdaterade.

Förslaget till en ny förordning (Cybersolidaritetsakten)

Förordningsförslaget syftar till att i) stärka EU:s gemensamma förmåga att upptäcka cybersäkerhetshot och upprätta lägesbilder, ii) stärka beredskapen hos kritiska entiteter inom EU och stärka solidariteten genom att utveckla gemensam responskapacitet för att bemöta betydande eller storskaliga cybersäkerhetsincidenter, iii) förbättra unionens motståndskraft, samt att iv) bidra till effektiva svarsåtgärder genom att utvärdera och granska betydande och storskaliga incidenter.

Förordningsförslaget är indelat i fem kapitel. Det första kapitlet redogör för förordningens mål och syften vilka är att detektera, stärka beredskapen för samt reagera på cybersäkerhetshot och incidenter, att stärka beredskapen i kritiska och mycket kritiska sektorer inom unionen, samt att stärka motståndskraften genom att utvärdera och bedöma betydande eller storskaliga incidenter. Kapitlet innehåller även förslag till de tre åtgärder som föreslås: (i) inrättandet av en ’cybersköld’, (ii) skapandet av en ’cyber-nödmekanism’, samt (iii) etableringen av en ’utvärderingsmekanism’.

I det andra kapitlet redogörs för kommissionens förslag om att etablera en ’cybersköld’ (’European Cyber Shield’). Det övergripande syftet med cyberskölden är att utveckla kapaciteten i unionen för att upptäcka, analysera och behandla data som rör cyberhot och incidenter. ’Cyberskölden’ ska finansieras genom programmet för ett digital Europa (DIGITAL). Den europeiska cyberskölden föreslås bestå av nationella säkerhetsoperationscenter samt gränsöverskridande säkerhetsoperationscenter. Enligt förslaget ska varje medlemsstat som ansöker om dessa specifika finansieringsmedel från EU utse ett nationellt säkerhetsoperationscenter. Ett gränsöverskridande säkerhetsoperationscenter föreslås bestå av minst tre medlemsstater som representeras av varsitt nationellt säkerhetsoperationscenter. Vidare anger kapitlet hur samverkan och informationsutbyte ska ske inom och mellan de gränsöverskridande säkerhetsoperationscentrumen, samt hur samverkan och informationsdelning ska ske gentemot unionens entiteter. Baserat på intresseanmälan ska ett värdkonsortium (’Hosting Consortium’) väljas ut av ECCC för att delta i gemensam upphandling av verktyg och infrastruktur tillsammans med ECCC.

Det tredje kapitlet redogör för kommissionens förslag om att etablera en ’cyber-nödmekanism’ (’Cyber Emergency Mechanism’) i syfte att förbättra unionens motståndskraft mot större cybersäkerhetshot samt stärka unionens beredskap för och hantering av de kortsiktiga konsekvenserna av betydande och storskaliga cybersäkerhetsincidenter och kriser. Cyber-nödmekanismen ska stödja i) beredskapsåtgärder, inklusive koordinerade beredskapstester av entiteter i kritiska sektorer, ii) svarsåtgärder utförda av betrodda privata leverantörer som ingår i en s.k. cybersäkerhetsreserven vilken beskrivs nedan, samt iii) åtgärder som omfattar ömsesidigt stöd mellan medlemsstater. Cyber-nödmekanismen föreslås finansieras genom DIGITAL. Förberedelsearbetet för cyber-nödmekanismen inkluderar koordinerade förberedande tester av entiteter i kritiska sektorer.

Kommissionen föreslår att det ska etableras en cybersäkerhetsreserv (’EU Cybersecurity Reserve’). Den föreslås bestå av incidentresponstjänster från betrodda privata leverantörer. Dessa leverantörer föreslås väljas ut på grundval av ett antal kriterier som listas i förordningen. Det finns även möjlighet för tredjeland att efterfråga stöd från cybersäkerhetsreserven om de har ingått ett associeringsavtal inom ramen för DIGITAL.

I det fjärde kapitlet presenteras kommissionens förslag om att etablera en incidentutvärderingsmekanism (’Cybersecurity Incident Review Mechanism’). Enisa ska ansvara för att utvärdera och bedöma hot och

sårbarheter samt mildra effekterna i relation till en särskilt betydande eller storskalig cybersäkerhetsincident. Förslaget medför att Enisa, på begäran av kommissionen, EU-Cyclone[1] eller CSIRT-nätverket[2], ska inkomma med en utvärdering och granskning av hot, sårbarheter och hanteringen avseende en betydande eller storskalig cybersäkerhetsincident. Om det är relevant ska rapporteringen delas med unionens höga representant. Informationen som delas ska skydda konfidentiell information i enlighet med EU-lagstiftning eller nationell lagstiftning gällande skydd av känslig eller säkerhetsklassad information.

I det femte kapitlet finns vissa slutbestämmelser med förslag till ändringar i förordning (EU) 2021/694. I kapitlet föreslås kommissionen också inom fyra år från förordningens ikraftträdande komma in med en utvärderingsrapport av förordningens genomförande till Europaparlamentet och rådet samt bestämmelser om förordningens ikraftträdande.

Förordningsförslaget med tillhörande annex innebär även en ändring i förordning (EU) 2021/694 om inrättande av programmet för ett digitalt Europa (DIGITAL). Det särskilda programmålet ’Cybersäkerhet och förtroende’ kompletteras med att programmet ska stödja utvecklingen av cyberskölden, inklusive utveckling, utplacering och drift av nationella och gränsöverskridande säkerhetsoperationscenter. Förslaget innebär vidare att programmet för ett digitalt Europa (DIGITAL) ska finansiera etableringen och driften av cyber-nödmekanismen inklusive inrättandet av en cyberreserv.

De föreslagna upphandlingsförfaranden för EU:s cybersäkerhetsreserv innebär att kommissionen och Enisa fungerar som ett centralt inköpsorgan för att upphandla på uppdrag av medlemsstaternas cyberkrishanteringsmyndigheter och CSIRTs[3], eller å unionens institutioner, organ och byråers vägnar. Kommissionen och Enisa kan också agera som grossist genom att köpa, lagra och sälja vidare eller donera varor och tjänster, inklusive uthyrning, till unionens institutioner, organ och byråer. Av ändringsförslagen framgår att kommissionen och Enisa kan agera som en central upphandlingsfunktion å tredjelands vägnar, förutsatt att landet i fråga är associerat med programmet för ett digitalt Europa (DIGITAL) enligt artikel 10. Ändringsförslagen innebär även att en begäran om upphandling räcker från en enskild unionsinstitution, -organ eller -byrå för att kommissionen eller Enisa ska ha mandat att agera.

[1] Se 4.2 Fackuttryck/termer.

[2] Se 4.2 Fackuttryck/termer.

[3] Se 4.2 Fackuttryck/termer.

1.3 Gällande svenska regler och förslagets effekt på dessa

EU:s cybersäkerhetsakt kompletteras av bestämmelser på nationell nivå. Bestämmelserna finns i lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt och förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Till följd av att EU:s cybersäkerhetsakt, utöver certifiering av IKT-produkter, IKT-tjänster och IKT-processer, enligt förslaget även kommer att reglera certifiering av leverantörer av cybersäkerhetstjänster bedöms bland annat vissa ändringar behöva göras i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Förslaget till en ny cybersolidaritetsförordning kan för Sveriges del innebära ytterligare justeringar och ändringar i gällande lagstiftning. Förordningen kan exempelvis behöva kompletteras med nationella bestämmelser, bland annat för inrättandet av ett nationellt säkerhetsoperationscenter samt dess förhållande till befintliga svenska institutioner som till exempel CERT-SE. En fortsatt analys av hur förslaget påverkar nuvarande svenska bestämmelser behöver därför göras.

Det behöver även analyseras hur de föreslagna akterna förhåller sig till exempelvis NIS2-direktivet och annan befintlig EU-rättslig reglering samt genomförandet av sådan i svensk lagstiftning.

1.4 Budgetära konsekvenser / Konsekvensanalys

Inrättandet av akademin föreslås stödjas med 10 miljoner euro från DIGITAL.

De föreslagna ändringarna i Cybersäkerhetsakten kan ha mindre budgetära konsekvenser för Försvarets materielverk som är nationell myndighet för cybersäkerhetscertifiering. Eventuella kostnader som förslagen kan leda till för den nationella budgeten ska finansieras i linje med de principer om neutralitet för statens budget som riksdagen beslutat om (prop. 1994/95:40, bet. 1994/95FiU5, rskr. 1994/95:67). Utgiftsdrivande åtgärder på EU-budgeten behöver finansieras genom omprioriteringar i den fleråriga budgetramen (MFF). De föreslagna ändringarna i Cybersäkerhetsakten förväntas inte ha budgetära konsekvenser för kommuner och regioner.

Förslaget till en ny cybersolidaritetsakt har inget separat stödanslag utan anslag föreslås tas från existerande medel i EU:s långtidsbudget (2021–2027) och DIGITAL. Förslaget föreslås finansieras under DIGITAL och dess särskilda mål ’Cybersäkerhet’. Den totala budgeten inkluderar en ökning på 100 miljoner euro som i denna förordning föreslås omfördelas från andra särskilda mål (Artificiell intelligens och Avancerade digitala färdigheter).

Av dessa 100 miljoner euro kommer en del att förstärka den budget som förvaltas av ECCC för att genomföra åtgärder för säkerhetsoperationscentren. Dessutom kommer den extra finansieringen att syfta till att stödja inrättandet av cyberreserven inom ramen för cyber-nödmekanismen.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar initiativ som utgår från medlemsstaternas behov som bidrar till stärkt och effektiv EU-samverkan på cybersäkerhetsområdet och som bidrar till en höjd cybersäkerhet. Regeringen ställer sig positiv till initiativet om en cybersäkerhetskompetensakademi och ställer sig bakom förslaget om ändringar i cybersäkerhetsakten som möjliggör certifiering av leverantörer av cybersäkerhetstjänster.

Regeringen anser att det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs och bedömer att undantag för nationell säkerhet behöver beaktas genomgående och tydliggöras i förordningsförslaget, i synnerhet i de artiklar som rör cyberskölden och cyber-nödmekanismen.

Regeringen bedömer att kommissionens definition av ’säkerhetsoperationscenter’ och begreppet ’cybersköld’ behöver förtydligas. Enligt regeringen innebär förslaget om ’cyberskölden’ de facto ett förslag om fördjupat CERT-samarbete och anser vidare att det bör förtydligas vad cyberskölden innebär för nationell säkerhet och personlig integritet.

Regeringen understryker att informationsdelning mellan medlemsstater ska ske på frivillig basis och att det behöver finnas tydliga överenskommelser om hur känslig information hanteras. Regeringen ser positivt på att kommissionen vill underlätta privat-offentlig samverkan men noterar att det finns begränsningar för vad en utomstående aktör kan bistå med vid incidenter.

Regeringen anser att det är viktigt att en EU-gemensam ’cyberreserv’ inte medför en snedvriden konkurrens inom området.

Förslaget till en cybersolidaritetsakt kan komma att ha effekter på finansieringen av satsningar på andra områden av vikt för Sverige.

Regeringen anser att sådana undanträngningseffekter bör beaktas. Regeringen avser att agera i linje med Sveriges budgetrestriktiva hållning. Utgiftsdrivande åtgärder på EU-budgeten behöver finansieras genom omprioriteringar i den fleråriga budgetramen (MFF).

Regeringen vill framhålla vikten av samverkan mellan olika EU-entiteter, exempelvis mellan Enisa och ECCC, och att möjliga synergier mellan EU:s interna och externa initiativ tas tillvara. Regeringen anser att EU och Nato bör verka kompletterande och att onödig duplicering bör undvikas.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Ärendet har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Den rättsliga grunden för förslaget till en ny cybersolidaritetsakt är artikel 173 (3) och artikel 322 (1) p. (a) i fördraget om den Europeiska unionens funktionssätt (FEUF). Förslaget syftar till att stärka industrin och servicesektorns konkurrenskraft genom att förbättra cybersäkerheten på den digitala inre marknaden. Den föreslagna nödmekanismen ska ha möjlighet till en viss flexibilitet angående den finansiella hanteringen särskilt när det gäller automatisk överföring av medel till nästkommande år.

Den rättsliga grunden för ändringen i cybersäkerhetsförordningen är, liksom för den ursprungliga förordningen, art 114 i FEUF. Förslaget, liksom urspungsförordningen syftar till att undvika en fragmentering av den inre marknaden genom att möjliggöra certifiering av cybersäkerhetstjänster på unionsnivå.

För båda akterna är det ordinarie lagstiftningsförfarandet tillämpligt. Enligt artikel 294 i fördraget beslutar rådet med kvalificerad majoritet och Europaparlamentet är medbeslutande.

3.2 Subsidiaritets- och proportionalitetsprincipen

När det gäller förslaget till en ny cybersolidaritetsakt framhåller kommissionen att cybersäkerhethotets gränsöverskridande karaktär innebär att syftet med den föreslagna förordningen inte kan uppnås på nationell nivå. Stöd och åtgärder på unionsnivå medför fördelar eftersom det undviker dubblering av åtgärder inom unionen och medlemsstaterna. Det innebär bättre användande av tillgängliga medel och bättre tillvaratagande av tidigare lärdomar. Det föreslagna stödet på unionsnivå ska komplettera åtgärder på nationell nivå. Kommissionen framhåller att de föreslagna åtgärderna inte går utöver vad som är nödvändigt för att uppnå cybersolidaritetsaktens mål och påverkar inte medlemsstaternas ansvar för nationell säkerhet, allmän säkerhet eller möjligheterna att förebygga, utreda eller lagföra brott.

När det gäller förslaget till ändring i cybersäkerhetsförordningen anger kommissionen att genom certifiering av leverantörer av cybersäkerhetstjänster till företag, myndigheter och andra organisationer undviks fragmentisering på den inre marknaden. Detta kan svårligen uppnås om varje enskild medlemsstat sätter upp egna riktlinjer. Kommissionen anser att förslaget inte går utöver vad som är strikt nödvändigt för att uppå syftet.

Regeringen delar kommissionens bedömning att båda de föreslagna akterna är förenliga med subsidiaritets- och proportionalitetsprincipen med reservation för vad som angetts ovan (se under rubriken 2.1 Preliminär svensk ståndpunkt) om förtydliganden angående nationell säkerhet.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Ärendet kommer att hanteras i den horisontella rådsarbetsgruppen för cyberfrågor (HWPCI). Förslaget kommer troligen att behandlas under Sveriges EU-ordförandeskap den 1 januari till och med den 30 juni 2023.

4.2 Fackuttryck/termer

CERT: En förkortning för *'Computer Emergency Response Team')*. En funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga it-relaterade incidenter.

CSIRT: En förkortning för *'Computer Security Incident Response Teams'*. CSIRT-nätverket, som etablerades genom NIS-direktivet (EU) 2016/1148, är ett nätverk av nationellt utpekade CERT-funktioner för hantering av it-säkerhetsincidenter. CERT-SE vid MSB är Sveriges nationella CSIRT.

Cybersäkerhetscertifiering: Avser utvärdering av en IKT-produkt, IKT-tjänst eller IKT-process utifrån fastställda kriterier i en certifieringsordning. Om IKT-produkten, IKT-tjänsten eller IKT-processen uppfyller kriterierna utfärdas ett certifikat av behörigt organ.

ECCC: En förkortning för *'the European Cybersecurity Competence Centre'*. Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning. Inrättades genom förordning (EU) 2021/887.

Enisa; EU:s cybersäkerhetsbyrå.

EU-CyCLONe: En förkortning för *'the European Cyber Crisis Liaison Organisation Network'*. Det europeiska kontaktnätverket för cyberkriser. Inrättades genom direktiv (EU) 2022/2555, NIS2-direktivet. EU-CyCLONe ska stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

NIS2-direktivet: Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 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.

Programmet för ett digitalt Europa (DIGITAL): Ett EU-finansieringsprogram inriktat på att sprida digital teknik till företag, medborgare och offentliga förvaltningar.

SOC (eng. 'Security Operations Center'): Ett begrepp inom information- och cybersäkerhet som vanligen tillskrivs en funktion med uppgift att monitorera nätverk och informationssystem, samt detektera, analysera och varna om eventuella säkerhetsincidenter.