Hallituksen esitys eduskunnalle laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettaviksi Finanssivalvonnasta annettua lakia, luottolaitostoiminnasta annettua lakia, sijoituspalvelulakia, maksulaitoslakia, kaupankäynnistä rahoitusvälineillä annettua lakia, sijoitusrahastolakia, vaihtoehtorahastojen hoitajista annettua lakia, lisäeläkesäätiöistä ja lisäeläkekassoista annettua lakia, vakuutusyhtiölakia, Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annettua lakia ja valtion erityisrahoitusyhtiöstä annettua lakia.

Esitys sisältää ehdotukset finanssialan digitaalisesta häiriönsietokyvystä annettua Euroopan parlamentin ja neuvoston asetusta (jäljempänä *DORA-asetus*) täydentäviksi kansallisiksi säännöksiksi. Lisäksi esityksellä pantaisiin täytäntöön Euroopan parlamentin ja neuvoston direktiivi eräiden direktiivien muuttamisesta finanssialan digitaalisen häiriönsietokyvyn osalta (jäljempänä *DORA-muutosdirektiivi*).

Esitys sisältää lisäksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (jäljempänä *NIS2-direktiivi*) sekä kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiivin (jäljempänä *CER-direktiivi*) kansallista täytäntöönpanoa täydentävät ehdotukset pankkitoiminnan ja finanssimarkkinoiden infrastruktuurin osalta.

Finanssivalvonnasta annetussa laissa ehdotetaan säädettävän Finanssivalvonnan toimimisesta DORA-asetuksen tarkoittamana toimivaltaisena viranomaisena sekä NIS2-direktiivin ja CER-direktiivin tarkoittamana toimivaltaisena viranomaisena pankkitoiminnan ja rahoitusmarkkinoiden infrastruktuurin osalta. Finanssivalvonnan tehtäviä täydennettäisiin tehtävillä edistää finanssimarkkinoilla toimivien kyberturvallisia toimintatapoja sekä edistää finanssimarkkinoiden kriittisten toimijoiden häiriönsietokykyä. Finanssivalvonnan velvollisuudet toimia yhteistyössä muiden viranomaisten kanssa kyberturvallisuuden edistämiseksi ehdotetaan koottavan uuteen pykälään. Lisäksi lain hallinnollisia seuraamuksia koskevia säännöksiä ehdotetaan täydennettävän DORA-asetuksen johdosta ja laissa tarkoitettujen muiden finanssimarkkinoilla toimivien joukkoon lisättäisiin DORA-asetuksen soveltamisalaan kuuluva TVT-palveluntarjoajana oleva kolmas osapuoli.

Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annettua lakia ja valtion erityisrahoitusyhtiöstä annettua lakia muutettaisiin siten, että Teollisen yhteistyön rahasto Oy ja Finnvera Oyj jätettäisiin DORA-asetuksen soveltamisalan ulkopuolelle.

Muiden muutettaviksi ehdotettujen lakien osalta DORA-muutosdirektiivi edellyttää säädettävän vaatimuksista hallinnoida verkko- ja tietojärjestelmiä DORA-asetuksen mukaisesti sekä eräistä muista muutoksista.

Lait on tarkoitettu tulemaan voimaan 17.1.2025.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Euroopan parlamentti ja neuvosto antoivat 14.12.2022 asetuksen (EU) 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (jäljempänä *DORA-asetus*). Asetus on julkaistu Euroopan unionin virallisessa lehdessä 27.12.2022 ja se on tullut voimaan kahdentenakymmenentenä päivänä julkaisusta eli 16.1.2023. Asetusta sovelletaan 17.1.2025 alkaen. Jäsenvaltioiden on julkaistava asetuksen toimeenpanon edellyttämät kansallisten säännösten muutokset viimeistään 17.1.2025. Samassa Euroopan unionin virallisessa lehdessä julkaistiin Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2556 direktiivien 2009/65/EY, 2009/138/EY, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 ja (EU) 2016/2341 muuttamisesta finanssialan digitaalisen häiriönsietokyvyn osalta (jäljempänä *DORA-muutosdirektiivi*), joka tuli DORA-asetuksen tavoin voimaan kahdentenakymmenentenä päivänä julkaisusta, eli 16.1.2023. Jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät säännökset viimeistään 17.1.2025.

DORA-asetus ja DORA-muutosdirektiivi ovat osa Euroopan komission toimenpidepakettia, jolla pyritään edistämään ja tukemaan digitaalisen rahoituksen tarjoamia mahdollisuuksia innovoinnin ja kilpailun näkökulmasta, luomaan uusia vaihtoehtoja nykyisten rahoitus- ja maksupalveluiden ohelle, sekä lieventämään digitaaliseen rahoitukseen liittyviä riskejä. Pakettiin kuuluu uusi digitaalisen rahoituksen strategia, jonka tavoitteena on edistää EU:n rahoitusalan digitalisaation tasoa ja varmistaa eurooppalaisten kuluttajien ja yritysten hyötyminen digitaalisesta rahoituksesta.

Digitaalisen rahoituksen pakettiin kuuluvat DORA-asetuksen, DORA-muutosdirektiivin ja digitaalisen rahoituksen strategian ohella Euroopan kryptovarojen markkinoita koskeva asetus ja hajautetun tilikirjan teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmä.

DORA-asetuksen ja DORA-muutosdirektiivin lisäksi Euroopan parlamentti ja neuvosto antoivat 14.12.2022 direktiivin (EU) 2022/2555 toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (jäljempänä *NIS2-direktiivi*) sekä direktiivin (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta (jäljempänä *CER-direktiivi*). Koska finanssialan toimijoiden digitaalista häiriönsietokykyä säännellään kattavasti DORA-asetuksessa, NIS2- ja CER-direktiiveistä toimijoille aiheutuvia velvoitteita ei tule päällekkäisen sääntelyn ja tarpeettoman hallinnollisen rasituksen välttämiseksi soveltaa niihin finanssialan toimijoihin, jotka kuuluvat mainittujen direktiivien soveltamisalaan. Kyseiset toimijat on kuitenkin tärkeää huomioida näiden direktiivien mukaisissa kansallisissa strategioissa ja toimenpiteissä ja viranomaisten välisissä yhteistyörakenteissa, jotta voidaan varmistaa johdonmukaisuus muun muassa jäsenvaltioiden hyväksymien kyberturvallisuusstrategioiden kanssa sekä viranomaisten välinen tiedonkulku.

1.2 Valmistelu

EU-säädösten valmistelu

Komissio julkaisi 24.9.2020 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014 ja (EU) N:o 909/2014 muuttamisesta, sekä ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi direktiivien 2006/43/EY, 2009/65/EY, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 ja (EU) 216/2341 muuttamisesta. Samalla komissio julkaisi myös lainsäädäntöehdotukset Euroopan parlamentin ja neuvoston asetukseksi kryptovarojen markkinoinnista ja direktiivin (EU) 2019/1937 muuttamisesta (*MiCA*) ja Euroopan parlamentin ja neuvoston asetukseksi hajautetun tilikirjan teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmästä (*DLT-pilotti*). Lainsäädäntöehdotukset ovat osa komission digitaalisen rahoituksen pakettia (KOM(2020) 591 lopullinen).

Komission asetus- ja direktiiviehdotukset sekä luonnos valtioneuvoston kirjelmäksi eduskunnalle komission ehdotuksista olivat lausuntokierroksella EU-asioiden komitean alaisessa rahoituspalvelut ja pääomaliikkeet -jaostossa (jaosto EU-10) lokakuussa 2020. Komission ehdotuksista annettiin eduskunnalle U-kirjelmä U 58/2020 vp. Ehdotusten käsittely aloitettiin neuvoston rahoituspalvelutyöryhmässä 30.9.2020.

Valtioneuvosto suhtautui myönteisesti lainsäädäntöehdotuksiin ja yhtyi komission näkemykseen siitä, että palveluiden luotettavan toiminnan ja rahoitusmarkkinoiden vakauden turvaamiseksi on tärkeää vahvistaa rahoitusmarkkinoiden digitaalista häiriönsietokykyä. Asetuksen tavoitteet TVT-riskienhallintaan ja kyberturvallisuuteen liittyvien säännösten yhtenäistämisestä olivat tervetulleita, mutta sääntelykehystä vahvistettaessa tulisi ottaa huomioon kriittisten rahoitusmarkkinapalveluiden turvaamiseen liittyvät järjestelyt kansallisen turvallisuuden näkökulmasta.

Valtioneuvosto kannatti esitetyn suhteellisuusperiaatteen soveltamista, kunhan sen käyttö punnitaan tarkasti olemassa olevat riskit huomioon ottaen. Ehdotettua uutta ylätason valvontakehikkoa pidettiin hyväksyttävänä, mutta valtioneuvosto suhtautui varauksella kehikkoa koskevaan hallintorakenteeseen. Valtioneuvosto huomautti, että rakenteessa tulisi huomioida selkeät toimivaltuudet ja vastuualueet kansallisten ja Euroopan viranomaisten kesken.

Viranomaisten keskinäinen tiedonkulku ja häiriöraportointi tulisi toteuttaa tarkoituksenmukaisella tavalla, mihin tulee valtioneuvoston mukaan kiinnittää huomiota ehdotuksen jatkokäsittelyssä. Valtioneuvosto korostaa muun ohella, että unionin toiminnassa on tärkeää systeemisen kokonaisturvallisuusajattelun mukaisten toimintamallien kehittäminen.

Eduskunnan talousvaliokunta yhtyi asiassa valtioneuvoston kantaan korostaen eräitä näkökohtia (TaVL 26/2020 vp). Suhteellisuusperiaatteen osalta talousvaliokunta huomautti, että olennaista on arvioida nimenomaan toimijan vaikutusta markkinaan, eikä yksinomaan sen kokoa, sillä laajavaikutteinen ongelma voi lähteä liikkeelle myös pienen toimijan riskienhallinnan laiminlyönnistä. Lisäksi talousvaliokunta huomautti, että pitkälle harmonisoidun finanssialan Euroopan tasoisen sääntelyn kosketuspinta kansallisen turvallisuuden varmistamiseen tähtäävään sääntelyyn on kriittinen kohta lainsäädännön tavoitteiden toteutumisen kannalta.

Hallituksen esityksen valmistelu

Hallituksen esitys on valmisteltu valtiovarainministeriössä virkatyönä. Työhön on osallistunut myös sosiaali- ja terveysministeriö. Esitysluonnos lähetettiin julkiselle lausuntokierrokselle [xx.xx.xxxx]. Lausuntopalautteesta ja sen huomioon ottamisesta hallituksen esityksessä kerrotaan jaksossa 5.

Hallituksen esityksen valmisteluasiakirjat ovat saatavilla julkisessa palvelussa osoitteessa valtioneuvosto.fi/hankkeet tunnuksella VM067:00/2023.

2 EU-säädöksen tavoitteet ja pääasiallinen sisältö

Yleiset säännökset

DORA-asetuksen I lukuun sisältyvät yleiset säännökset sen kohteesta, soveltamisalasta, määritelmistä ja suhteellisuusperiaatteesta.

Asetuksessa vahvistetaan yhteisen digitaalisen häiriönsietokyvyn korkean tason saavuttamiseksi yhdenmukaiset vaatimukset, jotka koskevat finanssiyhteisöjen liiketoimintaprosesseja tukevien verkko- ja tietojärjestelmien turvallisuutta. Asetuksen 2 artiklassa säädetään asetuksen soveltamisalasta. Soveltamisen piiriin kuuluvat 2 artiklan 1 kohdan a–t alakohdissa tarkemmin määritetyt toimijat, joista käytetään yhteisnimitystä finanssiyhteisöt, sekä TVT-palveluntarjoajana olevat kolmannet osapuolet. Asetusta ei sovelleta direktiivin 2011/61/EU 3 artiklan 2 kohdassa tarkoitettuihin vaihtoehtoisten sijoitusrahastojen hoitajiin, direktiivin 2009/138/EY 4 artiklassa tarkoitettuihin vakuutus- ja jälleenvakuutusyrityksiin, ammatillisia lisäeläkkeitä tarjoaviin laitoksiin, jotka hallinnoivat eläkejärjestelmiä, joissa on yhteensä enintään 15 jäsentä, luonnollisiin tai oikeushenkilöihin, joihin sovelletaan poikkeusta direktiivin 2014/65/EU 2 ja 3 artiklan nojalla, vakuutus- ja jälleenvakuutusedustajiin ja sivutoimisiin vakuutusedustajiin, jotka ovat mikroyrityksiä taikka pieniä tai keskisuuria yrityksiä, eikä direktiivin 2013/36/EU 2 artiklan 5 kohdan 3 alakohdassa tarkoitettuihin postisiirtoa hoitaviin laitoksiin. Soveltamisalan ulkopuolelle voidaan jäsenvaltioiden toimesta jättää direktiivin 2013/36/EU 2 artiklan 5 kohdan 4–23 alakohdassa tarkoitetut yhteisöt, jotka sijaitsevat niiden alueella. Suomen osalta asetusta voidaan siis päättää olla soveltamatta Teollisen yhteistyön rahasto Oy:hyn ja Finnvera Oyj:hin.

Digitaalisella häiriönsietokyvyllä tarkoitetaan asetuksessa finanssiyhteisön kykyä luoda ja turvata toimintavarmuutensa ja luotettavuutensa ja tarkastella sitä uudelleen varmistamalla joko suoraan tai epäsuorasti TVT-palveluntarjoajana olevien kolmansien osapuolten tarjoamia palveluja käyttäen kaikki TVT-valmiudet, jotka tarvitaan finanssiyhteisön käyttämien verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi ja jotka tukevat finanssipalvelujen tarjonnan jatkumista ja niiden laatua myös häiriöiden aikana. TVT-riski määritellään asetuksessa tarkoittamaan mitä tahansa kohtuudella tunnistettavissa olevaa verkko- ja tietojärjestelmien käyttöön liittyvää olosuhdetta, joka toteutuessaan voi vaarantaa verkko- ja tietojärjestelmien, minkä tahansa teknologiasta riippuvaisen välineen tai prosessin, toimintojen ja prosessien tai palvelujen tarjoamisen turvallisuuden aiheuttamalla kielteisiä vaikutuksia digitaalisessa tai fyysisessä ympäristössä. Verkko- ja tietojärjestelmän ja niiden turvallisuuden määritelmien osalta asetuksessa viitataan NIS2-direktiivin asianomaisiin määritelmiin. Kyberuhalla tarkoitetaan asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä ’kyberuhkaa’, tarkoittaen potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.

Asetuksen 4 artiklassa säädetään suhteellisuusperiaatteesta. Artiklan mukaan asetuksen velvoitteita on sovellettava suhteellisuusperiaatteen mukaisesti niin, että ne ovat oikeassa suhteessa yhteisöjen kokoon ja yleiseen riskiprofiiliin, sekä niiden palvelujen, toiminnan ja toimintojen luonteeseen, laajuuteen ja monitahoisuuteen nähden. Artiklassa vaaditaan myös, että toimivaltaiset viranomaiset ottavat tarkastelussaan huomioon sen, miten suhteellisuusperiaatetta sovelletaan kunkin finanssiyhteisön toimesta.

TVT-riskin hallinta

Asetuksen II luku sisältää TVT-riskin hallintaa koskevat säännökset. Asetuksen 5 artiklan mukaan finanssiyhteisöillä tulee olla sisäinen hallinto- ja valvontakehys, jolla varmistetaan TVT-riskin tehokas ja järkevä hallinnointi digitaalisen häiriönsietokyvyn korkean tason ylläpitämiseksi. Yhteisön ylimmän hallintoelimen on huolehdittava riskinhallintajärjestelmän järjestelyistä ja valvonnasta ja vastattava niistä.

Tarkemmat TVT-riskin hallintaa koskevat sisällölliset säännökset sisältyvät asetuksen II luvun II jaksoon. Asetuksen 6 artiklassa säädetään, että finanssiyhteisöillä on oltava osana yleistä riskinhallintajärjestelmäänsä vankka, kattava ja hyvin dokumentoitu TVT-riskinhallintajärjestelmä. Artiklassa säädetään TVT-riskinhallintajärjestelmän sisältövaatimuksista, ajantasaisesta tiedonjaosta viranomaisille, valvonnan siirtämisestä erilliselle valvontatoimelle, järjestelmän dokumentoinnista ja uudelleentarkastelusta, sekä sen ottamisesta sisäisen tarkastuksen ja seurantaprosessin piiriin. TVT-riskinhallintajärjestelmän on sisällettävä digitaalisen häiriönsietokyvyn strategia ja jossa on oltava mukana erityiset artiklassa tarkemmin eritellyt keinot, joilla pyrkiä TVT-tavoitteisiin.

Asetuksen 7 artiklassa säädetään finanssiyhteisöille asetetusta vaatimuksesta ylläpitää sellaisia TVT-järjestelmiä, -protokollia ja -välineitä, jotka ovat tarkoituksenmukaisia, luotettavia, omaavat riittävän kapasiteetin ja ovat teknisesti kestäviä suuren tietomäärän käsittelyyn tarvittaessa. Osana TVT-riskin hallintaa finanssiyhteisöjen on 8 artiklan mukaan yksilöitävä, luokiteltava ja dokumentoitava kaikki TVT:n tukemat liiketoiminnot, tehtävät ja vastuut, kyseisiä toimintoja tukevat tieto-omaisuus ja TVT-omaisuus sekä tehtävänsä ja riippuvuutensa suhteessa TVT-riskiin. Yksilöintivaatimus ulottuu myös TVT-riskin lähteisiin, tieto- ja TVT-omaisuuteen, verkkoresursseihin ja laitteistoihin, sekä TVT-palveluntarjoajina toimivista kolmansista osapuolista riippuviin prosesseihin ja niihin liittyviin kytkentöihin.

Asetuksen 9 artiklan mukaan finanssiyhteisöjen on jatkuvasti seurattava ja valvottava TVT-järjestelmien toimintaa ja minimoitava niihin liittyvien riskien vaikutus järjestelmien toimintakykyyn. Finanssiyhteisöillä on oltava sellaiset TVT-turvallisuutta koskevat menettelyt ja välineet, joilla pystytään varmistamaan järjestelmien korkeatasoinen häiriönsietokyky, jatkuvuus ja käytettävyys. Finanssiyhteisöllä on oltava käytössään mekanismit, joiden avulla pystytään nopeasti havaitsemaan TVT-liitännäiset poikkeamat ja niissä on oltava määritettynä tietyt hälytystasot ja -kriteerit TVT-poikkeamiin liittyvien menettelyjen käynnistämiseksi. Finanssiyhteisöjen on asetuksen 11 artiklan mukaisesti otettava käyttöön toimintaperiaatteet, joilla voidaan varmistaa niiden kriittisten tai tärkeiden toimintojen jatkuvuus, sekä TVT-poikkeamiin reagointi ja niistä toipuminen. Finanssiyhteisöillä on oltava asianmukaiset TVT-liiketoiminnan jatkuvuutta koskevat suunnitelmat sekä TVT-reagointi- ja palautumissuunnitelmat, joita on testattava vuosittain. Tätä varten finanssiyhteisöjen on myös perustettava varmuuskopiointi- ja palautusmenettelyt ja -järjestelmät.

Asetuksen 13 artiklan mukaan TVT-riskienhallintajärjestelmää on jatkuvasti tarkasteltava ja laajavaikutteisten TVT-poikkeamien jälkeen on järjestettävä jälkitarkastelu, jossa analysoidaan poikkeaman syytä ja määritetään se, miten poikkeamiin reagoimista ja TVT-riskienhallintajärjestelmää voidaan kehittää. Finanssiyhteisöjen on 14 artiklan mukaan myös toteutettava kriisiviestintäsuunnitelmia, joilla mahdollistetaan tehokas viestintä asiakkaille, vastapuolille ja suurelle yleisölle.

Euroopan valvontaviranomaiset laativat asetuksen 15 artiklan mukaan TVT-riskinhallintavälineiden, -menetelmien, -menettelyjen ja -politiikkatoimien yhdenmukaistamiseksi teknisten

sääntelystandardien luonnoksia artiklassa luetelluista asioista. Komissiolle siirretään valta täydentää asetusta hyväksymällä mainitut tekniset sääntelystandardit. Asetuksen 16 artiklassa säädetään yksinkertaistettua TVT-riskinhallintajärjestelmää koskevista vaatimuksista tietyille finanssiyhteisöille.

TVT:hen liittyvien poikkeamien hallinta, luokittelu ja raportointi

Asetuksen III luvussa säädetään finanssiyhteisöjen velvoitteesta TVT-poikkeamien hallintaan, luokitteluun ja raportointiin. Yhteisöjen on 17 artiklan mukaan määriteltävä, laadittava ja toteutettava hallintaprosessi, jonka avulla voidaan havaita ja hallinnoida TVT-poikkeamia ja ilmoittaa niistä eteenpäin. Kaikki TVT:hen liittyvät poikkeamat ja merkittävät kyberuhat tulee kirjata. Finanssiyhteisöjen tulee myös luokitella TVT-poikkeamat ja määritellä niiden vaikutukset 18 artiklan 1 kohdan a–f alakohdissa tarkemmin määritellyillä kriteereillä. Näihin kriteereihin kuuluvat muun muassa poikkeaman kesto, vaikutusalueen maantieteellinen laajuus sekä vaikutusten kohteena olevien palvelujen kriittisyys.

Finanssiyhteisöillä on 19 artiklan mukaan velvollisuus raportoida laajavaikutteisista TVT-poikkeamista asetuksessa tarkoitetulle asianomaiselle toimivaltaiselle viranomaiselle. Lisäksi finanssiyhteisöillä on asetuksen mukaan vapaaehtoinen mahdollisuus ilmoittaa merkittävistä kyberuhista asianomaiselle viranomaiselle. Riippuen siitä onko kyse finanssiyhteisön velvollisuudesta vai vapaaehtoisuudesta, on tiedon vastaanottavan asianomaisen viranomaisen toimitettava tai se voi toimittaa tiedon eteenpäin muille viranomaisille. Euroopan valvontaviranomaiset laativat teknisten sääntelystandardien luonnoksia muun muassa TVT-poikkeamien olennaisuusrajojen sekä raportoinnin sisällön osalta ja komissiolle siirretään valta täydentää asetusta hyväksymällä mainitut tekniset sääntelystandardit.

Digitaalisen häiriönsietokyvyn testaus

Asetuksen IV lukuun sisältyvät säännökset digitaalisen häiriönsietokyvyn testauksesta. Finanssiyhteisöjen on otettava käyttöönsä kattava digitaalisen häiriönsietokyvyn testausohjelma, jota toteutetaan riskiperusteista lähestymistapaa noudattaen. Asetuksen 26 artiklan mukaan erikseen yksilöityjen finanssiyhteisöjen on suoritettava vähintään kolmen vuoden välein kehittynyt testaus uhkaperusteisen tunkeutumistestauksen avulla, kattaen finanssiyhteisön useat tai kaikki kriittiset tai tärkeät toiminnot. Lisäksi säädetään uhkaperusteisen tunkeutumistestauksen suorittamiseen käytettäviä testaajia koskevat vaatimukset.

Kolmansiin osapuoliin liittyvän TVT-riskin hallinta

Asetuksen V luvussa säädetään kolmansiin osapuoliin liittyvän TVT-riskin hallinnasta. Luvun I jaksossa säädetään kolmansiin osapuoliin liittyvän TVT-riskin moitteetonta hallintaa koskevista keskeisistä periaatteista. Finanssiyhteisöjen on hallinnoitava kolmansiin osapuoliin liittyvää TVT-riskiä 28 artiklassa mainittujen yleisten periaatteiden mukaisesti ja hyväksyttävä kolmansiin osapuoliin liittyvää TVT-riskiä koskeva strategia. Artikla sisältää lisäksi TVT-palvelujen käyttöä koskevan sopimusjärjestelyn toteuttamista koskevia vaatimuksia. Kriittisiä tai tärkeitä toimintoja tukevien TVT-palvelujen käyttöä koskevista suunnitelluista sopimusjärjestelyistä on ilmoitettava etukäteen toimivaltaiselle viranomaiselle. Kriittisiä tai tärkeitä toimintoja tukevien TVT-palvelujen osalta finanssiyhteisöjen on otettava käyttöön irtautumisstrategiat. Asetuksen 29 artiklan mukaan finanssiyhteisöjen on 28 artiklan 4 kohdan c alakohdassa tarkoitettua riskien määritystä ja arviointia suorittaessaan myös otettava huomioon ne riskit, joita TVT-palveluiden keskittyneestä hankkimisesta samalta tai keskenään läheisesti liitoksisissa

olevilta palveluntarjoajilta saattaa syntyä. Tähän liittyen finanssiyhteisöjen on punnittava erilaisia vaihtoehtoja liittyen esimerkiksi siihen, tulisiko TVT-palveluja hankkia useammalta eri palveluntarjoajalta keskittymäriskin minimoimiseksi. Asetuksen 30 artikla sisältää keskeiset sopimusmääräykset finanssiyhteisön ja TVT-palveluita tarjoavan kolmannen osapuolen keskinäistä sopimusta varten.

Luvun II jaksossa säädetään kriittisten TVT-palveluntarjoajina olevien kolmansien osapuolten valvontakehyksestä. Asetuksessa velvoitetaan, että Euroopan valvontaviranomaiset nimeävät finanssiyhteisöjen kannalta kriittiset TVT-palveluntarjoajina olevat kolmannet osapuolet ja nimittävät kullekin kriittiselle kolmannelle osapuolelle päävalvojaksi Euroopan valvontaviranomaisen. Euroopan valvontaviranomaiset ovat Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 1093/2010 perustettu Euroopan pankkiviranomainen (EPV), Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 1094/2010 perustettu Euroopan vakuutus- ja lisäeläkeviranomainen (EIOPA) ja asetuksella (EU) N:o 1095/2010 perustettu Euroopan arvopaperimarkkinaviranomainen (ESMA). Nimeäminen perustuu muun muassa niiden finanssiyhteisöjen systeemiseen merkitykseen, jotka tukeutuvat asianomaisen TVT-palveluntarjoajana olevan kolmannen osapuolen palveluihin. Kriittisten palveluntarjoajien nimeämistä ei sovelleta sellaisiin TVT-palveluita tarjoaviin kolmansiin osapuoliin, jotka tarjoavat palvelujaan yksinomaan yhdessä jäsenvaltiossa ja vain kyseisessä valtiossa toimiville finanssiyhteisöille. Valvontakehyksen rakenteesta säädetään 32 artiklassa. Yhteiskomitean on perustettava alakomiteakseen valvontafoorumi, jonka tehtävänä on tukea kriittisten TVT-palveluita tarjoavien kolmansien osapuolien päävalvojana toimivan valvontaviranomaisen työtä. Valvontafoorumi koostuu 32 artiklan 4 kohdan a-e alakohdissa määritellyistä toimijoista. Jäsenvaltioiden osalta valvontafoorumiin on osallistuttava yksi korkean tason edustaja asetuksen 46 artiklassa tarkoitetusta kunkin jäsenvaltion asianomaisen toimivaltaisen viranomaisen kulloisestakin henkilöstöstä ja tarvittaessa yksi 46 artiklassa tarkoitetun toimivaltaisen viranomaisen lisäedustaja kustakin jäsenvaltiosta tarkkailijana. Jäsenvaltioiden on nimettävä ja ilmoitettava päävalvojalle se viranomainen, jonka henkilöstön jäsen on edellä tarkoitettu korkean tason edustaja.

Asetuksen 31 artiklan mukaisesti nimitetty päävalvoja valvoo nimettyjä kriittisiä TVT-palveluntarjoajana olevia kolmansia osapuolia 33 artiklassa säädettyjen tehtävien mukaisesti. Päävalvoja arvioi, onko kullakin kriittisellä TVT-palveluntarjoajana olevalla kolmannella osapuolella kattavat, luotettavat ja toimivat säännöt, menettelyt, mekanismit ja järjestelyt, joilla hallita TVT-riskiä, jonka se voi finanssiyhteisöille aiheuttaa. Valvontaa koordinoidaan 34 artiklan nojalla perustettavan yhteisen valvontaverkoston puitteissa. Asetuksen 35 artiklassa on säädetty päävalvojan valtuuksista sille säädettyjen tehtävien hoitamiseksi. Päävalvojalla on valtuudet muun muassa pyytää kaikkia asiaankuuluvia tietoja ja asiakirjoja 37 artiklan mukaisesti sekä suorittaa 38 artiklan mukaisia yleisiä tutkimuksia ja 39 artiklan mukaisia tarkastuksia. Yhtenä päävalvojan valtuutena on uhkasakon määrääminen TVT-palveluita tarjoavalle kolmannelle osapuolelle, mikäli tämä ei noudata sille toteutettavaksi vaadittuja toimenpiteitä. Uhkasakko on artiklan 9 kohdan mukaisesti hallinnollinen ja täytäntöönpanokelpoinen. Sen täytäntöönpanoon sovelletaan sen jäsenvaltion säännöksiä, jonka alueella kolmanteen osapuoleen kohdistuvat tutkimukset ja tilojen tarkastaminen tapahtuu. Asianomaisen jäsenvaltion tuomioistuimet ovat toimivaltaisia tutkimaan virheellistä täytäntöönpanoa koskevat valitukset.

Asetuksen 36 artiklassa säädetään päävalvojan valtuuksista tilanteissa, joissa niiden käyttö kohdistuu kolmansissa maissa sijaitseviin, kriittisen TVT-palveluita unionin finanssiyhtiöille tarjoavan, kolmannen osapuolen omistuksessa tai käytössä oleviin tiloihin, jotka ovat yhteydessä sen liiketoimintaan, toimintoihin tai palveluihin. Valtuuksista on säädetty 35 artiklan 1 kohdan a–b alakohdissa, 38 artiklan 2 kohdan a, b ja d alakohdissa, sekä 39 artiklan 1 kohdassa ja 2 kohdan a alakohdassa. Jotta kyseisiä säännöksiä voidaan soveltaa, on EPV:n, ESMAn tai

EIOPAn sovittava kolmannen maan asiaankuuluvien viranomaisten kanssa hallinnollisista yhteistyöjärjestelyistä, jotta päävalvoja voi käyttää valtuuksiaan sujuvasti yhteistyössä kyseiseen kolmanteen maahan nimetyn ryhmän kanssa. Edellä mainittu ei kuitenkaan saa 36 artiklan mukaan rajoittaa unionin toimielinten tai jäsenvaltioiden toimivaltaa, eikä siitä saa seurata oikeudellisia velvoitteita unionille tai jäsenvaltioille. Toiminta ei myöskään saa estää jäsenvaltioita ja niiden toimivaltaisia viranomaisia tekemästä kahden- tai monenvälisiä järjestelyjä kolmansien maiden ja näiden asiaankuuluvien viranomaisten kanssa.

Asetuksen 40 artiklan mukaan päävalvojan avustajana valvontatoimien suorittamisessa on kutakin kriittistä TVT-palveluntarjoajana toimivaa kolmatta osapuolta varten perustettu tutkintaryhmä. Ryhmän kokoonpanosta on säädetty tarkemmin 40 artiklan 2 kohdan a–d alakohdissa. Jäsenvaltioiden osalta tutkintaryhmään kuuluvat kriittisen TVT-palveluntarjoajana olevan kolmannen osapuolen TVT-palveluja käyttäviä finanssiyhteisöjä valvovat asianomaiset toimivaltaiset viranomaiset sekä yksi vapaaehtoispohjalta osallistuva toimivaltainen kansallinen viranomainen samasta jäsenvaltiosta, johon kyseinen kriittinen TVT-palveluntarjoaja on sijoittautunut. Kriittisten TVT-palveluntarjoajana olevien kolmansien osapuolten on 60 kalenteripäivän kuluessa siitä, kun ne ovat vastaanottaneet 35 artiklan 1 kohdan d alakohdan nojalla annetut päävalvojan suositukset, joko ilmoitettava päävalvojalle aikovansa noudattaa suosituksia tai annettava perusteltu selitys tällaisten suositusten noudattamatta jättämiselle. Asetuksen 42 artiklassa säädetään toimivaltaisten viranomaisten jatkotoimenpiteistä näissä tilanteissa. Viimesijaisena toimenpiteenä toimivaltaiset viranomaiset voivat tehdä päätöksen, jonka mukaan finanssiyhteisöjä vaaditaan tilapäisesti joko osittain tai kokonaan keskeyttämään kriittisen TVT-palveluntarjoajana olevan kolmannen osapuolen tarjoaman palvelun käyttö tai käyttöönotto, tai vaaditaan finanssiyhteisöjä kokonaan tai osittain irtisanomaan kriittisten TVT-palveluntarjoajana olevien kolmansien osapuolten kanssa tehdyt sopimusjärjestelyt.

Tietojenvaihtojärjestelyt

Finanssiyhteisöille on säädetty asetuksessa mahdollisuus vaihtaa keskenään kyberuhkia koskevia tietoja ja tiedustelutietoja, kunhan kyseisten tietojen vaihto täyttää DORA:n 45 artiklan 1 kohdan a–c alakohdissa mainitut kriteerit. Tietojenvaihtojärjestelyissä on määriteltävä osallistumisedellytykset ja vahvistettava säännöt viranomaisten osallistumisesta ja osallistumisen ominaisuudesta, TVT-palveluntarjoajana toimivien kolmansien osapuolien osallistumisesta, sekä operatiivisista elementeistä. Finanssiyhteisöjen on myös ilmoitettava toimivaltaisille viranomaisille osallistumisestaan tietojenvaihtojärjestelyihin.

Toimivaltaiset viranomaiset

Asetuksen VII luvussa säädetään toimivaltaisista viranomaisista, joiden on 46 artiklan mukaisesti varmistettava asetuksessa säädettyjen velvoitteiden noudattaminen asiaa koskevissa säädöksissä annettujen valtuuksien mukaisesti.

Euroopan valvontaviranomaiset ja toimivaltaiset viranomaiset voivat osallistua NIS2-direktiivin 14 artiklalla perustetun yhteistyöryhmän toimintaan asioissa, jotka koskevat niiden valvontatoimia finanssilaitosten osalta. Toimivaltaiset viranomaiset voivat tarvittaessa kuulla NIS2-direktiivin mukaisesti nimettyjä tai perustettuja keskitettyjä yhteyspisteitä ja CSIRT-yksiköitä sekä vaihtaa tietoja niiden kanssa. Toimivaltaiset viranomaiset voivat muutoinkin sopia yhteistyöjärjestelyistä mainitun direktiivin mukaisten viranomaisten kanssa ja niiden on tehtävä läheistä yhteistyötä keskenään ja tarvittaessa päävalvojan kanssa.

Asetuksen 50 artiklassa säädetään sääntelyn noudattamisen varmistamiseksi tarpeellisista hallinnollisista seuraamuksista ja korjaavista toimenpiteistä, mikä edellyttää jäsenvaltioilta täydentävää kansallista sääntelyä. Lähtökohtana on, että toimivaltaisilla viranomaisilla on oltava kaikki asetuksen mukaisten tehtäviensä hoitamiseen tarvittavat valtuudet valvoa, tutkia ja määrätä seuraamuksia. Tässä tarkoituksessa jäsenvaltioiden on vahvistettava säännöt, jotka koskevat asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, ja varmistettava niiden tehokas täytäntöönpano, sanotun kuitenkaan rajoittamatta jäsenvaltioiden oikeutta päättää siitä, että ne eivät säädä hallinnollisia seuraamuksia tai korjaavia toimenpiteitä koskevia sääntöjä sellaisten rikkomisten osalta, joihin sovelletaan niiden kansallisen lainsäädännön mukaisia rikosoikeudellisia seuraamuksia. Jäsenvaltioiden on myös annettava toimivaltaisille viranomaisille valtuudet soveltaa ainakin sellaisia seuraamuksia, jotka on määritelty tarkemmin 50 artiklan 4 kohdan a–e alakohdissa, sekä toimivalta soveltaa hallinnollisia seuraamuksia ja korjaavia toimenpiteitä ylimmän hallintoelimen jäseniin ja muihin, jotka ovat kansallisen lainsäädännön mukaan vastuussa rikkomisesta. Kaikki päätökset näiden seuraamusten ja toimenpiteiden määräämiseksi on perusteltava asianmukaisesti ja niihin on voitava hakea muutosta. Toimivaltaiset viranomaiset käyttävät valtuuksiaan määrätä 50 artiklassa tarkoitettuja hallinnollisia seuraamuksia ja korjaavia toimenpiteitä kansallisen oikeudellisen kehyksensä mukaisesti.

Jäsenvaltioiden on ilmoitettava viimeistään 17.1.2025 komissiolle, ESMAlle, EPV:lle ja EIOPAlle asetuksen VII luvun täytäntöönpanoa koskevat lakinsa, asetuksensa ja hallinnolliset määräyksensä, mukaan lukien asiaa koskevat rikosoikeudelliset säännökset, sekä ilman aiheetonta viivästystä ilmoitettava komissiolle, ESMAlle, EPV:lle ja EIOPAlle myöhemmistä muutoksista kyseisiin säännöksiin.

Asetuksen suhde NIS2- ja CER-direktiiveihin

NIS2-direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso kaikkialla unionissa sisämarkkinoiden toiminnan parantamiseksi. Tätä varten direktiivissä vahvistetaan jäsenvaltioiden velvoitteet hyväksyä kansalliset kyberturvallisuusstrategiat sekä nimetä tai perustaa toimivaltaiset viranomaiset, kyberkriisinhallintaviranomaiset, kyberturvallisuusalan keskitetyt yhteyspisteet ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt); kyberturvallisuusriskien hallintatoimenpiteet ja raportointivelvoitteet direktiivin liitteessä I tai II tarkoitettua toimijatyyppiä oleville toimijoille ja CER-direktiivissä kriittisiksi toimijoiksi määritetyille toimijoille; kyberturvallisuustietojen jakamista koskevat säännöt ja velvoitteet sekä jäsenvaltioiden valvonta- ja täytäntöönpanovelvoitteet. NIS2-direktiivin sisältöä on kuvattu yksityiskohtaisemmin *[direktiivin kansallista täytäntöönpanoa koskevassa hallituksen esityksessä, täydennetään myöhemmin]*.

NIS2-direktiivin mukaisiin erittäin kriittisiin toimialoihin kuuluvat pankkitoiminta ja finanssimarkkinoiden infrastruktuurit ja niiden osalta direktiivin 2 artiklan mukaisin edellytyksin kolme finanssiyhteisön tyyppiä: luottolaitokset, kauppapaikkojen ylläpitäjät ja keskusvastapuolet. DORA-asetus on eritysasäädös (*lex specialis*) suhteessa NIS2-direktiiviin. Sen vuoksi jäsenvaltioiden ei pitäisi soveltaa NIS2-direktiivin säännöksiä, jotka koskevat kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa, DORA-asetuksen soveltamisalaan kuuluviin finanssialan toimijoihin. Asetuksen johdanto-osan 16 kappaleessa todetaan, että samalla on tärkeää säilyttää vahva yhteys finanssialan ja unionin horisontaalisen kyberturvallisuuskehyksen välillä, jotta voidaan varmistaa johdonmukaisuus jäsenvaltioiden hyväksymien kyberturvallisuusstrategioiden kanssa ja saattaa finanssivalvojien tietoon kyberturvallisuuspoikkeamat, jotka vaikuttavat kyseisen direktiivin piiriin kuuluviin muihin aloihin.

Asetuksen johdanto-osan 18 kappaleen mukaan, jotta voitaisiin mahdollistaa monialainen oppiminen ja hyödyntää tehokkaasti muilta aloilta saatuja kokemuksia kyberuhkiin vastaamisesta, NIS2-direktiivissä tarkoitettujen finanssiyhteisöjen olisi pysyttävä osana kyseisen direktiivin ”ekosysteemiä” (esimerkiksi verkko- ja tietoturva-alan yhteistyöryhmä ja tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt eli CSIRT-yksiköt). Euroopan valvontaviranomaisten ja kansallisten toimivaltaisten viranomaisten olisi voitava osallistua kyseisen direktiivin mukaisiin strategisiin toimintapoliittisiin keskusteluihin sekä verkko- ja tietoturva-alan yhteistyöryhmän tekniseen työhön ja vaihtaa tietoja ja tehdä edelleen yhteistyötä kyseisen direktiivin mukaisesti nimettyjen tai perustettujen keskitettyjen yhteyspisteiden kanssa. NIS2-direktiivin johdanto-osan 28 kappaleessa todetaan lisäksi, että DORA-asetuksen mukaisten toimivaltaisten viranomaisten olisi myös toimitettava tiedot laajavaikutteisista TVT:hen liittyvistä poikkeamista ja tapauksen mukaan merkittävistä kyberuhkista tämän direktiivin mukaisille CSIRT-yksiköille, toimivaltaisille viranomaisille tai keskitetyille yhteyspisteille. Tämä voidaan toteuttaa tarjoamalla välitön pääsy poikkeamailmoituksiin ja toimittamalla ne eteenpäin joko suoraan tai poikkeamailmoituksia käsittelevän keskitetyn asiointipisteen kautta. Lisäksi jäsenvaltioiden olisi edelleen sisällytettävä finanssiala kyberturvallisuusstrategioihinsa, ja CSIRT-yksiköt voivat kattaa finanssialan toiminnassaan. Komission tiedonannossa NIS2-direktiivin 4 artiklan 1 ja 2 kohdan soveltamisesta (2023/C 328/02) todetaan lisäksi, että NIS2-direktiivin kansallisia kriisinhallintakehyksiä koskevaa 9 artiklaa ja Euroopan kyberkriisien yhteysorganisaatioiden verkosto EU-CyCLONe:a koskevaa 16 artiklaa olisi sovellettava kokonaisuudessaan toimialoihin alakohtaisten unionin säädösten olemassaolosta huolimatta.

CER-direktiivillä säädetään jäsenvaltioiden velvoitteista toteuttaa eritvisiä toimenpiteitä, joilla varmistetaan Euroopan unionin toiminnasta tehdyn sopimuksen 114 artiklan soveltamisalaan kuuluvien välttämättömien yhteiskunnan toimintojen tai taloudellisen toiminnan ylläpitämisen kannalta keskeisten palvelujen häiriötön tarjonta sisämarkkinoilla, ja erityisesti määrittää kriittiset toimijat sekä antaa niille tukea niiden velvoitteiden täyttämiseksi; säädetään kriittisten toimijoiden velvoitteista, joiden tarkoituksena on parantaa niiden häiriönsietokykyä ja kykyä tarjota palveluja sisämarkkinoilla; vahvistetaan säännöt, jotka koskevat kriittisten toimijoiden valvontaa, täytäntöönpanon valvontaa; Euroopan kannalta erityisen merkittävien kriittisten toimijoiden määrittämistä ja näille toteutettavia neuvontaoperaatioita, jotta arvioidaan toimenpiteitä, joita kyseiset toimijat ovat toteuttaneet täyttääkseen III luvun mukaiset velvoitteensa; vahvistetaan yhteiset yhteistyö- ja raportointimenettelyt tämän direktiivin soveltamiseksi sekä säädetään toimenpiteistä kriittisten toimijoiden korkeatasoisen häiriönsietokyvyn saavuttamiseksi, jotta keskeisten palvelujen tarjonta unionissa voidaan turvata ja parantaa sisämarkkinoiden toimintaa. CER-direktiivin sisältöä on kuvattu yksityiskohtaisemmin *[direktiivin kansallista täytäntöönpanoa koskevassa hallituksen esityksessä, täydennetään myöhemmin]*.

CER-direktiivin mukaisiin toimialoihin kuuluvat pankkiala ja rahoitusmarkkinoiden infrastruktuuri ja niiden osalta direktiivin 6 artiklan mukaisesti kriittisiksi määritetyt toimijat kolmesta finanssiyhteisön tyypistä: luottolaitokset, kauppapaikkojen ylläpitäjät ja keskusvastapuolet. CER-direktiivin johdanto-osan 21 kappaleessa todetaan, että koska finanssialan toimijoiden häiriönsietokyky on finanssipalveluja koskevassa unionin lainsäädännössä katettu laajasti, CER-direktiivin 11 artiklaa sekä III, IV ja VI lukua ei olisi sovellettava kyseisiin toimijoihin, jotta voidaan välttää päällekkäisyydet ja tarpeeton hallinnollinen rasitus. Kun otetaan huomioon finanssitoimialan toimijoiden tarjoamien palvelujen merkitys kaikkiin muihin toimialoihin kuuluville kriittisille toimijoille, jäsenvaltioiden olisi kuitenkin määritettävä direktiivissä säädettyjen perusteiden mukaan ja direktiivin mukaista menettelyä noudattaen finanssitoimialan toimijat kriittisiksi toimijoiksi. Direktiivin II luvussa säädettyjä strategioita, jäsenvaltioiden riskinarviointia ja tukitoimenpiteitä olisi näin ollen sovellettava. Jäsenvaltioiden olisi voitava hyväksyä

tai pitää voimassa kansallisen lainsäädännön säännöksiä saavuttaakseen korkeamman häiriönsietokyvyn tason kyseisten kriittisten toimijoiden osalta edellyttäen, että kyseiset säännökset ovat sovellettavan unionin oikeuden mukaisia.

DORA-muutosdirektiivi

DORA-muutosdirektiivissä säädetään muutoksista useisiin finanssiyhteisöjä koskeviin Euroopan parlamentin ja neuvoston direktiiveihin, jotka sisältävät sääntelyä finanssialan TVT-riskin hallintaan liittyvistä vaatimuksista. Näihin lukeutuvat direktiivi 2009/65/EY siirtokelpoisiin arvopapereihin kohdistuvaa yhteistä sijoitustoimintaa harjoittavia yrityksiä (yhteissijoitusyritykset) koskevien lakien, asetusten ja hallinnollisten määräysten yhteensovittamisesta (jäljempänä *sijoitusrahastodirektiivi*), direktiivi 2009/138/EY vakuutus- ja jälleenvakuutustoiminnan aloittamisesta ja harjoittamisesta (jäljempänä *Solvenssi II -direktiivi*), direktiivi 2011/61/EU vaihtoehtoisten sijoitusrahastojen hoitajista ja direktiivin 2003/41/EY ja 2009/65/EY sekä asetuksen (EY) N:o 1060/2009 ja (EU) N:o 1095/2010 muuttamisesta (jäljempänä *AIFM-direktiivi*), direktiivi 2013/36/EU oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta (jäljempänä *luottolaitosdirektiivi*), direktiivi 2014/59/EU luottolaitosten ja sijoituspalveluyritysten elvytys- ja kriisinratkaisukehyksestä sekä neuvoston direktiivin 82/891/ETY, Euroopan parlamentin ja neuvoston direktiivien 2001/24/EY, 2002/47/EY, 2004/25/EY, 2005/56/EY, 2007/36/EY, 2011/35/EU, 2012/30/EU ja 2013/36/EU ja asetusten (EU) N:o 1093/2010 ja (EU) N:o 648/2012 muuttamisesta (jäljempänä *kriisinratkaisudirektiivi*), direktiivi 2014/65/EU rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta (jäljempänä *MiFID II -direktiivi*), direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (jäljempänä *maksupalveludirektiivi*) sekä direktiivi (EU) 2016/2341 ammatillisia lisäeläkkeitä tarjoavien laitosten toiminnasta ja valvonnasta (jäljempänä *IORP II -direktiivi*).

Muutosten tarkoituksena on varmistaa mainittujen direktiivien johdonmukaisuus DORA-asetuksen kanssa. DORA-muutosdirektiivin johdanto-osan 3 kappaleen mukaan muutokset ovat tarpeen oikeudellisen selkeyden ja johdonmukaisuuden lisäämiseksi siltä osin, miten kyseisten direktiivien mukaisesti toimiluvan saaneisiin ja valvottuihin finanssialan yhteisöihin sovelletaan erilaisia digitaalista häiriönsietokykyä koskevia vaatimuksia, jotka ovat tarpeen niiden toiminnan harjoittamiseksi ja palvelujen tarjoamiseksi. Finanssiyhteisöjen on osana sisäistä hallintoaan ja riskienhallinnan menettelyjään hallinnoitava verkko- ja tietojärjestelmiään DORA-asetuksen mukaisesti. Muutosten tarkka sisältö vaihtelee sen mukaan, millä tavoin toiminnan järjestämisestä, riskinhallinnasta sekä häiriönsietokykyä ja toiminnan jatkuvuuden turvaamista koskevista vaatimuksista on eri direktiiveissä säädetty.

Direktiivi sisältää myös eräitä muita muutoksia. Luottolaitosdirektiivin 97 artiklan mukaisen vakavaraisuuden arviointiprosessin soveltamisalaa on muutettu siten, että se viittaa nimenomaisesti DORA-asetuksessa vahvistettuihin vaatimuksiin ja kattaa erityisesti luottolaitosten kyseisen asetuksen mukaisesti suorittamissa digitaalista häiriönsietokykyä koskevissa testeissä ilmenneet riskit. Luottolaitosdirektiiviin on DORA-muutosdirektiivillä myös lisätty säännös, jonka mukaan toimivaltaisella viranomaisella tulee olla oikeus vaatia kaikkia tehtäviensä hoitamisen kannalta tarpeellisia tietoja myös TVT-palveluntarjoajana olevilta kolmansilta osapuolilta. Kriisinratkaisudirektiivin muutoksilla puolestaan huomioidaan digitaalinen häiriönsieto-

kyky ja DORA-asetuksen säätäminen luottolaitosten ja sijoituspalveluyritysten elvytys- ja kriisinratkaisusuunnitelmien sisältöä koskevissa vaatimuksissa sekä purkamis- ja uudelleenjärjestämismahdollisuuksien arviointia koskevissa vaatimuksissa.

Direktiivin johdanto-osan 9 kappaleen mukaan muita TVT-riskivaatimuksia on useissa tapauksissa jo vahvistettu delegoiduissa säädöksissä ja täytäntöönpanosäädöksissä, jotka on hyväksytty toimivaltaisen Euroopan valvontaviranomaisen laatimien teknisten sääntely- ja täytäntöönpanostandardien luonnosten perusteella. Koska DORA-asetuksen säännökset muodostavat vastedes oikeudellisen kehyksen TVT-riskille finanssialalla, sijoitusrahastodirektiivissä, Solvenssi II -direktiivissä, AIFM-direktiivissä ja MiFID II -direktiivissä annettuja tiettyjä valtuutuksia antaa delegoituja säädöksiä ja täytäntöönpanosäädöksiä muutetaan poistamalla TVT-riskiä koskevat säännökset kyseisten valtuutuksien soveltamisalasta.

DORA-muutosdirektiivin 9 artiklan mukaan jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät säännökset viimeistään 17.1.2025. Jäsenvaltioiden on sovellettava kyseisiä säännöksiä samasta päivästä lukien.

3 Nykytila ja sen arviointi

3.1 Laki Finanssivalvonnasta

Finanssivalvonnasta annetun lain (878/2008) 3 §:ssä säädetään Finanssivalvonnan tehtävistä. Pykälän 1 momentin mukaan Finanssivalvonnan tehtävänä on valvoa finanssimarkkinoilla toimivien toimintaa niin kuin tässä laissa ja muualla laissa säädetään. Finanssivalvonta edistää lisäksi hyvien menettelytapojen noudattamista finanssimarkkinoilla sekä yleisön tietämystä finanssimarkkinoista.

Pykälän 2 ja 3 momentissa säädetään Finanssivalvonnan erityisistä tehtäväalueista. Lain esitöiden (HE 66/2008 vp, s. 83) mukaan pykälän tarkoituksena on kuvata Finanssivalvonnan tärkeimmät tehtävät. Se missä laajuudessa Finanssivalvonta kutakin tehtäväaluetta hoitaisi ja kuinka paljon voimavaroja se kuhunkin niistä kohdistaisi, jäisi riippumaan niistä tarkemmista tavoitteista ja toiminnan painopisteistä, joita Finanssivalvonnan johtokunta Finanssivalvonnan toiminnalle kulloinkin asettaa. Pykälän 2 momentissa säädetään niistä Finanssivalvonnan tehtävistä, joiden tarkempi sisältö määräytyy sen mukaan, mitä muualla laissa säädetään. Pykälän 3 momentissa puolestaan säädetään sellaisista yleisemmistä tehtävistä, joiden osalta Finanssivalvonnan toimivalta perustuu yksinomaan tähän pykälään.

Finanssivalvonnan tehtäviin kuuluu muun muassa pykälän 2 momentin 2 kohdan mukaan valvoa, että finanssimarkkinoilla toimivat noudattavat niihin sovellettavia finanssimarkkinoita koskevia säännöksiä, niiden nojalla annettuja määräyksiä, toimilupansa ehtoja ja toimintaansa koskevia sääntöjä sekä pykälän 3 momentin 6 kohdan mukaan osallistua viranomaisten väliseen kotimaiseen yhteistyöhön ja momentin 7 kohdan mukaan osallistua lain 3 a §:ssä tarkoitetun Euroopan finanssivalvontajärjestelmän puitteissa tapahtuvaan yhteistyöhön Euroopan unionissa sekä muuhun viranomaisten kansainväliseen yhteistyöhön.

Finanssivalvonnan valvontavaltuuksista säädetään Finanssivalvonnasta annetun lain 3 luvussa. Lain 18 §:n mukaan valvottavan ja muun finanssimarkkinoilla toimivan on salassapitosäännösten estämättä ilman aiheetonta viivytystä toimitettava Finanssivalvonnalle sen pyytämät tiedot ja selvitykset, jotka ovat tarpeen Finanssivalvonnalle laissa säädetyn tehtävän hoitamiseksi. Vastaava velvollisuus on sillä, jolla on kirjanpitolain (1336/1997) 1 luvun 5 §:ssä tarkoitettu määräysvalta valvottavassa tai muussa finanssimarkkinoilla toimivassa tai joka on valvottavan tai muun finanssimarkkinoilla toimivan määräysvallassa. Vastaava koskee myös yritystä, joka

valvottavan tai muun finanssimarkkinoilla toimivan asiamiehenä tai sijoituspalvelulain 7 luvun 6 §:ssä tarkoitettuna sidonnaisasiamiehenä taikka muuten valvottavan tai muun finanssimarkkinoilla toimivan toimeksiannosta hoitaa tämän liiketoimintaan, kirjanpitoon, tietojärjestelmään, riskienhallintaan tai sisäiseen valvontaan liittyviä tehtäviä. Tiedonsaantioikeus ulottuu lain 19 §:n nojalla myös Finanssivalvonnalle laissa säädetyn valvontatehtävän hoitamiseksi tarpeellisten tietojen saamiseen valvottavan ja muun finanssimarkkinoilla toimivan tilintarkastajalta sekä yksilöityä valvontatointa varten valvonnan kannalta välttämättömiin tietoihin muulta, jolla voidaan perustellusta syystä olettaa olevan valvontatoimen kannalta tarpeellista tietoa.

Lain 22 §:n mukaan Finanssivalvonnalla on oikeus tarvittaessa kutsua kuultavaksi 18, 19 ja 21 §:ssä tarkoitetun oikeushenkilön edustaja tai sen palveluksessa oleva henkilö taikka mainituissa pykälissä tarkoitettu luonnollinen henkilö. Kuulemiseen sovelletaan, mitä hallintolaissa (434/2003) säädetään asian suullisesta käsittelystä. Kutsun noudattamatta jättämisen perusteella ei voida asettaa 33 a §:ssä tarkoitettua uhkasakkoa eikä määrätä 4 luvussa tarkoitettua hallinnollista seuraamusta.

Lain 24 §:n 1 momentin mukaan Finanssivalvonnalla on salassapitosäännösten estämättä oikeus saada tarkastettavakseen valvottavan ja muun finanssimarkkinoilla toimivan toimipaikassa tämän toimintaa ja hallintoa koskevat asiakirjat, tallenteet puhelinkeskusteluista ja sähköisestä viestinnästä, muut tietoliikennetiedot sekä tietojärjestelmät siinä laajuudessa kuin se on tarpeen Finanssivalvonnalle laissa säädetyn valvontatehtävän hoitamiseksi. Finanssivalvonnalla on oikeus saada valvottavalta ja muulta finanssimarkkinoilla toimivalta maksutta tarpeelliset jäljennökset tässä pykälässä tarkoitetuista asiakirjoista ja muista tallenteista ja tietoliikennetiedoista. Pykälän 2 momentin mukaan, mitä 1 momentissa säädetään valvottavasta ja muusta finanssimarkkinoilla toimivasta, koskee myös yritystä, joka valvottavan tai muun finanssimarkkinoilla toimivan asiamiehenä tai sijoituspalvelulain 7 luvun 6 §:ssä tarkoitettuna sidonnaisasiamiehenä taikka muuten valvottavan tai muun finanssimarkkinoilla toimivan toimeksiannosta hoitaa tämän liiketoimintaan, kirjanpitoon, tietojärjestelmään, riskienhallintaan tai sisäiseen valvontaan liittyviä tehtäviä. Pykälän 3 momentin mukaan Finanssivalvonnalla on lisäksi salassapitosäännösten estämättä oikeus saada lain 19, 21 ja 23 §:ssä tarkoitetuilta henkilöiltä ja yrityksiltä tarkastettavakseen asiakirjat ja tallenteet, jotka sisältävät mainituissa pykälissä tarkoitettuja tietoja.

Finanssivalvonnalla on lain 25 b §:n nojalla oikeus tehtäviensä suorittamiseksi saada pyynnöstä poliisilta virka-apua.

Lain 33 §:ssä säädetään toimeenpanokiellosta ja oikaisukehotuksesta. Pykälän 1 momentin mukaan Finanssivalvonta voi kieltää valvottavan tai muun finanssimarkkinoilla toimivan tekemän päätöksen täytäntöönpanon tai valvottavan tai muun finanssimarkkinoilla toimivan suunnitteleman toimenpiteen toteutuksen, jos päätös tai toimenpide on ristiriidassa valvottavaan tai muuhun finanssimarkkinoilla toimivaan sovellettavien finanssimarkkinoita koskevien säännösten tai niiden nojalla annettujen määräysten, toimiluvan ehtojen taikka valvottavan tai muun finanssimarkkinoilla toimivan toimintaa koskevien sääntöjen kanssa. Jos valvottava tai muu finanssimarkkinoilla toimiva on pannut 1 momentissa tarkoitetun päätöksen täytäntöön tai toteuttanut 1 momentissa tarkoitetun muun toimenpiteen, Finanssivalvonta voi pykälän 2 momentin mukaan velvoittaa valvottavan tai muun finanssimarkkinoilla toimivan ryhtymään toimenpiteisiin päätöksen täytäntöönpanon tai toteutetun toimenpiteen peruuttamiseksi tai oikaisun aikaansaamiseksi. Finanssivalvonnan on varattava valvottavalle tai muulle finanssimarkkinoilla toimivalle kohtuullinen määräaika päätöksen täytäntöönpanon tai toteutetun toimenpiteen peruuttamiseksi tai oikaisun aikaansaamiseksi, jollei se vaaranna vakavasti finanssimarkkinoiden valvonnalle 1 §:ssä säädettyjen tavoitteiden toteutumista. Pykälän 3 momentin mukaan Finanssivalvonta voi velvoittaa valvottavan tai muun finanssimarkkinoilla toimivan lopettamaan toi-

minnassaan soveltamansa menettelyn ja kieltää menettelyn uudistamisen, jos menettely on ristiriidassa 1 momentissa tarkoitettujen säännösten, määräysten, toimiluvan ehtojen taikka sääntöjen kanssa. Finanssivalvonnan on varattava valvottavalle tai muulle finanssimarkkinoilla toimivalle kohtuullinen määräaika menettelyn korjaamiseksi, jollei se vaaranna vakavasti finanssimarkkinoiden valvonnalle 1 §:ssä säädettyjen tavoitteiden toteutumista. Pykälän 5 momentin mukaisesti pykälässä tarkoitettu kielto tai oikaisukehotus voidaan, jos siihen on erityistä syytä, kohdistaa myös valvottavan tai muun finanssimarkkinoilla toimivan palveluksessa olevaan tai muuhun, joka toimii hänen lukuunsa.

Lain 33 a §:ssä säädetään uhkasakosta. Jos valvottava tai muu finanssimarkkinoilla toimiva toiminnassaan laiminlyö noudattaa finanssimarkkinoita koskevia säännöksiä tai niiden nojalla annettuja määräyksiä, Finanssivalvonnan 33 §:n nojalla antamaa toimeenpanokieltoa tai oikaisukehotusta taikka muuta Finanssivalvonnan lain nojalla antamaa määräystä tai kieltoa, toimilupansa ehtoja tai toimintaansa koskevia sääntöjä, Finanssivalvonta voi uhkasakolla velvoittaa valvottavan tai muun finanssimarkkinoilla toimivan täyttämään velvollisuutensa, jos laiminlyönti ei ole vähäinen. Uhkasakko voidaan, jos siihen on erityistä syytä, kohdistaa myös valvottavan tai muun finanssimarkkinoilla toimivan palveluksessa olevaan tai muuhun, joka toimii hänen lukuunsa. Finanssivalvonta voi uhkasakolla velvoittaa 18, 19, 21, 23 ja 24 §:ssä tarkoitetun täyttämään mainituissa pykälissä säädetyn velvollisuutensa, jos laiminlyönti ei ole vähäinen.

Lain 34 §:n mukaan Finanssivalvonta voi valvottavan tai muun finanssimarkkinoilla toimivan valvonnan kannalta tarpeellisen, erityistä asiantuntemusta vaativan asian selvittämiseksi käyttää tilintarkastajaa tai muuta ulkopuolista asiantuntijaa. Tällä on tehtävässään 18, 19, 23 ja 24 §:n mukaiset oikeudet ja hän toimii rikosoikeudellisella virkavastuulla hoitaessaan tämän lain mukaisesti annettuja julkisoikeudellisia hallintotehtäviä.

Finanssivalvonnasta annetun lain 4 luvussa säädetään hallinnollisista seuraamuksista, joita ovat 38 §:n mukainen rikemaksu, 39 §:n mukainen julkinen varoitus ja 40 §:n mukainen seuraamusmaksu. Rikemaksua ja seuraamusmaksua koskevissa pykälissä luetellaan ne lainkohdat, joiden laiminlyönnin tai rikkomisen seurauksena kyseinen seuraamus voidaan määrätä. Lain 38 §:n 4 momentin mukaan, jos teko tai laiminlyönti on erityisen moitittava, rikemaksun sijaan voidaan määrätä seuraamusmaksu.

Lain 39 §:n mukaan Finanssivalvonta antaa valvottavalle ja muulle finanssimarkkinoilla toimivalle julkisen varoituksen, jos tämä tahallaan tai huolimattomuudesta menettelee muiden kuin 38 §:n 1 momentissa taikka 40 §:n 1 tai 2 momentissa tarkoitettujen finanssimarkkinoita koskevien säännösten tai niiden nojalla annettujen määräysten vastaisesti ja edellyttäen, ettei asia kokonaisuutena arvioiden anna aihetta ankarampiin toimenpiteisiin.

Lain 40 §:n 3 momentin mukaan seuraamusmaksua ei voida määrätä luonnolliselle henkilölle teosta tai laiminlyönnistä, joka on laissa säädetty rangaistavaksi. Finanssivalvonta voi kuitenkin määrätä seuraamusmaksun ja jättää asian ilmoittamatta esitutkintaviranomaiselle, jos teko tai laiminlyönti on sen haitallisuus, siitä ilmenevä tekijän syyllisyys sekä siitä saatu hyöty ja muut tekoon tai laiminlyöntiin liittyvät seikat huomioon ottaen kokonaisuutena arvioiden vähäinen. Pykälän 4 momentin mukaan seuraamusmaksu voidaan määrätä oikeushenkilölle määrättävän seuraamusmaksun lisäksi tai sen sijasta sellaiselle oikeushenkilön johtoon kuuluvalle henkilölle, jonka velvollisuuksien vastainen edellä tässä pykälässä säädetty teko tai laiminlyönti on. Kyseiselle henkilölle määrättävän seuraamusmaksun edellytyksenä on, että henkilö on merkittävällä tavalla myötävaikuttanut tekoon tai laiminlyöntiin.

Lain 41 §:ssä säädetään tarkemmin seuraamusmaksun määräämisestä. Pykälän 2 momentin mukaan seuraamusmaksun määrä perustuu kokonaisarviointiin, kuten myös rikemaksun määrääminen lain 38 §:n 2 momentin mukaan. Seuraamusmaksun määrää arvioitaessa on otettava huomioon menettelyn laatu, laajuus ja kestoaika sekä tekijän taloudellinen asema. Lisäksi arvioinnissa on otettava huomioon menettelyllä saavutettu hyöty ja sillä aiheutettu vahinko, jos ne ovat määritettävissä, tekijän yhteistyö Finanssivalvonnan kanssa asian selvittämiseksi ja toimenpiteet rikkomisen toistumisen estämiseksi, muut ja aiemmat finanssimarkkinoita koskeviin säännöksiin kohdistuneet rikkomukset ja laiminlyönnit sekä menettelyn mahdolliset vaikutukset rahoitusjärjestelmän vakaudelle.

Lain 42 §:n 1 momentin mukaan Finanssivalvonta voi jättää rikemaksun määräämättä tai julkisen varoituksen antamatta, jos 1) edellä 38 tai 39 §:ssä tarkoitettu on oma-aloitteisesti ryhtynyt riittäviin toimenpiteisiin virheen korjaamiseksi välittömästi virheen havaitsemisen jälkeen ja ilmoittanut virheestä viivytyksettä Finanssivalvonnalle, eikä virhe tai laiminlyönti ole vakava tai toistuva; 2) virheellistä menettelyä on pidettävä vähäisenä; tai 3) rikemaksun määräämistä tai julkisen varoituksen antamista on muutoin pidettävä ilmeisen kohtuuttomana. Pykälän 2 momentin mukaan Finanssivalvonta voi seuraamusmaksun määräämisen sijaan antaa julkisen varoituksen 1 momentin 2 ja 3 kohdassa säädetyillä perusteilla. Pykälän 3 momentin mukaan rikemaksua tai seuraamusmaksua ei voida määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Rikemaksua tai seuraamusmaksua ei voida määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio.

Lain 43 §:n 1 momentin mukaan Finanssivalvonnan on julkistettava päätös, jossa määrätään rikemaksu, julkinen varoitus tai seuraamusmaksu viipymättä sen jälkeen, kun päätöksestä on ilmoitettu sen kohteena olevalle henkilölle. Julkistamisesta on käytävä ilmi, onko seuraamuksen antamista tai määräämistä koskeva päätös lainvoimainen, rikkomisen luonne ja tyyppi sekä rikkomisesta vastuussa olevan henkilöllisyys. Seuraamusta koskevat tiedot on pidettävä Finanssivalvonnan internetsivuilla viiden vuoden ajan. Pykälän 2 momentin mukaisin edellytyksin Finanssivalvonta voi lykätä seuraamusta koskevan päätöksen julkistamista, julkistaa seuraamusta koskevan päätöksen ilman seuraamuksen kohteena olevan henkilön nimeä tai jättää seuraamusta koskevan päätöksen julkistamatta, jos seuraamuksen kohteena olevan luonnollisen henkilön tai oikeushenkilön nimen julkistaminen olisi kohtuutonta, tai jos seuraamuksen julkistaminen vaarantaisi finanssimarkkinoiden vakauden tai meneillään olevan viranomaistutkinnan. Mitä pykälässä säädetään rikemaksun, julkisen varoituksen ja seuraamusmaksun julkistamisesta, sovelletaan myös muun muassa lain 33 ja 33 a §:ssä tarkoitettujen päätösten julkistamiseen.

Finanssivalvonnasta annetun lain 6 luku sisältää säännöksiä muun muassa Finanssivalvonnan yhteistyöstä ulkomaan viranomaisten kanssa sekä EU-säädösten noudattamisen valvonnasta. Voimassa oleva 50 p § ja 52 a § on säädetty toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 (*verkko- ja tietoturvadirektiivi*) toimeenpanemiseksi.

Lain 50 p §:n mukaan Finanssivalvonta toimii verkko- ja tietoturvadirektiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta.

Lain 52 a §:n mukaan Finanssivalvonnan on tehtävä yhteistyötä verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa Liikenne- ja viestintäviraston kanssa. Finanssivalvonnalla on tätä tarkoitusta varten oikeus salassapitosäännösten estämättä luovuttaa tietoja Liikenne- ja viestintävirastolle. Pykälällä on pantu täytäntöön verkko- ja tietoturvadirektiivin 10 artikla direktiivin liitteen II toimialojen 3 ja 4 osalta. Direktiivin 10 artiklassa säädetään kansallisen tason

viranomaisyhteistyöstä. Jos saman jäsenvaltion toimivaltainen viranomainen, keskitetty yhteyspiste ja CSIRT-toimija ovat erillisiä, niiden on tehtävä yhteistyötä direktiivissä säädettyjen velvollisuuksien täyttämisen osalta. Jäsenvaltioiden on varmistettava, että joko toimivaltaiset viranomaiset tai CSIRT-toimijat saavat direktiivin nojalla toimitetut poikkeamia koskevat ilmoitukset. Jos jäsenvaltio päättää, että CSIRT-toimijat eivät saa ilmoituksia, CSIRT-toimijoille on, siinä määrin kuin on tarpeen niiden tehtävien täyttämiseksi, annettava pääsy tietoihin, jotka koskevat keskeisten palvelujen tarjoajien direktiivin 14 artiklan 3 ja 5 kohdan nojalla ilmoittamia poikkeamia. Jäsenvaltioiden on varmistettava, että toimivaltaiset viranomaiset tai CSIRT-toimijat ilmoittavat keskitetyille yhteyspisteille tämän direktiivin nojalla toimitetuista poikkeamia koskevista ilmoituksista. Verkko- ja tietoturvadirektiivin tarkoittamana keskitettynä yhteyspisteenä ja CSIRT-toimijana on Liikenne- ja viestintäviraston Kyberturvallisuuskeskus.

Finanssivalvonnasta annetun lain 18 §:n 2 momentin mukaan Finanssivalvonta voi antaa määräyksiä muun muassa valvottavan sisäistä valvontaa ja riskienhallintaa koskevien tietojen säännöllisestä toimittamisesta ja toimittamistavasta Finanssivalvonnalle. Finanssivalvonta on antanut määräykset ja ohjeet operatiivisen riskin hallinnasta rahoitussektorin valvottavissa (Määräykset ja ohjeet 8/2014), jotka ovat tulleet voimaan 1.2.2015.

Osana mainittuja määräyksiä ja ohjeita Finanssivalvonta on antanut määräykset sisäistä valvontaa, riskienhallintaa ja häiriöitä koskevien tietojen toimittamisesta Finanssivalvonnalle, jotka ovat tulleet voimaan 1.1.2020. Valvottavan tulee tehdä ensi-ilmoitus Finanssivalvonnalle asiakkaille tarjotuissa palveluissa sekä maksu- ja tietojärjestelmissä esiintyneistä merkittävistä häiriöistä ja virheistä viipymättä niiden ilmaannuttua. Maksujenvälityksessä ja korttimaksamisessa merkittäviksi häiriöiksi katsotaan esimerkiksi suurta määrää asiakkaita koskeva häiriö tai viivästys. Merkittävä häiriö on myös verkkoja tietoturvallisuuteen liittyvä häiriö tai poikkeama sekä häiriö, jossa asiakastietoja on joutunut ulkopuoliselle taholle. Finanssivalvonnalle tulee ilmoittaa viipymättä myös sellaiset häiriöt ja virheet, jotka haittaavat tai vaarantavat valvottavan kykyä jatkaa liiketoimintaansa tai vastata velvoitteistaan. Valvottavan tulee tehdä Finanssivalvonnalle täydentävä ilmoitus häiriön tarkemmista yksityiskohdista mahdollisimman pian ensimmäisen ilmoituksen tekemisen jälkeen ja loppuraportti, kun häiriön varsinainen syy on selvitetty. Ilmoitus tulee tehdä ainakin seuraaviin ryhmiin kuuluvista häiriöistä: murtautuminen tietojärjestelmään; tietojen paljastuminen asiattomille; tietoturvaloukkaus; haittaohjelman levittäminen tietojärjestelmään ja palvelunestohyökkäys.

Lisäksi Finanssivalvonta on antanut määräykset ja ohjeet henki- ja vahinkovakuutusyhtiön toiminnan aloittamisesta ja hallintojärjestelmästä (Määräykset ja ohjeet 6/2015), jotka ovat tulleet voimaan 1.1.2016 ja sisältävät määräyksiä ja ohjeita tietojärjestelmien ja tietoturvallisuuden järjestämisestä osana operatiivisten riskien hallintaa henki- ja vahinkovakuutusyhtiöissä sekä tietojen ilmoittamisesta Finanssivalvonnalle. Finanssivalvonnan määräykset henki- ja vahinkovakuutusyhtiöille toiminnan häiriöistä ja virheistä tehtävästä ilmoituksesta vastaavat pääosin yllä muiden rahoitussektorin valvottavien osalta annettuja määräyksiä.

3.2 DORA-asetuksen edellyttämät muutokset Finanssivalvonnan valvontavaltuuksiin

DORA-asetus on Suomessa suoraan sovellettavaa oikeutta. Asetuksen soveltamisalaan kuuluvat finanssiyhteisöt ovat siten velvoitettuja noudattamaan asetuksen sääntelyä ilman erillisiä kansallisia täytäntöönpanotoimia. Finanssivalvonta on Suomessa DORA-asetuksen 46 artiklan tarkoittama toimivaltainen viranomainen. Finanssivalvonnan tehtävänä on valvoa, että finanssimarkkinoilla toimivat noudattavat niihin sovellettavia finanssimarkkinoita koskevia säännöksiä, joihin jatkossa sisältyy myös DORA-asetus. Asetuksen 50 artiklan 1 kohta edellyttää, että toimivaltaisilla viranomaisilla on oltava kaikki asetuksen mukaisten tehtäviensä hoitamiseen

tarvittavat valtuudet valvoa, tutkia ja määrätä seuraamuksia. Toimivaltaisen viranomaisen valtuuksista säädetään pääosin kansallisessa lainsäädännössä, joten tältä osin asetus edellyttää kansallisia sääntelytoimia.

DORA-asetuksen 50 artiklan 2 kohdan a alakohdan mukaan mainittuihin valtuuksiin on kuuluttava valtuudet saada tutustua kaikkiin asiakirjoihin tai muuhun dataan, joilla toimivaltainen viranomainen katsoo olevan merkitystä tehtäviensä suorittamisen kannalta, ja oikeus saada tai ottaa jäljennös niistä. Artiklan 2 kohdan b alakohdan mukaan toimivaltaisella viranomaisella on oltava valtuudet suorittaa paikalla tehtäviä tarkastuksia tai tutkimuksia, joiden yhteydessä voidaan muun muassa pyytää finanssiyhteisöjen edustajilta suullisia tai kirjallisia selvityksiä tutkimuksen kohteeseen ja tarkoitukseen liittyvistä tosiseikoista tai asiakirjoista ja tallentaa vastaukset sekä haastatella ketä tahansa muuta haastatteluun suostuvaa luonnollista henkilöä tai oikeushenkilöä tutkimuksen kohteeseen liittyvien tietojen keräämiseksi. Kyseiset valtuudet sisältyvät Finanssivalvonnasta annetun lain 18, 19, 22 ja 24 §:ään.

DORA-asetuksen 50 artiklan 2 kohdan c alakohdan mukaan toimivaltaisella viranomaisella on oltava valtuudet vaatia oikaisevia ja korjaavia toimenpiteitä, jos asetuksen vaatimuksia rikotaan. Artiklan 3 kohdan mukaan jäsenvaltioiden on vahvistettava säännöt, jotka koskevat asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, ja varmistettava niiden tehokas täytäntöönpano, sanotun kuitenkaan rajoittamatta jäsenvaltioiden oikeutta määrätä rikosoikeudellisia seuraamuksia asetuksen 52 artiklan mukaisesti. Kyseisten seuraamusten ja toimenpiteiden on oltava tehokkaita, oikeasuhteisia ja varoittavia.

Hallinnollisia seuraamuksia ja korjaavia toimenpiteitä koskevia vaatimuksia tarkennetaan DORA-asetuksen 50 artiklan 4 kohdassa. Kohdan a ja b alakohdan mukaan jäsenvaltioiden on annettava asetuksen rikkomistapauksissa toimivaltaisille viranomaisille valtuudet antaa määräys, jossa kyseessä olevaa luonnollista henkilöä tai oikeushenkilöä vaaditaan lopettamaan asetuksen vastainen toiminta ja pidättäytymään toistamasta kyseistä toimintaa sekä vaatia sellaisen käytännön tai menettelytavan tilapäistä tai pysyvää lopettamista, jonka toimivaltainen viranomainen katsoo olevan ristiriidassa asetuksen säännösten kanssa, ja estää kyseisen käytännön tai menettelytavan toistuminen. Kyseiset valtuudet sisältyvät Finanssivalvonnasta annetun lain 33 §:ään.

DORA-asetuksen 50 artiklan 4 kohdan c alakohdan mukaan toimivaltaisille viranomaisille on annettava valtuudet ottaa käyttöön minkä tahansa tyyppisiä, myös taloudellisia, toimenpiteitä sen varmistamiseksi, että finanssiyhteisöt jatkavat lakisääteisten vaatimusten noudattamista. Kyseiset valtuudet sisältyvät uhkasakon osalta Finanssivalvonnasta annetun lain 33 a §:ään. Lisäksi lain 4 luvun hallinnollisia seuraamuksia koskevat säännökset ovat tältä osin merkityksellisiä. Lain rikemaksua ja seuraamusmaksua koskevissa säännöksissä luetellaan ne säännökset, joiden laiminlyönnin tai rikkomisen seurauksena kyseinen seuraamus voidaan määrätä. Näitä säännöksiä olisi täydennettävä siten, että seuraamus voidaan määrätä DORA-asetuksen asianomaisten säännösten laiminlyönnin tai rikkomisen johdosta. Lain mukaiset hallinnolliset seuraamukset mahdollistavat nopean ja tehokkaan puuttumisen lainsäädännön vastaiseen menettelyyn, mikä tehostaa finanssiyhteisöihin kohdistettavaa valvontaa. Hallinnollisia seuraamuksia koskevat säännökset turvaavat lakisääteisten vaatimusten noudattamista myös niiden yleisen ennalta estävän vaikutuksen kautta.

DORA-asetuksen 50 artiklan 4 kohdan d alakohdan mukaan toimivaltaisilla viranomaisilla on kansallisen lainsäädännön mahdollistamissa puitteissa oltava valtuudet vaatia teleoperaattorin hallussa olevia dataliikennetietoja, jos voidaan perustellusti epäillä asetuksen rikkomista ja jos tällaiset tiedot voivat olla merkityksellisiä asetuksen rikkomista koskevan tutkinnan kannalta. Finanssivalvonnalle ei ole kansallisessa lainsäädännössä annettu oikeutta vaatia teleoperaattorin

hallussa olevia tietoliikennetietoja. Asiaa on arvioitu EU:n markkinoiden väärinkäyttöasetukseen (EU) N:o 596/2014 liittyvien lakiehdotusten säätämisen yhteydessä (ks. HE 65/2016 vp., s. 27). Markkinoiden väärinkäyttöasetus sisältää DORA-asetusta vastaavan säännöksen valtuudesta vaatia teleoperaattorin hallussa olevia dataliikennetietoja kansallisen lainsäädännön mahdollistamissa puitteissa. Suomessa oikeus saada televalvontatietoja on pakkokeinolaissa (806/2011) säädetyin edellytyksin ainoastaan poliisilla, joka voi muun muassa törkeissä sisäpiirintiedon väärinkäyttöepäilyissä tai markkinoiden vääristämisepäilyissä saada tuomioistuimelta luvan televalvontatietoihin. Tätä lähestymistapaa ei ole perusteltua lähteä muuttamaan ilman perusteellista arviointia Finanssivalvonnan nykyisten tutkintavaltuuksien riittävyydestä. Ratkaisua jättää tällainen valtuus kansallisesti säätämättä on pidettävä myös DORA-asetuksen perusteella mahdollisena.

Asetuksen 50 artiklan 4 kohdan e alakohdan mukaan toimivaltaisille viranomaisille on annettava valtuudet antaa julkisia ilmoituksia, mukaan lukien julkiset lausumat, joissa ilmoitetaan luonnollisen henkilön tai oikeushenkilön henkilöllisyys ja rikkomisen luonne. Kyseiset valtuudet sisältyvät Finanssivalvonnasta annetun lain 43 §:ään. Mitä pykälässä säädetään rikemaksun, julkisen varoituksen ja seuraamusmaksun julkistamisesta, sovelletaan myös lain 33 §:ssä tarkoitettua toimeenpanokieltoa ja oikaisukehotusta sekä 33 a §:ssä tarkoitettua uhkasakkoa koskevien päätösten julkistamiseen. Asetuksen 54 artiklassa annetaan lisäksi erillisiä suoraan sovellettavia säännöksiä hallinnollisten seuraamusten julkaisemisesta. Toimivaltaisten viranomaisten on julkaistava virallisilla verkkosivustoillaan ilman aiheetonta viivytystä kaikki hallinnollisen seuraamuksen määräämistä koskevat päätökset, joihin ei voi hakea muutosta, sen jälkeen, kun kyseinen päätös on annettu tiedoksi seuraamuksen kohteena olevalle henkilölle. Artikla sisältää lisäksi julkaisemisvelvollisuutta koskevia poikkeuksia sekä muita tarkentavia säännöksiä. Finanssivalvonnan tulee kansallisen lainsäädännön ohella ottaa mainitut säännökset huomioon toiminnassaan. Asiasta olisi perusteltua sisällyttää informatiivinen viittaussäännös Finanssivalvonnasta annettuun lakiin.

DORA-asetuksen 50 artiklan 5 kohdan mukaan, jos artiklan 2 kohdan c alakohtaa ja 4 kohtaa sovelletaan oikeushenkilöihin, jäsenvaltioiden on annettava toimivaltaisille viranomaisille toimivalta soveltaa kansallisessa lainsäädännössä säädetyin edellytyksin hallinnollisia seuraamuksia ja korjaavia toimenpiteitä ylimmän hallintoelimen jäseniin ja muihin luonnollisiin henkilöihin, jotka ovat kansallisen lainsäädännön mukaan vastuussa rikkomisesta. Tätä koskevat säännökset sisältyvät Finanssivalvonnasta annetun lain 33 §:n 5 momenttiin ja 40 §:n 4 momenttiin.

Asetuksen 50 artiklan 6 kohdan mukaan jäsenvaltioiden on varmistettava, että kaikki päätökset, joilla määrätään artiklan 2 kohdan c alakohdassa säädettyjä hallinnollisia seuraamuksia tai korjaavia toimenpiteitä, ovat asianmukaisesti perusteltuja ja että niihin voidaan hakea muutosta. Muutoksenhausta Finanssivalvonnan päätökseen säädetään Finanssivalvonnasta annetun lain 73 §:ssä. Hallintomenettelyä koskevat säännökset sisältyvät hallintolakiin.

DORA-asetuksen 51 artiklan 2 kohdan mukaan, kun toimivaltaiset viranomaiset määrittävät 50 artiklan mukaisesti määrättävän hallinnollisen seuraamuksen tai korjaavan toimenpiteen tyyppiä ja tasoa, niiden on otettava huomioon, missä määrin rikkominen on tahallinen tai tuottamuksellinen, ja kaikki muut asiaan vaikuttavat olosuhteet, mukaan lukien tapauksen mukaan seuraavat:
a) rikkomisen olennaisuus, vakavuus ja kesto;
b) rikkomuksesta vastuussa olevan luonnollisen henkilön tai oikeushenkilön vastuun aste;
c) vastuussa olevan luonnollisen henkilön tai oikeushenkilön taloudellinen vahvuus;
d) vastuussa olevan luonnollisen henkilön tai oikeushenkilön saamien voittojen tai näiden välttämien tappioiden suuruus, jos ne ovat määritettävissä;
e) rikkomisen kolmansille osapuolille aiheuttamat tappiot, jos ne ovat määritettävissä;

f) se, missä määrin vastuussa oleva luonnollinen henkilö tai oikeushenkilö on tehnyt yhteistyötä toimivaltaisen viranomaisen kanssa, sanotun kuitenkaan rajoittamatta tarvetta varmistaa, että kyseinen luonnollinen henkilö tai oikeushenkilö joutuu luopumaan saamistaan voitoista tai välttämistään tappioista;
g) vastuussa olevan luonnollisen henkilön tai oikeushenkilön aiempi syyllistyminen rikkomiseen.

Rikemaksun ja seuraamusmaksun määrittämisessä huomioitavista tekijöistä säädetään Finanssivalvonnasta annetun lain 38 §:n 2 momentissa ja 41 §:n 2 momentissa. Määrättävän rike- tai seuraamusmaksun määrä perustuu kokonaisarviointiin. DORA-asetuksen mukaisten velvoitteiden laiminlyönnin tai rikkomisen johdosta määrättävää seuraamusta määritettäessä tulee ottaa huomioon ainakin kaikki asetuksen 51 artiklan 2 kohdassa mainitut seikat ja olosuhteet sekä kaikki muut asiaan vaikuttavat olosuhteet. Kohta koskee sekä hallinnollisen seuraamuksen että muun korjaavan toimenpiteen määräämistä. Finanssivalvonnan tulee kansallisen lainsäädännön ohella ottaa toiminnassaan huomioon mainitut suoraan sovellettavat säännökset. Asiasta olisi perusteltua sisällyttää informatiivinen viittaussäännös Finanssivalvonnasta annettuun lakiin.

DORA-asetuksen 52 artiklan mukaan jäsenvaltiot voivat päättää, että ne eivät säädä hallinnollisia seuraamuksia tai korjaavia toimenpiteitä koskevia sääntöjä sellaisten rikkomisten osalta, joihin sovelletaan niiden kansallisen lainsäädännön mukaisia rikosoikeudellisia seuraamuksia. Asiaa koskeva säännös sisältyy Finanssivalvonnasta annetun lain 40 §:n 3 momenttiin.

Edellä sanotun perusteella voidaan todeta, että Finanssivalvonnasta annetun lain 3 luvun mukaiset Finanssivalvonnan valvontavaltuudet antavat Finanssivalvonnalle DORA-asetuksen 50 artiklan edellyttämät kattavat valtuudet tutkia ja valvoa asetuksen noudattamista, eikä näitä säännöksiä siten ole tarpeen muuttaa asetuksen johdosta. Sen sijaan lain 4 luvun mukaisten hallinnollisten seuraamusten osalta on edellä todettu tarve täydentävälle kansalliselle sääntelylle, jotta voidaan varmistaa tehokkaat, oikeasuhteiset ja varoittavat hallinnolliset seuraamukset DORA-asetuksen edellyttämällä tavalla.

Osana DORA-asetuksen mukaisten velvoitteiden noudattamisen valvontaa, Finanssivalvonnan tehtäviin kuuluu valvoa, että finanssiyhteisöt hallitsevat asianmukaisesti kolmansiin osapuoliin liittyvää TVT-riskiä. Kun finanssiyhteisöt tukeutuvat toiminnassaan TVT-palveluntarjoajana olevien kolmansien osapuolten palveluihin, TVT-riskin kokonaisvaltainen arviointi edellyttää näkyvyyttä myös palveluntarjoajan toimintaan, vaikka vastuu asetuksen velvoitteiden noudattamisesta säilyykin finanssiyhteisöllä. Valvonta ulottuu näin ollen epäsuorasti myös asetuksessa tarkoitettujen TVT-palveluntarjoajana olevien kolmansien osapuolten toimintaan ja niiden omiin TVT-riskinhallintamenettelyihin. Tämän vuoksi lakiin tulee tehdä tarpeelliset muutokset Finanssivalvonnan valvontavaltuuksien ulottamiseksi TVT-palveluntarjoajana oleviin kolmansiin osapuoliin. Tämä on tarpeen myös sen vuoksi, että DORA-muutosdirektiivin mukaan toimivaltaisella viranomaisella tulee olla oikeus vaatia kaikkia tehtäviensä hoitamisen kannalta tarpeellisia tietoja myös TVT-palveluntarjoajana olevilta kolmansilta osapuolilta. Tästä seuraa myös, että toimivaltaisella viranomaisella tulee luottolaitosdirektiivin 65 artiklan 3 kohdan mukaisesti olla oikeus suorittaa kaikki tarpeelliset TVT-palveluntarjoajana olevaa kolmatta osapuolta koskevat tutkimukset sekä valtuudet suorittaa kaikki tarpeelliset tarkastukset palveluntarjoajan liiketiloissa.

3.3 DORA-asetuksen edellyttämät muut muutokset Finanssivalvonnasta annettuun lakiin

DORA-asetuksen 19 artiklan 6 kohdan mukaan toimivaltaisen viranomaisen on artiklan 4 kohdassa tarkoitetun laajavaikutteista TVT:hen liittyvää poikkeamaa koskevan ilmoituksen ja ra-

portin saatuaan hyvissä ajoin toimitettava poikkeamaa koskevat yksityiskohtaiset tiedot soveltuvin osin niiden toimivallan perusteella EPV:lle, ESMAlle tai EIOPAlle; tarpeen mukaan EKP:lle; NIS2-direktiivin mukaisesti nimetyille tai perustetuille toimivaltaisille viranomaisille, keskitetyille yhteyspisteille tai CSIRT-yksiköille; kriisinratkaisuviranomaisille sekä muille kansallisen lainsäädännön mukaisille asianomaisille viranomaisille. Lisäksi finanssiyhteisöt voivat vapaaehtoisesti ilmoittaa merkittävistä kyberuhkista asianomaiselle toimivaltaiselle viranomaiselle, jos ne pitävät uhkaa merkittävänä rahoitusjärjestelmän, palvelujen käyttäjien tai asiakkaiden kannalta. Asianomainen toimivaltainen viranomainen voi artiklan 2 kohdan nojalla toimittaa tällaisia tietoja edellä mainituille viranomaisille. Näin ollen Finanssivalvonnalla olisi suoraan DORA-asetuksen 19 artiklan nojalla oikeus salassapitosäännösten estämättä luovuttaa artiklassa tarkoitettuja laajavaikutteisia TVT:hen liittyviä poikkeamia ja merkittäviä kyberuhkia koskevia tietoja mainituille viranomaisille. DORA-asetuksen 55 artiklassa säädetään asetuksen nojalla saatuja, vaihdettuja ja toimitettuja luottamuksellisia tietoja koskevasta salassapitovelvollisuudesta. Tiedot, jotka koskevat liiketoiminta- tai toimintaolosuhteita ja muita taloudellisia tai henkilökohtaisia asioita, on katsottava luottamuksellisiksi ja niihin on sovellettava salassapitovelvollisuutta koskevia vaatimuksia. Koska asetus on suoraan sovellettavaa oikeutta, ei kansalliseen lainsäädäntöön olisi näiden tietojen luovuttamisen osalta tarpeen tehdä muutoksia. Kyberturvallisuutta koskevan ajantasaisen tilannekuvan muodostamiseksi ja sektorit ylittävän koordinoinnin edistämiseksi Finanssivalvonnan on tärkeätä välittää saamansa häiriöilmoitukset ilman aiheetonta viivytystä Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen ja muiden keskeisten viranomaisten tietoon. Muita keskeisiä tahoja ovat ainakin rahoitusjärjestelmän kriisinhallinnan yhteistoiminta-asiakirjan osapuolet, joita Finanssivalvonnan ohella ovat valtiovarainministeriö, sosiaali- ja terveysministeriö, Suomen Pankki ja Rahoitusvakausvirasto.

Finanssivalvonnasta annetun lain 18 §:n 2 momentin säännöstä, jonka nojalla Finanssivalvonta voi antaa määräyksiä tiettyjen tietojen toimittamisesta, ei ole tarpeen muuttaa DORA-asetuksen johdosta. Mainitun säännöksen nojalla annettavissa määräyksissä on kuitenkin huomioitava, että finanssiyhteisöt ovat suoraan DORA-asetuksen 19 artiklan nojalla velvollisia raportoimaan laajavaikutteisista TVT:hen liittyvistä poikkeamista. Määräyksiin ei tule sisältyä asetuksen kanssa päällekkäisiä raportointivelvollisuuksia. Samalla DORA-asetus ei kuitenkaan estä antamasta muita raportointia koskevia määräyksiä 18 §:n 2 momentin tai muiden soveltuvien kansallisten säännösten nojalla. Finanssiyhteisöjen on asetuksen 17 artiklan 2 kohdan mukaan kirjattava kaikki TVT:hen liittyvät poikkeamat ja merkittävät kyberuhat. Erityisesti jos yleinen kyberturvallisuustilanne ja ajantasaisen tilannekuvan muodostaminen sitä edellyttää, voi olla perusteltua edellyttää määräyksissä finanssiyhteisöjä tai joitakin finanssiyhteisöjen tyyppejä raportoimaan Finanssivalvonnalle myös muista kuin laajavaikutteisista poikkeamista.

DORA-asetuksen 26 artiklan 9 kohdan mukaan jäsenvaltiot voivat nimetä rahoitusalan yhden viranomaisen, joka vastaa rahoitusalalla uhkaperusteiseen tunkeutumistestaukseen kansallisella tasolla liittyvistä asioista, ja antaa sille kaikki tätä koskevat toimivaltuudet ja tehtävät. Jos mainittua nimeämistä ei ole tehty ja rajoittamatta valtuuksia yksilöidä finanssiyhteisöt, joiden on suoritettava uhkaperusteinen tunkeutumistestaus, toimivaltainen viranomainen voi artiklan 10 kohdan nojalla siirtää joidenkin tai kaikkien DORA-asetuksen 26 ja 27 artiklassa tarkoitettujen tehtävien hoitamisen toiselle finanssialan kansalliselle viranomaiselle. Tältä osin asetus ei siis edellytä kansallista sääntelyä ja Finanssivalvonta voisi tehdä mainitun tehtäväsiirron suoraan DORA-asetuksen nojalla. Mahdollisella tehtäväsiirrolla olisi vaikutuksia resurssien kohdentamiseen ja siksi se olisi perusteltua toteuttaa yhteisymmärryksessä osapuolten kesken. Käytännössä asetuksessa tarkoitettu toinen finanssialan kansallinen viranomainen voisi olla Suomen Pankki, joka vastaa nykyisin TIBER-FI-toimintamallista. TIBER-FI on Suomen finanssialan toimijoiden käyttöön laadittu kehikko finanssialan kriittisten toimintojen toimintavarmuuden varmistamiseksi kohdennettujen kyberhyökkäysten varalta. Se perustuu Euroopan keskuspankin TIBER-EU-toimintamalliin finanssialan kyberturvallisuuden kehittämiseksi. TIBER-EU on

systemaattinen, kontrolloitu ja ajantasaiseen kyberturvallisuuden uhkatietoon pohjautuva toimintamalli Red Team -tietoturvatestausten suorittamiseksi. DORA-asetuksen nojalla Finanssivalvonta yksilöisi ne finanssiyhteisöt, joilta edellytetään uhkaperusteisen tunkeutumistestauksen tekemistä. Osana DORA-asetuksen noudattamisen valvontaa tulisi varmistaa, että kyseiset finanssiyhteisöt suorittavat testauksen vaatimusten mukaisesti. Viranomaisten on myös annettava finanssiyhteisöille todistus, jossa vahvistetaan, että testi on suoritettu viranomaiselle toimitetuissa asiakirjoissa osoitetun mukaisesti vaatimuksia noudattaen. Tämän kaltaiset tehtävät kuuluvat luontevasti valvovan viranomaisen eli Finanssivalvonnan vastuulle, kun taas Suomen Pankki vastaisi jatkossakin testauksessa käytettävän toimintamallin ylläpidosta.

3.4 Muut Finanssivalvonnasta annetun lain muutostarpeet

Verkko- ja tietoturvadirektiivi on kumottu NIS2-direktiivillä. Tämän vuoksi Finanssivalvonnasta annetun lain 50 p §:n ja 52 a §:n säännöksiä Finanssivalvonnan toimimisesta verkko- ja tietoturvadirektiivissä tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta ja Finanssivalvonnan velvollisuudesta tehdä yhteistyötä verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa Liikenne- ja viestintäviraston kanssa on tarpeen muuttaa. Finanssivalvonnan yhteistyö Liikenne- ja viestintäviraston ja sen Kyberturvallisuuskeskuksen kanssa olisi jatkossakin finanssimarkkinoiden kyberturvallisuuden ja häiriönsietokyvyn edistämisen kannalta keskeistä. Viranomaisyhteistyön merkitystä olisi perusteltua edelleen korostaa lainsäädännössä. Lisäksi säännöksissä on tarpeen huomioida CER-direktiivi sen liitteen toimialojen 3 ja 4 osalta. Vaikka CER-direktiivin velvoitteita ei sovelleta näiden toimialojen kriittisiin toimijoihin, direktiivi edellyttää erityisesti kriittisten toimijoiden tukemista niiden häiriönsietokyvyn parantamiseksi.

3.5 DORA-muutosdirektiivin edellyttämät muutokset kansalliseen lainsäädäntöön

Kuten edellä on todettu, finanssialan TVT-riskin hallintaan liittyvistä vaatimuksista säädetään tällä hetkellä useissa Euroopan parlamentin ja neuvoston direktiiveissä. Kyseiset vaatimukset, ja siten myös niiden täytäntöön panemiseksi annetut kansalliset säännökset, ovat vaihtelevia. DORA-muutosdirektiivissä säädetään muutoksista, joilla pyritään varmistamaan sääntelyn johdonmukaisuus DORA-asetuksen kanssa. Direktiivin säännösten johdosta tarpeelliset muutokset olisi tehtävä luottolaitostoiminnasta annettuun lakiin (610/2014), sijoituspalvelulakiin (747/2012), maksulaitoslakiin (297/2010), kaupankäynnistä rahoitusvälineillä annettuun lakiin (1070/2017), sijoitusrahastolakiin (213/2019), vaihtoehtorahastojen hoitajista annettuun lakiin (162/2014), lisäeläkesäätiöistä ja lisäeläkekassoista annettuun lakiin (947/2021) ja vakuutusyhtiölakiin (521/2008). Käytännössä näissä muutoksissa kyse on pääosin vaatimuksista hallinnoida verkko- ja tietojärjestelmiä DORA-asetuksen mukaisesti osana sisäistä hallintoa sekä riskienhallinnan menettelyjä. Lisäksi liiketoiminnan jatkuvuutta koskevia suunnitelmia koskevaa sääntelyä on luottolaitosten osalta luottolaitosdirektiivissä ja algoritmista kaupankäyntiä harjoittavan sijoituspalveluyrityksen ja säännellyn markkinan osalta MiFID II -direktiivissä täsmennetty siten, että näihin suunnitelmiin sisältyvät DORA-asetuksen mukaiset tieto- ja viestintätekniikan liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja suunnitelmat ja tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmat. Koska asetus on kyseessä oleviin finanssiyhteisöihin nähden suoraan sovellettavaa oikeutta, on tällainen sääntely luonteeltaan pääasiallisesti informatiivista, ja siten DORA-muutosdirektiivin täytäntöön panemiseksi olisi pääosin riittävää lisätä asianomaisiin lainkohtiin tarvittavat viittaukset DORA-asetukseen.

DORA-muutosdirektiivi edellyttää myös eräitä sisällöllisiä muutoksia kansalliseen lainsäädäntöön. Kuten edellä on todettu, luottolaitosdirektiiviä on muutettu siten, että toimivaltaisella viranomaisella tulee olla oikeus vaatia kaikkia tehtäviensä hoitamisen kannalta tarpeellisia tietoja

myös TVT-palveluntarjoajana olevilta kolmansilta osapuolilta. Tämä toteutettaisiin muuttamalla Finanssivalvonnasta annettua lakia. Lisäksi luottolaitosdirektiivin mukaista vakavaraisuuden arviointiprosessin soveltamisalaa on muutettu siten, että arvioinnissa on huomioitava DORA-asetuksen IV luvun mukaisen digitaalisen häiriönsietokyvyn testauksen paljastamat riskit. Luottolaitostoiminnasta annettua lakia olisi täsmennettävä tältä osin. Maksupalveludirektiivin 96 artiklan 1–5 kohdan poikkeamista raportointia koskevia säännöksiä ei jatkossa sovelleta DORA-asetuksen soveltamisalaan kuuluviin maksupalveluntarjoajiin. Maksulaitoslakia olisi muutettava tältä osin.

Seuraavassa kuvataan ne DORA-muutosdirektiivin kohdat, jotka eivät edellytä muutoksia kansalliseen lain tasoiseen sääntelyyn. Muilta osin lakiehdotusten yksityiskohtaisissa perusteluissa on kuvattu tarkemmin kunkin DORA-muutosdirektiivin kohdan täytäntöönpano.

DORA-muutosdirektiivin 7 artiklan 1 kohta, jolla käsite ”tietotekniikka” korvataan käsitteellä ”tieto- ja viestintätekniikka” maksupalveludirektiivin 3 artiklan j kohdan säännöksessä direktiivin soveltamisalan ulkopuolelle jätettävistä maksupalveluiden tarjoamista tukevista palveluista, ei edellytä muutoksia kansalliseen lainsäädäntöön. Soveltamisalan rajaus on tältä osin pantu täytäntöön maksulaitoslain yksityiskohtaisilla perusteluilla (HE 172/2009 vp., s. 30). Myöskään DORA-muutosdirektiivin 7 artiklan 3 kohta, jolla käsite ”tietotekninen järjestelmä” on korvattu käsitteellä ”tieto- ja viestintätekniikan järjestelmä” maksupalveludirektiivin 19 artiklan 6 kohdan toisessa alakohdassa, ei edellytä kansallisia täytäntöönpanotoimia. Tieto- ja viestintätekniikan järjestelmät mainitaan esimerkkinä tärkeästä operatiivisesta toiminnosta, jollaisen saa ulkoistaa ainoastaan tietyin edellytyksin. Kansalliseen lakiin tätä esimerkinomaista mainintaa ei ole sisällytetty.

DORA-muutosdirektiivin 5 artiklan 1 kohdan c alakohta ja 7 artiklan 6 kohta koskevat EPV:n teknisiä sääntelystandardeja, eivätkä ne siten edellytä muutoksia kansalliseen lainsäädäntöön. Direktiivin 5 artikla, sen 1 kohdan c alakohtaa lukuun ottamatta, ja 7 artiklan 2 kohta puolestaan koskevat asioita, joista säädetään kansallisesti asetustasoisesti. Luvussa 7 (Lakia alemman asteinen sääntely) on kuvattu direktiivin edellyttämiä muutoksia kansalliseen asetustasoiseen sääntelyyn.

Siltä osin kuin DORA-muutosdirektiivillä muutetaan tiettyjä valtuutuksia antaa delegoituja säädöksiä ja täytäntöönpanosäädöksiä poistamalla TVT-riskiä koskevat säännökset kyseisten valtuutuksien soveltamisalasta (direktiivin 1 artiklan 2 kohta, 2 artiklan 2 kohta, 3 artikla AIFM-direktiivin 18 artiklan 2 kohdan osalta sekä 6 artiklan 2 kohdan b alakohta ja 4 kohdan c alakohta), direktiivistä ei aiheudu muutostarpeita kansalliseen lainsäädäntöön.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Finanssivalvonnasta annettuun lakiin ehdotetaan tehtävän DORA-asetuksesta aiheutuvat muutokset sekä NIS2- ja CER-direktiivien kansallista täytäntöönpanoa täydentävät muutokset. Laissa säädettäisiin Finanssivalvonnan toimimisesta DORA-asetuksen tarkoittamana toimivaltaisena viranomaisena sekä NIS2-direktiivin ja CER-direktiivin tarkoittamana toimivaltaisena viranomaisena pankkitoiminnan ja rahoitusmarkkinoiden infrastruktuurin osalta.

Finanssivalvonnan yleistehtävää täydentäviä erityisiä tehtäväalueita ehdotetaan täydennettävän tehtävillä edistää finanssimarkkinoilla toimivien kyberturvallisia toimintatapoja sekä edistää kriittisten toimijoiden häiriönsietokykyä.

Finanssivalvonnan velvollisuudet toimia yhteistyössä muiden viranomaisten kanssa kyberturvallisuuden edistämiseksi kansallisella tasolla sekä EU-säädösten nojalla perustettujen EU:n laajuisten yhteistyöjärjestelyjen puitteissa ehdotetaan koottavan uuteen pykälään.

Finanssivalvonnasta annetun lain hallinnollisia seuraamuksia koskevia säännöksiä ehdotetaan täydennettävän DORA-asetuksen johdosta. Finanssivalvonta voisi määrätä seuraamusmaksun sille, joka laiminlyö tai rikkoo DORA-asetuksen mukaisen velvoitteensa. Asetuksen mukaisen yksinkertaistettua TVT-riskienhallintajärjestelmää koskevan velvoitteen laiminlyönnin tai rikkomisen johdosta voitaisiin määrätä rikemaksu. Laissa tarkoitettujen muiden finanssimarkkinoilla toimivien joukkoon lisättäisiin DORA-asetuksessa tarkoitettu TVT-palveluntarjoajana oleva kolmas osapuoli, jolloin Finanssivalvonnan yleiset toimivaltuudet ulottuisivat myös näihin toimijoihin.

Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annettua lakia (291/1979) ja valtion erityisrahoitusyhtiöstä annettua lakia (443/1998) muutettaisiin siten, että Teollisen yhteistyön rahasto Oy ja Finnvera Oyj jätettäisiin DORA-asetuksen soveltamisalan ulkopuolelle.

Lisäksi esityksellä pantaisiin täytäntöön DORA-muutosdirektiivi. Luottolaitostoiminnasta annettuun lakiin, sijoituspalvelulakiin, maksulaitoslakiin, kaupankäynnistä rahoitusvälineillä annettuun lakiin, sijoitusrahastolakiin, vaihtoehtorahastojen hoitajista annettuun lakiin, lisäeläkesäätiöistä ja lisäeläkekassoista annettuun lakiin ja vakuutusyhtiölakiin ehdotetaan tehtävän direktiivin edellyttämät muutokset.

4.2 Pääasialliset vaikutukset

Taloudelliset vaikutukset

DORA-asetus on Suomessa suoraan sovellettavaa oikeutta ja asetuksen soveltamisalaan kuuluvat finanssiyhteisöt ovat velvoitettuja noudattamaan asetuksen sääntelyä ilman erillisiä kansallisia täytäntöönpanotoimia. Finanssiyhteisöihin kohdistuvat toiminnalliset ja taloudelliset vaikutukset aiheutuvat siten pääosin suoraan asetuksen sääntelystä. Tässä hallituksen esityksessä ehdotetut säännökset täydentävät DORA-asetusta erityisesti Finanssivalvonnan tehtävien, toimivaltuuksien ja hallinnollisten seuraamusten määräämisen osalta. Esityksessä ei ehdoteta DORA-asetuksen soveltamisalaan kuuluville toimijoille uusia tai asetuksen säännöksiä pidemmälle meneviä velvoitteita. Tässä yhteydessä kuvataan kuitenkin lyhyesti EU-sääntelystä toimijoille aiheutuvia vaikutuksia.

DORA-asetuksen merkittävimmät taloudelliset vaikutukset kohdistuvat finanssialalla toimiviin yrityksiin, finanssialan toiminnan valvojiin ja TVT-palveluita finanssialalle tuottaviin kolmansiin osapuoliin. Taloudellisia vaikutuksia saattaa arvion mukaan kohdistua myös finanssialan toimijoiden asiakkaisiin, sijoittajiin ja kuluttajiin. Sääntelystä aiheutuvat taloudelliset vaikutukset voivat olla kertaluonteisia tai jatkuvia. Suomessa asetuksen soveltamisalaan ja näin ollen myös hallituksen esityksen vaikutuspiiriin kuuluu satoja erilaisia, eri kokoisia ja muutenkin rakenteeltaan ja liiketoiminnaltaan erilaisia toimijoita.

Suomessa finanssialan kyberriskeihin varautuminen ja niiden huomioiminen on yleisesti ottaen hyvällä tasolla. Finanssialan toimijat on velvoitettu ottamaan huomioon kyberriskit osana operatiivisen riskin hallintaa ja näihin velvoitteisiin on jo vastattu kehittämällä toimenpiteitä kyberriskeihin varautumista varten. Osa DORA-asetuksen vaatimuksista on kuitenkin uusia tai minimitasoa tarkentavia, jolloin tarvittavat tietotekniikkajärjestelmiin kohdistuvat päivitykset ja

muut muutokset voivat aiheuttaa niitä käyttäville yrityksille kertaluontoisia kustannuksia. Lisäksi erityisesti vakuutusedustajille vaatimukset ovat täysin uusia, sillä vakuutusedustajien operatiivista riskien hallintaa ei aikaisemmin ole säännelty. Tarkkaa arviota kustannusten määrästä on vaikea antaa, sillä toimijoille aiheutuvat kustannukset riippuvat pääasiassa siitä, millä tasolla heidän vanhat TVT-järjestelmänsä ovat DORA-asetuksen vaatimuksiin verrattuna. Kustannukset tulevat kuitenkin Suomessa olemaan todennäköisesti kohtuullisia, sillä suurten toimijoiden TVT-järjestelmien voidaan lähtökohtaisesti olettaa olevan pitkälti jo vaatimusten mukaisia ja pienempiin toimijoihin sovelletaan suhteellisuusperiaatteen mukaisesti lievempiä vaatimuksia.

DORA-asetuksen tarkoituksena on yksinkertaistaa ja yhdenmukaistaa TVT-järjestelmien testausvaatimuksia ja TVT-riskitapahtumien raportointia unionin alueella. Euroopan valvontaviranomaiset ovat arviossaan todenneet, että uhkaperusteiseen tunkeutumistestaukseen liittyvien jatkuvien kustannusten osuus tulisi olemaan asianomaisten yritysten TVT-kokonaisbudjetista 0,1–0,3 prosenttia. Yhdenmukaisista testauskäytännöistä hyötyisivät erityisesti rajatylittävät pankit, joista 44 suurimpaa voisivat saavuttaa jopa 11–88 miljoonan euron hyödyn vuositasolla. Päällekkäisten riskitapahtumien raportointivaatimuksien poistaminen puolestaan keventäisi etenkin suurten pankkien hallinnollista taakkaa, joka voisi tuoda niille unionin tasolla säästöjä 40–100 miljoonaa euroa vuodessa.

DORA-asetuksen implementoinnin arvioidaan vähentävän kyberhäiriötilanteista aiheutuvia suoria kustannuksia ja mahdollisesti laajempia rahoitusvakautta koskevia negatiivisia vaikutuksia. Komission mukaan arviolta yksi viidestä kyberriskitilanteesta tapahtuu finanssisektorilla, ja EU:n osuuden maailmantaloudesta ollessa noin 21 % voivat kybertapahtumista aiheutuvat negatiiviset vaikutukset unionin tasolla olla vuodessa useita miljardeja Yhdysvaltain dollareita. Soveltamalla näitä komission arvioita ja oletuksia voidaan todeta, että vuonna 2018 kybertapahtumien negatiivisten vaikutusten summa Suomessa oli arviolta 2,9–39 miljoonaa Yhdysvaltain dollaria. Samaa kaavaa soveltamalla, mikäli vaikutuksista saataisiin vähennettyä kymmenenkin prosenttia, tarkoittaisi se Suomelle 0,29–3,9 miljoonan Yhdysvaltain dollarin vuosittaista säästöä. Komission arvion mukaan kymmenen prosentin vähennys on realistinen, mutta todennäköisesti vaikutus tulee olemaan vieläkin suurempi.

DORA-asetuksen velvoitteista aiheutuvien valvontaviranomaisten lisätehtävien arvioidaan aiheuttavan asianomaisille viranomaisille vähäisiä kustannuksia henkilöstön lisäämisen johdosta. Työmäärää voi lisätä esimerkiksi häiriöilmoitusten kasvava määrä. Komission arvion mukaan TVT-palveluntarjoajana olevien kolmansien osapuolten valvonnasta aiheutuvien tehtävien johdosta johtavan viranomaisen kokoaikaisten työntekijöiden määrä tulee kasvamaan 1–5 työntekijän verran ja osallistuvien viranomaisten vastaavasti keskimäärin 0,25 työntekijän verran.

TVT-palveluita finanssialalle tarjoavien kolmansien osapuolten toiminta saattaa arvion mukaan olla DORA-asetuksen taloudellisten vaikutusten piirissä sen seurauksena, että valvontaviranomaiset velvoittavat heitä muuttamaan järjestelmiään DORA-asetuksen velvoitteiden mukaisiksi. Kolmansien osapuolien tulee myös sopeuttaa organisaatiotaan toimintansa valvonnan mahdollistamiseksi siten, että se sopii DORA-asetuksen velvoitekehikkoon, josta tulee koitumaan kustannuksia. Komission arvion mukaan nämä kustannukset tulisivat kuitenkin pysymään kohtuullisina, etenkin mikäli horisontaalinen ja alakohtainen valvontajärjestelmä TVT-palveluntarjoajina toimiville kolmansille osapuolille syntyy tulevaisuudessa.

Finanssialan toimijoiden asiakkaat, sijoittajat ja kuluttajat voivat olla marginaalisten taloudellisten vaikutusten piirissä. Arvion mukaan on mahdollista, että finanssialalla toimivat yritykset rahoittavat osan DORA-asetuksen implementoinnista aiheutuvista kustannuksista lopulta erilaisina asiakas- ja palvelumaksujen korotuksina.

Vaikutukset viranomaisten toimintaan

Hallituksen esityksellä ei arvioida olevan merkittäviä vaikutuksia Finanssivalvonnan toimintaan. Finanssivalvonta hoitaisi tehtävät nykyisten resurssiensa puitteissa, uudelleenkohdentamalla tarvittaessa olemassa olevia resursseja DORA-asetuksesta aiheutuvien tehtävien hoitamiseen, ja päättäisi asetuksen mukaisten velvoitteiden valvonnan tarkemmasta toteuttamisesta ja kulloisistakin painopisteistä. Ehdotuksilla täsmennetään Finanssivalvonnalle jo nykyisen verkko- ja tietoturvadirektiivin mukaisena toimivaltaisena viranomaisena kuuluvia velvoitteita. Myös viranomaisyhteistyö kansallisella ja kansainvälisellä tasolla kuuluu Finanssivalvonnan tehtäviin jo nykyisin. DORA-asetuksen viranomaisyhteistyötä ja tietojenvaihtoa koskevat säännökset asettavat kuitenkin myös Finanssivalvonnan toiminnalle aiempaa yksityiskohtaisempia vaatimuksia esimerkiksi uusien EU-tason yhteistyörakenteiden muodossa. Finanssivalvonnan edustaja muun muassa osallistuisi kriittisten TVT-palveluntarjoajina olevien kolmansien osapuolten valvontakehykseen sisältyvän valvontafoorumin toimintaan sekä tarpeen mukaan NIS2-direktiivin mukaisen yhteistyöryhmän toimintaan.

Tämän esityksen mukaisten viranomaisyhteistyötä koskevien ehdotusten tavoitteena on korostaa aktiivisen viranomaisyhteistyön merkitystä kyberturvallisuuteen liittyvien tehtävien tuloksellisen hoitamisen kannalta ja selkeyttää Finanssivalvonnan ja muiden viranomaisten välisen yhteistyön järjestämistä. Viime kädessä yhteistyön muodot ja tarkemmat toteuttamistavat jäisivät Finanssivalvonnan ja muiden yhteistyöhön osallistuvien viranomaisten kesken määritettäviksi, siltä osin kuin yhteistyöstä ei ole tarkemmin erikseen säädetty. Kyberturvallisuuden sektorit ylittävän koordinoinnin edistämiseksi Finanssivalvonnan on erityisen tärkeätä välittää saamansa häiriöilmoitukset ilman aiheetonta viivytystä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tietoon.

Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

DORA-asetuksen implementoinnin myötä yleisen luottamuksen rahoitusmarkkinoihin voidaan arvioida kasvavan, joka hyödyttää lopulta kaikkia markkinaosapuolia. Digitaaliseen häiriönsietokykyyn liittyvien vaatimusten ollessa yhtenäisiä koko unionin alueella, säilyy sijoittajien luottamustaso finanssialan toimijoiden vakauteen arvioidusti korkealla ja halukkuus sijoittaa kyberturvallisuuden ylläpidon ja kehittämisen kannalta tärkeisiin ratkaisuihin vahvana.

Digitaalisen häiriönsietokyvyn ylläpitäminen ja kehittäminen finanssialan toimijoiden keskuudessa varmistaa myös vahvan kuluttajien ja sijoittajien suojan. Kun alan toimijat pystyvät suojelemaan itseään kyberhyökkäyksiltä ja -häiriöiltä, pystyvät ne myös varmistamaan arkipäiväisten toimintojensa jatkuvuuden ja asiakkaiden ja sijoittajien tehokkaan palvelun, sekä heidän tietojensa ja varojensa suojaamisen.

5 Muut toteuttamisvaihtoehdot

Toimivaltaisen viranomaisen valtuudet ja hallinnolliset seuraamukset

DORA-asetuksen 50 artikla edellyttää edellä tarkemmin kuvatulla tavalla, että toimivaltaisilla viranomaisilla on oltava kaikki asetuksen mukaisten tehtäviensä hoitamiseen tarvittavat valtuudet valvoa, tutkia ja määrätä seuraamuksia. Jäsenvaltioiden on vahvistettava säännöt, jotka koskevat asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, ja varmistettava niiden tehokas täytäntöönpano. Seuraamusten ja toimenpiteiden on oltava tehokkaita, oikeasuhteisia ja varoittavia. Lisäksi asetuksen 51 artiklan 1 kohdassa to-

detaan, että toimivaltaisten viranomaisten on käytettävä valtuuksiaan määrätä 50 artiklassa tarkoitettuja hallinnollisia seuraamuksia ja korjaavia toimenpiteitä kansallisen oikeudellisen kehyksensä mukaisesti. Asetuksen 52 artiklan mukaan jäsenvaltiot voivat päättää, että ne eivät säädä hallinnollisia seuraamuksia tai korjaavia toimenpiteitä koskevia sääntöjä sellaisten rikkomisten osalta, joihin sovelletaan niiden kansallisen lainsäädännön mukaisia rikosoikeudellisia seuraamuksia.

DORA-asetuksen 50–52 artiklan asettamissa puitteissa on jäsenvaltioiden tarkemmassa harkinnassa, miten valvontavaltuuksista säädetään. Tässä esityksessä omaksutun lähtökohdan mukaisesti pyritään nykyiseen nähden mahdollisimman vähäiseen lisäsääntelyyn. Asetuksen tarkoittama toimivaltainen viranomainen on Suomessa Finanssivalvonta. Finanssivalvonnasta annettu laki sisältää kattavat säännökset Finanssivalvonnan valvontavaltuuksista, joiden arvioidaan täyttävän asetuksen edellytykset. Hallituksen esityksessä ei näin ollen esitetä Finanssivalvonnalle uudenlaisia valvontavaltuuksia. TVT-palveluntarjoajana olevan kolmannen osapuolen sisällyttäminen Finanssivalvonnasta annetussa laissa tarkoitettujen muiden finanssimarkkinoilla toimivien joukkoon olisi sääntelyteknisesti yksinkertaisin tapa ulottaa tarvittavat Finanssivalvonnan valvontavaltuudet myös näihin toimijoihin.

Finanssivalvonnan rikemaksua ja seuraamusmaksua koskevissa säännöksissä luetellaan ne säännökset, joiden laiminlyönnin tai rikkomisen seurauksena kyseinen seuraamus voidaan määrätä. Näitä säännöksiä olisi täydennettävä siten, että seuraamus voidaan määrätä DORA-asetuksen asianomaisten säännösten laiminlyönnin tai rikkomisen johdosta. Ilman nimenomaisia säännöksiä Finanssivalvonta ei voisi määrätä muuta hallinnollista seuraamusta kuin Finanssivalvonnasta annetun lain 39 §:n mukaisen julkisen varoituksen. Tätä ei voitaisi pitää riittävänä, sillä DORA-asetus edellyttää myös taloudellisten seuraamusten olemassaoloa. Hallituksen esityksessä ehdotetaan, että Finanssivalvonta voisi määrätä seuraamusmaksun DORA-asetuksen 5–15, 17–19, 24–27 tai 28–30 artiklan laiminlyönnin tai rikkomisen johdosta. Sääntelyn oikeasuhtaisuutta turvaa osaltaan se, että Finanssivalvonta voi seuraamusmaksun määräämisen sijaan antaa julkisen varoituksen, jos virheellistä menettelyä on pidettävä vähäisenä. Asetuksen 16 artiklan mukaisen yksinkertaistettua TVT-riskinhallintajärjestelmää koskevan sääntelyn laiminlyönnin tai rikkomisen johdosta taas voitaisiin määrätä lievempi seuraamus, eli rikemaksu. Vaihtoehtoisia sääntelytapoja olisivat esimerkiksi DORA-asetuksen mukaisten velvoitteiden rikkomisen asettaminen kokonaisuudessaan pelkästään rikemaksun alaiseksi tai myös yksinkertaistettua TVT-riskinhallintajärjestelmää koskevan velvoitteen rikkomisen asettaminen seuraamusmaksun alaiseksi. Hallituksen esityksen mukaisen toteuttamistavan arvioidaan kuitenkin parhaiten turvaavan yhtäältä sääntelyn tehokkuuden ja varoittavuuden, ja toisaalta oikeasuhteisuuden. DORA-asetuksen mukaisten velvoitteiden rikkomista ei ehdoteta säädettävän rikosoikeudellisesti rangaistavaksi, sillä asetus ei tätä edellytä ja hallinnollisten seuraamusten voidaan arvioida olevan riittäviä.

Raportointi tieto- ja viestintätekniikkaan liittyvistä poikkeamista

Finanssiyhteisöjen on raportoitava laajavaikutteisista TVT:hen liittyvistä poikkeamista toimivaltaiselle viranomaiselle DORA-asetuksen 19 artiklan mukaisesti. Artiklan 1 kohdan kuudennen alakohdan mukaan jäsenvaltiot voivat lisäksi päättää, että joidenkin tai kaikkien finanssiyhteisöjen on myös toimitettava artiklassa tarkoitetut ilmoitukset ja raportit NIS2-direktiivin mukaisesti nimetyille tai perustetuille tietoturvaloukkauksiin reagoiville ja niitä tutkiville CSIRT-yksiköille. NIS2-direktiivin mukaisena CSIRT-yksikkönä Suomessa toimii Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Finanssiyhteisöt voitaisiin siis velvoittaa raportoimaan poikkeamista Finanssivalvonnan ohella Kyberturvallisuuskeskukselle, jolloin poikkeamailmoi-

tukset tulisivat sen tietoon samanaikaisesti Finanssivalvonnan kanssa. Päällekkäisten raportointivelvoitteiden välttämiseksi, ja koska toimivaltaisen viranomaisen on joka tapauksessa hyvissä ajoin toimitettava laajavaikutteista TVT:hen liittyvää poikkeamaa koskevat yksityiskohtaiset tiedot myös CSIRT-yksikölle, hallituksen esityksessä ei ehdoteta otettavan käyttöön mainittua lisäraportointivelvoitetta.

DORA-asetuksen 19 artiklan 2 kohdan kolmannen alakohdan mukaan jäsenvaltiot voivat päättää, että ne finanssiyhteisöt, jotka ilmoittavat vapaaehtoisesti merkittävästä kyberuhasta, voivat toimittaa kyseisen ilmoituksen myös CSIRT-yksikölle. Hallituksen esitykseen ei sisälly tätä koskevia ehdotuksia, eikä asiasta ylipäätään ole tarpeen säätää lain tasolla.

Luottolaitosdirektiivin nojalla vapautetut laitokset

DORA-asetuksen 2 artiklan 4 kohdan mukaan jäsenvaltiot voivat jättää asetuksen soveltamisalan ulkopuolelle luottolaitosdirektiivin 2 artiklan 5 kohdan 4–23 alakohdassa tarkoitetut yhteisöt, jotka sijaitsevat niiden alueella. Jos jäsenvaltio päättää olla soveltamatta asetuksen 2 artiklan 4 kohdassa tarkoitettua vaihtoehtoa, tällaiseen yhteisöön sovelletaan asetuksen 16 artiklan mukaista yksinkertaistettua TVT-riskinhallintajärjestelmää. Lisäksi asetuksen 46 artiklan perusteella luottolaitosdirektiivin mukaisen toimivaltaisen viranomaisen, Suomessa Finanssivalvonnan, on näiden toimijoiden osalta varmistettava asetuksessa säädettyjen velvoitteiden noudattaminen asiaa koskevissa säädöksissä annettujen valtuuksien mukaisesti. Suomen osalta tämä optio koskee Teollisen yhteistyön rahasto Oy:tä ja Finnvera Oyj:tä. Teollisen yhteistyön rahasto Oy eli Finnfund kuuluu ulkoministeriön hallinnonalaan ja sen toiminnasta säädetään Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annetussa laissa. Finnvera Oyj puolestaan kuuluu työ- ja elinkeinoministeriön hallinnonalaan ja sen toiminnasta säädetään valtion erityisrahoitusyhtiöstä annetussa laissa. Kumpaankaan toimijaan ei sovelleta luottolaitostoiminnasta annettua lakia eikä Finanssivalvonta nykyisin valvo niiden toimintaa.

Hallituksen esityksessä esitetään käytettävän mainittu jäsenvaltio-optio. Teollisen yhteistyön rahasto Oy ja Finnvera Oyj jätettäisiin siis DORA-asetuksen soveltamisalan ulkopuolelle. Jos jäsenvaltio-optiota ei käytettäisi, tulisi tässä yhteydessä säätää Finanssivalvonnan tehtävästä valvoa DORA-asetuksessa säädettyjen velvoitteiden noudattamista Teollisen yhteistyön rahasto Oy:n ja Finnvera Oyj:n osalta sekä tähän liittyvistä tarpeellisista valvontavaltuuksista ja toimijoilta perittävistä valvontamaksuista. Erillisten valvontajärjestelyjen luomista yksittäisen säädöksen osalta ei voida pitää tarkoituksenmukaisena, vaan mainittuihin toimijoihin kohdistettavaa ohjausta ja valvontaa tulee arvioida kokonaisuutena niitä koskevan lainsäädännön uudistamisen yhteydessä. Sekä Teollisen yhteistyön rahasto Oy:n että Finnvera Oyj:n osalta on parhaillaan käynnissä lainsäädännön uudistamista koskevat hankkeet, joiden yhteydessä voidaan asiallisesti arvioida DORA-asetuksen soveltamista näihin toimijoihin. Omistajaohjauksen keinoin voidaan myös huolehtia laadultaan ja laajuudeltaan DORA-asetuksen mukaisia velvoitteita vastaavien TVT-riskinhallintamenettelyjen noudattamisesta Teollisen yhteistyön rahasto Oy:n ja Finnvera Oyj:n toiminnassa siitä huolimatta, että ne eivät kuuluisi asetuksen soveltamisalaan.

Uhkaperusteista tunkeutumistestausta koskevat toimivaltuudet ja tehtävät

DORA-asetuksen 26 artiklan 9 kohdan mukaan jäsenvaltiot voivat nimetä rahoitusalan yhden viranomaisen, joka vastaa rahoitusalalla uhkaperusteiseen tunkeutumistestaukseen kansallisella tasolla liittyvistä asioista, ja antaa sille kaikki tätä koskevat toimivaltuudet ja tehtävät. Jos mainittua nimeämistä ei ole tehty ja rajoittamatta valtuuksia yksilöidä finanssiyhteisöt, joiden on suoritettava uhkaperusteinen tunkeutumistestaus, toimivaltainen viranomainen voi artiklan 10

kohdan nojalla siirtää joidenkin tai kaikkien DORA-asetuksen 26 ja 27 artiklassa tarkoitettujen tehtävien hoitamisen toiselle finanssialan kansalliselle viranomaiselle.

DORA-asetus ei siis tältä osin edellytä kansallista sääntelyä. Hallituksen esityksessä ei ehdoteta tehtävän DORA-asetuksen 26 artiklan 9 kohdan mukaista nimeämistä. Käytännössä asetuksessa tarkoitettu toinen finanssialan kansallinen viranomainen voisi Suomen tapauksessa olla Suomen Pankki, joka vastaa nykyisin TIBER-FI-toimintamallista, joten vaihtoehtoinen ratkaisu olisi säätää uhkaperusteiseen tunkeutumistestaukseen kansallisella tasolla liittyvät asiat Suomen Pankin tehtäväksi. Kuten edellä on kuvattu, uhkaperusteista tunkeutumistestausta koskevien valvontatehtävien olisi lähtökohtaisesti perusteltua kuulua Finanssivalvonnan vastuulle. Ehdotettu toteuttamistapa on myös joustavampi ja mahdollistaa tarpeen mukaan asian myöhemmän uudelleen tarkastelun ilman tarvetta kaikissa tapauksissa muuttaa lakia.

6 Lausuntopalaute

[täydennetään lausuntokierroksen jälkeen]

7 Säännöskohtaiset perustelut

7.1 Laki Finanssivalvonnasta annetun lain muuttamisesta

3 §. *Tehtävät.* Voimassa olevassa pykälässä säädetään Finanssivalvonnan tehtävistä. Pykälän 1 momentissa säädetään Finanssivalvonnan yleistehtävästä valvoa finanssimarkkinoilla toimivien toimintaa niin kuin tässä laissa ja muualla laissa säädetään sekä edistää lisäksi hyvien menettelytapojen noudattamista finanssimarkkinoilla sekä yleisön tietämystä finanssimarkkinoista. Yleistehtävää täydentävät 2 ja 3 momentin säännökset Finanssivalvonnan erityisistä tehtäväalueista. Finanssivalvonnan tehtäviin kuuluu muun ohella osallistua viranomaisten väliseen kotimaiseen yhteistyöhön, sekä osallistua paitsi Euroopan finanssivalvontajärjestelmän puitteissa tapahtuvaan yhteistyöhön Euroopan unionissa, myös muuhun viranomaisten kansainväliseen yhteistyöhön.

Rahoitusmarkkinoiden kyberturvallisuuden ja häiriönsietokyvyn kasvavan yhteiskunnallisen merkityksen ja niitä koskevan EU-lainsäädännön johdosta Finanssivalvonnan tehtäviä on syytä täsmentää erityisillä tehtävillä edistää finanssimarkkinoilla toimivien kyberturvallisia toimintatapoja sekä edistää kriittisten toimijoiden häiriönsietokykyä. Rahoitusmarkkinat ovat yhteiskunnallisesti merkittävä instituutio, jonka muuttuvaa yhteiskunnallista merkitystä kuvastaa yhä etenevä digitalisoituminen ja tieto- ja viestintäteknisten ratkaisujen kriittinen merkitys finanssipalvelujen tarjoamisen kannalta, vakavan verkkorikollisuuden aiheuttamien riskien kasvu, sekä Suomen turvallisuusympäristön muutos. Näistä syistä kaikkien finanssimarkkinoilla toimivien kyberturvallisuuden korkea taso sekä kriittisiksi määriteltyjen toimijoiden häiriönsietokyvyn parantaminen ovat yhteiskunnallisesti aiempaa yhä tärkeämpiä tavoitteita. Kyse olisi luonteeltaan tehtävistä, joiden tarkempi sisältö ja niihin liittyvät Finanssivalvonnan toimivaltuudet määräytyvät sen mukaan, mitä niistä muualla lainsäädännössä säädetään.

Ehdotetun uuden 6 a kohdan mukaan Finanssivalvonnan tehtävänä olisi edistää finanssimarkkinoilla toimivien kyberturvallisia toimintatapoja. Ehdotetun 50 p §:n 1 momentin mukaan Finanssivalvonta toimisi DORA-asetuksen 46 artiklan tarkoittamana toimivaltaisena viranomaisena. Finanssivalvonnan tehtävä DORA-asetusta valvovana ja sen mukaisiin yhteistyöjärjestelyihin osallistuvana viranomaisena on keskeisin osa kyberturvallisten toimintatapojen edistämistä. Lisäksi Finanssivalvonta on NIS2-direktiivin 8 artiklan 1 kohdassa tarkoitettu toimivaltainen viranomainen pankkialan ja rahoitusmarkkinoiden infrastruktuurin osalta. Valvontateh-

tävänsä ohella Finanssivalvonta edistää kyberturvallisuutta muun muassa ylläpitämällä ja jakamalla tilannekuvaa tietoturvapoikkeamista ja kyberhyökkäyksistä sekä osallistumalla huoltovarmuusorganisaation toimintaan. Muun muassa parhaiden käytäntöjen, kyberturvallisuusosaamisen ja uudenlaisia kyberuhkia koskevan ajantasaisimman tiedon vastavuoroinen jakaminen yli toimialarajojen tehostaa voimavarojen käyttöä ja hyödyttää siten myös finanssimarkkinoiden toimijoita.

Ehdotetun uuden 6 b kohdan mukaan Finanssivalvonnan tehtävänä olisi edistää finanssimarkkinoiden kriittisten toimijoiden häiriönsietokykyä. Finanssivalvonta on CER-direktiivin 9 artiklan 1 kohdan tarkoittama toimivaltainen viranomainen pankkialan ja rahoitusmarkkinoiden infrastruktuurin osalta. CER-direktiivin 10 artikla edellyttää kriittisten toimijoiden tukemista niiden häiriönsietokyvyn parantamiseksi ja niiden välisen tiedonvaihdon edistämiseksi. Direktiivin 9 artiklan 5 kohdan ja 10 artiklan 3 kohdan mukaan toimivaltaisen viranomaisen on tarvittaessa kuultava kriittisiä toimijoita ja asianomaisia osapuolia ja tehtävä yhteistyötä niiden kanssa.

Ehdotettujen uusien tehtävien kannalta keskeistä olisi kyberturvallisuuden edistämiseksi tehtävä viranomaisyhteistyö, josta säädettäisiin tarkemmin lakiin ehdotetussa uudessa 3 f §:ssä, sekä asianomaisten viranomaisten välinen tietojenvaihto.

3 f §. *Viranomaisyhteistyö kyberturvallisuuden edistämiseksi.* Lakiin ehdotetaan lisättäväksi uusi 3 f §, johon koottaisiin Finanssivalvonnan velvollisuudet toimia yhteistyössä muiden viranomaisten kanssa kyberturvallisuuden edistämiseksi kansallisella tasolla sekä EU-säädösten nojalla perustettujen EU:n laajuisten yhteistyöjärjestelyjen puitteissa. Viranomaisyhteistyö kansallisella ja kansainvälisellä tasolla kuuluu Finanssivalvonnan tehtäviin jo nykyisin. Pykälän tavoitteena on korostaa aktiivisen viranomaisyhteistyön merkitystä kyberturvallisuuteen liittyvien tehtävien tuloksellisen hoitamisen kannalta ja selkeyttää Finanssivalvonnan ja muiden viranomaisten välisen yhteistyön järjestämistä. Viranomaisyhteistyössä on keskeistä DORA-asetuksen mukainen yhteistyö, mukaan lukien yhteistyö NIS2-direktiivillä perustettujen rakenteiden ja viranomaisten kanssa, kansallisella tasolla erityisesti toiminta Liikenne- ja viestintäviraston yhteydessä toimivan kyberturvallisuuskeskuksen ja sen CSIRT-toiminnon kanssa. Muita tarpeellisia yhteistyötahoja voivat olla muun muassa NIS2-direktiivin mukaiset toimivaltaiset viranomaiset muilla direktiivin mukaisilla toimialoilla, asianomaiset ministeriöt, Suomen Pankki, huoltovarmuuskeskus, sekä Euroopan valvontaviranomaiset ja muut kyberturvallisuuden edistämiseen osallistuvat EU-viranomaiset ja ETA-valtioiden toimivaltaiset viranomaiset. Yhteistyöhön kuuluu olennaisesti myös viranomaisten välinen tietojenvaihto, jossa jaettavat tiedot voisivat sisältää esimerkiksi tietoja tietoturvallisuuteen liittyvistä häiriöistä ja parhaista käytännöistä häiriöiden ehkäisemiseksi ja niihin vastaamiseksi.

Pykälän 1 momentissa ehdotetaan säädettäväksi yleisesti Finanssivalvonnan velvollisuudesta toimia tieto- ja viestintätekniikkaan liittyvien häiriöiden hallitsemiseksi ja vaikutusten pienentämiseksi yhteistyössä valtiovarainministeriön, sosiaali- ja terveysministeriön, Suomen Pankin, Rahoitusvakausviraston, Liikenne- ja viestintäviraston ja muiden asianomaisten viranomaisten kanssa. Ehdotettu säännös täydentää Finanssivalvonnasta annetun lain 3 §:n 3 momentin 6 kohdan mukaista Finanssivalvonnan yleistä velvoitetta osallistua viranomaisten väliseen kotimaiseen yhteistyöhön. Yhteistyön muodot ja tarkemmat toteuttamistavat jäisivät Finanssivalvonnan ja muiden yhteistyöhön osallistuvien viranomaisten kesken määritettäviksi, siltä osin kuin yhteistyöstä ei ole tarkemmin erikseen säädetty.

Pykälän 2 momentissa ehdotetaan säädettäväksi Finanssivalvonnan osallistumisesta DORA-asetuksen 32 ja 47–49 artiklan mukaiseen yhteistyöhön. DORA-asetuksen 32 artiklassa säädе-

tään kriittisten TVT-palvelutarjoajina olevien kolmansien osapuolten valvontakehyksestä. Finanssivalvonta osallistuisi valvontakehykseen kuuluvan valvontafoorumin toimintaan ja nimettäisiin toimivaltaiseksi viranomaiseksi 32 artiklan 5 kohdan mukaisesti. DORA-asetuksen 47 artiklassa säädetään yhteistyöstä NIS2-direktiivillä perustettujen rakenteiden ja viranomaisten kanssa kansallisella ja EU-tasolla. Finanssivalvonta voi osallistua NIS2-direktiivissä tarkoitetun yhteistyöryhmän toimintaan asioissa, jotka koskevat sen valvontatoimia finanssilaitosten osalta. Finanssivalvonta voi myös tarvittaessa kuulla NIS2-direktiivin mukaisesti nimettyjä viranomaisia, kansallisesti siis Liikenne- ja viestintävirastoa ja sen yhteydessä toimivaa kyberturvallisuuskeskusta, sekä vaihtaa tietoja niiden kanssa, pyytää tarpeellista teknistä neuvontaa ja sopia yhteistyöjärjestelyjä. Lisäksi DORA-asetuksen 48–49 artiklassa säädetään muista kansainvälisen viranomaisyhteistyön muodoista. Toimivaltaisten viranomaisten, Euroopan valvontaviranomaisten ja EKP:n on tehtävä tiivistä yhteistyötä keskenään ja vaihdettava tietoja suorittaakseen niille DORA-asetuksessa säädetyt tehtävät sekä koordinoitava valvontatoimiaan. Viranomaiset voivat muun muassa ottaa tarvittaessa käyttöön mekanismeja, joiden avulla voidaan jakaa toimivia käytäntöjä finanssialan eri sektoreiden välillä tilannetietoisuuden parantamiseksi ja yhteisten kyberhaavoittuvuuksien ja -riskien tunnistamiseksi eri sektoreilla. Ehdotetussa momentissa säädettäisiin lisäksi siitä, että Finanssivalvonta toimii muutoinkin yhteistyössä Euroopan keskuspankin, Euroopan järjestelmäriskikomitean, Euroopan unionin kyberturvallisuusviraston (ENISA), Euroopan valvontaviranomaisten, muiden EU-viranomaisten sekä ulkomaisten ETA-valvontaviranomaisten kanssa tieto- ja viestintätekniikkaan liittyvien häiriöiden hallitsemiseksi ja vaikutusten pienentämiseksi. Finanssivalvonta osallistuu lisäksi Euroopan laajuisen systeemisten kyberpoikkeamien koordinointikehyksen toimintaan. Koordinaatiokehys perustuu Euroopan järjestelmäriskikomitean 2.12.2021 antamaan suositukseen EJRK/2021/17. Finanssivalvonta on voimassa olevan lainsäädännön nojalla ilmoitettu koordinaatiokehyksen kansalliseksi yhteyspisteeksi kesäkuussa 2023.

Pykälän ehdotettu 3 momentti korvaisi lain kumottavaksi ehdotetun 52 a §:n. Momentissa säädettäisiin Finanssivalvonnalle velvoite tehdä yhteistyötä Liikenne- ja viestintäviraston kanssa verkko- ja tietoturvadirektiivin kumonneen NIS2-direktiivin mukaisten tehtävien hoitamisessa. Ehdotettu säännös täydentää edellä mainittuja DORA-asetuksen viranomaisyhteistyötä koskevia säännöksiä sekä korostaa Finanssivalvonnan ja Liikenne- ja viestintäviraston välisen yhteistyön erityistä merkitystä. Kyberturvallisuuskeskus on Suomessa NIS2-direktiivin mukainen keskitetty yhteyspiste ja CSIRT-yksikkö. Kyberturvallisuuden sektorit ylittävän koordinoinnin edistämiseksi Finanssivalvonnan on erityisen tärkeätä välittää saamansa häiriöilmoitukset ilman aiheetonta viivytystä Kyberturvallisuuskeskuksen tietoon, jotta niiden perusteella voidaan muodostaa parempi kokonaiskäsitys vallitsevasta kyberturvallisuustilanteesta. Velvollisuudesta toimittaa laajavaikutteista TVT:hen liittyvää poikkeamaa koskevat tiedot säädetään DORA-asetuksen 19 artiklan 6 kohdassa. Kyberturvallisuuskeskuksen tehtävistä on säädetty liikenne- ja viestintävirastosta annetun lain 3 §:ssä. Myös NIS2-direktiivin mukaiset toimivaltaiset viranomaiset muilla direktiivin mukaisilla toimialoilla voivat olla tarpeellisia yhteistyötahoja.

Pykälän ehdotetussa 4 momentissa säädettäisiin Finanssivalvonnalle velvoite tehdä viranomaisyhteistyötä CER-direktiivin mukaisten tehtävien hoitamiseksi, kriittisten toimijoiden häiriönsietokyvyn parantamiseksi ja niiden välisen vapaaehtoisen tiedonvaihdon edistämiseksi valtiovarainministeriön, sisäministeriön, Huoltovarmuuskeskuksen ja muiden asianomaisten viranomaisten kanssa.

Momentilla täydennetään CER-direktiivin täytäntöön panemiseksi annettavan kansallisen yleislain säännöksiä direktiivin liitteen toimialojen 3 (pankkitoiminta) ja 4 (rahoitusmarkkinoiden infrastruktuuri) osalta. CER-direktiivin 9 artiklan 5 kohdan mukaan kunkin jäsenvaltion on varmistettava, että sen toimivaltainen viranomainen kuulee tarvittaessa unionin ja kansallisen lain-

säädännön mukaisesti muita asianomaisia kansallisia viranomaisia, mukaan lukien pelastuspalvelusta, lainvalvonnasta ja henkilötietojen suojasta vastaavia viranomaisia, sekä kriittisiä toimijoita ja asianomaisia osapuolia ja tekee yhteistyötä niiden kanssa. CER-direktiivin 10 artiklan 1 kohdan mukaan jäsenvaltioiden on tuettava kriittisiä toimijoita niiden häiriönsietokyvyn parantamiseksi. Tukeen voi kuulua ohjemateriaalin ja menetelmien laatiminen, tuki kriittisten toimijoiden häiriönsietokykyä testaavien harjoitusten järjestämisessä ja niiden henkilöstön neuvonta ja koulutus. Lisäksi 10 artiklan 3 kohdan mukaan kriittisten toimijoiden välistä vapaaehtoista tiedonvaihtoa on helpotettava. Viranomaisyhteistyö on tärkeää myös hallinnollisten päällekkäisyyksien välttämiseksi, ohjeiden kattavuuden varmistamiseksi ja harjoitustoiminnan vahvistamiseksi. Viranomaisyhteistyöhön voi kuulua myös valmiussuunnittelua, harjoittelua tai muuta viranomaisyhteistyötä esimerkiksi puolustusvoimien, poliisin ja pelastustoimen kanssa. Yhteistyön muodot ja tarkemmat toteuttamistavat jäisivät näiltäkin osin Finanssivalvonnan ja muiden yhteistyöhön osallistuvien viranomaisten kesken määritettäviksi.

CER-puitelain 7 §:ssä toiminnan yleinen ohjaus, yhteensovittaminen, seuranta ja kehittäminen säädettäisiin kuuluvaksi sisäministeriölle (yhteensovittamistehtävää hoitava ministeriö). Lisäksi sisäministeriölle säädettäisiin muun muassa velvollisuus huolehtia kriittisten toimijoiden häiriönsietokykyä koskevan kansallisen strategian ja kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevan kansallisen riskinarvioinnin valmistelusta. Huoltovarmuuskeskuksen tehtävänä on muun muassa tukea ministeriöitä, vaihtaa tietoja ja parhaita käytäntöjä sekä antaa tarvittaessa CER-direktiivin 10 artiklan 1 kohdassa tarkoitettua tukea kriittiselle toimijalle. Kriittisen toimijan määrittämistä koskevan asian ratkaisee se ministeriö, jonka toimialaan käsiteltävä toimija kuuluu. Toimialoista pankkitoiminta ja rahoitusmarkkinoiden kriittinen infrastruktuuri kuuluvat valtioneuvostossa valtiovarainministeriön vastuulle.

5 §. *Muut finanssimarkkinoilla toimivat*. Ehdotetulla muutoksella lisättäisiin muiden finanssimarkkinoilla toimivien joukkoon DORA-asetuksessa tarkoitettu ja asetuksen soveltamisalaan kuuluva TVT-palveluntarjoajana oleva kolmas osapuoli. DORA-asetuksen 3 artiklan 19 alakohdan mukaan näitä ovat yritykset, jotka tarjoavat asetuksen tarkoittamia TVT-palveluja.

Lainkohdan muutos tarkoittaisi Finanssivalvonnan lain 18–22 ja 24 §:n mukaisten tiedonsaanti- ja tarkastusvaltuuksien ja 33–34 §:n mukaisten yleisten toimivaltuuksien ulottamista TVT-palveluntarjoajana oleviin kolmansiin osapuoliin. Yleisiin toimivaltuuksiin kuuluvat 33 §:n mukainen toimeenpanokielto, 33 a §:n mukainen uhkasakko sekä oikeus käyttää 34 §:n tarkoittamaa ulkopuolista asiantuntijaa. Lainsäädäntöön sisältyy jo nykyisin eräitä asiaa koskevia säännöksiä. Voimassa olevan lain 18 §:n mukainen Finanssivalvonnan oikeus saada tietoja valvottavalta ja muulta finanssimarkkinoilla sekä 24 §:n mukainen tarkastusoikeus kohdistuu yritykseen, joka valvottavan tai muun finanssimarkkinoilla toimivan toimeksiannosta hoitaa tämän tietojärjestelmään liittyviä tehtäviä.

Ehdotettu muutos on tarpeellinen, koska DORA-asetuksen mukaisiin velvoitteisiin kuuluu, että finanssiyhteisöt hallitsevat asianmukaisesti kolmansiin osapuoliin liittyvää TVT-riskiä. Asetuksen noudattamisen valvonta ulottuu näin ollen epäsuorasti myös TVT-palveluntarjoajana olevien kolmansien osapuolten toimintaan. DORA-asetus edellyttää, että Finanssivalvonnalla on kaikki asetuksen mukaisten tehtäviensä hoitamiseen tarvittavat valtuudet. TVT-palveluntarjoajana olevan kolmannen osapuolen sisällyttäminen muiden finanssimarkkinoilla toimivien joukkoon olisi sääntelyteknisesti yksinkertaisin tapa ulottaa tarvittavat Finanssivalvonnan valvontavaltuudet myös näihin toimijoihin. Samalla on huomioitava, että lainsäädännön mukaisia valtuuksia on mahdollista käyttää vain siinä määrin, kuin se on Finanssivalvonnan tehtävien hoitamiseksi tarpeen. TVT-palveluntarjoajana olevien kolmansien osapuolten osalta voidaan erityisesti tiedonsaanti- ja tarkastusvaltuuksien arvioida olevan keskeisiä. TVT-palveluntarjo-

ajana olevia kolmansia osapuolia ei edellä sanotun perusteella ehdoteta lisättävän Finanssivalvonnan valvontamaksuista annetun lain (1209/2023) mukaisen maksuvelvollisuuden piiriin. DORA-asetus sisältää erillisen kriittisten TVT-palveluntarjoajina olevien kolmansien osapuolten valvontakehyksen, johon liittyy myös Euroopan valvontaviranomaisen perimä valvontamaksu.

Ehdotetulla muutoksella myös pantaisiin täytäntöön DORA-muutosdirektiivin 4 artiklan 1 kohdassa säädetty muutos luottolaitosdirektiivin 65 artiklan 3 kohdan a alakohdan vi alakohtaan, jonka mukaan toimivaltaisella viranomaisella tulee olla oikeus vaatia kaikkia tehtäviensä hoitamisen kannalta tarpeellisia tietoja myös TVT-palveluntarjoajana olevilta kolmansilta osapuolilta. DORA-muutosdirektiivin mukaisen muutoksen myötä myös luottolaitosdirektiivin 65 artiklan 3 kohdan b ja c alakohtaa sovelletaan TVT-palveluntarjoajana oleviin kolmansiin osapuoliin. Mainittujen lainkohtien mukaan toimivaltaisella viranomaisella tulee olla valtuudet suorittaa kaikki tarpeelliset a alakohdassa tarkoitettuja, asianomaiseen jäsenvaltioon sijoittautuneita tai siellä olevia henkilöitä koskevat tutkimukset, jotka ovat tarpeen toimivaltaisten viranomaisten tehtävien hoitamiseksi sekä valtuudet suorittaa unionin oikeudessa säädettyjä muita edellytyksiä noudattaen kaikki tarpeelliset tarkastukset a alakohdassa tarkoitettujen oikeushenkilöiden liiketiloissa.

Rahoitusvakausviranomaisesta annetun lain (1195/2014) 7 luvun 4 § mukaan rahoitusmarkkinoilla toimivan oikeushenkilön ja tämän palveluksessa olevan luonnollisen henkilön on salassapitosäännösten estämättä ilman aiheetonta viivytystä toimitettava virastolle sen pyytämät tiedot ja selvitykset, jotka ovat välttämättömiä virastolle tässä laissa tai kriisinratkaisulaissa säädetyn tehtävän hoitamiseksi. Rahoitusvakausviranomaisesta annetun lain 3 §:n 1 momentin 13 kohdan mukaan rahoitusmarkkinoilla toimivalla oikeushenkilöllä tarkoitetaan Finanssivalvonnasta annetun lain 4 §:ssä tarkoitettua valvottavaa tai 5 §:ssä tarkoitettua muuta finanssimarkkinoilla toimivaa. Ehdotettu muutos selkeyttää näin ollen myös DORA-asetuksen 30 artiklan 2 kohdan g alakohdan vaatimusta, joka edellyttää finanssiyhteisön ja TVT-palveluntarjoajana olevan kolmannen osapuolen välisen sopimuksen sisältävän TVT-palveluntarjoajana olevalle kolmannelle osapuolelle velvollisuuden tehdä täysimääräisesti yhteistyötä toimivaltaisten viranomaisten ja finanssiyhteisön kriisinratkaisuviranomaisten kanssa.

38 §. *Rikemaksu.* Pykälän 1 momenttiin lisättäisiin uusi 12 kohta, jonka mukaan Finanssivalvonta voisi määrätä 12 kohdan mukaisesti rikemaksun sille, joka tahallaan tai huolimattomuudesta laiminlyö tai rikkoo DORA-asetuksen 16 artiklassa säädetyn TVT-riskin hallintavelvollisuuden. Artiklan mukaista yksinkertaistettua riskienhallintajärjestelmää ovat velvollisia noudattamaan kooltaan ja systeemiseltä merkitykseltään pienimmät rahoitusmarkkinoiden toimijat. Tällainen rike olisi katsottavissa luonteeltaan vähäiseksi, joten siitä ei ole tarpeen määrätä moitittavammille rikkomuksille ja laiminlyönneille tarkoitettua seuraamusmaksua. Säännös perustuu DORA-asetuksen 50 artiklan 3 kohtaan, joka edellyttää jäsenvaltioiden saattavan voimaan asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, joiden on oltava tehokkaita, oikeasuhteisia ja varoittavia.

Samalla momentin 11 kohtaan tehtäisiin uuden 12 kohdan lisäämisestä johtuva tekninen muutos.

Sanktiointi olisi tarpeen ennen kaikkea rahoitusmarkkinoiden yleisen luotettavuuden turvaamiseksi. Suhteellisuusperiaatteen mukaisesti kooltaan ja systeemiseltä merkitykseltään pienten rahoitusmarkkinoiden toimijoiden voidaan edellyttää hallitsevan tieto- ja viestintätekniikan riskejä 16 artiklan mukaisen yksinkertaistetun TVT-riskinhallintajärjestelmän avulla.

40 §. *Seuraamusmaksu*. Pykälän 2 momentin uudessa 13 kohdassa ehdotetaan säädettäväksi Finanssivalvonnan toimivallasta määrätä seuraamusmaksu DORA-asetuksen 5–15, 17–19, 24–27 tai 28–30 artiklan vastaisista teoista. Säännös perustuu DORA-asetuksen 50 artiklan 3 kohtaan, joka edellyttää jäsenvaltioiden saattavan voimaan asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, joiden on oltava tehokkaita, oikeasuhteisia ja varoittavia. Momentin 11 ja 12 kohdassa tehdään lisäksi tarvittavat tekniset muutokset.

Seuraamusmaksu on vakava hallinnollinen seuraamus, jonka soveltamisalaan kuuluvissa rikkomuksissa ja laiminlyönneissä on lähtökohtaisesti kyse erittäin moitittavista teoista ja laiminlyönneistä (HE 32/2012 vp, s. 85). Seuraamusmaksun sijaan voidaan laissa säädetyin perustein poikkeuksellisesti antaa julkinen varoitus, jos lain vastaista menettelyä olisi pidettävä esimerkiksi vähäisenä. Säännös vastaa muita finanssimarkkinoiden sektoreita koskevia säädöksiä. Säännöksestä ilmenee Finanssivalvonnan lähtökohtainen velvollisuus seuraamusmaksun määräämiselle laissa säädetyin edellytyksin. Finanssivalvonta ottaa mahdollisessa seuraamusharkinnassaan huomioon hallintolain 6 §:ssä tarkoitetut hallinnon oikeusperiaatteet sekä Finanssivalvonnasta annetussa laissa ja DORA-asetuksessa säädetyt hallinnollisen seuraamuksen määräämistä ja määräämättä jättämistä koskevat säännökset.

44 §. *EU:n DORA-asetuksen rikkomista koskevat säännökset*. Lain kumotun 44 §:n tilalle lisättäisiin uusi pykälä, joka sisältäisi informatiivisen viittauksen DORA-asetuksen 51 artiklan 2 kohtaan ja 54 artiklaan. Mainituissa asetuksen kohdissa on kyse suoraan sovellettavista säännöksistä, jotka koskevat Finanssivalvontaa sen valvoessa asetuksen noudattamista. Tämän vuoksi lakiin olisi perusteltua sisällyttää niitä koskeva viittaus. Asetuksen 51 artiklan 2 kohta koskee asetuksen 50 artiklassa tarkoitetun hallinnollisen seuraamuksen tai korjaavan toimenpiteen määrittämisessä huomioon otettavia seikkoja. Asetuksen 54 artikla puolestaan sisältää säännöksiä hallinnollisten seuraamusten julkaisemisesta.

50 p §. *Toiminta EU:n DORA-asetuksessa, NIS2-direktiivissä, sekä CER-direktiivissä tarkoitettuna toimivaltaisena viranomaisena.* Pykälässä säädetään nykyisin Finanssivalvonnan toimimisesta verkko- ja tietoturvadirektiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta. Uuden EU-sääntelyn ja verkko- ja tietoturvadirektiivin kumoamisen myötä pykälä ehdotetaan muutettavaksi. Ehdotetun 1 momentin mukaan Finanssivalvonta toimii DORA-asetuksen 46 artiklan tarkoittamana toimivaltaisena viranomaisena. Finanssivalvonta valvoisi siten DORA-asetuksen säännösten noudattamista ja sillä olisi käytössään asetuksessa mainitut valvonta-, tutkinta- ja seuraamusvaltuudet siten, kuin laissa säädetään. Finanssivalvonnalla osallistuisi myös asetuksessa tarkoitettuun viranomaisten väliseen yhteistyöhön.

Ehdotettu pykälän 2 momentti vastaa sisällöltään voimassa olevaa pykälää. Momentissa säädettäisiin siitä, että Finanssivalvonta toimii NIS2-direktiivin 8 artiklan 1 kohdassa tarkoitettuna liitteen I toimialojen 3 ja 4 toimivaltaisena viranomaisena. Direktiivin mainitun kohdan mukaan jäsenvaltion on nimettävä yksi tai useampi viranomainen, joka vastaa kyberturvallisuudesta ja direktiivin VII luvun mukaisista valvontatehtävistä. Suomessa toimii useita Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdassa määriteltyjä luottolaitoksia sekä yksi Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU 4 artiklan 24 kohdassa määritelty kauppapaikkojen ylläpitäjä. Sen sijaan Suomessa ei toimi Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 2 artiklan 1 kohdassa määriteltyjä keskusvastapuolia. Kuten edellä on todettu, NIS2-direktiivin säännöksiä, jotka koskevat kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa, ei kuitenkaan sovelleta DORA-asetuksen soveltamisalaan kuuluviin finanssialan toimijoihin. Siten ehdotetussa

momentissa tarkoitettuna toimivaltaisena viranomaisena toimiminen pitäisi käytännössä sisällään tarvittavan viranomaisyhteistyön ja tietojenvaihdon muiden NIS2-direktiivin mukaisten viranomaisten kanssa. NIS2-direktiivin mukaiset kansallinen kyberturvallisuusstrategia ja kansalliset kyberkriisinhallintakehykset sekä Euroopan kyberkriisien yhteysorganisaatioiden verkosto EU-CyCLONe kattaisivat myös direktiivin soveltamisalaan kuuluvat finanssialan sektorit.

Pykälän 3 momentissa ehdotetaan säädettäväksi Finanssivalvonnan toimimisesta CER-direktiivin 9 artiklan 1 kohdan tarkoittamana toimivaltaisena viranomaisena direktiivin liitteen toimialojen 3 (pankkiala) ja 4 (rahoitusmarkkinoiden infrastruktuuri) osalta. Jäsenvaltiot määrittävät erikseen kriittiset toimijat liitteessä tarkoitetuilla toimialoilla. Lähtökohtaisesti toimialoihin 3 ja 4 kuuluvien kriittisten toimijoiden toimivaltaisia viranomaisia ovat DORA-asetuksessa tarkoitetut toimivaltaiset viranomaiset. Finanssivalvonta vastaisi siten direktiivin säännösten asianmukaisesta soveltamisesta ja tarvittaessa täytäntöönpanosta. Finanssivalvonta olisi velvollinen tekemään yhteistyötä direktiivin mukaisten tehtäviensä hoitamisessa, mistä säädettäisiin tarkemmin lakiehdotuksen 3 f §:n 4 momentissa. CER-direktiivin velvoitteita ei kuitenkaan sovelleta DORA-asetuksen soveltamisalaan kuuluviin finanssialan toimijoihin. Finanssivalvonnan CER-direktiivin mukaisiin tehtäviin kuuluu viranomaisyhteistyön ohella direktiivin 10 artiklan mukaisesti kriittisten toimijoiden tukeminen niiden häiriönsietokyvyn parantamiseksi sekä yhteistyö, tiedonvaihto ja hyvien käytäntöjen jakaminen kriittisten toimijoiden kanssa.

52 a §. *Yhteistyö ja tietojenvaihto verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa.* Säännös ehdotetaan kumottavaksi. Kyberturvallisuuden edistämiseksi tehtävää yhteistyötä koskevat säännökset sisältyisivät jatkossa ehdotettuun uuteen 3 f §:ään.

71 §. *Oikeus ja velvollisuus luovuttaa tietoja.* Pykälään on koottu säännökset, joiden nojalla Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä tietoja muille viranomaisille. Pykälän 1 momenttiin lisättäisiin uusi 20 kohta, jonka mukaan Finanssivalvonnalla on oikeus luovuttaa tietoja Liikenne- ja viestintävirastolle lain 3 f §:n 3 momentissa tarkoitetun yhteistyön toteuttamista varten. Samalla momentin 19 kohtaan tehtäisiin uuden 20 kohdan lisäämisestä johtuva tekninen muutos. Voimassa olevassa laissa vastaava säännös sisältyy lain 52 a §:ään, joka ehdotetaan kumottavaksi. Oikeutta tietojen luovuttamiseen täsmentää pykälän 2 momentti, jonka mukaan Finanssivalvonnalla on oikeus luovuttaa vain sellaisia tietoja, jotka ovat tarpeen kunkin 1 momentissa mainitun viranomaisen tehtävien suorittamiseksi. DORA-asetuksen 19 artikla sisältää lisäksi suoraan sovellettavia säännöksiä Finanssivalvonnan velvollisuudesta toimittaa laajavaikutteista TVT:hen liittyvää poikkeamaa koskevat yksityiskohtaiset tiedot muille asianomaisille viranomaisille sekä oikeudesta toimittaa näille viranomaisille merkittäviä kyberuhkia koskevia tietoja.

7.2 Laki luottolaitostoiminnasta annetun lain muuttamisesta

9 luku **Riskien hallinta**

2 §. *Riskienhallintajärjestelmälle asetettavat yleiset vaatimukset*. Pykälän 1 momenttia ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 4 artiklan 2 kohdassa säädetyn muutoksen luottolaitosdirektiivin 74 artiklan 1 kohdan ensimmäiseen alakohtaan. Momenttiin lisättäisiin uusi 4 kohta, jolloin nykyinen 4 kohta siirtyisi 5 kohdaksi. Luottolaitoksen hallinto- ja ohjausjärjestelmiin kuuluisivat muun ohella DORA-asetuksen ja sen nojalla annettujen säännösten mukaiset verkko- ja tietojärjestelmät.

16 §. *Operatiivinen riski*. Pykälän 3 momenttia ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 4 artiklan 3 kohdassa säädetyn muutoksen luottolaitosdirektiivin 85

artiklan 2 kohtaan. Luottolaitoksella on oltava käytössä varautumissuunnitelmat ja liiketoiminnan jatkuvuutta koskevat suunnitelmat. Direktiivin muutoksella täsmennetään, että mainittuihin suunnitelmiin sisältyvät myös TVT-riskiä koskevat liiketoiminnan jatkuvuus-, reagointi- ja palautumissuunnitelmat DORA-asetuksessa vahvistettujen vaatimusten mukaisesti. Momenttiin ehdotetaan lisättäväksi viittaus DORA-asetuksen 11 artiklaan, jossa säädetään luottolaitoksen tieto- ja viestintätekniikan liiketoiminnan jatkuvuutta koskevista toimintaperiaatteista ja suunnitelmista sekä tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmista.

11 luku **Luottolaitoksen valvonta**

2 §. *Valvojan arvio*. Pykälän 2 momenttiin ehdotetaan lisättäväksi uusi 11 kohta ottamaan huomioon DORA-muutosdirektiivin 4 artiklan 4 kohdassa säädetyn muutoksen luottolaitosdirektiivin 97 artiklan 1 kohtaan. Valvojan arviossa luottolaitokseen kohdistuvista riskeistä ja siitä, täyttääkö luottolaitos lain 9 ja 10 luvussa ja EU:n vakavaraisuusasetuksessa säädetyt vaatimukset, tulisi uuden kohdan mukaan ottaa huomioon DORA-asetuksen IV luvun mukaisen digitaalisen häiriönsietokyvyn testauksen paljastamat riskit. Samalla momentin 10 kohtaan tehtäisiin uuden 11 kohdan lisäämisestä johtuva tekninen muutos.

7.3 Laki sijoituspalvelulain 7 luvun 2 §:n ja 7 a luvun 1 §:n muuttamisesta

7 luku **Sijoituspalveluyrityksen toiminnan järjestäminen**

2 §. *Toiminnan luotettava järjestäminen*. Pykälän 3–5 momenttia ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 6 artiklan 1 kohdassa säädetyn muutoksen MiFID II -direktiivin 16 artiklan 4 ja 5 kohtiin. Sen mukaan sijoituspalveluyrityksen toiminnan luotettava järjestäminen edellyttää jatkossa DORA-asetuksen ja sen nojalla annettujen säännösten noudattamista, mukaan lukien DORA-asetuksessa säädettyjen vaatimusten mukainen tiedonsiirtovälineiden suojaus ja todentaminen. Pykälän 3 ja 5 momenttiin ehdotetaan tältä osin tarvittavia muutoksia. Pykälän 4 momenttia muutettaisiin vastaamaan DORA-muutosdirektiivillä muutettua MiFID II -direktiivin 16 artiklan 5 kohdan ensimmäistä alakohtaa, johon ei enää sisälly mainintaa tehokkaista valvonta- ja turvajärjestelyistä tietojenkäsittelyjärjestelmiä varten.

7 a luku **Algoritminen kaupankäynti ja suora sähköinen markkinoillepääsy**

1 §. *Algoritminen kaupankäynti*. Pykälän 1 momentin 1 kohtaa ja 2 momenttia ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 6 artiklan 2 kohdassa säädetyn muutoksen MiFID II -direktiivin 17 artiklan 1 kohtaan. Ehdotusten mukaan algoritmistä kaupankäyntiä harjoittavan sijoituspalveluyrityksen käytössä olisi oltava käytössä tehokkaat järjestelmät ja riskinhallintamenetelmät, joiden avulla voidaan varmistaa sen kaupankäyntijärjestelmien häiriönsietokyky ja riittävä kapasiteetti DORA-asetuksessa vahvistettujen vaatimusten mukaisesti. Tällaisella sijoituspalveluyrityksellä olisi lisäksi oltava DORA-asetuksen 11 artiklan mukaiset TVT-liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja suunnitelmat ja tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmat ja sen olisi varmistettava, että sen järjestelmät ovat kaikilta osin testattuja ja niitä valvotaan asianmukaisesti, jotta ne täyttävät asetuksessa ja sen nojalla säädetyt vaatimukset.

7.4 Laki maksulaitoslain 19 a ja 19 b §:n muuttamisesta

19 a §. *Operatiivisten ja turvallisuusriskien hallinta*. Voimassa olevassa pykälässä säädetään maksulaitosta, maksulaitoslain 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavaa henkilöä ja maksulaitoslain 7 b §:ssä tarkoitettua tilitietopalvelun tarjoajaa koskevista riskinhallintavelvoitteista. Pykälää sovelletaan lisäksi luottolaitostoiminnasta annetun lain 9 luvun

16 §:n 4 momentin viittaussäännöksen nojalla luottolaitokseen. Mainitut toimijat kuuluvat DORA-asetuksen soveltamisalaan. Pykälän 1 momentti ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 7 artiklan 4 kohdassa säädetyn muutoksen maksupalveludirektiivin 95 artiklan 1 kohtaan. Momenttiin lisättäisiin mainittua direktiivin kohtaa vastaava informatiivinen säännös, jonka mukaan se, mitä momentissa säädetään, ei rajoita DORA-asetuksen II luvun ja sen nojalla annettujen säännösten soveltamista.

19 b §. *Poikkeamista ja petoksista ilmoittaminen*. Voimassa olevassa pykälässä säädetään poikkeamista ja petoksista ilmoittamista koskevista velvoitteista. Pykälää sovelletaan samoihin toimijoihin kuin lain 19 a §:ää. Pykälä ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 7 artiklan 5 kohdassa säädetyn muutoksen maksupalveludirektiivin 96 artiklaan. Sen perusteella artiklan 1–5 kohtaa, jotka on pantu täytäntöön voimassa olevan pykälän 1 ja 3 momentilla, ei jatkossa enää sovelleta edellä mainittuihin toimijoihin. Sen vuoksi nämä säännökset poistettaisiin laista.

Pykälän 1 momentti vastaisi voimassa olevan pykälän 2 momenttia. Tällä säännöksellä on pantu täytäntöön maksupalveludirektiivin 68 artiklan 6 kohta, jota ei DORA-muutosdirektiivillä ole muutettu. Pykälän 2 momentti vastaisi voimassa olevan pykälän 4 momenttia. Tällä säännöksellä on pantu täytäntöön maksupalveludirektiivin 96 artiklan 6 kohta, jota ei DORA-muutosdirektiivillä ole muutettu. Pykälän 3 momentti vastaisi voimassa olevan pykälän 5 momenttia.

Pykälän 4 momentti sisältäisi informatiivisen viittauksen DORA-asetuksen poikkeamailmoituksia koskevaan sääntelyyn. Maksulaitoksen, 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavan henkilön, tilitietopalvelun tarjoajan ja sähköisen rahan liikkeeseenlaskijan velvollisuudesta ilmoittaa tieto- ja viestintätekniikkaan sekä toiminnan harjoittamiseen tai turvallisuuteen vaikuttaviin maksuihin liittyvistä poikkeamista säädetään DORA-asetuksen III luvussa.

7.5 Laki kaupankäynnistä rahoitusvälineillä annetun lain 3 luvun 1 ja 18 §:n muuttamisesta

3 luku **Säännellyn markkinan toiminnan järjestäminen**

1 §. *Säännellyn markkinan toiminnan järjestämistä koskevat vaatimukset*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 6 artiklan 3 kohdassa ja 4 kohdan a alakohdassa säädetyn muutoksen MiFID II -direktiivin 47 artiklaan ja 48 artiklan 6 kohtaan. Muutosdirektiivillä MiFID II -direktiivin 47 artiklan 1 kohdan b alakohtaa on muutettu, saman kohdan c alakohta on kumottu ja 48 artiklan 1 kohtaa muutettu.

Voimassa olevan pykälän 1 momentissa säädetään säännellyn markkinan toiminnan järjestämisestä, mukaan lukien riskien hallinnasta. Momenttia täydennettäisiin DORA-muutosdirektiivin 6 artiklan 3 kohdan edellyttämällä tavalla vaatimuksella hallita tieto- ja viestintätekniikkaan liittyviä riskejä DORA-asetuksen II luvun ja sen nojalla annettujen säännösten mukaisesti.

Voimassa olevassa pykälän 3 momentissa säädetään pörssin kaupankäyntijärjestelmän häiriönsietokyvystä MIFID II -direktiivin 47 artiklan 1 kohdan c ja 48 artiklan 1 kohdan mukaisesti. Pykälän 3 momenttia ehdotetaan muutettavaksi direktiivin uuden sanamuodon mukaiseksi. Säännellyn markkinan olisi ylläpidettävä toiminnallista häiriönsietokykyään DORA-asetuksen II luvussa vahvistettuja vaatimuksia noudattaen ja sen käytössä olisi oltava tehokkaat liiketoiminnan jatkuvuutta koskevat järjestelyt, joihin lukeutuvat DORA-asetuksen 11 artiklan mukaisesti laaditut TVT-liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja suunnitelmat ja TVT-reagointi- ja palautumissuunnitelmat.

18 §. *Algoritminen kaupankäynti*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 6 artiklan 4 kohdan a alakohdassa säädetyn muutoksen MiFID II -direktiivin 48 artiklan 6 kohtaan. Pörssin järjestelmien ja menettelytapojen sisältämä velvoite kaupankäyntiosapuolille testata algoritmejaan pörssin tarjoamassa testausympäristössä tulisi toteuttaa DORA-asetuksen II ja IV luvun ja sen nojalla annettujen säännösten mukaisesti.

7.6 Laki sijoitusrahastolain 5 luvun 1 §:n muuttamisesta

5 luku **Vakavaraisuus ja riskienhallinta**

1 §. *Rahastoyhtiön riskienhallinta*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 1 artiklassa säädetyn muutoksen sijoitusrahastodirektiivin 12 artiklan 1 kohdan toisen alakohdan a alakohtaan. Direktiiviin on lisätty viittaus verkko- ja tietojärjestelmiin, jotka on perustettu ja joita hallinnoidaan DORA-asetusta noudattaen. Osana rahastoyhtiön riskienhallintaa, sähköisen tietojenkäsittelyn valvonta- ja suojajärjestelyjen on jatkossa oltava DORA-asetuksen ja sen nojalla annettujen säännösten mukaisia.

7.7 Laki vaihtoehtorahaston hoitajista annetun lain 7 luvun 2 §:n muuttamisesta

7 luku **Toiminnan järjestäminen**

2 §. *Hallinto- ja valvontajärjestelyt*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 3 artiklassa säädetyn muutoksen AIFM-direktiivin 18 artiklaan. Sähköisen tietojenkäsittelyn valvonta- ja suojajärjestelyjen on jatkossa oltava DORA-asetuksen ja sen nojalla annettujen säännösten mukaisia.

7.8 Laki lisäeläkesäätiöistä ja lisäeläkekassoista annetun lain 1 luvun 13 §:n ja 3 luvun 12 §:n muuttamisesta

1 luku **Lain soveltaminen ja toiminnan keskeiset periaatteet**

13 §. *Säännökset, joiden soveltaminen riippuu vakuutettujen lukumäärästä*. Pykälää ehdotetaan muutettavaksi siten, että lain 3 luvun 12 §:ään lisättävä uusi 4 momentti soveltuu myös sellaiseen lisäeläkelaitokseen, jossa on vähemmän kuin 100 vakuutettua. DORA-asetuksen mukainen yksinkertaistettu TVT-riskienhallintajärjestelmä soveltuu lisäeläkelaitoksiin, joissa on yli 15 vakuutettua, mutta vähemmän kuin 100 vakuutettua.

3 luku **Johto ja hallintojärjestelmä**

12 §. *Toimintaperiaatteet, sisäisen valvonnan järjestelmä ja varautumissuunnitelma*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 8 artiklassa säädetyn muutoksen direktiivin (EU) 2016/2341 21 artiklan 5 kohtaan.

7.9 Laki vakuutusyhtiölain 6 luvun 8 §:n muuttamisesta

6 luku **Vakuutusyhtiön johto, hallintojärjestelmä ja varojen sijoittaminen**

8 §. *Yleiset hallintovaatimukset*. Pykälää ehdotetaan muutettavaksi ottamaan huomioon DORA-muutosdirektiivin 2 artiklassa säädetyn muutoksen Solvenssi II -direktiivin 41 artiklan 4 kohtaan.

7.10 Laki Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annetun lain 1 §:n muuttamisesta

1 §. Pykälään ehdotetaan lisättävän uusi 5 momentti, jonka mukaan DORA-asetusta ei sovellettaisi Teollisen yhteistyön rahasto Oy:öön. Muutoksella hyödynnettäisiin yhtiön osalta DORA-asetuksen 2 artiklan 4 kohdan mukainen optio, jonka mukaan jäsenvaltiot voivat jättää asetuksen soveltamisalan ulkopuolelle luottolaitosdirektiivin 2 artiklan 5 kohdan 4–23 alakohdassa tarkoitetut yhteisöt, jotka sijaitsevat niiden alueella. Jos jäsenvaltio-optiota ei käytettäisi, tulisi tässä yhteydessä säätää Finanssivalvonnan tehtävästä valvoa DORA-asetuksessa säädettyjen velvoitteiden noudattamista yhtiön osalta sekä tähän liittyvistä tarpeellisista valvontavaltuuksista ja valvontamaksuista. Erillisten valvontajärjestelyjen luomista yksittäisen säädöksen osalta ei voida pitää tarkoituksenmukaisena, vaan ohjausta ja valvontaa tulee arvioida kokonaisuutena yhtiötä koskevan lainsäädännön uudistamisen yhteydessä.

7.11 Laki valtion erityisrahoitusyhtiöstä annetun lain 3 §:n muuttamisesta

3 §. *Hallinto*. Pykälään lisättäisiin uusi 5 momentti, jonka mukaan DORA-asetusta ei sovellettaisi Finnvera Oyj:hin. Muutoksella hyödynnettäisiin DORA-asetuksen 2 artiklan 4 kohdan mukainen optio Finnvera Oyj:n osalta vastaavin perustein kuin edellä on todettu Teollisen yhteistyön rahasto Oy:n osalta.

8 Lakia alemman asteinen sääntely

DORA-muutosdirektiivin 5 artiklan täytäntöönpano edellyttää muutoksia seuraaviin asetuksiin: valtiovarainministeriön asetus luottolaitosten ja sijoituspalveluyritysten kriisinratkaisusuunnitelmien laatimiseksi toimitettavista ja niihin sisällytettävistä tiedoista (1284/2014), valtiovarainministeriön asetus seikoista, jotka on otettava huomioon arvioitaessa luottolaitoksen ja sijoituspalveluyrityksen taikka konsernin purkamis- ja uudelleenjärjestämismahdollisuuksia (1285/2014), valtiovarainministeriön asetus luottolaitoksen ja sijoituspalveluyrityksen elvytyssuunnitelmiin sisällytettävistä tiedoista (1286/2014). Muutostarpeet johtuvat edellä kuvatuista kriisinratkaisudirektiivin muutoksista, joilla huomioidaan digitaalinen häiriönsietokyky ja DORA-asetuksen säätäminen luottolaitosten ja sijoituspalveluyritysten elvytys- ja kriisinratkaisusuunnitelmien sisältöä koskevissa vaatimuksissa sekä purkamis- ja uudelleenjärjestämismahdollisuuksien arviointia koskevissa vaatimuksissa.

Lisäksi DORA-muutosdirektiivin 7 artiklan 2 kohdan täytäntöönpano edellyttää muutoksia maksulaitoksen toimilupahakemukseen liitettävistä selvityksistä annettuun valtiovarainministeriön asetukseen (1040/2017).

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan 17.1.2025.

10 Esityksen riippuvuus muista esityksistä

[täydennetään]

11 Suhde perustuslakiin ja säätämisjärjestys

Suomen perustuslain (731/1999) 18 §:n 1 momentin mukaan jokaisella on oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla ja elinkeinolla.

Rahoitusmarkkinalainsäädäntö ja siihen liittyvät Finanssivalvonnan valvontavaltuudet merkitsevät rajoituksia elinkeinovapauteen. Voimassa oleva Finanssivalvonnasta annettu laki on tarpeellisilta osin saatettu voimaan perustuslakivaliokunnan myötävaikutuksella.

Hallituksen esityksessä ei ehdoteta Finanssivalvonnalle uudenlaisia toimivaltuuksia eikä muutenkaan lainsäädännön peruslähtökohtia ehdoteta muutettavan. Esityksen 1. lakiehdotuksella lisättäisiin muiden finanssimarkkinoilla toimivien joukkoon DORA-asetuksessa tarkoitettu ja asetuksen soveltamisalaan kuuluva TVT-palveluntarjoajana oleva kolmas osapuoli. Näin Finanssivalvonnan valvontavaltuudet ulotettaisiin TVT-palveluntarjoajana oleviin kolmansiin osapuoliin. Valvontavaltuuksien käyttäminen on mahdollista siinä määrin, kuin se on tarpeen Finanssivalvonnalle laissa säädetyn valvontatehtävän hoitamiseksi. Asiallisesti kyse ei ole merkittävästä muutoksesta

Ehdotetut toimivaltuudet ovat merkityksellisiä perustuslain 18 §:n 1 momentin mukaisen elinkeinon ja ammatin harjoittamisen vapauden kannalta. Perustuslakivaliokunta ei ole pitänyt tällaisia valtuuksia valtiosäännön kannalta ongelmallisina (esimerkiksi PeVL 67/2002 ja PeVL 28/2008 vp).

Perustuslain 21 §:n mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla.

Finanssivalvonnasta annetun lain hallinnollisia seuraamuksia koskevia säännöksiä ehdotetaan täydennettävän DORA-asetuksen johdosta. DORA-asetus edellyttää jäsenvaltioiden saattavan voimaan asetuksen rikkomiseen liittyviä asianmukaisia hallinnollisia seuraamuksia ja korjaavia toimenpiteitä, joiden on oltava tehokkaita, oikeasuhteisia ja varoittavia. Finanssivalvonta voisi määrätä seuraamusmaksun sille, joka laiminlyö tai rikkoo DORA-asetuksen mukaisen velvoitteensa. Asetuksen mukaisen yksinkertaistettua TVT-riskienhallintajärjestelmää koskevan velvoitteen laiminlyönnin tai rikkomisen johdosta voitaisiin määrätä rikemaksu.

Perustuslakivaliokunnan vakiintuneen tulkinnan mukaan tällaiset seuraamusmaksut eivät ole perustuslain 81 §:n mielessä sen paremmin veroja kuin maksujakaan, vaan lainvastaisesta teosta määrättäviä sanktioluonteisia hallinnollisia seuraamuksia. Valiokunta on asiallisesti rinnastanut rangaistusluonteisen taloudellisen seuraamuksen rikosoikeudelliseen seuraamukseen (PeVL 14/2013 vp, PeVL 17/2012 vp, PeVL 9/2012 vp, s. 2, PeVL 55/2005 vp, s. 2 ja PeVL 32/2005 vp, s. 2). Hallinnollisen seuraamuksen yleisistä perusteista on säädettävä perustuslain 2 §:n 3 momentin edellyttämällä tavalla lailla, koska sen määräämiseen sisältyy julkisen vallan käyttöä. Valiokunta on myös katsonut, että kyse on merkittävästä julkisen vallan käytöstä.

Laissa on täsmällisesti ja selkeästi säädettävä maksuvelvollisuuden ja maksun suuruuden perusteista sekä maksuvelvollisen oikeusturvasta samoin kuin lain täytäntöönpanon perusteista (PeVL 14/2013 vp, PeVL 17/2012 vp, PeVL 9/2012 vp, s. 2, PeVL 57/2010 vp, s. 2, PeVL 55/2005 vp, s. 2 ja PeVL 32/2005 vp, s. 2–3). Vaikka perustuslain 8 §:n rikosoikeudellisen laillisuusperiaatteen täsmällisyysvaatimus ei sellaisenaan kohdistu hallinnollisten seuraamusten sääntelyyn, ei tarkkuuden yleistä vaatimusta kuitenkaan voida tällaisen sääntelyn yhteydessä sivuuttaa (PeVL 14/2013 vp, PeVL 17/2012 vp, PeVL 9/2012 vp, s. 2, PeVL 57/2010 vp, s. 2 ja PeVL 74/2002 vp, s. 5). Lisäksi säännösten on täytettävä sanktioiden oikeasuhtaisuuteen liittyvät vaatimukset (PeVL 28/2014 vp, PeVL 15/2014 vp). Hallinnollisten sanktioiden osalta on

vielä huomattava, etteivät ne saa menettelynsä puolesta muodostua perustuslain 21 §:ssä tarkoitetun syyttömyysolettaman vastaisiksi eivätkä ne voi myöskään perustua puhtaasti käännettyyn todistustaakkaan taikka ankaraan objektiiviseen vastuuseen (ks. myös PeVL 32/2005 vp, s. 3 ja PeVL 4/2004 vp, s. 7–8).

Esityksen 1. lakiehdotuksiin sisältyvät säännökset hallinnollisista seuraamuksista vastaavat luonteeltaan voimassa olevaan lainsäädäntöön jo sisältyviä säännöksiä, jotka on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 17/2012 vp, PeVL 15/2016 vp ja PeVL 43/2013 vp). Finanssivalvonnasta annetun lain rikemaksua ja seuraamusmaksua koskevissa säännöksissä luetellaan ne säännökset, joiden laiminlyönnin tai rikkomisen seurauksena kyseinen seuraamus voidaan määrätä. Näitä säännöksiä täydennettäisiin siten, että seuraamus voidaan määrätä DORA-asetuksen asianomaisten säännösten laiminlyönnin tai rikkomisen johdosta. Rikemaksun ja seuraamusmaksun määräämisen muita edellytyksiä ja määräämistä koskevaa menettelyä ei ehdoteta muutettavan.

Ilman nimenomaisia säännöksiä Finanssivalvonta ei voi määrätä mitään muuta hallinnollista seuraamusta kuin Finanssivalvonnasta annetun lain 39 §:n mukaisen julkisen varoituksen. Jos DORA-asetuksen mukaisiin velvoitteisiin kohdistuvien rikkomusten tai laiminlyöntien seuraamuksista ei tarkemmin säädettäisi, Finanssivalvonta voisi siis ainoastaan antaa rikkomuksesta tai laiminlyönnistä julkisen varoituksen, mutta ei euromääräisiä hallinnollisia seuraamuksia. Finanssivalvonta ei näin ollen pystyisi välttämättä puuttumaan tehokkaasti mahdollisiin rikkomuksiin.

Finanssivalvonnasta annetun lain hallinnollisia seuraamuksia koskevissa säännöksissä huomioidaan yhtäältä seuraamusten täsmällisyys ja oikeasuhtaisuus ja toisaalta seuraamusten käytön joustavuus ja varoittavuus. Finanssivalvonnalla tulee olla joustavat mahdollisuudet määrätä kussakin lainsäädännön rikkomis- tai laiminlyöntitapauksessa vallitsevat olosuhteet huomioon ottaen tarkoituksenmukaisin seuraamus. Lain mukaiset hallinnolliset seuraamukset mahdollistavat nopean ja tehokkaan puuttumisen finanssimarkkinalainsäädännön vastaiseen menettelyyn, mikä tehostaa finanssimarkkinoiden julkista valvontaa. DORA-asetuksen 16 artiklassa säädetään yksinkertaistettua TVT-riskinhallintajärjestelmää koskevista vaatimuksista, joita sovelletaan tiettyihin pienempiin toimijoihin. Näiden vaatimusten laiminlyönnin tai rikkomisen osalta seuraamusmaksua lievempi seuraamus eli rikemaksu olisi lähtökohtaisesti riittävä. Hallinnollisten seuraamusten määräämistä koskevat säännökset mahdollistavat muutoinkin Finanssivalvonnalle tarpeenmukaisen harkinnan. Finanssivalvonnasta annetun lain 41 §:n mukaan seuraamusmaksun määräämisessä Finanssivalvonnan on käytettävä kokonaisarviointia ja ottaa huomioon muun muassa menettelyn laatu, laajuus ja kestoaika sekä tekijän taloudellinen asema. Samoin lain 38 §:n mukaan rikemaksun suuruus perustuu kokonaisarviointiin. Rikemaksun suuruutta arvioitaessa on otettava huomioon menettelyn laatu, laajuus ja kestoaika. Lain 42 §:n mukaan Finanssivalvonta voi vähäisissä rikkomustapauksissa muuttaa seuraamusmaksun julkiseksi varoitukseksi tai jättää rikemaksun määräämättä.

Hallitus katsoo, että ehdotetut lait voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Ponsi

Koska finanssialan kyberturvallisuutta ja häiriönsietokykyä koskevassa asetuksessa on säännöksiä, joita ehdotetaan täydennettäviksi lailla ja asiaa koskevissa direktiiveissä on säännöksiä, jotka ehdotetaan pantaviksi täytäntöön lailla, annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

Finanssivalvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan Finanssivalvonnasta annetun lain (878/2008) 52 a §, sellaisena kuin se on laissa 959/2018,

muutetaan 5 §:n 40 kohta, 38 §:n 1 momentin 11 kohta, 40 §:n 2 momentin 11 ja 12 kohta, 50 p § ja 71 §:n 1 momentin 19 kohta,

sellaisina kuin ne ovat, 5 §:n 40 kohta ja 38 §:n 1 momentin 11 kohta laissa 184/2023, 40 §:n 2 momentin 11 ja 12 kohta laissa 214/2022, 50 p § laissa 291/2018 ja 71 §:n 1 momentin 19 kohta laissa 524/2021, sekä

lisätään 3 §:n 2 momenttiin, sellaisena kuin se on osaksi laeissa 1198/2014, 1145/2015, 1442/2016, 445/2023 ja 1261/2023, uusi 6 a ja 6 b kohta, lakiin uusi 3 f §, 5 §:ään, sellaisena kuin se on laeissa 752/2012, 902/2012, 254/2013, 170/2014, 198/2015, 520/2016, 737/2016, 1442/2016, 228/2017, 575/2017, 893/2017, 1071/2017, 241/2018, 1229/2018, 215/2019, 296/2019, 517/2019, 574/2019, 963/2019, 316/2020, 524/2021, 599/2021, 205/2022, 184/2023 ja 192/2023, uusi 41 kohta, 38 §:n 1 momenttiin, sellaisena kuin se on laeissa 752/2012, 254/2013, 1198/2014, 1055/2016, 893/2017, 316/2020, 379/2021, 153/2022, 205/2022 ja 184/2023, uusi 12 kohta, 40 §:n 2 momenttiin, sellaisena kuin se on laeissa 1071/2017, 1108/2018, 316/2020, 379/2021, 599/2021, 941/2021 ja 214/2022, uusi 13 kohta, lakiin siitä lailla 1071/2017 kumotun 44 §:n tilalle uusi 44 § ja 71 §:n 1 momenttiin, sellaisena kuin se on osaksi laeissa 752/2012, 611/2014, 651/2014, 1198/2014, 505/2015, 520/2016, 1442/2016, 446/2017, 1071/2017, 402/2018, 574/2019, 569/2020, 270/2021 ja 524/2021, uusi 20 kohta seuraavasti:

3 §

Tehtävät

— —

Laissa erikseen säädettyjen tehtäviensä toteuttamiseksi Finanssivalvonta:

— —

6 a) edistää finanssimarkkinoilla toimivien kyberturvallisia toimintatapoja;

6 b) edistää finanssimarkkinoiden kriittisten toimijoiden häiriönsietokykyä;

— —

3 f §

Viranomaisyhteistyö kyberturvallisuuden ja häiriönsietokyvyn edistämiseksi

Finanssivalvonta toimii yhteistyössä valtiovarainministeriön, sosiaali- ja terveysministeriön, Suomen Pankin, Rahoitusvakausviraston, Liikenne- ja viestintäviraston ja muiden asianomaisten viranomaisten kanssa tieto- ja viestintätekniikkaan liittyvien häiriöiden hallitsemiseksi ja vaikutusten pienentämiseksi.

Finanssivalvonta osallistuu finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011

muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554, jäljempänä *EU:n DORA-asetus*, 32 ja 47–49 artiklan mukaiseen viranomaisyhteistyöhön ja Euroopan laajuiseen systeemisten kyberpoikkeamien koordinointikehyksen toimintaan, sekä muutoin toimii yhteistyössä Euroopan keskuspankin, Euroopan järjestelmäriskikomitean, Euroopan kyberturvallisuusviraston, Euroopan valvontaviranomaisten, muiden EU-viranomaisten sekä ulkomaisten ETA-valvontaviranomaisten kanssa tieto- ja viestintätekniikkaan liittyvien häiriöiden hallitsemiseksi ja vaikutusten pienentämiseksi.

Finanssivalvonnan on tehtävä yhteistyötä toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555, jäljempänä *NIS2-direktiivi*, mukaisten tehtävien hoitamisessa Liikenne- ja viestintäviraston kanssa.

Finanssivalvonnan on tehtävä yhteistyötä kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557, jäljempänä *CER-direktiivi*, mukaisten tehtävien hoitamiseksi, kriittisten toimijoiden häiriönsietokyvyn parantamiseksi ja niiden välisen vapaaehtoisen tiedonvaihdon edistämiseksi valtiovarainministeriön, sisäministeriön, Huoltovarmuuskeskuksen ja muiden asianomaisten viranomaisten kanssa.

5 §

Muut finanssimarkkinoilla toimivat

Muulla finanssimarkkinoilla toimivalla tarkoitetaan tässä laissa:

— —

40) sitä, joka on eräiden luotonantajien ja luotonvälittäjien rekisteröinnistä annetun lain (186/2023) 4 §:n perusteella velvollinen ilmoittautumaan Finanssivalvonnan pitämään luotonantaja- ja vertaislainanvälittäjärekisteriin;

41) EU:n DORA-asetuksessa tarkoitettua TVT-palveluntarjoajana olevaa kolmatta osapuolta.

38 §

Rikemaksu

Finanssivalvonta määrää rikemaksun sille, joka tahallaan tai huolimattomuudesta:

— —

11) laiminlyö tai rikkoo eräiden luotonantajien ja luotonvälittäjien rekisteröinnistä annetun lain 8 §:n 3 momentissa säädetyn ilmoitusvelvollisuuden;

12) laiminlyö tai rikkoo EU:n DORA-asetuksen 16 artiklassa säädetyn TVT-riskin hallintavelvollisuuden.

— —

40 §

Seuraamusmaksu

— —

Seuraamusmaksu määrätään myös sille, joka tahallaan tai huolimattomuudesta laiminlyö tai rikkoo:

— —

11) kestävää sijoittamista helpottavasta kehyksestä ja asetuksen (EU) 2019/2088 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2020/852, jäljempänä *taksonomia-asetus*, 5 artiklan säännöksiä ympäristön kannalta kestävien sijoitusten avoimuudesta ennen sopimuksen tekemistä annettavissa tiedoissa ja määräaikaiskatsauksissa, 6 artiklan säännöksiä ympäristöominaisuuksia edistävien rahoitustuotteiden avoimuudesta ennen sopimuksen tekemistä annettavissa tiedoissa ja määräaikaiskatsauksissa tai 7 artiklan säännöksiä muiden rahoitustuotteiden avoimuudesta ennen sopimuksen tekemistä annettavissa tiedoissa ja määräaikaiskatsauksissa;

12) PEPP-asetuksen 5–7 artiklan säännöksiä rekisteröintivelvollisuudesta ja säännöksiä virheellisten tai harhaanjohtavien tietojen antamisesta, joiden perusteella PEPP-tuote on rekisteröity Euroopan vakuutus- ja lisäeläkeviranomaisen pitämään julkiseen keskusrekisteriin, 18 artiklan säännöksiä siirrettävyyspalvelun tarjoamisesta, 19 artiklan säännöksiä PEPP-tuotteen alatilin käyttämisestä, 20 artiklan säännöksiä uuden alatilin avaamista koskevista tiedonantovelvollisuuksista, 21 artiklan säännöksiä siirrettävyyttä koskevien tietojen toimittamisesta toimivaltaisille viranomaisille, 22 artiklan säännöksiä PEPP-tarjoajia ja PEPP-jakelijoita koskevasta yleisperiaatteesta, 23 artiklan säännöksiä erityyppisiin PEPP-tarjoajiin tai PEPP-jakelijoihin sovellettavasta jakelujärjestelystä, 24 artiklan säännöksiä sähköisestä jakelusta ja muiden pysyvien välineiden käyttämisestä, 25 artiklan säännöksiä tuotehallintavaatimuksista, 26 artiklan säännöksiä PEPP-avaintietoasiakirjasta, 27 artiklan säännöksiä PEPP-avaintietoasiakirjan kielestä, 28 artiklan säännöksiä PEPP-avaintietoasiakirjan sisällöstä, 29 artiklan säännöksiä markkinointiaineistosta, 30 artiklan säännöksiä PEPP-avaintietoasiakirjan tarkistamisesta, 31 artiklan säännöksiä siviilioikeudellisesta vastuusta, 32 artiklan säännöksiä biometrisiä riskejä kattavista PEPP-sopimuksista, 33 artiklan säännöksiä PEPP-avaintietoasiakirjan toimittamisesta, 34 artiklan säännöksiä PEPP-asiakkaan tarpeiden ja vaatimusten täsmentämisestä ja neuvonnan antamisesta, 35 artiklan säännöksiä PEPP-etuusotetta koskevista yleisistä säännöksistä, 36 artiklan säännöksiä PEPP-etuusotteen sisällöstä, 37 artiklan säännöksiä PEPP-etuusotetta täydentävistä lisätiedoista, 38 artiklan säännöksiä PEPP-säästäjille eläkkeelle siirtymistä edeltävässä vaiheessa ja PEPP-edunsaajille maksatusvaiheessa annettavista tiedoista, 39 artiklan säännöksiä PEPP-säästäjille ja PEPP-edunsaajille pyynnöstä annettavista tiedoista, 40 artiklan säännöksiä yleisistä säännöksistä koskien raportointia kansallisille viranomaisille, 41 artiklan säännöksiä kerryttämisvaiheen sijoittamista koskevista säännöistä, 42 artiklan säännöksiä PEPP-säästäjien sijoitusvaihtoehtoja koskevista yleisistä säännöksistä, 43 artiklan säännöksiä PEPP-säästäjän tekemästä sijoitusvaihtoehdon valinnasta, 44 artiklan säännöksiä valitun sijoitusvaihtoehdon muuttamisen edellytyksistä, 45 artiklan säännöksiä PEPP-perustuotteesta, 46 artiklan säännöksiä riskien vähentämistekniikoista, 47 artiklan säännöksiä kerryttämisvaiheeseen liittyvistä ehdoista, 48 artiklan säännöksiä säilytysyhteisön säilytys- ja valvontatehtävistä, 50 artiklan säännöksiä PEPP-asiakkaiden valitusten ratkaisemisesta, 52 artiklan säännöksiä vaihtopalvelun tarjoamisesta, 53 artiklan säännöksiä vaihtopalvelun käynnistämisestä, 54 artiklan säännöksiä vaihtopalveluun liittyvistä maksuista, 55 artiklan säännöksiä PEPP-säästäjien suojaamisesta taloudellisilta tappioilta tai 56 artiklan säännöksiä vaihtopalvelua koskevista tiedoista;

13) EU:n DORA-asetuksen 5–15 artiklan säännöksiä TVT-riskin hallinnasta, 17–19 artiklan säännöksiä TVT:hen liittyvien poikkeamien hallinnasta, luokittelusta ja raportoinnista, 24–27 artiklan säännöksiä digitaalisen häiriönsietokyvyn testauksesta tai 28–30 artiklan säännöksiä kolmansiin osapuoliin liittyvän TVT-riskin hallinnasta.

— —

44 §

EU:n DORA-asetuksen rikkomista koskevat säännökset

EU:n DORA-asetuksen 51 artiklan 2 kohdassa ja 54 artiklassa säädetään asetuksen mukaisten vaatimusten rikkomisen johdosta määrättävän hallinnollisen seuraamuksen määräämisessä tai

muun päätöksen tekemisessä huomioon otettavista seikoista sekä hallinnollisten seuraamusten julkistamisesta.

50 p §

Toiminta EU:n DORA-asetuksessa, NIS2-direktiivissä ja CER-direktiivissä tarkoitettuna toimivaltaisena viranomaisena

Finanssivalvonta toimii EU:n DORA-asetuksen 46 artiklan tarkoittamana toimivaltaisena viranomaisena.

Finanssivalvonta toimii NIS2-direktiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen I toimialojen 3 ja 4 osalta.

Finanssivalvonta toimii CER-direktiivin 9 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen toimialojen 3 ja 4 osalta.

71 §

Oikeus ja velvollisuus luovuttaa tietoja

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:

— —

19) Euroopan komissiolle sellaisia finanssimarkkinoiden valvontaan liittyviä tietoja, jotka ovat tarpeen komissiolle säädetyn toimivallan käyttämiseksi;

20) Liikenne- ja viestintävirastolle 3 f §:n 3 momentissa tarkoitetun yhteistyön toteuttamista varten.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

2.

Laki

luottolaitostoiminnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan luottolaitostoiminnasta annetun lain (610/2014) 9 luvun 2 §:n 1 momentin 4 kohta ja 16 §:n 3 momentti sekä 11 luvun 2 §:n 2 momentin 10 kohta,

sellaisena kuin niistä on 11 luvun 2 §:n 2 momentin 10 kohta laissa 233/2021, sekä

lisätään 9 luvun 2 §:n 1 momenttiin uusi 4 kohta, jolloin nykyinen 4 kohta siirtyy 5 kohdaksi, ja 11 luvun 2 §:n 2 momenttiin, sellaisena kuin se on laissa 233/2021, uusi 11 kohta seuraavasti:

9 luku

Riskien hallinta

2 §

Riskienhallintajärjestelmälle asetettavat yleiset vaatimukset

Luottolaitoksella on oltava tehokkaat ja luotettavat sekä kirjallisesti kuvatut hallinto- ja ohjausjärjestelmät luottolaitokseen ja sen toimintaan kohdistuvien nykyisten ja tulevien riskien tunnistamiseksi, hallitsemiseksi, rajoittamiseksi, seuraamiseksi ja riskeistä raportoimiseksi. Näihin kuuluvat:

— —

4) Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten mukaiset verkko- ja tietojärjestelmät;

5) palkitsemisjärjestelmiä koskevat toimintaperiaatteet ja menettelytavat, jotka ovat sopusoinnussa terveen ja tehokkaan riskienhallinnan kanssa ja edistävät sitä.

— —

16 §

Operatiivinen riski

— —

Luottolaitoksella on oltava varautumis- ja jatkuvuussuunnitelmat liiketoiminnan vakaviin häiriöihin varautumiseen, toiminnan jatkuvuuden turvaamiseen sekä häiriötilanteissa aiheutuvien vahinkojen rajoittamiseen. Mainittuihin suunnitelmiin sisällytettävistä luottolaitoksen tieto- ja viestintätekniikan liiketoiminnan jatkuvuutta koskevista toimintaperiaatteista ja suunnitelmista sekä tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmista säädetään Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 11 artiklassa.

— —

11 luku

Luottolaitoksen valvonta

2 §

Valvojan arvio

— —

Edellä 1 momentissa tarkoitetussa valvojan arviossa tulee ottaa huomioon ainakin:

— —

10) luottolaitokseen kohdistuva rahoitustaseen korkoriski;

11) Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 IV luvun mukaisen digitaalisen häiriönsietokyvyn testauksen paljastamat riskit.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

3.

Laki

sijoituspalvelulain 7 luvun 2 §:n ja 7 a luvun 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sijoituspalvelulain (747/2012) 7 luvun 2 §:n 3–5 momentti sekä 7 a luvun 1 §:n 1 momentin 1 kohta ja 2 momentti, sellaisina kuin ne ovat laissa 1069/2017, seuraavasti:

7 luku

Sijoituspalveluyrityksen toiminnan järjestäminen

2 §

Toiminnan luotettava järjestäminen

— —

Sijoituspalveluyrityksen on toteutettava kohtuulliset toimenpiteet sijoituspalvelujen tarjoamisen ja sijoitustoiminnan harjoittamisen jatkuvuuden ja säännönmukaisuuden turvaamiseksi. Tätä varten sijoituspalveluyrityksen on käytettävä tarkoituksenmukaisia ja oikeasuhteisia järjestelmiä, resursseja ja menettelyjä. Sähköisen tietojenkäsittelyn valvonta- ja suojajärjestelyjen on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännöksien mukaisia.

Sijoituspalveluyrityksellä on oltava moitteettomat hallinto- ja kirjanpitomenettelyt, omat sisäiset valvontamekanismit sekä tehokkaat riskinarviointimenettelyt.

Sijoituspalveluyrityksellä on oltava käytössään vakaat turvajärjestelmät, joiden avulla voidaan varmistaa tiedonsiirtovälineiden suojaus ja todentaminen Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten edellyttämällä tavalla, minimoida tiedon turmeltumisen ja luvattoman käytön riski ja estää tietojen vuotaminen ja jotka turvaavat tiedon luottamuksellisuuden kaikissa vaiheissa, rajoittamatta Finanssivalvonnan pääsyä tietoihin.

— —

7 a luku

Algoritminen kaupankäynti ja suora sähköinen markkinoillepääsy

1 §

Algoritminen kaupankäynti

Algoritmista kaupankäyntiä harjoittavalla sijoituspalveluyrityksellä on oltava käytössään sen harjoittamaan liiketoimintaan soveltuvat tehokkaat järjestelmät ja riskienhallintamenetelmät, joiden avulla voidaan:

1) varmistaa sen kaupankäyntijärjestelmien häiriönsietokyky ja riittävä kapasiteetti Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 II luvun ja sen nojalla annettujen säännösten mukaisesti sekä asianmukaiset kaupankäynnin raja-arvot ja limiitit;

— —

Edellä 1 momentissa tarkoitetulla sijoituspalveluyrityksellä on lisäksi oltava käytössään tehokkaat liiketoiminnan jatkuvuutta koskevat järjestelyt, joiden avulla voidaan korjata sen kaupankäyntijärjestelmissä esiintyvät häiriöt. Sijoituspalveluyrityksellä on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 11 artiklan mukaiset tieto- ja viestintätekniikan liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja suunnitelmat sekä tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmat. Sijoituspalveluyrityksen on varmistettava, että sen järjestelmät ovat kaikilta osin testattuja ja niitä valvotaan asianmukaisesti, jotta ne täyttävät 1 ja 2 momentissa sekä Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2554 ja sen nojalla säädetyt vaatimukset.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

4.

Laki

maksulaitoslain 19 a ja 19 b §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan maksulaitoslain (297/2010) 19 a §:n 1 momentti ja 19 b §, sellaisina kuin ne ovat laissa 890/2017, seuraavasti:

19 a §

Operatiivisten ja turvallisuusriskien hallinta

Maksulaitoksen, 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavan henkilön ja 7 b §:ssä tarkoitetun tilitietopalvelun tarjoajan on luotava riittävä riskienhallintajärjestelmä riskienhallintatoimenpiteistä ja valvontamekanismeista tarjoamiensa maksupalveluiden operatiivisten ja turvallisuusriskien hallitsemiseksi. Niillä on oltava tehokas poikkeamien hallintamenettely ja niiden on kyettävä havaitsemaan ja luokittelemaan merkittävät operatiiviset ja turvapoikkeamat. Mitä tässä momentissa säädetään, ei rajoita Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 II luvun ja sen nojalla annettujen säännösten soveltamista.

— —

19 b §

Poikkeamista ja petoksista ilmoittaminen

Tiliä pitävän maksulaitoksen ja 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavan henkilön on ilmoitettava Finanssivalvonnalle, jos se havaitsee, että tilitietopalvelun tai maksutoimeksiantopalvelun tarjoaja käyttää maksutiliä oikeudettomasti tai petollisesti ja tilinpitäjä sen perusteella estää tilitietopalvelun tai maksutoimeksiantopalvelun tarjoajan pääsyn maksutilille. Ilmoituksen on sisällettävä riittävät tiedot poikkeamasta sekä toimenpiteet sen johdosta. Finanssivalvonnan on arvioitava tapaus ja ryhdyttävä tarvittaviin toimenpiteisiin.

Maksulaitoksen, 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavan henkilön ja 7 b §:ssä tarkoitettujen tilitietopalvelun tarjoajan on toimitettava vähintään vuosittain Finanssivalvonnalle tilastotiedot maksuvälineisiin liittyvistä petoksista. Finanssivalvonnan on toimitettava nämä tiedot kootusti Euroopan pankkiviranomaiselle ja Euroopan keskuspankille. Finanssivalvonta voi antaa tarkempia määräyksiä tässä momentissa tarkoitetusta raportointivelvollisuudesta.

Mitä 1 ja 2 momentissa säädetään, ei sovelleta sähkörahayhteisöön.

Maksulaitoksen, 7 §:ssä tarkoitetun poikkeuksen nojalla maksupalveluita tarjoavan henkilön, tilitietopalvelun tarjoajan ja sähköisen rahan liikkeeseenlaskijan velvollisuudesta ilmoittaa tieto- ja viestintätekniikkaan sekä toiminnan harjoittamiseen tai turvallisuuteen vaikuttaviin maksuihin liittyvistä poikkeamista säädetään Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 III luvussa.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

5.

Laki

kaupankäynnistä rahoitusvälineillä annetun lain 3 luvun 1 ja 18 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan kaupankäynnistä rahoitusvälineillä annetun lain (1070/2017) 3 luvun 1 §:n 1 ja 3 momentti sekä 18 §:n 1 momentin 1 kohta, sellaisina kuin ne ovat laissa 259/2019, seuraavasti:

3 luku

Säännellyn markkinan toiminnan järjestäminen

1 §

Säännellyn markkinan toiminnan järjestämistä koskevat vaatimukset

Pörssin toiminta on järjestettävä sen liiketoiminnan laatu ja laajuus huomioon ottaen luotettavalla tavalla. Pörssin on varmistettava toimintaansa liittyvien riskien hallinta ja toimintansa jatkuvuus kaikissa tilanteissa. Pörssin on hallittava tieto- ja viestintätekniikkaan liittyviä riskejä Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 II luvun ja sen nojalla annettujen säännösten mukaisesti.

— —

Pörssin on varmistettava kaupankäyntijärjestelmän toiminnan luotettavuus ja jatkuvuus myös häiriötilanteissa. Pörssillä on oltava toiminnallinen häiriönsietokyky, jota sen on ylläpidettävä Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 II luvun ja sen nojalla annettujen säännösten mukaisesti ja siten varmistettava, että sillä on riittävä kaupankäyntijärjestelmien häiriönsietokyky, riittävä kapasiteetti toimeksiantojen ja viestien ruuhkahuippujen käsittelyyn ja varmistettava asianmukainen kaupankäynti markkinoiden vakavissa stressiolosuhteissa. Sään-

nellyn markkinan palvelujen jatkuvuuden varmistamiseksi pörssillä on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 11 artiklan mukaiset tieto- ja viestintätekniikan liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet ja suunnitelmat, sekä tieto- ja viestintätekniikan reagointi- ja palautumissuunnitelmat. Pörssin on testattava säännöllisesti kuormituskokein kaupankäyntijärjestelmän toimintaa edellä kuvattujen vaatimusten täyttämiseksi.

18 §

Algoritminen kaupankäynti

Pörssillä on oltava käytössään tehokkaat järjestelmät ja menettelytavat, sen varmistamiseksi, että algoritminen kaupankäynti ei aiheuta tai ole omiaan aiheuttamaan tavanomaisesta poikkeavia kaupankäyntiolosuhteita ja että pörssi voi käsitellä kaikkia algoritmisesta kaupankäynnistä aiheutuneita tavanomaisesta poikkeavia kaupankäyntiolosuhteita. Pörssin järjestelmien ja menettelytapojen tulee sisältää:

1) velvoite kaupankäyntiosapuolille testata algoritmejaan pörssin tarjoamassa testausympäristössä Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 II ja IV luvun ja sen nojalla annettujen säännösten mukaisesti;

Tämä laki tulee voimaan päivänä kuuta 20 .

6.

Laki

sijoitusrahastolain 5 luvun 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sijoitusrahastolain (213/2019) 5 luvun 1 §:n 1 momentti seuraavasti:

5 luku

Vakavaraisuus ja riskienhallinta

1 §

Rahastoyhtiön riskienhallinta

Rahastoyhtiö ei saa toiminnassaan ottaa niin suurta riskiä, että siitä aiheutuu olennaista vaaraa rahastoyhtiön vakavaraisuudelle. Rahastoyhtiöllä on oltava toimintaansa nähden riittävä sisäinen valvonta ja riittävät riskienhallintajärjestelmät. Sähköisen tietojenkäsittelyn valvonta- ja suojajärjestelyjen on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten mukaisia.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

7.

Laki

vaihtoehtorahastojen hoitajista annetun lain 7 luvun 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan vaihtoehtorahastojen hoitajista annetun lain (162/2014) 7 luvun 2 §:n 1 momentti seuraavasti:

7 luku

Toiminnan järjestäminen

2 §

Hallinto- ja valvontajärjestelyt

Vaihtoehtorahastojen hoitajalla on oltava luotettavat hallinto- ja kirjanpitomenettelyt. Sähköisen tietojenkäsittelyn valvonta- ja suojajärjestelyjen on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten mukaisia.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

8.

Laki

lisäeläkesäätiöistä ja lisäeläkekassoista annetun lain 3 luvun 12 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan lisäeläkesäätiöistä ja lisäeläkekassoista annetun lain (947/2021) 1 luvun 13 §:n 1 momentti,
lisätään 3 luvun 12 §:ään uusi 4 momentti seuraavasti:

1 luku

Lain soveltaminen ja toiminnan keskeiset periaatteet

13 §

Säännökset, joiden soveltaminen riippuu vakuutettujen lukumäärästä

Lisäeläkelaitokseen, jossa on vähemmän kuin 100 vakuutettua (*pieni lisäeläkelaitos*), ei sovelleta 3 luvun 1 ja 5–11 §:ää, 12 §:n 1–3 momenttia, 13 ja 15–17 §:ää, 4 luvun 2 §:ää, 6 luvun 27–35 §:ää, 7 luvun 1 §:ää, 2 §:n 2 momenttia, 4, 5 ja 8–12 §:ää, 13 lukua eikä 15 luvun 1–6 ja 8–10 §:ää.

— —

3 luku

Johto ja hallintojärjestelmä

12 §

Toimintaperiaatteet, sisäisen valvonnan järjestelmä ja varautumissuunnitelma

— —

Lisäeläkelaitoksen verkko- ja tietojärjestelmien on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten mukaisia.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

9.

Laki

vakuutusyhtiölain 6 luvun 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan vakuutusyhtiölain (521/2008) 6 luvun 8 §:n 4 momentti, sellaisena kuin se on laissa 981/2013, seuraavasti:

6 luku

Vakuutusyhtiön johto, hallintojärjestelmä ja varojen sijoittaminen

8 §

Yleiset hallintovaatimukset

— —

Vakuutusyhtiön on varmistettava toimintansa jatkuvuus ja toimintavarmuus. Tätä varten yhtiöllä on oltava jatkuvuussuunnitelma. Vakuutusyhtiön verkko- ja tietojärjestelmien on oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 ja sen nojalla annettujen säännösten mukaisia.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

10.

Laki

Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annetun lain 1 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään Teollisen yhteistyön rahasto Oy -nimisestä osakeyhtiöstä annetun lain (291/1979) 1 §:ään, sellaisena kuin se on osaksi laeissa 1617/1991 ja 1083/2000, uusi 5 momentti seuraavasti:

1 §

— —

Yhtiöön ei sovelleta Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

11.

Laki

valtion erityisrahoitusyhtiöstä annetun lain 3 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään valtion erityisrahoitusyhtiöstä annetun lain (443/1998) 3 §:ään, sellaisena kuin se on osaksi laissa 1545/2011, uusi 5 momentti seuraavasti:

3 §

Hallinto

— —

Yhtiöön ei sovelleta Euroopan parlamentin ja neuvoston asetusta (EU) 2022/2554.

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä x.x.20xx

Pääministeri

Petteri Orpo

..ministeri Etunimi Sukunimi