IV Rahoitussektori

Määräykset ja ohjeet 8/2014 Operatiivisen riskin hallinta rahoitussektorin valvottavissa: Yhteenveto ja palaute lausunnoista

Viittaus	**Kommentit perusteluineen (ja mahdollinen muotoiluehdotus)**	**Finanssivalvonnan vastaus**
Yleiset kommentit	*Voimaantulo* Nasdaq Helsinki toteaa, että valvottavatiedotteessa 2.8.2019 ei kerrota milloin uusittava Määräysluonnos on tarkoitus saattaa voimaan. Jos Finanssivalvonta edellä esitetyistä syistä huolimatta päätyy siihen, että Määräysluonnos ulotetaan nykyistä standardia laajemmin pörsseihin, voimaantulolle on asetettava riittävän pitkä siirtymäaika (4-6kk).	Voimaantulolle tullaan asettamaan riittävä siirtymäaika.
Lukukohtaiset kommentit		
Luku 1.1.1.	Nasdaq Helsinki Oy toteaa, että määräysluonnoksen soveltamisalaa on laajennettu, sillä kohdan 1.1.1 mu-	Finanssivalvonta toteaa, että raportointivelvollisuuden laajentaminen pörssiin on perusteltua pörssin

	kaan Finanssivalvonnalle tehtäviä ilmoituksia toiminnan häiriöistä ja virheistä koskevaa lukua 9.1 sovellettaisiin jatkossa myös pörssiin. Pörssi pitää tärkeänä operatiivisen riskin hallinnan järjestämistä, mutta katsoo, että luottolaitosten ja sijoituspalveluyritysten toiminta ja asiakaskunta eroavat siinä määrin pörssitoiminnasta, ettei ole tarkoituksenmukaista asettaa näille samoja standardeja häiriötilanteiden raportointiin. Pörssi on osa amerikkalaista Nasdaq -konsernia, jonka pohjoismaisen alakonsernin emoyhtiönä toimii Nasdaq Nordic Oy. Alakonserniin kuuluvat Pörssin lisäksi muun muassa Ruotsin, Tanskan ja Islannin pörssit. Tehokkuuden ja toimintavarmuuden kannalta on tarpeellista, että Pörssien toimintaa, muun muassa häiriötilanteiden raportointia, hoidetaan mahdollisuuksien mukaan keskitetysti. Tällöin ei ole tarkoituksenmukaista, että yksittäisen maan finanssivalvoja asettaa pörssille määräyksiä, jotka rajoittavat keskitettyä häiriötilanteiden raportointia. Finanssivalvonta toimii useissa Pörssiä koskevissa valvontakysymyksissä yhdessä pohjoismaisten finanssivalvojien kanssa. Määräysluonnoksen mukaiset raportointimenettelyt soveltuvat varsin huonosti käytössä oleviin yhteispohjoismaisesti sovittuihin käytäntöihin, jotka ovat Pörssin	toiminnan kriittisyyden vuoksi. Raportointivelvollisuudesta on säädetty laissa kaupankäynnistä rahoitusvälineillä (1070/2017). Finanssivalvonta ottaa kuitenkin huomioon yhteispohjoismaisen toiminnan ja sen keskitetyn ja yhtenäisen raportointitavan ja täsmentää siitä syystä 9.1. luvun määräyksiä ja ohjeita siten, että raportointi voidaan toteuttaa Pörssin yhteispohjoismaisen raportoinnin yhteydessä.

	näkemyksen mukaan toimineet hyvin. Kun operatiivisten riskien hallintaa koskevia määräyksiä ja ohjeita viimeksi päivitettiin, Finanssivalvonta arvioi, ettei lukua 9 ollut tarpeen ulottaa pörsseihin. Pörssin näkemyksen mukaan uusi sääntely, mukaan lukien Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6.7.2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, ei anna aihetta laajentaa soveltamisalaa tältä osin. Edellä mainituilla perusteilla Pörssi katsoo, että Finanssivalvonnan ei tulisi soveltaa Määräysluonnoksen lukua 9.1 Pörssiin.	
Luku 9.1, kohta 2	OP-ryhmä katsoo, että operatiivista riskiä koskevissa määräyksien ja ohjeiden kohtaa 9.1. (2) pitäisi täsmentää. Tietosuoja-asetuksen ja määräysluonnoksen kriteerit tietoturva-/tietosuojaloukkauksille ovat hieman erilaiset. Valvottavalla on velvollisuus raportoida tietojen paljastumisesta asiattomille tietosuoja-asetuksen raportointivelvoitteiden mukaisesti. Tietosuoja-asetuksen ilmoitusvelvollisuus sekä tietosuojavaltuutetulle että rekisteröidyille perustuu valvottavan omaan riskiarvioon.	Finanssivalvonta toteaa, että määräyksiä ja ohjeita täsmennetään siten, että raportointivelvollisuus on yhdenmukainen tietosuojasääntelyn raportointivelvoitteiden osalta.

	Luonnoksessa esitetty sanamuoto voi johtaa siihen, että ”tietojen paljastumista” koskevasta tapahtumasta ilmoitetaan aina Finanssivalvonnalle, mutta ei välttämättä tietosuojavaltuutetulle, jos valvottava katsoo, että tapahtuneesta ei aiheudu riskiä rekisteröidyille. Myöskään määrittelyt koskien ”poikkeamia” ja ”häiriöitä” eivät ole yhdenmukaisia tietosuojaasetuksen kanssa ja tämä saattaa aiheuttaa epäselvyyttä valvottavien näkökulmasta. Lähtökohtana tulisi olla, että ei-teknisistä tietosuoja-asetuksen mukaisista tietoturvaloukkauksista (esim. inhimillinen virhe sähköpostin lähetyksessä) ilmoitettaisiin tietosuojavaltuutetulle/rekisteröidyille valvottavan oman riskiarvion perusteella. Toisin sanoen esitämme, että valvottavalla tulisi olla velvollisuus ilmoittaa Finanssivalvonnalle ainoastaan sellaisista merkittävistä teknisistä häiriöistä, joissa tietoja paljastuu asiattomille. Aktia Pankki Oyj kiinnittää huomiota kohdan 9.1. (2) sanamuotoon, jossa on virhe: Maksujenvälityksessä ja korttimaksamisessa merkittäviksi häiriöiksi katsotaan esimerkiksi suurta määrää asiakkaita koskeva häiriö tai viivästys sekä häiriö.	Finanssivalvonta korjaa kohdan 9.1. (2) sanamuodon.

	Aktia Pankki Oyj toteaa, että määräyksien kohdan 9.1 (2) ja 9.1 (4) tekstit antavat kuvan, että kaikki tapaukset, myös yksittäisiä asiakkaita koskevat, joissa asiakastietoja on päätynyt ulkopuoliselle taholle, olisi ilmoitettava Finanssivalvonnalle. Pankin mielestä tällaisissa yksittäistapauksissa ei useinkaan ole kyse merkittävistä häiriöistä. Kyse voi olla esimerkiksi siitä, että toimihenkilö on vahingossa lähettänyt viestin väärälle henkilölle. Myöskään tietosuoja-asetus ei velvoita kaikkien tapausten ilmoittamista Tietosuojavaltuutetulle. Ehdotamme, että tätä kohtaa täsmennettäisiin ja yhtenäistettäisiin tietosuojavaltuutetun vaatimusten kanssa. Samoin kohtaa 9.1. (4). Aktia toteaa myös, että tietoturvallisuushäiriöiden osalta kaikki verkko- ja tietoturvallisuuteen liittyvät häiriöt eivät olisi merkittäviä vaan niissä voi olla lieviä häiriöitä tai poikkeamia sisäisitä ohjeistoista, jotka kyetään hoitamaan ilman vaikutusta esim. asiakaspalveluun tai vaarantamatta assettien tietoturvallisuutta. Ehdotamme, että tietoturvallisuustapahtumien osalta merkittävyys kytkettäisiin asiakaspalvelun häiriintymiseen.	Finanssivalvonta toteaa, että määräyksiä ja ohjeita täsmennetään siten, että raportointivelvollisuus on yhdenmukainen tietosuojasääntelyn raportointivelvoitteiden osalta. Tietoturvallisuuteen liittyvien häiriöiden osalta Finanssivalvonta toteaa, että merkittävyyttä ei aina voida arvioida asiakkaille tarjottavien häiriintymisen kannalta. Häiriö voi olla vakava myös muiden kuin asiakkaille tarjottavien palveluiden osalta ja vaikuttaa valvottavan kannalta kriittiseen toimintaan.

Luku 9.1, kohta 4	OP-ryhmä esittää, että palvelunestohyökkäystä koskeva raportointi siirretään alakohdasta 9.1(4) alakohdan 9.1(5) alle eli raportoitavaksi vain, jos palvelunestohyökkäyksellä on vaikutuksia asiakkaan saamaan palveluun. Perusteluna esitämme, että pieniä hyökkäyksiä tai hyökkäyksen yrityksiä, jotka eivät vaikuta asiakkaan saamaan palveluun, tulee usein ja jokaisesta tällaisesta tehtävä raportointi vaatii valvottavalta resursseja.	Finanssivalvonta toteaa, että määräyksiä ja ohjeita muutetaan siten, että merkittävyys kytketään asiakkaille tarjottavien palveluiden häiriöihin.
	Finanssiala ry toteaa, että luonnoksen kohdan 9.1 alakohta 4 edellyttää, että haittaohjelman levittäminen tietojärjestelmään tulisi raportoida Finanssivalvonnalle. FA pitää ilmaisua tulkinnanvaraisena, koska se voisi kattaa esim. tilanteet, joissa saastuneen liitetiedoston sisältävä viesti on päässyt sisään yrityksen sähköpostijärjestelmään, vaikka viesti olisikin sittemmin poistettu organisaation tietoturvaohjeiden mukaisesti. FA ehdottaakin, että raportointi rajoitettaisiin tilanteisiin, jossa haittaohjelma on päässyt leviämään rahoitusalan yrityksen tietojärjestelmään.	Finanssivalvonta toteaa, että raportointiin liittyviä määräyksiä ja ohjeita muutetaan täsmällisemmiksi tietoturvallisuuteen liittyvien häiriöiden osalta.
	Saman alakohdan mukaisesti toimijan tulisi myös raportoida kaikki palvelunestohyökkäykset. FA pitää velvoitetta tarpeettoman laajana ja esittää, että se rajataan vain hyökkäyksiin, jotka ovat	Finanssivalvonta toteaa, että määräyksiä ja ohjeita muutetaan ehdotuksen mukaisesti.

	ilmenneet yrityksen toimintojen tai asiakkaille tarjottavien palvelujen näkyvänä häiriönä. Rahoitusalan yritysten ohella käytännössä kaikkiin yksityisen ja julkisen sektoriin toimijoihin kohdistuu jatkuvia palvelunestohyökkäyksiä, joista valtaosa torjutaan menestyksellisesti ja vain murto-osa aiheuttaa näkyviä vaikutuksia yrityksen sisäisiin toimintoihin tai asiakkaille näkyviin palveluihin. Aktia Pankki Oyj toteaa, että määräyksien kohdan 9.1 (2) ja 9.1 (4) tekstit antavat kuvan, että kaikki tapaukset, myös yksittäisiä asiakkaita koskevat, joissa asiakastietoja on päätynyt ulkopuoliselle taholle, olisi ilmoitettava Finanssivalvonnalle. Pankin mielestä tällaisissa yksittäistapauksissa ei useinkaan ole kyse merkittävistä häiriöistä. Kyse voi olla esimerkiksi siitä, että toimihenkilö on vahingossa lähettänyt viestin väärälle henkilölle. Myöskään tietosuoja-asetus ei velvoita kaikkien tapausten ilmoittamista Tietosuojavaltuutetulle. Ehdotamme, että tätä kohtaa täsmennettäisiin ja yhtenäistettäisiin tietosuojavaltuutetun vaatimusten kanssa.	Finanssivalvonta toteaa, että raportointiin liittyviä määräyksiä ja ohjeita muutetaan täsmällisemmiksi tietoturvallisuuteen liittyvien häiriöiden osalta siten, että merkittävyys kytketään asiakkaille tarjottavien palveluiden häiriöihin.

Luku 9.1, kohta 9	Luonnoksen kohdan 9.1 alakohdan 9 mukaisesti Finanssivalvonnalle tehtävä ilmoitus ei poistaisi valvottavan velvollisuutta raportoida tietojen paljastumisesta asiattomille myös tietosuojaasetuksen raportointivelvoitteiden mukaisesti. Tietosuoja-asetuksen asettamat raportointivelvoitteet ovat laajoja ja FA pitää tärkeänä, ettei niitä pyritä edelleen laajentamaan rahoitustoimialan osalta. Rahoitusalan toimijat ovat panostaneet merkittävästi tietosuojaasetuksen toimeenpanoon ja FA katsoo, että tältä osin asetuksen vaatimusten ja sen edellyttämien toimintatapojen noudattamisen tulisi riittää. Tällöin Finanssivalvonnalle raportoitavat tietosuojatapahtumat rajattaisiin niihin, jotka ilmoitetaan tietosuojavaltuutetulle.	Finanssivalvonta toteaa, että luvun 9.1. kohdan 9 ohje on tarpeellinen, mutta kohtaa 9.1. (2) täsmennetään siten, että Finanssivalvonnalle tulee raportoida tietosuojapoikkeamien osalta vain tapahtumat, joista on velvollisuus raportoida myös Tietosuojavaltuutetulle.