VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

HE laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 67/2024 vp)

TALOUSVALIOKUNTA 19.6.2024

NEUVOTTELEVA VIRKAMIES MATTI SILLANMÄKI

DORA-asetus

- Asetus finanssialan digitaalisesta häiriönsietokyvystä (EU) 2022/2554 (DORA-asetus) yhdenmukaistaa rahoitusalan digitaalista häiriönsietokykyä koskevan sääntelyn EU:ssa.
- Asetusta sovelletaan laajasti rahoitusalan toimijoihin.
- Asetuksen keskeisenä sisältönä tieto- ja viestintätekniikan riskinhallintaa ja järjestelmien testaamista koskevat vaatimukset, TVT-poikkeamien hallinta ja raportointi, TVT-palvelujen ulkoistamiseen liittyvien riskien hallinta ja kriittisten TVT-palveluntarjoajien EU:n laajuinen valvontakehikko.
- Kansallisesti säädettävä erityisesti toimivaltaisen viranomaisen valvontavaltuuksista ja asetuksen rikkomisen perusteella määrättävistä seuraamuksista.
- Asetuksen edellyttämiä kansallisia säännöksiä sovellettava 17.1.2025 alkaen.

DORA-muutosdirektiivi

- DORA-asetuksen yhteydessä annettiin lisäksi DORA-muutosdirektiivi (EU) 2022/2556, jossa säädettiin useisiin direktiiveihin muutoksia, joiden tarkoituksena on varmistaa niiden johdonmukaisuus DORA-asetuksen kanssa.
- Käytännössä suurelta osin kyse vaatimuksista hallinnoida verkko- ja tietojärjestelmiä DORA-asetuksen mukaisesti osana sisäistä hallintoa sekä riskienhallinnan menettelyjä. Lisäksi esim. maksulaitosten osalta poistetaan direktiivistä asetuksen kanssa päällekkäisiä raportointivelvoitteita.

NIS 2 - ja CER-direktiivit

- Samaan aikaan DORA:n kanssa annettiin myös ns. NIS 2 -direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa ja ns. CER-direktiivi kriittisten toimijoiden häiriönsietokyvystä.
- Direktiivien soveltamisalassa kolme finanssiyhteisön tyyppiä: luottolaitokset, kauppapaikkojen ylläpitäjät ja keskusvastapuolet.
- Direktiivien velvoitteita ei sovelleta kyseisiin finanssialan toimijoihin, koska DORA-asetus sisältää niitä koskevat yksityiskohtaiset säännökset. Ne kuitenkin huomioidaan mm. direktiivien mukaisissa kansallisissa strategioissa ja viranomaisten yhteistyövelvoitteissa.

Fiva-lakiin ehdotettavat 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 tehtäviin lisättäisiin tehtävä 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 (uusi 3 f §).

Fiva-lakiin ehdotettavat muutokset

- Fiva-lain hallinnollisia seuraamuksia koskevia säännöksiä ehdotetaan täydennettävän DORA-asetuksen johdosta. Fiva 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 TVT-palveluntarjoajana oleva kolmas osapuoli, jolloin Fivan yleiset toimivaltuudet ulottuisivat myös näihin toimijoihin.
- Lisäksi eräitä viittaussäännöksiä ym. teknisluonteisia muutoksia.

Muihin lakeihin ehdotettavat muutokset

- Asianomaisiin lakeihin lisätään DORA-muutosdirektiivin edellyttämät viittaukset DORA-asetuksen velvoitteisiin.
- Luottolaitoslain mukaisessa ns. valvojan arviossa tulisi ottaa huomioon DORA-asetuksen IV luvun mukaisen digitaalisen häiriönsietokyvyn testauksen paljastamat riskit.
- Maksulaitoslain 19 b §:stä poistetaan voimassa olevan 1 ja 3 momentin säännökset poikkeamailmoituksista ja lisätään informatiivinen viittaus DORA-asetuksen poikkeamailmoituksia koskevaan sääntelyyn.

Kansallinen liikkumavara

- **Finanssiyhteisöille ei ehdoteta DORA-asetuksen velvoitteita pidemmälle meneviä kansallisia velvoitteita.**
- DORA-asetus mahdollistaa Teollisen yhteistyön rahasto Oy:n ja Finnvera Oyj:n jättämisen DORA-asetuksen soveltamisalan ulkopuolelle. Fiva ei nykyisellään valvo kumpaakaan toimijaa. Ehdotetaan käytettävän kansallinen liikkumavara tältä osin.
- DORA-asetuksen mukaan jäsenvaltiot voivat päättää, että finanssiyhteisöjen on raportoitava TVT-poikkeamista DORA-viranomaisen lisäksi NIS 2 –direktiivin mukaiselle viranomaiselle (Suomessa Kyberturvallisuuskeskus). Ei ehdoteta otettavan käyttöön mainittua lisäraportointivelvoitetta.