EUROOPAN KESKUSPANKIN LAUSUNTO,

annettu 11 päivänä huhtikuuta 2022,

ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta

(CON/2022/14)

(2022/C 233/03)

Johdanto ja oikeusperusta

Euroopan komissio hyväksyi 16 päivänä joulukuuta 2020 ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvallisuustason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta ([1]) (jäljempänä ”ehdotettu direktiivi”). Euroopan unionin neuvosto hyväksyi 3 päivänä joulukuuta 2021 ehdotettua direktiiviä koskevan yleisnäkemyksen ([2]). Euroopan keskuspankin (EKP) toimivalta antaa lausunto perustuu Euroopan unionin toiminnasta tehdyn sopimuksen 127 artiklan 4 kohdan toiseen alakohtaan, sillä ehdotettu direktiivi sisältää EKP:n toimivaltaan kuuluvia säännöksiä, jotka koskevat erityisesti maksujärjestelmien moitteettoman toiminnan edistämistä, myötävaikuttamista rahoitusjärjestelmän vakauteen liittyvän toimivaltaisten viranomaisten politiikan moitteettomaan harjoittamiseen sekä luottolaitosten toiminnan vakauden valvontaan liittyviä EKP:n tehtäviä perussopimuksen 127 artiklan 2 kohdan neljännen luetelmakohdan, 127 artiklan 5 kohdan 127 artiklan 6 kohdan mukaisesti. Tämän lausunnon on antanut EKP:n neuvosto Euroopan keskuspankin työjärjestyksen 17.5 artiklan ensimmäisen virkkeen mukaisesti.

Yleiset huomautukset

EKP tukee vahvasti ehdotetun direktiivin tavoitteita, jotka koskevat kyberuhkien sietokyvyn parantamista kaikilla asiaankuuluvilla aloilla, epäjohdonmukaisuuksien vähentämistä sisämarkkinoilla sekä tilannetietoisuuden ja kollektiivisen valmistautumis- ja reagointikyvyn parantamista varmistamalla tehokas yhteistyö unionissa.

EKP toteaa, että on tärkeää säilyttää kiinteät yhteydet ehdotetun direktiivin ja rahoitussektorin välillä. Rahoitussektorin olisi pysyttävä osana verkko- ja tietojärjestelmien ekosysteemiä, jotta voidaan edistää tieto- ja viestintätekniikkaan liittyvien riskien johdonmukaista arviointia kaikkialla unionissa ja edistää tehokasta monialaista tietojenvaihtoa ja yhteistyötä kyberuhkien käsittelyssä. Tätä varten toimivaltaisten viranomaisten olisi finanssialan digitaalisesta häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston asetusehdotuksen ([3]) (jäljempänä ”DORA-asetusehdotus”), mukaisesti voitava osallistua verkko- ja tietoturva-alan yhteistyöryhmän strategisiin poliittisiin keskusteluihin ja tekniseen työhön sekä vaihtaa tietoja ja tehdä edelleen yhteistyötä ehdotetussa direktiivissä tarkoitettujen keskitettyjen yhteyspisteiden ja tietoturvaloukkauksiin reagoivien kansallisten ryhmien kanssa ([4]).

1. Ehdotetun direktiivin soveltamisala

1.1 EKP ymmärtää, että DORA-asetusehdotus on suhteessa rahoitusalan yhteisöihin, jotka määritetään keskeisten palvelujen tarjoajiksi, alakohtainen unionin säädös, jolla otetaan käyttöön kyberturvariskien hallintaa ja poikkeamista raportointia koskevia vaatimuksia, jotka vastaavat vaikutukseltaan ehdotetussa direktiivissä säädettyjä vaatimuksia ([5]). Sen vuoksi ehdotetun direktiivin säännöksiä, jotka liittyvät kyberturvariskien hallintaan, raportointivelvoitteisiin, tietojen jakamiseen sekä valvontaan ja täytäntöönpanoon, ei sovelleta DORA-asetusehdotuksen soveltamisalaan kuuluviin finanssialan yhteisöihin ([6]). Kuten ehdotetun direktiivin johdanto-osan kappaleissa

([1]) COM(2020) 823 final.
([2]) Luettavissa neuvoston verkkosivuilla osoitteessa www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Ks. ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi finanssialan digitaalisesta häiriönsietokyvystä 4 päivänä kesäkuuta 2021 annetun Euroopan keskuspankin lausunnon CON/2021/20 (EUVL C 343, 26.8.2021, s. 1) 1.5 kohta. Kaikki EKP:n lausunnot julkaistaan EUR-Lex-sivustolla. DORA-asetusehdotuksen 17 artiklan 5 kohta; ehdotetun direktiivin 11 artikla.
([5]) Ehdotetun direktiivin 2 artiklan 6 kohta.
([6]) Ks. ehdotetun direktiivin johdanto-osan 13 kappale ja 2 artiklan 6 kohta.

selvennetään, ehdotetun direktiivin sijasta olisi sovellettava DORA-asetusehdotuksen säännöksiä, jotka liittyvät TVT-riskien hallintatoimenpiteisiin, TVT:hen liittyvien poikkeamien hallintaan ja poikkeamista raportointiin, digitaalisen häiriönsietokyvyn testaukseen, tietojenvaihtojärjestelyihin ja kolmannen osapuolen TVT-riskiin ([7]).

1.2 EKP panee myös merkille, että neuvosto esittää ehdotettua direktiiviä koskevassa yleisnäkemyksessään muutosta, jonka mukaan ehdotettua direktiiviä ei sovelleta ”toimijoihin, jotka harjoittavat oikeuslaitoksille, kansanedustuslaitoksille tai keskuspankeille kuuluvaa toimintaa” ([8]). EKP katsoo, että ehdotettu muutos kattaisi kaikki Euroopan keskuspankkijärjestelmän (EKPJ) perustehtävät ja toimivaltuudet, joista määrätään Euroopan unionin toiminnasta tehdyn sopimuksen 127 artiklan 2 kohdassa ja Euroopan keskuspankkijärjestelmän ja Euroopan keskuspankin perussäännön, jäljempänä ”EKPJ:n perussääntö”, 3.1 artiklassa, kuten maksujärjestelmien moitteettoman toiminnan edistämisen. Eurojärjestelmän omistamien ja hallinnoimien rahoitusmarkkinainfrastruktuurien, kuten TARGET2- ja TARGET2-Securities-järjestelmien, katsotaan kuuluvan neuvoston ehdotukseen sulkea keskuspankit ehdotetun direktiivin soveltamisalan ulkopuolelle.

2. **EKPJ:n ja eurojärjestelmän yleisvalvonnalliset toimivaltuudet**

2.1 EKPJ:n ensisijaisena tavoitteena on pitää yllä hintatason vakautta, ja Euroopan unionin toiminnasta tehdyn sopimuksen 127 artiklan 2 kohdan mukaisesti yksi EKPJ:n perustehtävistä on maksujärjestelmien moitteettoman toiminnan edistäminen ([9]). Tämän perustehtävän hoitamisen yhteydessä EKP ja kansalliset keskuspankit voivat tarjota järjestelyjä ja EKP voi antaa asetuksia selvitys- ja maksujärjestelmien tehokkuuden ja vakauden varmistamiseksi yhteisössä ja kolmansien maiden kanssa ([10]). Osana valvontatehtäviensä hoitamista EKP on antanut Euroopan keskuspankin asetuksen (EU) N:o 795/2014 (EKP/2014/28) ([11]) (jäljempänä ”SIPS-asetus”), jolla rahoitusmarkkinainfrastruktuureja koskevat CPSS:n ja IOSCO:n periaatteet ([12]) muunnetaan suoraan sovellettavaksi lainsäädännöksi. SIPS-asetuksessa vahvistetaan vaatimukset suuria ja pieniä maksuja välittäville maksujärjestelmille, jotka ovat systeemisesti merkittäviä, riippumatta siitä, ovatko ne julkisessa vai yksityisessä omistuksessa. SIPS-asetuksessa vahvistettuihin vaatimuksiin sisältyy jo muun muassa operatiivisen riskin hallinnointi ja kyberturvallisuusjärjestelyjen käyttöönotto ([13]).

2.2 Järjestelmän kannalta merkittävien maksujärjestelmien lisäksi eurojärjestelmän yleisvalvonta kattaa muut kuin järjestelmän kannalta merkittävät maksujärjestelmät, sähköiset maksuvälineet ja -järjestelyt sekä muut infrastruktuurit ja kriittiset palveluntarjoajat eurojärjestelmän yleisvalvontaa koskevan puiteasiakirjan mukaisesti ([14]). Ehdotetun direktiivin soveltamisalaan ei nimenomaisesti sisällytetä maksujärjestelmiä ja muita eurojärjestelmän yleisvalvonnan piiriin kuuluvia järjestelyjä ([15]). Koska ehdotetulla direktiivillä luodaan yhdenmukaistamisen vähimmäistaso ([16]), jäsenvaltioiden antama täytäntöönpanolainsäädäntö voisi kuitenkin olla päällekkäistä eurojärjestelmän yleisvalvontavallan kanssa. Tämän välttämiseksi ehdotetun direktiivin johdanto-osassa olisi nimenomaisesti tunnustettava perustamissopimuksen ja EKPJ:n perussäännön mukainen EKPJ:n toimivalta sekä SIPS-asetuksen ja yleensä eurojärjestelmän yleisvalvontajärjestelmän mukainen eurojärjestelmän toimivalta.

([7]) Ehdotetun direktiivin johdanto-osan 13 kappale.
([8]) Ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen 2 artiklan 3 a kohdan ensimmäisen alakohdan b alakohta.
([9]) Perussopimuksen 127 artiklan 2 kohta, ja vastaavasti EKPJ:n perussäännön 3.1 artikla.
([10]) EKPJ:n perussäännön 22 artikla.
([11]) Euroopan keskuspankin asetus (EU) N:o 795/2014, annettu 3 päivänä heinäkuuta 2014, systeemisesti merkittäviä maksujärjestelmiä koskevista yleisvalvontavaatimuksista (EKP/2014/28) (EUVL L 217, 23.7.2014, s. 16).
([12]) Ks. maksu- ja selvityskomitean (CPSS) ja Kansainvälisen arvopaperimarkkinavalvojien yhteisön (IOSCO) teknisen komitean rahoitusmarkkinainfrastruktuureja koskevat periaatteet, jotka on julkaistu huhtikuussa 2012 ja ovat luettavissa kansainvälisen selvityspankin verkkosivuilta osoitteessa www.bis.org. Niiden velvoitteessa D todetaan, että ”kaikkien CPSS:n ja IOSCO:n jäsenten odotetaan soveltavan periaatteita asianomaisiin rahoitusmarkkinainfrastruktuureihin lainkäyttöalueellaan niin täysimääräisesti kuin niiden lainkäyttöalueen sääntelyssä sallitaan”.
([13]) Asetuksen (EU) N:o 795/2014 (EKP/2014/28) 15 artikla.
([14]) Eurojärjestelmän yleisvalvontaa koskeva puiteasiakirja (Eurosystem oversight policy framework), tarkistettu versio, heinäkuu 2016, luettavissa EKP:n verkkosivuilla osoitteessa www.ecb.europa.eu.
([15]) Ehdotetun direktiivin 2 artikla ja I ja II liite.
([16]) Ehdotetun direktiivin 3 artikla.

3. **Kolmansiin osapuoliin liittyvät TVT-riskit, laajamittaisten poikkeamien ja kriisien hallinta, tietojen jakaminen ja kansallinen kyberturvallisuusstrategia**

3.1 *Kolmansiin osapuoliin liittyvien TVT-riskien hallinta*

3.1.1 Ehdotetussa direktiivissä annetaan toimivaltaisille viranomaisille valtuudet keskeisiä toimijoita koskevia täytäntöönpanovaltuuksiaan käyttäessään antaa sitovia ohjeita tai määrätä näitä toimijoita korjaamaan havaitut puutteet tai ehdotetun direktiivin velvoitteiden rikkomiset ([17]). Samalla DORA-asetusehdotuksen mukaisesti nimetty päävalvoja voi antaa kriittisille TVT-palveluntarjoajana oleville kolmansille osapuolille suosituksia ulkoistamiskäytäntöjen ja kolmansien osapuolten TVT-keskittymän mahdollisesti aiheuttamien järjestelmäriskien hallitsemiseksi ([18]).

3.1.2 Ottaen huomioon, että ehdotetun direktiivin mukainen tärkeä toimija voidaan myös nimetä kriittiseksi TVT-palveluntarjoajana olevaksi kolmanneksi osapuoleksi DORA-asetusehdotuksen mukaisesti, EKP toistaa ([19]), että ristiriitaisten suositusten ja sitovien ohjeiden antamista olisi vältettävä. Tältä osin EKP panee tyytyväisenä merkille ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen. Tämän lähestymistavan mukaan toimivaltaisten viranomaisten on ilmoitettava DORA-asetusehdotuksen nojalla perustetulle valvontafoorumille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan suhteessa keskeiseen toimijaan, joka on nimetty DORA-asetusehdotuksen nojalla kriittiseksi TVT-palvelujen tarjoajana olevaksi kolmanneksi osapuoleksi ([20]).

3.2 *Laajamittaisten poikkeamien ja kriisien hallinta*

3.2.1 Ehdotetun direktiivin mukaisesti ([21]) jäsenvaltioiden on nimettävä yksi tai useampi toimivaltainen viranomainen, joka vastaa laajamittaisten poikkeamien ja kriisien hallinnasta. Kuten ehdotetun direktiivin johdanto-osan kappaleissa selvennetään, laajamittaisella poikkeamalla olisi tarkoitettava poikkeamaa, jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon tai jonka aiheuttama häiriö ylittää yksittäisen jäsenvaltion valmiudet reagoida siihen. Laajamittaiset poikkeamat voivat muuttua todellisiksi kriiseiksi, jotka estävät sisämarkkinoiden moitteettoman toiminnan ([22]).

3.2.2 Vaikka DORA-asetusehdotuksen mukaisesti nimetyt toimivaltaiset viranomaiset ovat edelleen vastuussa finanssiyhteisöjen kyberturvallisuuspoikkeamien hallinnasta, yhteistyö ehdotetun direktiivin nojalla perustettujen rakenteiden ja viranomaisten kanssa on ratkaisevan tärkeää koordinoidun reagoinnin varmistamiseksi kaikkialla unionissa. Tätä varten EKP suosittelee, että DORA-asetusehdotuksen mukaisesti nimetyt toimivaltaiset viranomaiset, myös EKP, osallistuisivat Euroopan kyberkriisien yhteysorganisaatioiden verkostoon (EU-CyCLONe) ([23]), kun laajamittaiset kyberturvallisuuspoikkeamat ja -kriisit vaikuttavat finanssialaan.

3.3 *Tietojen jakaminen*

3.3.1 Kuten edellä todettiin, EKP tukee voimakkaasti DORA-asetusehdotuksen mukaisesti nimettyjen toimivaltaisten viranomaisten yhteistyötä ehdotetun direktiivin mukaisesti perustettujen rakenteiden ja viranomaisten kanssa. Viranomaisten välinen tietojenvaihto voi erityisesti mahdollistaa monialaisen oppimisen, edistää kyberhyökkäysten ehkäisemistä ja tehokasta hallintaa ja edistää tieto- ja viestintätekniikkaan liittyvien riskien johdonmukaista arviointia kaikkialla unionissa. EKP korostaa kuitenkin, että tietojenvaihdon olisi tapahduttava silloin, kun käytössä on selkeästi määritellyt luokitus- ja tietojenvaihtojärjestelyt, joihin liittyy riittävät suojatoimet luottamuksellisuuden varmistamiseksi ([24]). EKP on tyytyväinen ehdotettua direktiiviä koskevaan neuvoston yleisnäkemykseen, jossa

([17]) Ehdotetun direktiivin 29 artiklan 4 kohdan b alakohta.
([18]) DORA-asetusehdotuksen 31 artikla.
([19]) Ks. lausunnon CON/2021/20 1.2 kohta.
([20]) Ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen 29 artiklan 10 kohta.
([21]) Ehdotetun direktiivin 7 artiklan 1 kohta.
([22]) Ehdotetun direktiivin johdanto-osan 27 kappale.
([23]) Ehdotetun direktiivin 14 artikla.
([24]) Ks. lausunnon CON/2021/20 1.5 kohta.

ehdotetaan asiaankuuluvien tietojen säännöllistä vaihtoa viranomaisten välillä ([25]), yhteistyöjärjestelyjen perustamista tietojenvaihtojärjestelyjen määrittämiseksi ([26]) sekä poikkeamia koskevien ilmoitusten automaattista ja suoraa välittämistä ([27]). Tässä yhteydessä olisi varmistettava, että DORA-asetusehdotuksen ([28]) tai asiaa koskevan alakohtaisen lainsäädännön ([29]) nojalla luottamuksellisia tietoja voidaan vaihtaa ehdotetussa direktiivissä tarkoitettujen toimivaltaisten viranomaisten kanssa vain, kun tietojenvaihto on tarpeen, jotta toimivaltaiset viranomaiset voivat soveltaa ehdotetun direktiivin säännöksiä ([30]).

3.4 *Kansallinen kyberturvallisuusstrategia*

3.4.1 Ehdotetun direktiivin mukaan jäsenvaltioiden on hyväksyttävä kansalliset kyberturvallisuusstrategiat, joissa määritellään strategiset tavoitteet ja asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi ([31]). Kuten ehdotetun direktiivin johdanto-osan kappaleissa selvennetään, jäsenvaltioiden olisi edelleen sisällytettävä rahoitusala omiin kyberturvallisuusstrategioihinsa ([32]). Suuntaa-antavasti jäsenvaltioiden olisi osana kansallisia kyberturvallisuusstrategioitaan hyväksyttävä toimintapolitiikkoja, joilla puututaan kyberturvallisuuteen toimitusketjussa sellaisten tieto- ja viestintätekniikan tuotteiden ja palvelujen osalta, joita toimijat käyttävät palvelujensa tarjoamiseen. Rahoitusalan osalta kansallisten kyberturvallisuusstrategioiden olisi oltava yhdenmukaisia DORA-asetusehdotukseen perustuvan sääntelykehyksen kanssa. Tältä osin EKP katsoo, että tarvitaan lisäselvennyksiä sen varmistamiseksi, että kansalliset kyberturvallisuusstrategiat ovat yhdenmukaisia alakohtaisen lainsäädännön kanssa.

Niiltä osin kuin EKP suosittaa ehdotettua direktiiviä muutettavaksi, tarkat muutosehdotukset perusteluineen on esitetty teknisessä työasiakirjassa, johon on liitetty selvitys. Tekninen työasiakirja on luettavissa englanninkielisenä EUR-Lex-verkkosivustolla.

Tehty Frankfurt am Mainissa 11 päivänä huhtikuuta 2022.

EKP:n puheenjohtaja
Christine LAGARDE

([25]) Ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen 11 artiklan 5 kohta.
([26]) Ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen johdanto-osan 23 a kappale.
([27]) Ehdotettua direktiiviä koskevan neuvoston yleisnäkemyksen johdanto-osan 13 kappale.
([28]) DORA-asetuksen 49 artikla.
([29]) Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU, annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta (EUVL L 176, 27.6.2013, s. 338), 53–62 artikla.
([30]) Ehdotetun direktiivin 2 artiklan 5 kohta ja 11 artiklan 4 kohta.
([31]) Ehdotetun direktiivin 5 artikla.
([32]) Ehdotetun direktiivin johdanto-osan 13 kappale.