U 102/2018 rd

Statsrådets skrivelse till riksdagen om förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska kommissionens förslag av den 12 september 2018 om Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum samt en promemoria om förslagen.

Helsingfors den 10 januari 2019

Näringsminister Mika Lintilä

Handelsråd Antti Eskola

ARBETS- OCH NÄRINGSMINISTERIET | PROMEMORIA | EU/2018/1532

10.1.2019

FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM INRÄTTANDE AV EUROPEISKA KOMPETENSCENTRUMET FÖR CYBERSÄKERHET INOM NÄRINGSLIV, TEKNIK OCH FORSKNING OCH AV NÄTVERKET AV NATIONELLA SAMORDNINGSCENTRUM

1 Förslagets bakgrund

Utvecklingen inom cybersäkerhetsområdet sker snabbt och därför lade kommissionen och unionens höga representant för utrikesfrågor och säkerhetspolitik i september 2017 fram ett gemensamt meddelande om *resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*. Syftet med förslaget är att stärka unionens resiliens, avskräckning och hantering av cyberattacker. I meddelandet ingick förslag till åtgärder som att stärka Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) samt skapa en frivillig EU-ram för cybersäkerhetscertifiering för att öka cybersäkerheten hos produkter och tjänster i den digitala världen. Dessutom ingick i förslagen en konkret plan för snabb och samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser.

I meddelandet betonades det att det ligger i unionens strategiska intresse att säkerställa och bibehålla nödvändig teknisk kapacitet inom cybersäkerhet samt utveckla kapaciteten för att trygga den digitala inre marknaden. Speciellt viktigt är det att skydda kritiska nätverk och informationssystem samt tillhandahålla grundläggande cybersäkerhetstjänster. Unionen ska själv kunna säkra sina digitala tillgångar och konkurrera på den globala cybersäkerhetsmarknaden.

I dag är unionen nettoimportör av cybersäkerhetsprodukter och lösningar och i stor utsträckning beroende av leverantörer utanför Europa. Värdet på den globala cybersäkerhetsmarknaden uppgår till 600 miljarder euro och marknaden väntas växa de kommande fem åren med i genomsnitt 17 procent sett till försäljningen samt antalet företag och arbetsplatser. Ur marknadsperspektiv finns emellertid bara sex EU medlemsstater bland de 20 länder som är marknadsledande inom cybersäkerhet.

I Europa finns omfattande sakkunskap inom området och i EU finns uppskattningsvis 660 kompetenskluster inom området. Insatserna inom forskarsamhället och näringslivet för Europas cybersäkerhetsområde är emellertid fragmenterade, saknar inriktning och ett gemensamt mål, vilket hämmar EU:s konkurrenskraft. Även investeringarna i området är otillräckliga och inte heller synergieffekterna mellan den civila och den försvarsrelaterade cybersäkerhetssektorn tillvaratas fullt ut.

Unionen kunde genomföra investeringar i en betydligt större utsträckning. Den behöver dock en effektivare mekanism för samordning för att skapa en varaktig kapacitet, slå samman insatser, förena kompetens och stimulera utvecklingen av sådana innovativa lösningar som motsvarar näringslivets utmaningar cybersäkerhet när det gäller ny teknik med flera användningsområden (t.ex. artificiell intelligens, kvantberäkning, blockkedjor och säkra digitala identiteter).

I rådets slutsatser av november 2017 ombads kommissionen göra en snabb konsekvensbedömning av möjliga alternativ att inrätta ett nätverk av kompetenscenter för cybersäkerhet, där ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet står i centrum samt ge ett lagstiftningsförslag om detta.

Baserat på ovanstående lämnade Europeiska kommissionen den 12 september 2018 ett förslag (COM(2018) 630 final) till Europaparlamentets och rådets förordning om att inrätta ett europeiskt kompetenscenter för näringslivet, teknik och forskningskompetens inom cybersäkerhet samt ett nätverk av nationella samordningscentrum för cybersäkerhet. Dessa skulle stödja kompetensgemenskapen för cybersäkerhet.

2 Förslagets mål

Målet med förslaget är att ännu effektivare än tidigare möjliggöra förebyggande av cyberhot och samordnadet när man svarar mot dessa för de nationella myndigheterna i medlemsstaterna och för näringslivet samt tillgången till högklassig kompetens, produkter och lösningar för cybersäkerhet. Syftet är att i synnerhet hjälpa europeiska företag inom cybersäkerhetsområdet att utveckla och införa nya och bättre produkter och lösningar för cybersäkerhet, stödja företag i undanröjandet av marknadsrelaterade hinder samt öka marknadsandelen för de europeiska företagen genom att trygga spelregler för rättvis konkurrens och öppna marknader. Initiativet hjälper också företag i olika sektorer att öka cybersäkerheten hos sina produkter och vända cybersäkerheten till en konkurrensfördel.

Syftet är att med hjälp av det center och nätverk som inrättas bevara och utveckla den tekniska och industriella kapaciteten för cybersäkerheten, vilket är nödvändigt för att trygga en Digital inre marknad. Målet är också att öka konkurrenskraften för unionens cybersäkerhetsindustri och främja målet att göra cybersäkerhet till en konkurrensfördel för unionens övriga industrigrenar. Med hjälp av mekanismen är det möjligt att samla, dela och säkra befintlig kompetens, möjliggöra gemensamma investeringar i kostnadsmässigt omfattande infrastruktur, gynna införandet av EU:s produkter och lösningar för cybersäkerhet, genomföra långsiktigt strategiskt samarbete mellan näringslivet, forskarsamhällen och stater samt överbygga kompetensklyftor i anslutning till cybersäkerhet.

3 Aktörer som inrättas genom förordningen och nätverksstruktur

Genom förordningen inrättas *Ett kompetenscentrum på Europanivå*, vars uppgift är att förvalta de medel som riktas till programmen för ett Digitalt Europa och Horisont Europa under programperioden 2021–2027, genomföra de delar som gäller cybersäkerhet för dessa program, bistå med att samordna det nätverk som bildas av medlemsstaternas nationella centrum och en mera omfattande gemenskap i genomförandet av agendan för cybersäkerhetsteknik samt påskynda gemensamma investeringar för EU, medlemsstaterna och industrin samt ibruktagandet av produkter och lösningar.

Förutom ovanstående skulle kompetenscentrumet ha i uppgift att

• stärka kompetenser i anslutning till cybersäkerheten, information och infrastruktur som stöd för industrin, offentliga aktörer och forskarsamhällen,

• gynna ibruktagandet av omfattande cybersäkerhetsprodukter och -lösningar som representerar kompetens i toppklass i Europeiska unionen,

• stödja minskandet av kompetensklyftor i anslutning till cybersäkerhet i EU-området,

• främja forskning och utveckling inom cybersäkerhet,

• stärka det civila och militära samarbetet inom tekniker med dubbla användningsområden samt deras tillämpningsområden, och

• stärka synergieffekten mellan det civila och militära och i anslutning till Europeiska försvarsfonden.

Enligt artikel 11 i förslaget till förordning omfattar kompetenscentrumets struktur en styrelse, verkställande direktör och en rådgivande näringslivs- och vetenskapsnämnd. Enligt artikel 15 har EU 50 procent av rösterna och varje deltagande medlemsstat har en röst. Styrelsen fattar beslut med en majoritet av minst 75 procent alla röster, inbegripet rösterna från de medlemmar som är frånvarande, när rösterna står för minst 75 procent av det totala ekonomiska bidraget till kompetenscentrumet.

I fråga om *kompetensnätverket och de nationella samordningscentrumen* utser medlemsstaterna nationella kontaktpunkter och meddelar dem till kommissionen. Kriteriet är att centrumen har tillgång till den tekniska kompetensen inom cybersäkerhet och att de har möjlighet att samarbeta med industrin, kompetensen inom området och med den offentliga sektorn. Målet är att bygga nationella kompetenser och forma kontakter med redan befintliga initiativ. Nationella samordningscentrum kan få finansiering och förmedla den vidare till tredje parter.

Kompetensnätverkets uppgift är att stödja kompetenscentrumet i genomförandet av dess uppgifter samt fungera som nationella kontaktpunkter och gynna medverkan i samarbetet för aktörer inom industrin och andra aktörer på nationell nivå. De nationella samordningscentrumen har även i uppgift att bedöma medlemsstaternas aktörer när de söker sig till kompetenssamarbetet, skapa synergier mellan centrala aktörer på nationell och regional nivå, främja utvecklingen av nationella och lokala ekosystem samt inrikta åtgärder mot sektorspecifika industriella utmaningar för cybersäkerhet.

Kompetensgemenskapen utformar en omfattande, öppen och mångformig grupp, som består av cybersäkerhetens intresseparter inom forskningsområdet samt olika aktörer inom den privata och offentliga sektorn både inom den civila och militära sektorn. Tillträde till gemenskapen förutsätter kompetens inom forskning, industriell utveckling eller utbildning. Medlemsstatens nationella samordningscentrum gör en bedömning av om medlemsstaternas aktörer är lämpliga och ackrediteringen för gemenskapen. Det är endast möjligt att ackreditera aktörer som finns på EU-området. Kompetensgemenskapen har i uppgift att

• stödja kompetenscentrumet och nätverket i deras uppgifter och för att de ska uppnå sina mål,

• stärka och sprida kompetens som gäller cybersäkerhet i EU, samt

• delta i genomförandet av åtgärder som nätverket och centrumet främjar samt arbetsgrupper i anslutning till dem.

4 Rättslig grund

Genom den föreslagna rättsakten inrättas en struktur och institution, som har i uppgift att genomföra de åtgärder inom cybersäkerhet som ingår i programmet för ett digitalt Europa och Horisont Europa-programmet. I rättsakten fastställs syftet med institutionen och dess uppgifter samt dess administrativa struktur. Inrättande av en sådan EU-institution förutsättar att en förordning utfärdas. Dessutom skulle det inrättas ett nätverk av nationella samordningscentrum och en kompetensgemenskap. Den rättsliga grunden för den föreslagna rättsakten är artiklarna 173, 187 och 188 (i tillämpliga delar) i fördraget om Europeiska unionens funktionssätt (EUF).

5 Effekter på den nationella lagstiftningen inkl. Ålands ställning

Det är fråga om ett förslag till EU-förordning som är direkt tillämplig i medlemsstaterna. Enligt bedömningen ger förordningen inte upphov till behov av ändringar i den nationella lagstiftningen.

6 Övriga konsekvenser

Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket för nationella samordningscentrum för cybersäkerhet påskyndar utvecklingen och införandet av cybersäkerhetsteknik samt kompletterar byggandet av kompetenser i EU och på nationell nivå.

Förslaget bygger på den tidigare grund som skapats i medlemsstaterna och med hjälp av en avtalsbaserad partnerskapsmodell för den offentliga och privata sektorn. Syftet är att stärka EU:s cybersäkerhetskompetens med hjälp av nätverket av nationella samordningscentrum och kompetenscentrum på Europanivå.

Mervärdet på EU-nivå förväntas utgöras av en progressiv europeisk cyberteknik som vidareutvecklas, omfattande investeringar som planeras bli genomförda och av att de samlas på Europanivå samt av lösningar som fungerar i hela EU.

Konsekvenser för företag

Genom den föreslagna förordningen skapas inga nya lagstadgade skyldigheter för företag. I synnerhet utvecklingskostnaderna för de små och medelstora företagens innovativa och cybersäkra produkter kommer sannolikt att sjunka, eftersom initiativet möjliggör en sammanslagning av resurser, när det investeras i nödvändiga kapaciteter på medlemsstatsnivå eller Europanivå t.ex. genom att i samarbete skaffa nödvändiga testnings- och försöksinfrastrukturer för cybersäkerheten. Industrin och små och medelstora företag kunde använda dessa resurser inom olika sektorer för att försäkra sig om att deras produkter är cybersäkra och för att göra cybersäkerhet till en konkurrensfördel för sig själva.

Merparten av företagen är små och medelstora företag eller mikroföretag, som ofta har sämre kapacitet inom cybersäkerheten än det finns i stora företag. De nationella samordningscentrumen kunde speciellt dra nytta av dessa företag.

Ekonomiska konsekvenser

Kompetenscentrumets finansiering skulle omfatta 1 981 668 000 euro ur programmet för ett Digitalt Europa, inklusive högst 23 746 000 euro till administrativa kostnader, samt den finansieringsandel som senare fastställs för Horisont Europa-programmet i den strategiska planeringsprocessen.

Enligt artikel 22.1 i förslaget till förordning ska de deltagande medlemsstaterna lämna ett totalt bidrag till kompetenscentrumets driftskostnader och administrativa kostnader som uppgår till minst samma belopp som EU:s finansiering. I detta skede är det inte möjligt att göra en bedömning av de exakta kostnaderna och hur de fördelas, eftersom förhandlingarna i fråga om de finansieringsinstrument som ska användas pågår som en del av helheten med den fleråriga budgetramen. De EU-medel som kommer till medlemsstaterna ska styras via de nationella samordningscentrum som utses i de deltagande medlemsstaterna.

Målen med initiativet kan bäst uppnås om alla eller så många medlemsstater som möjligt deltar i det. Incitament för medverkan ges om rösträtten baserar sig på erlagd betalningsandel för medlemsstaten. Medlens som tas med i kompetenscentrumets budget utgörs av finansieringsandelar som de deltagande medlemsstaterna har anvisat till administrativa kostnader, finansieringsandelar till omkostnader och av andra medel. Industrins eventuella finansieringsandel genomförs projektspecifikt.

De nationella samordningscentrumen får direkt finansieringsstöd från EU för att genomföra uppgifter i anslutning till denna förordning. Formen på den finansiering som kompetenscentrumen förmedlar är till exempel understöd för pilotprojekt, ekonomiskt stöd till tredje parter, gemensam upphandling och arvoden som beviljas till tredje parter.

Det är meningen att verksamheten ska inledas 1.1.2021 och avslutas 31.12.2029. Konsekvenserna i anslutning till betalningsåtaganden infaller under åren 2021–2027.

7 Subsidiaritetsprincipen och proportionalitetsprincipen

EU måste med tanke på de tekniska cybersäkerhetsutmaningarnas karaktär och omfattning, liksom den otillräckliga samordningen av ansträngningar inom eller mellan industri, offentlig sektor och forskarsamhället, effektivare stödja samordning för att uppnå en kritisk massa resurser och en bättre hantering av kunskap och tillgångar. Detta är nödvändigt med tanke på de resurser som krävs för viss forskning, utveckling och användning av cybersäkerhetsteknik, tillgången till tvärdisciplinärt cybersäkerhetskunnande som ofta bara delvis är tillgängligt på nationell nivå samt de globala industriella värdekedjorna och konkurrenternas verksamhet på de globala marknaderna.

Omfattningen av de resurser och den sakkunskap som krävs är i allmänhet större än de enskilda medlemsstaternas insatser. Till exempel ett europatäckande nätverk för kvantkommunikation kan kräva investeringar på omkring 900 miljoner euro av EU, beroende på vilka investeringar medlemsstaterna gör och återanvändningen av befintlig infrastruktur. I förslaget ses initiativet vara avgörande för att slå samman finansiella resurser och möjliggöra denna typ av investeringar i EU. Målen för initiativen kan uppnås bättre på EU-nivå genom att slå samman insatser och undvika att de överlappar varandra. Detta bidrar till att skapa en kritisk massa av investeringar och säkerställa att offentlig finansiering används på ett optimalt sätt. I enlighet med proportionalitetsprincipen går förordningen inte utöver vad som är nödvändigt för att uppnå dessa mål.

Statsrådet anser att förslaget kan anses vara förenligt med subsidiaritets- och proportionalitetsprincipen.

8 Nationell behandling av förslaget och behandling inom Europeiska Unionen

Förslaget till förordning behandlas i rådets cyberarbetsgrupp och i konstellationen rådet för transport, telekommunikation och energi (telekommunikation).

Det behöriga parlamentsutskottet för förslaget till förordning är utskottet för industrifrågor, utrikeshandel, forskning och energi (ITRE).

Förslaget till förordning behandlas genom vanligt lagstiftningsförfarande.

Utkastet till U-skrivelse har behandlats genom skriftligt förfarande i kommittén för EU-ärenden i sektionen för den inre marknaden (EU8), sektionen för näringspolitik (EU13), sektionen för kommunikation (EU19) och sektionen för forskning och innovationer (EU20) 4.–8.10.2018.

9 Statsrådets ståndpunkt

Statsrådet förhåller sig som sin initiala ståndpunkt positivt till förslaget om inrättande av Europeiska kompetenscentrumet för cybersäkerhet och nätverket av nationella samordningscentrum och till förslagets allmänna mål. Europas konkurrenskraft ska förstärkas och då är en insats på EU-nivå för innovationer, forskning, kompetens och investeringar viktig.

Vid planeringen av nya strukturer bör det beaktas att utvecklingen av cybersäkerhetsprodukter och -teknik inte leds av myndigheterna, utan sker i första hand i företag som verkar på marknadsvillkor i den globala konkurrensen. Statsrådet anser det vara viktigt att kompetenscentrumet för cybersäkerhet och nätverksverksamheten i anslutning till det drar nytta av både finländska företag och myndighetsaktörer. Det är viktigt att se till att förslaget inte medför en onödig administrativ börda som i synnerhet skadar företagens konkurrenskraft eller företagens och övriga parters operativa verksamhet.

Statsrådet anser det viktigt att säkerställa att uppgifterna eller behörigheten för centrumen eller nätverket och de befintliga aktörerna och samarbetsorganen inte överlappar varandra. I synnerhet ska det ses till att det föreslagna kompetenscentrumet och EU:s byrå för nät- och informationssäkerhet ENISA inte har uppgifter som överlappar varandra. Dessutom är det viktigt att sörja för synergieffekterna mellan EU:s olika instrument och program, såsom programmet för ett digitalt Europa, Horisont Europa och kohesionspolitiken samt den helhet som kompletterar varandra i fråga om kontaktytorna till centrumet och nätverket.

Enligt kommissionens förslag ska finansieringen av kompetenscentrumet täckas genom programmet för ett digitalt Europa och Horisont Europa-programmet i EU:s budgetram 2021—2027 samt med finansiering från deltagande medlemsstater till ett belopp som motsvarar EU-finansieringen. Enligt kommissionens förslag ska en avsevärd del (25 %) av den finansiering som föreslås för programmet för ett digitalt Europa kanaliseras till kompetenscentrumet för cybersäkerhet. Statsrådet kommer att precisera sin ståndpunkt till den föreslagna finansieringen för kompetenscentrumet för cybersäkerhet och det nationella nätverket i och med att behandlingen framskrider. Hänsyn ska tas till den tidigare fastställda nivån på programmet för ett digitalt Europa, vilket leder till att finansieringen av kompetenscentrumet för cybersäkerhet kommer att omfatta ungefär hälften av finansieringen för programmet för ett digitalt Europa i sin helhet.

Statsrådet kommer att separat ta ställning till dimensioneringen av finansieringen för kommissionens programförslag 2021—2027 som en del av budgetramshelheten.

Statsrådet fortsätter att närmare analysera förslaget till förordning och preciserar sina ställningstaganden med en kompletterande U-skrivelse med beaktande av den närmare analysen.