

Asia: VN/19122/2023

Lausuntopyyntö hallituksen esitysluonnoksesta laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräksi siihen liittyviksi laeiksi

Lausuntokysymykset

Finanssivalvonnasta annettua lakia koskevat näkemykset

Lausuntopyynnön kohteena olevalla hallituksen esityksellä toimeenpannaan rahoitusalaan koskien DORA-asetuksen ja tähän liittyvän muutosdirektiivin sekä kriittisen infrastruktuurin suojaamista koskevan CER-direktiivin ja tietoturvallisuusdirektiivin muutosdirektiivin (NIS2) edellyttämät kansallisen lainsäädännön mukautukset. Kokonaisuus on monitahoinen, koska osa säädöskokonaisuuden oikeusvaikutuksista seuraa suoraan sovellettavasta asetuksesta, osa (eri direktiiveihin perustuvista) kansallisen lainsäädännön muutoksista ja osa viranomaisten soveltamiskäytännöstä sekä EU-oikeudellisesta delegoidusta norminannosta.

Edellä todetusta EU-lainsäädännön rakenteesta seuraa, että merkittävimmät tarpeet kansallisen lainsäädännön mukautuksiin koskevat lähinnä Finanssivalvontaa koskevaa sääntelyä. DORA-asetuksen suoraan sovellettavat säännökset vaikuttavat samalla myös merkittävästi myös kriisinratkaisuviranomaisten, kuten Rahoitusvakausviraston toimintaan. Luonnoksen perusteella ei siten saa kokonaiskuvaa sääntelyllä tavoiteltavista kokonaisvaikutuksista viranomaisten toimintaan ja myös tarvittavaan yhteistyöhön. Ottaen huomioon lainsäädännön esitöiden merkitys myös soveltamistoimintaa ohjaavana oikeuslähteenä, Rahoitusvakausvirasto pitää tärkeänä, että ehdotuksen perustelujen täydennetään kuvaamaan kattavammin ehdotuksen vaikutukset myös kriisinratkaisuviranomaisiin ja viranomaisten väliseen yhteistoimintaan. Näitä vaikutuksia kriisinratkaisuviranomaisten toimintaan on esitetty tämän lausunnon eri jaksoissa.

CER-direktiivin vaikutuksia Finanssivalvonnan toimintaan ja tehtäviin on luonnoksessa käsitelty varsin suppeasti. Näitä vaikutuksia ei ole myöskään kuvattu samanaikaisesti sisäministeriössä valmisteltavana olevassa hallituksen esityksessä. Rahoitusvakausviraston näkemyksen mukaan ehdotusten perustelujen olisi näiltä osin tarpeen täsmentää.

Rahoitusvakausviraston käsityksen mukaan rahoitusalan osalta erityinen merkitys olisi CER-direktiivin ja sitä täytäntöönpanevan kansallisen lainsäädännön määräyksillä kansallisesta kriittisen infrastruktuurin suojaamisen strategiasta ja riskiarviosta. Rahoitusvakausviraston käsityksen mukaan toimiessaan CER-direktiivin mukaisena kansallisesti toimivaltaisena viranomaisena ja DORA-asetuksen mukaisena toimivaltaisena viranomaisena, Finanssivalvonnan tulisi ottaa huomioon mainitut kriittisen infrastruktuurin suojamista koskeva strategia ja riskinarvioinnit mitoittaessaan ja kohdentaessaan valvontatoimintaansa. Rahoitusvakausviraston näkemyksen mukaan tämä on merkittävin CER-direktiivin vaikutus rahoitusalan toiminnan osalta ja selkeyden vuoksi tämä sääntelyn yhteisvaikutus olisi tarpeen kuvata esityksessä tarkemmin.

DORA-asetuksen myötä laitosten operatiivinen resilienssi ja IT-järjestelmät nousevat kriittiseksi osaksi viranomaisten tilannekuvaa. Kuten esityksessä todetaan, aktiivinen viranomaisyhteistyö on erittäin tärkeää kyberturvallisuuteen liittyvien tehtävien tuloksellisen hoitamisen kannalta.

Ehdotuksen mukaan Finanssivalvonnasta annettuun lakiin lisättäisiin uusi 3 f § viranomaisyhteistyöstä kyberturvallisuuden edistämiseksi. Ehdotetulla pykälällä varmistettaisiin kyberturvallisuuteen liittyvää viranomaisyhteistyötä niin, että Finanssivalvonta toimisi yhteyspisteenä viranomaisyhteistyölle, jolla häiriöitä hallitaan ja vaikutuksia pienennetään. Rahoitusvakausvirasto pitää ehdotettua uutta säännöstä, jossa Rahoitusvakausvirasto on mukana yhteistyössä, kannatettavana. Ehdotetun sääntelyn tarkoituksena on, että rahoitusalan osalta erilaiset häiriöraportointia koskevat tehtävät keskitetään Finanssivalvonnalle kattavan tilannekuvan varmistamiseksi ja raportointivelvollisten hallinnollisen taakan vähentämiseksi. Tilannekuvan muodostamisessa ja häiriötilannetietojen jakamisessa Finanssivalvonnan on tällöin huolehdittava siitä, että Finanssivalvonta huomioi aktiivisesti ja oma-aloitteisesti myös muiden viranomaisten tietotarpeet, eikä käsittele tietoja häiriötilanteista yksinomaan omien valvontatehtäviensä hoitamisen näkökulmasta.

DORA-asetuksesta seuraa, että valvonta ja kriisinratkaisuviranomaisten on toiminnassaan painotettava entistä enemmän operatiivisten riskien ja kriittisten järjestelmien jatkuvuuden turvaamista. Kyberturvallisuuteen liittyvää viranomaisyhteistyötä koskevassa 3 f §:ssä tarkoitetun yhteistyön lisäksi Rahoitusvakausvirasto tarvitsee tietoja kriisinratkaisun suunnitteluun ja laitoksen purettavuuden arviointiin. Näiden tehtävien hoito edellyttää Finanssivalvonnalta aktiivista ja säännöllistä tiedonvaihtoa Rahoitusvakausvirastolle. Koska tietoja tarvitaan säännöllisesti päivitettäviin suunnitelmiin ja arviointiin, tiedonvaihdon tulisi olla tarvittavilta osin säännöllistä ja määrämuotoista, eikä se voi perustua Rahoitusvakausviraston tapauskohtaisiin tietopyyntöihin.

Rahoitusvakausvirasto ehdottaa lisäämään Finanssivalvonnasta annettuun lakiin tarvittavat säännökset siitä, että Finanssivalvonta saisi SI-laitoksilta vastaavat tiedot kuin LSI-laitoksilta. DORA-asetuksessa tiedonvaihto ja yhteistyö on rakennettu EU-sääntelyn mukaisten toimivaltuuksien pohjalta. DORA:ssa tiedonvaihdosta ja yhteistyöstä on säädetty niin, että niitä laitoksia, jotka kuuluvat kriisinratkaisussa yhteisen kriisinratkaisuneuvoston SRB:n suoran toimivallan alle, koskeva tiedonvaihto ja yhteistyö tehdään kriisinratkaisuviranomaisista SRB:n kanssa ja niitä laitoksia, jotka kuuluvat kriisinratkaisuun liittyen Rahoitusvakausviraston suoran toimivallan alle, koskeva

tiedonvaihto ja yhteistyö tehdään Rahoitusvakausviraston kanssa. Kansallista tiedonvaihtoa ja yhteistyötä säädettäessä tulisi ottaa huomioon myös yksinomaan kansalliseen lainsäädäntöön perustuvat toimivaltuudet. Rahoitusvakausvirasto pyytää ottamaan huomioon, että suomalaiset SRB:n toimivallan alle kuuluvat laitokset voivat olla Rahoitusvakausviraston ylläpitämän huoltovarmuustilijärjestelmän piirissä. Huoltovarmuuteen liittyen tiedonvaihto on tarkoituksenmukaista järjestää kokonaan kansallisesti. Jotta tiedot voidaan luovuttaa Finanssivalvonnasta Rahoitusvakausvirastolle, tulee Rahoitusvakausviraston näkemyksen mukaan Finanssivalvonnan saada tiedot SI-laitoksilta kansallisen lainsäädännön perusteella.

DORA-asetuksen perusteella Rahoitusvakausvirasto voi pyytää LSI-laitoksilta tietoja niiden DORA-asetuksen perusteella tekemistä testeistä. Ottaen huomioon Rahoitusvakausviraston tehtävät kansallisesta talletussuojasta ja huoltovarmuustilijärjestelmän ylläpitämisestä vastaavana viranomaisena, Rahoitusvakausvirasto pitää tarpeellisena, että kansallisesti säädettäisiin vastaavasta oikeudesta myös SI-laitoksiin liittyen.

Ehdotuksen mukaan Finanssivalvonnasta annetun lain 5 §:n määritelmää muista finanssimarkkinoilla toimivista laajennettaisiin kattamaan DORA-asetuksessa tarkoitettu ja asetuksen soveltamisalaan kuuluva TVT-palveluntarjoajana oleva kolmas osapuoli. Ehdotettu lisäys laajentaisi samalla rahoitusvakausviranomaisesta annetun lain 7 luvun 4 §:n mukaista Rahoitusvakausviraston tiedonsaantioikeutta niin, että Rahoitusvakausvirastolla olisi mahdollisuus saada tietoja suoraan näiltä TVT-palveluntarjoajilta. DORA-asetuksen 30 artiklan 2 kohdan g-alakohdan mukaan näillä TVT-palveluntarjoajilla on velvollisuus tehdä täysimääräisesti yhteistyötä kriisinratkaisuviranomaisten kanssa. Rahoitusvakausviraston näkemyksen mukaan täysimääräinen yhteistyö on käsitteenä laajempi kuin kansallisessa laissa tunnustettu tietojen toimittaminen Rahoitusvakausviraston pyynnöstä. Tarvittaessa Rahoitusvakausvirasto voisi pyytää yhteistyötä suoraan DORA-asetuksen perusteella.

Luonnoksen vaikutusarviossa todetaan, että ehdotuksella ei katsota olevan merkittäviä vaikutuksia Finanssivalvonnan toimintaan. Rahoitusvakausviraston näkemyksen mukaan todettu vaikuttaa ristiriitaiselta useisiin ehdotettuihin valvontatoimivaltuuksien täsmennyksiin, valvottavilta edellytettäviin testeihin, tilannekuva-, neuvonta- ja yhteyspistetehtäviin sekä muun ohella DORA-asetuksen johdantolausekkeista ilmenevään unionin lainsäätäjän tarkoitukseen korottaa operatiivisen resilienssin valvonnan yhtäläistä merkitys vakaus- ja menettelytapavalvonnan rinnalle. Rahoitusvakausvirasto ei ota kantaa Finanssivalvonnan käytössä oleviin resursseihin, mutta toteaa, että unionin lainsäätäjän tarkoituksena on ollut nimenomaisesti kohdentaa toimivaltaisten viranomaisten toimintaa näihin tehtäviin.

Muita lakiehdotuksia koskevat näkemykset

-

Kansallisen liikkumavaran käyttämistä ja vaihtoehtoisia toteuttamistapoja koskevat huomiot

-

Muut mahdolliset huomiot hallituksen esityksestä

DORA-asetuksessa säädetään viranomaisten välisestä yhteistyöstä ja tiedonvaihdosta. Yhteistyö ja tiedonvaihto liittyy digitaalisen operatiivisen häiriönsietokyvyn huomioimiseen osana laitoksen purettavuuden arviointia ja laitoksen kriisinratkaisusuunnitelmaa laadittaessa. Rahoitusvakausviraston on tehtävä yhteistyötä ja vaihdettava tietoja toimivaltaisten viranomaisten, Rahoitusvakausviraston toimivallassa olevien laitosten, TVT-palveluntarjoajina olevien kolmansien osapuolien ja Euroopan valvontaviranomaisten kanssa.

Rahoitusvakausvirasto ehdottaa, että kansalliseen lainsäädäntöön lisättäisiin informatiivinen viittaus Rahoitusvakausviraston tehtäviin esimerkiksi toteamalla rahoitusvakausviranomaisesta annetussa laissa, että Rahoitusvakausviraston tehtävistä eräissä tilanteissa säädetään EU:n DORA-asetuksessa. Rahoitusvakausviranomaisesta annetun lain mukaisesti Rahoitusvakausvirasto huolehtii sille muussa laissa tai asetuksessa säädetyistä tehtävistä. On kuitenkin epäselvää, kattaako tämä viittaus kansalliseen lainsäädäntöön ja asetukseen myös suoraan sovellettavat EU-säännökset. Tämän vuoksi informatiivinen viittaus EU-säännökseen lisäisi Rahoitusvakausviraston näkemyksen mukaan selkeyttä.

DORA-asetuksen lähtökohtana on, että laitoksen testauksen tavoitteena on kriittisten toimintojen jatkuvuus. Kriittisillä toiminnoilla tarkoitetaan DORA-asetuksessa määritelmän mukaan samoja toimintoja, joiden jatkuvuus turvattaisiin kriisinratkaisussa. Rahoitusvakausvirasto pitää kriittisten toimintojen mainittua liityntää perusteltuna, sillä se mahdollistaa viranomaisyhteistyössä esimerkiksi testauksen kohdentamisen ja häiriöilmoitusten tarkemman arvioinnin niiden palvelujen ja IT-järjestelmien osalta, jotka on kriisinratkaisusuunnittelussa ennalta tunnistettu kriittisiin toimintoihin kytkeytyviksi.

Rahoitusvakausvirasto kiinnittää kuitenkin huomiota siihen, että kyberhyökkäys voi kohdistua myös laitoksen sellaiseen osaan, joka ei kuulu edellä mainitun määritelmän piiriin, vaan on muutoin olennainen kriisinratkaisun tai talletussuojan toteuttamiselle. Rahoitusvakausviraston näkemyksen mukaan viranomaisilla on voimassa olevassa lainsäädännössä laajat toimivaltuudet vaatia laitoksilta sellaisia toimia, joilla turvataan viranomastehtävien suorittaminen ja laitoksen purettavuus kriisinratkaisulla tai tavanomaisella maksukyvyttömyysmenettelyllä.

DORA-asetuksen mukaisesti Rahoitusvakausviraston tulee huomioida laitoksen operatiivinen häiriönsietokyky arvioidessaan laitoksen purettavuutta. Rahoitusvakausvirasto yhtyy luonnoksessa esitettyyn näkemyksen tarpeesta päivittää tämän johdosta valtiovarainministeriön asetusta seikoista, jotka on otettava huomioon arvioitaessa luottolaitoksen ja sijoituspalveluyrityksen taikka konsernin purkamis- ja uudelleenjärjestämismahdollisuuksia (1285/2014).

Kriittisten ja olennaisten palveluiden määrittelyyn ja tunnistamiseen liittyen on tehty paljon töitä kriisinratkaisusuunnittelun toiminnallista jatkuvuutta koskevan osa-alueen valmistelun yhteydessä. Rahoitusvakausvirasto on valmis jakamaan oppejaan ja tekemään yhteistyötä parhaiden käytäntöjen

jakamiseksi laajemminkin vastaavassa työssä muiden finanssialan toimijoiden, kuin luottolaitosten, sekä muiden sektoreiden osalta.

DORA-asetuksen 49 artiklassa säädetään sektorirajat ylittävistä harjoituksista, joissa harjoiteltavaan skenaarioon kuuluu kyberhyökkäys. Kyberriskit voivat realisoituessaan nopeasti siirtyä taloudelliseksi ongelmatilanteeksi. Rahoitusvakausviraston näkemyksen mukaan kyberskenaarioita on tarpeen harjoitella DORA-asetuksen mukaisen Euroopan valvontaviranomaisten harjoittelun lisäksi kansallisesti.

Luonnoksen vaikutusarviointia koskevassa jaksossa ei ole juurikaan arvioitu tai tunnistettu vaikutuksia muiden viranomaisten, kuin Finanssivalvonnan toimintaan. Edellä kuvatulla tavoin DORA-asetus edellyttää jatkossa toimenpiteitä myös Rahoitusvakausvirastolta osana kriisinratkaisun suunnittelua, purettavuuden arviointia ja kriisinratkaisuvalmiuksen kehittämistä. Lisäksi Rahoitusvakausviraston tulee jatkossa ottaa huomioon uuden kansallisen kriittistä infrastruktuurin suojaamisen strategioiden ja riskiarviointien vaatimukset toiminnassaan. Nämä vaatimukset kytkeytyvät suoraan Rahoitusvakausviraston olemassa oleviin tehtäviin, eikä niillä siten arvioida todennäköisesti olevan välittömiä resurssivaikutuksia, mutta viraston on huomioitava näiden vaatimusten täyttäminen omissa toiminta- ja yhteistyöprosesseissaan sekä esimerkiksi henkilöstön osaamisen kehittämisessä. Ehdotetun sääntelyn kokonaisvaikutusten hahmottamiseksi Rahoitusvakausvirasto pitää tärkeänä, että ehdotuksen vaikutusarvioita täsmennetään tältä osin.

Rahoitusvakausvirasto - Jaakko Weuro, ylijohdaja; Fanni Teinilä, juristi