

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojaan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Yleisesti

Tietoturvallisuuden hallinta ja sen valvonta finanssialalla on jo nykyisin vahvasti ja yksityiskohtaisesti säänneltyä. Ehdotettu Euroopan parlamentin ja neuvoston asetus finanssialan digitaalisesta häiriönsietokyvystä (nk. DORA-asetus, <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52020PC0595&from=EN>) tulee tarkentamaan vaatimuksia entisestään. Finanssivalvonta toivoo, että valmistelun yhteydessä arvioidaan vielä huolellisesti, onko lisäsääntelyä tarpeen ulottaa finanssialalle ottaen huomioon vireillä olevat muut sääntelyehdotukset, finanssialan voimassa oleva sääntely, Finanssivalvonnan ohjeet ja määräykset sekä finanssialan Eurooppalaisten valvontaviranomaisten (ESMA, EBA ja EIOPA) antama ohjeistus (esim. https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en).

Ehdotukset poliittisiksi linjauksiksi

- Kohdassa 3 tarkoitettaneen virkamiehiä, jotka valvovat toimialojen yritysten ja muiden toimijoiden tietoturvallisuuden hallintaa. Yksittäisen koulutusvaatimuksen sijaan työnantajavirastoilta voisi edellyttää sitoutumista virkamiesten osaamistason ja resurssien riittävyyden varmistamiseen.
- Kohdan 12 vaatimukset koskisivat ”Kriittisten toimialojen merkittävimpiä toimijoita”. Sääntelyn valmistelussa olisi pohdittava tarkasti, kuka määrittelee toimijan merkittävyyden ja millä menettelyllä määrittely tapahtuu.
- Kohdan 12 sertifiointivaatimus tulisi kohdistaa toimijalle tarkemmin toiminto/maakohtaisesti, huomioida alihankintaketjut ja yksilöidä standardin noudattamisen kattavuus. Sertifiointivaatimuksen sijaan tulisi harkita vaatimusta noudattaa standardia.

Väliraportin muut osat, kommentit:

-

Korhonen Pasi
Finanssivalvonta