U 58/2017 rd

Statsrådets skrivelse till riksdagen om ett förslag till Europaparlamentets och rådets förordning (”förordning om cybersäkerhet”)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska kommissionens förslag av den 13 september 2017 till Europaparlamentets och rådets förordning om Europeiska unionens byrå för nät- och informationssäkerhet ENISA och om upphävande av förordning EU 526/2013 samt om cybersäkerhetscertifiering av informations- och kommunikationsteknik.

Helsingfors 19 oktober 2017

Kommunikationsminister Anne Berner

Konsultativ tjänsteman Piia Nyström

KOMMUNIKAITONSMINISTE-RIET | PROMEMORIA | EU/2017/

13.10.2017

KOMMISSIONENS FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM EUROPEISKA UNIONENS BYRÅ FÖR NÄT- OCH INFORMATIONSSÄKERHET ENISA OCH OM UPPHÄVANDE AV FÖRORDNING EU 526/2013 SAMT OM CYBERSÄKERHETSCERTIFIERING AV INFORMATIONS- OCH KOMMUNIKATIONSTEKNIK (”FÖRORDNING OM CYBERSÄKERHET”)

1 Bakgrund och syften

Europeiska unionens byrå för nät- och informationssäkerhet ENISA inrättades år 2004 genom Europaparlamentets och rådets förordning för att under fem års tid förbättra unionens, medlemsstaternas och företagsvärldens förmåga att förebygga, hantera och lösa problem som rör nät- och informationssäkerhet. Efter det har byråns mandatperiod förlängts två gånger. Den nuvarande mandatperioden upphör i juni 2020.

Kommissionen gav 13.9.2017 ett förslag till europaparlamentets och rådets förordning om europeiska unionens byrå för nät- och informationssäkerhet ENISA och om upphävande av förordning EU 526/2013 samt om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”förordning om cybersäkerhet”) (COM/2017/477). Med det förslaget föreskriver man ett permanent mandat åt ENISA och skapar en ram för IKT-baserade produkter och tjänster för säkerhetscertifiering inom EU. Förslagets syfte är att säkra den inre marknadens verksamhet genom att stärka cybersäkerheten, motståndskraften och förtroendet inom EU.

ENISA ska enligt förslaget övergå från att vara Europeiska unionens byrå för nät- och informationssäkerhet till att bli Europeiska unionens byrå för cybersäkerhet, och bli en permanent EU-byrå.

2 Huvudsakligt innehåll

Kommissionen har valt att lägga fram förslaget som en förordning. Med förordningen upphäver man förordningen (EU 526/2013) som för tillfället reglerar ENISA:s verksamhet. Förordningen kan tillämpas direkt i medlemsstaterna.

Förordningsförslaget består av fyra delar. Den första delen innehåller författningsförslagets syfte, tillämpningsområde och definitioner. I förordningen föreskriver man om mål, uppgifter och organisation. Därutöver ger förordningen ramar för ett EU-omfattande certifieringssystem för säkerhetsprodukter.

Förordningsförslagets andra del innehåller bestämmelser som styr ENISA:s verksamhet. Målet för ENISA:s verksamhet är främjandet av informationssäkerhet på hög nivå inom EU. Avsikten är att byrån ska vara ett expertcentrum för cybersäkerhet, som hjälper såväl medlemsstater och unionsinstitutioner som offentliga och privata intressentgrupper i utvecklingsarbetet av cybersäkerhet och stärkandet av motståndskraften. Samtidigt skapar centret förutsättningar för samarbete mellan medlemsstaterna och andra aktörer. En del av byråns uppgifter är knutna till direktivet om nät- och informationssäkerhet (EU 1148/2016) och de samarbetsformer som inrättats på grundval av detta direktiv.

I förslaget har ENISA:s uppgifter delats upp under sju teman, som var och en har en egen artikel. Artiklarna avser utveckling och verkställande av unionens politik och unionsrätten, kapacitetsuppbyggnad, operativt samarbete inom unionen, främjande av cybersäkerhetsmarknaderna, ökande av kunskap och medvetenhet, forsknings- och innovationsverksamhet samt internationellt samarbete. ENISA har därutöver en central roll i förberedningen av certifieringsprogram i enlighet med ramen för certifiering av föreslagna EU-omfattande informations- och kommunikationstekniksżoner. Byrån fungerar även som sekretariat för en samarbetsgrupp bestående av nationella certifieringsmyndigheter.

Förutom syften och uppgifter, definieras även ENISA:s administrativa struktur i förordningsförslaget. Byrån har en direktion, en generaldirektör, en styrelse och en permanent intressentgrupp. Direktionen definierar allmänna riktlinjer för byråns verksamhet och utser en generaldirektör. Generaldirektören ansvarar för det dagliga ledandet av byrån och rapporterar till styrelsen. Styrelsen bereder direktionens beslut. Den permanenta intressentgruppen är ett rådgivande organ, med representanter från den privata sektorn, konsumentorganisationer och andra centrala intressentgrupper. Förslaget motsvarar i sina huvuddrag byråns nuvarande verksamhet i det avseende.

Förordningsförslagets tredje del innehåller bestämmelser, med vilka man skapar en EU-omfattande ram för certifiering av informations- och kommunikationsteknologitillgångar. Målsättningen är att reglera tillvägagångssätt, inom ramen för vilka man kan bevilja ett EU-omfattande certifikat för informations- och kommunikationsteknologiska varor som ett bevis på produkternas informationssäkerhet. Med certifikatet kan man visa att tillgången uppfyller de krav som ställts för certifiering angående informationens, funktionens eller tjänstens tillgång, äkthet, enhetlighet och konfidentialitet. Det centrala målet är att skapa ett system som grundar sig på ömsesidigt erkännande på så sätt att certifikatet som upprättats med stöd av den allmänna ramen erkänns i alla medlemsstater och att apparattillverkaren eller tjänsteleverantören inte längre behöver skaffa flera olika nationella certifikat för sin produkt.

Enligt förslaget bereder ENISA i samarbete med samarbetsgrupper inom nationella tillsynsmyndigheterna för certifiering och intressentgrupper (såsom industrin och standardiseringsorgan) ett förslag på krav som förutsätts för att få certifikatet (certifieringsprogram). Förordningen reglerar allmänna grundläggande mål (exempelvis skydda information från obehöriga, säkerställa tillgången på information, aktuell programuppdatering) kopplade till informationssäkerhet som behöver beaktas i dessa certifieringsprogram. De här målen ska beaktas vid skapandet av ett certifieringsprogram. Därutöver kan certifieringsprogrammen enligt förslaget delas upp i tre olika tillförlitlighetsnivåer (basic, substantial, high) beroende på hur tillförlitligt certifikatet fastställer informationssäkerhetsnivån.

I förordningsförslaget definieras de element, som ramenligt beviljade certifieringsprogram ska innehålla. Av certifieringsprogrammet framgår bland annat de tillgångskategorier som programmet berör, specificerade säkerhetskrav (dessa kan även grunda sig på exempelvis befintliga EU-omfattande eller internationella standarder), certifieringsprogrammets nivå av tillförlitlighet och de villkor utifrån vilka certifikatet kan beviljas.

Ett certifieringsprogram för en viss grupp av ICT-program eller -tjänster skapas utifrån ENISA:s förslag med kommissionens genomförandeakt. Certifieringen är frivillig, men förslaget lämnar en möjlighet att senare reglera ett obligatoriskt certifieringskrav inom unionen eller i nationell lagstiftning.

Förslaget begränsar medlemsstaternas möjligheter att skapa egna nationella certifieringsprogram. Enligt förslaget kan medlemsstaterna inte skapa nya nationella certifieringsprogram för informationssäkerhet, om de överlappar med de certifieringsprogram som grundats med stöd

av förslaget. Existerande nationell certifieringsorganisering fortsätter att gälla fram till ett förfallodatum som beslutats i nästa kommissions genomförandeakt. Certifikat som beviljas inom ramen för regleringen skulle gälla fram till att de går ut.

När kommissionen har godkänt certifieringsprogrammet, ansöker tillgångsproducenterna och tjänsteleverantörerna om certifiering hos ett organ för bedömning av överensstämmelse i enlighet med förordningsförslaget. Det kan finnas många sådana organ och de som ansöker kan välja vilken de vill ha. Bedömningsorganen ska uppfylla de krav som definieras i förordningsförslaget och dess bilaga. Enligt förslaget kan bedömningsorganet vara ett privat företag, om det kan anses vara oberoende och inga intressekonflikter uppstår. Bedömningsorganet godkänns av ett nationellt ackrediteringsorgan (Ackrediteringstjänsten FINAS i Finland) i enlighet med EU-förordningen (EG) nr 765/2008 (om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93). Tillsynsmyndigheterna för certifiering meddelar kommissionen om de organ för bedömning av överensstämmelse som ackrediterats i medlemsstaten.

Enligt förslaget ska medlemsstaten utse en nationell tillsynsmyndighet för certifiering. Det är fråga om en oberoende tillsynsmyndighet, till vilken medlemsstaten ska rikta tillräckligt med resurser för att den effektivt ska kunna utföra de uppgifter som den föreskrivits. Myndighetens uppgift är bland annat att följa och övervaka organ för bedömning av överensstämmelse samt verkställandet av den reglering som gäller certifieringens referensram och certifieringsprogram på nationell nivå. Tillsynsmyndigheten behandlar även klagomål rörande bedömningsorgan inom området och samarbetar med andra certifieringsmyndigheter. En sådan samarbetsform är en föreslagen samarbetsgrupp av tillsynsmyndigheter för certifiering, vars huvudsakliga uppgift är att vägleda kommissionen i frågor om certifiering och att stöda ENISA i beredningen av certifieringsprogram. Gruppen kan också föreslå för kommissionen att något certifieringsprogram ska skapas.

Förordningsförslagets fjärde del innehåller slutbestämmelser om bland annat ikraftträdande och upphävande av bestämmelser. Utvärdering och översyn av byråns verksamhet ska enligt förslaget utföras inom fem år från att förordningen träder i kraft. När den nya förordningen träder i kraft fortsätter den dåvarande generaldirektören och styrelsen tills mandatperioden tar slut. Även fattade beslut fortsätter att vara i kraft, förutsatt att de inte strider mot den nya förordningen.

3 Förslagets rättsliga grund och förhållande till subsidiaritetsprincipen och proportionalitetsprincipen

Som rättslig grund för förordningen föreslår kommissionen artikel 26 och 114 i fördraget om Europeiska unionens funktionssätt (FEUF). Förslaget behandlas i enlighet med artikel 294 i FEUF i vanlig lagstiftningsordning.

I enlighet med artikel 26 i FEUF godkänner unionen åtgärder, vars syfte är att upprätta den inre marknaden eller säkerställa dess funktion i enlighet med tillämpliga bestämmelser i fördragen. I enlighet med artikel 114 i FEUF kan unionen besluta om åtgärder för tillnärmning av sådana bestämmelser i lagar och andra författningar i medlemsstaterna som syftar till att upprätta den inre marknaden och få den att fungera.

Kommissionen påtalar att den föreslagna rättsliga grunden är densamma som hos den förordning (EU 526/2013) som reglerar ENISA:s nuvarande verksamhet och Europeiska unionens domstol anser den vara acceptabel (C-2017/04 Förenade konungariket Storbritannien och Nordirland mot Europaparlamentet och Europeiska unionens råd). Därutöver anser kommissionen att man i och med förslaget ökar samarbetet mellan medlemsstaterna särskilt när det gäl-

ler ENISA:s roll i genomförandet av förpliktelserna i direktivet om nät- och informationssäkerhet.

I fråga om regleringen av certifieringar anser kommissionen att avsaknaden av en gemensam rättslig ram har skapat splittring på den inre marknaden, vilket har skadat den europeiska ICT-marknadens utveckling och konkurrenskraft. Den föreslagna regleringen har som avsikt att angripa det här problemet.

Kommissionen anser att man inte kan öka den EU-omfattande cybertoleransen tillräckligt genom åtgärder som vidtas av enskilda medlemsstater och att det splittrade förhållningssättet till cybersäkerhet inte kan ses vara tillräckligt. Enligt kommissionen går de föreslagna åtgärderna inte över det som är nödvändigt för att uppnå de utsatta målen och hindrar inte heller medlemsstaternas åtgärder för att garantera nationell säkerhet.

4 Förslagets förhållande till förpliktelser gällande grundläggande och mänskliga rättigheter samt grundlagen

Enligt kommissionen har cybersäkerheten en väsentlig uppgift i genomförandet av skyddet av privatliv som regleras i artikel 7 och skyddet av personuppgifter som regleras i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Därutöver har cybersäkerheten en central roll när man strävar efter att skydda konfidentialiteten vid elektronisk kommunikation eller verkställa exempelvis yttrande-, tanke-, samvets- och religionsfrihet.

Skyddet för privatlivet och hemligheten i fråga om förtroliga meddelanden garanteras i 10 § i Finlands grundlag. I 10 § 1 mom. i grundlagen konstateras att närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. I grundlagen föreskrivs också bland annat om religions- och samvetsfrihet (11 §), yttrandefrihet (12 §) samt förenings- och församlingsfrihet (13 §).

5 Förslagets konsekvenser

Konsekvenser för EU:s budget

Normalt fattar man beslut om ENISA:s budget i samband med mångåriga finansieringsramar och EU:s årliga budgetar.

Konsekvenser för budgeten

Förslaget förutsätter att medlemsstaterna utser en nationell certifieringsmyndighet. Det här kan förutsätta förändringar i nationella myndigheters uppgifter och omprövning av anslagen i anslutning till myndigheternas verksamhet.

Konsekvenser för den nationella lagstiftningen

Kommissionens förslag om en nationell certifieringsmyndighet kan förutsätta förändringar i myndigheternas uppgifter och bestämmelser om behörighet. I Finland gäller för närvarande en lag om bedömningsorgan för informationssäkerhet (1405/2011), där det föreskrivs om ett förfarande genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet har sörjt för en viss informationssäkerhetsnivå. Enligt lagen godkänner Kommunikationsverket bedömningsorganen samt styr och övervakar deras verksamhet.

6 Ålands behörighet

I enlighet med 27 § i självstyrelselagen för Åland (1144/1991) har riket lagstiftande makt

i ärenden som berör handelssjöfart, luftfart, standardisering samt statliga myndigheters organisationsform och verksamhet.

7 Nationell behandling av förslaget och behandling inom Europeiska unionen

Finland har senast bildat sin ståndpunkt om revideringen av ENISA:s mandat i samband med halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden under sommaren 2017 (E 21/2015 rd, EKU 21/2017 rd). Finland har också tagit ställning till ärendet i samband med kommissionens meddelande om stärkandet av systemet för cyberresiliens (E 81/2016 rd).

Förslaget och U-skrivelsen kring det har behandlats på nationell nivå vid EU:s beredningssektioner (sektionen för kommunikation, sektionen för trafik, sektionen för den inre marknaden) 25–28 september 2017. Utlåtandena om U-skrivelsen var positiva. Finansministeriets budgetavdelning lade fram tillägg till Finlands ståndpunkt, vilka beaktades. I beredningen deltog förutom ministerier och centrala ämbetsverk även intresseorganisationer och representanter för intressentgrupper.

Det är meningen att förslaget ska behandlas vid rådets cyber- och telearbetsgrupps gemensamma sammanträden. Behandlingen är avsedd att börja under hösten 2017. Ordförande har som mål att upprätta en lägesrapport inför december månads transport-, telekommunikations- och energiråd.

Inom Europaparlamentet är utskottet för industrifrågor, forskning och energi ansvarigt utskott.

8 Statsrådets ståndpunkt

Statsrådet anser det vara viktigt att förslaget syftar till att stärka informationssäkerheten inom hela EU-området, förbättra tillgången på informationssäkra produkter och tjänster på den inre marknaden samt främja innovationer. Spetsprojektet i statsminister Juha Sipiläs regeringsprogram är att man bygger en tillväxtmiljö för digital affärsverksamhet i Finland. Målen i förordningsförslaget kan anses ligga i linje med regeringsprogrammet, den nationella informationssäkerhetsstrategin som upprättats med stöd av dess verkställighetsplan och cybersäkerhetsstrategin som godkändes av den föregående regeringen.

Statsrådet anser att förändringen av ENISA:s mandat till permanent förbättrar byråns verksamhetsförutsättningar. Det säkerställer verksamhetens kontinuitet och skapar nya möjligheter att rekrytera expertis på hög nivå inom byrån. ENISA:s verksamhet och mål ska utvärderas regelbundet, så att byrån på bästa sätt ska kunna tjäna den digitala inre marknaden som förändras och utvecklas med snabba cykler. Syftet ska vara användning av anslagen enligt principerna för en resultatrik, kostnadseffektiv och oklanderlig finansförvaltning.

Enligt stadsrådets uppfattning ska ENISA:s verksamhet utvecklas till att stärka den inre marknaden på de områden där tillgången på inbyggt informationssäkra produkter och tjänster, som svarar mot användarnas behov, inte tillfredsställer efterfrågan från användarna. Ett av dessa områden är det så kallade sakernas internet (Internet of Things, IoT), som avser den helhet som bildas av apparater, programvaror och andra tillgångar kopplade till informationsnätet. Kommissionen bedömer i sitt förslag att man inom EU under de följande årtiondena kommer att ta i bruk miljoner eller till och med miljarder digitala apparater anslutna till informationsnätverket. Statsrådet instämmer i kommissionens ståndpunkt att sakernas internet och andra

centrala resurser på den digitala inre marknaden, såsom dataekonomi och automatiserande trafik, endast kan nå sin fulla potential om de åtnjuter allmänt förtroende och deras informationssäkerhet ligger på en tillräckligt hög nivå. Statsrådet anser också att det är viktigt att användarna har möjlighet att skydda sin konfidentiella kommunikation och digitala information med krypterings- och säkerhetsprogram utvecklade utifrån konsumentbehov samt med andra teknologiska lösningar.

Syftet med ramen för certifiering av de föreslagna informations- och kommunikationsteknologitillgångarna kan anses vara lönsam i det avseendet att man med regleringen strävar efter att öka förtroendet för den digitala inre marknaden och minska företagens kostnader för certifiering. Effektiviteten i de föreslagna medlen och metoderna i förhållande till det eftersträvade målet ska emellertid utvärderas noggrant.

Statsrådet anser att ENISA och kommissionen ska främja särskilt utvecklingen av sådana standarder och certifieringar, med vars hjälp användare som inom olika branscher utnyttjar informationsteknik och sakernas internet i sin verksamhet bättre kan förvissa sig om den inbyggda informationssäkerheten hos apparater och programvaror kopplade till sakernas internet som erbjuds på EU:s inre marknad. I det här arbetet ska kommissionen och ENISA även beakta det standardiserings- och certifieringsarbete som redan pågår inom olika branscher för att förbättra informationssäkerheten och den digitala tjänsteproduktionen och undvika överlappning med detta. Statsrådet anser det också vara viktigt att certifieringsramarna som skapas med förordningsförslaget stöder utvecklingen av en säker automatisk trafik.

Statsrådet vill fästa uppmärksamhet på att ramen och certifieringsprogram som skapas med stöd av den potentiellt kan påverka en ganska stor grupp olika aktörer, eftersom de produkter och tjänster som faller inom den bransch som ramen fastställer har definierats brett i förordningsförslaget. En mer exakt definition görs i certifieringsprogrammen som beviljas genom kommissionen genomförandeakter och där de tillgångskategorier som gäller för programmet definieras. Påverkan, omfattning och ändamålsenlighet av förordningsförslaget och det tillämpningsområde på lägre nivå som beviljats med stöd av det, ska utvärderas i den fortsatta beredningen, så att man kan försäkra sig om att certifieringarna har en genuint positiv påverkan och att man får ut mer informationssäkra produkter och tjänster än tidigare, som även motsvarar användarnas behov.

Statsrådet anser det vara viktigt att standardiserings- och certifieringsverksamheten för informationssäkra produkter drar nytta av finska företag, men inte tillfogar dem extra administrativ belastning som skadar konkurrenskraften. Skyldigheterna i EU-regleringen för kontroll av informationssäkerhetsrisker ska även i fortsättningen kunna tillämpas som en del av riskhanteringen av annan affärsverksamhet. Man måste fästa särskild uppmärksamhet vid det här i myndighetsverksamhetens fortsatta beredning av ärenden som gäller förslaget. Den föreslagna regleringen ska även i sin helhet formuleras så att den eller motsvarande tillvägagångssätt inte orsakar extra administrativ belastning för den privata sektorn eller myndigheter och till att inte skapa en sinsemellan ojämlik ställning för olika aktörer.

Statsrådet anser att ENISA i sin verksamhet ska undvika överlappningar med nationella myndigheters verksamhet. Det operativa samarbetet ska i första hand utvecklas inom ramen för de nya samarbetsstrukturerna som regleras i direktivet om nät- och informationssäkerhet, för att få erfarenhet om hur effektiva de är. ENISA:s uppgifter och de skyldigheter som förordningsförslaget skapar för medlemsländerna ska ligga i linje med direktivet om nät- och informationssäkerhet.

Dessutom anser statsrådet att det är allmänt viktigt att även i fortsättningen noggrant följa utvecklingen av EU-institutionernas och myndigheternas administrativa utgifter och antal anställda. Man ska eftersträva att hålla en helhetsmässigt rimlig nivå på de här utgifterna.

9 Skribentens kontaktuppgifter

Piia Nyström Kommunikationsministeriet tfn 029 534 2969