Oletko valmistautunut DORA-asetuksen voimaantuloon?

Sami Rintala
Partner

Petteri Günther
Counsel

Finanssialan häiriönsietokyvystä annettu asetus, DORA (Digital Operational Resilience Act), tulee sovellettavaksi 17.1.2025 alkaen.

EU:n DORA-asetus parantaa finanssiyhteisöjen toimintavarmuutta käsittelemällä sen riippuvuutta tieto- ja viestintätekniikasta. DORA koskee kaikkia Finanssivalvonnan valvottavia, pois lukien työeläkeyhtiöt. DORA on olennainen myös finanssiyhteisöille ja tieto- ja viestintätekniikkapalvelujen (TVT) tarjoajille. Asetus sisältää niiden ja finanssiyhteisöjen välillä tehtyjä sopimuksia koskevia vaatimuksia, joiden tarkoituksena on tukea finanssiyhteisöjä noudattamaan niille asetettuja vaatimuksia häiriönsietokyvyn korkean tason saavuttamiseksi.

Finanssiyhteisöjen hallitukset ovat vastuussa DORA:n noudattamisen varmistamisesta. Tähän kuuluu tietoturvallisuuspolitiikkaa koskevien päätösten tekeminen, resurssien jakaminen politiikan toteuttamiseen ja yleisen vaatimustenmukaisuuden valvonta.

Mitä vaatimuksia DORA sisältää?

DORA rakentuu viiden keskeisen osa-alueen ympärille:

- Tieto- ja viestintätekniikan (TVT) riskien hallinta
- Laajamittaisten TVT:hen liittyvien poikkeamien raportointi ja vapaaehtoinen ilmoittaminen merkittävistä kyberuhista viranomaisille
- Digitaalisen häiriönsietokyvyn testaus
- Kyberuhkia ja haavoittuvuuksia koskevien tietojen ja tiedustelutietojen jakaminen

- Toimenpiteet, joilla varmistetaan, TVT-palveluntarjoajiin liittyvä riskien hallinta

DORA:ssa on erikseen palveluntarjoajien TVT-riskin hallintaan liittyviä vaatimuksia ja velvoitteita, jotka tulee toteuttaa ennen TVT-palvelun sopimusjärjestelyä. DORA sisältää myös keskeisiä sopimusmääräyksiä, jotka tulee sisällyttää finanssiyhteisöjen solmimiin sopimuksiin TVT-palveluntarjoajien kanssa. Sopimusmääräykset ovat laajempia, jos kyseessä on kriittisiä tai tärkeitä toimintoja tukevien TVT-palvelujen käyttöä koskeva sopimus.

DORA ja sen vaatimusten tärkeimmät tarkemmat yksityiskohdat on asetuksessa jätetty täsmennettäväksi toissijaisen sääntelyn kautta. Tähän kuuluvat tekniset sääntelystandardit (RTS) sekä täytäntöönpanostandardit (ITS). Euroopan komissio on tähän mennessä hyväksynyt seuraavan toissijaisen sääntelyn:

- DORA:n täydentämisestä teknisillä sääntelystandardeilla, joissa täsmennetään TVT:hen liittyvien poikkeamien ja kyberuhkien luokittelukriteerit, vahvistetaan olennaisuusrajat ja täsmennetään laajavaikutteisia poikkeamia koskevien raporttien yksityiskohdat
- DORA:n täydentämisestä teknisillä sääntelystandardeilla, joissa täsmennetään TVT-palveluntarjoajana olevien kolmansien osapuolten tarjoamien, kriittisiä tai tärkeitä toimintoja tukevien TVT-palvelujen käytöstä tehtyjä sopimusjärjestelyjä koskevien toimintaperiaatteiden yksityiskohtainen sisältö
- DORA:n täydentämisestä TVT-riskinhallintavälineitä, -menetelmiä, -menettelyjä ja -politiikkatoimia sekä yksinkertaistettua TVT-riskinhallintajärjestelmää koskevilla teknisillä sääntelystandardeilla
- DORA:n täydentämisestä täsmentämällä kriteerit TVT-palveluntarjoajana olevien kolmansien osapuolten nimeämiseksi finanssiyhteisöjen kannalta kriittisiksi
- DORA:n täydentämisestä määrittämällä päävalvojan kriittisiltä TVT-palveluntarjoajana olevilta kolmansilta osapuolilta perimien valvontamaksujen suuruus ja maksutapa

RTS:ien tarkoituksena on ohjata finanssiyhteisöjä ottamaan käyttöön kattavat ja toimivat käytännöt tieto- ja viestintätekniikkariskien hallintaa varten. Tähän sisältyy asianmukaisten toimenpiteiden tunnistaminen, arviointi ja toteuttaminen.

Jokaisen finanssiyhteisön tulee ottaa käyttöön useita toimenpiteitä ja menettelyjä esim.:

- Tieto- ja viestintätekniikan tietoturvan alalla salausavainten hallintaa koskevat toimintatavat, jossa otetaan huomioon tietojen luokittelu ja riskinarviointi ja jolla varmistetaan, että salausmenetelmät ovat asianmukaisia ja kohdennetaan tunnistettuihin erityisriskeihin.
- Toimintatapoja, jolla tunnistetaan ja seurataan haavoittuvuuksia ja uhkia sekä tieto- ja viestintäteknisten järjestelmien ja toimintojen sisäisten että ulkoisten haavoittuvuuksien ja uhkien osalta.
- Yksityiskohtainen menettely tieto- ja viestintäteknisen omaisuuden, johon on sisällyttävä myös tiedot, hallinnoimiseksi.
- Tuotantoympäristöjen hallinnointia koskeva toimintatapa, jossa tuotantoympäristöt erotetaan tiukasti testaus- ja kehitysympäristöistä eturistiriitojen välttämiseksi sekä tuotantotietoihin ja -järjestelmiin pääsyn ja niiden muutosten tiukan valvonnan varmistamiseksi.
- Menettely ohjelmistopakettien hankkimiseksi ja kehittämiseksi sekä tehokkaaksi ja turvalliseksi integroimiseksi olemassa olevaan tietotekniseen ympäristöön vahvistettujen liiketoiminta- ja tietoturvatavoitteiden mukaisesti.

Näiden toimintatapojen tarkoituksena on parantaa tietoon perustuvaa tieto- ja viestintätekniikan riskienhallintaa ja edistää prosessien yleistä optimointia ja tehokkuutta.

Yritysten on sopeuduttava lyhyessä ajassa

Monet finanssiyhteisöt ja TVT-palveluntarjoajat ovat jo aloittaneet DORA-implementointiprosessin, siinä laajuudessa kuin se on ollut mahdollista. Lisäksi niiden on pantava täytäntöön RTS:ssä määritellyt lisävaatimukset. RTS:ien ja ITS:ien toisen sarjan julkaiseminen ja vahvistaminen on viivästynyt, mikä hankaloittaa täydellisen vaatimustenmukaisuuden saavuttamista 17. tammikuuta 2025 mennessä.

Kun otetaan huomioon laajat vaatimukset ja tiukat määräajat, yritysten olisi hyvä ottaa käyttöön kattava edistymis- ja toimintaseurantaraportointikäytäntö, jolla voidaan valvoa vaatimustenmukaisuuden saavuttamista ja tarvittaessa esittää valvovalle viranomaiselle konkreettista näyttöä oikea-aikaisesta sitoutumisesta.

DLA Piper on luonut toimintamallin helpottamaan uuden sääntelyn haltuunottoa finanssiyhteisöjen toiminnassa. Esimerkiksi toimittajasopimusten osalta lähtökohtana on arvio nykytilasta: kuinka finanssiyhteisö on huomioinut alan valvontaviranomaisten ohjeistukset, jota DORA yhdenmukaistaa ja uudistaa. Tämän arvion pohjalta laaditaan ns. gap-analyysi, jonka pohjalta tunnistetaan miltä osin nykytila ei vastaa DORA:n vaatimuksiin. Gap-analyysi puolestaan mahdollistaa vaatimuksenmukaisuuden varmistamiseksi tarvittavien korjaavien toimenpiteiden suunnittelemisen. Näin askelmerkit DORA:n vaatimusten implementoimiseksi finanssiyhteisön toimintaan ovat selvillä. Käytännön toteutus vaatii esimerkiksi toimittajasopimusten uudelleenneuvottelemista niiden vaatimuksenmukaisuudessa tunnistettujen puutteiden korjaamiseksi.

Vaikka toissijaisena sääntelynä annettavien teknisten sääntelystandardien (RTS) lopullisia versioita joudutaan vielä joiltain osin odottamaan, DORA:n haltuunotto kannattaa aloittaa viimeistään nyt ja huomioida täsmentyvät vaatimukset työn edetessä. Sääntelyn haltuunoton aloittaminen jo ennen kaikkien sääntelystandardien lopullisten versioiden vahvistamista tulee osoittautumaan arvokkaaksi, koska DORA:n tavoitteena olevan digitaalisen häiriönsietokyvyn varmistaminen itsessään on prosessi. Kyseessä on projektin sijaan jatkuva tekeminen, joka tulee ottaa osaksi finanssiyhteisöjen päivittäistä toimintaa.

On myös keskeistä vahvistaa erityisesti finanssiyhteisöjen johtoryhmien DORA-osaamista, jotta ne ovat riittävästi valmistautuneet huolehtimaan sääntelyn asettamien velvollisuuksien noudattamisesta. Tulevat kuukaudet tammikuun 17. päivään asti ovat ratkaisevan tärkeitä, jotta kaikkien DORA-vaatimusten asianmukainen noudattaminen voidaan varmistaa.

Ota yhteyttä, jos yrityksessäsi tarvitaan juridista neuvontaa DORA:an liittyvissä kysymyksissä.