24.11.2023

Diaari 82/010/2023 ja
DARK 23/010/82

VN/18157/2023

Kansaneläkelaitoksen lausunto luonnokseen hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö on pyytänyt lausuntoa Kansaneläkelaitokselta lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi.

Kansaneläkelaitoksen lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kela katsoo, että kyberturvallisuuden riskienhallinnasta säädettävä laki on yhteiskunnan turvallisuuden kannalta tarpeellinen ja tukee direktiivin soveltamisalaan kuuluvien toimijoiden kyberturvallisuuden tason parantamista.

Luonnoksen luvun 4.2.2 kohdassa terveyssektori (s. 56) käytetään käsitettä turvallisuussuunnitelma, jolla tarkoitetaan asiakastietolain (703/2023) 77 §:ssä määriteltyä tietoturvasuunnitelmaa. Vaikka kyse ei ole lakiin kirjattavasta käsitteestä, tulisi se selvyyden vuoksi muuttaa vastaamaan asiakastietolain mukaista muotoilua.

Riskienhallintavelvoitetta koskevat huomiot

Esitetyn lain 11 §:ssä säädettäisiin valvovalle viranomaiselle määräyksenantovaltuus liittyen esimerkiksi siihen, milloin saman pykälän 1 momentissa tarkoitettu poikkeama on merkittävä. Tältä osin on huomioitava, että asiakastietolain (703/2023) 90 § sisältää Terveyden ja hyvinvoinnin (THL) laitokselle kuuluvan määräyksenantovaltuuden liittyen siihen, milloin pykälässä tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta. Vastaavasti asiakastietolain 82 § sisältää THL:lle kuuluvan määräyksen antovaltuuden liittyen siihen liittyen, mitkä ovat saman pykälän momentissa tarkoitettuja merkittäviä poikkeamia ja miten niitä koskevat ilmoitukset tehdään. Asiakastietolaki edellyttää, että olennaisten vaatimusten merkittävistä poikkeamista on ilmoitettava kaikille järjestelmää käyttäville palvelunantajille ja apteekeille.

Edellä esitetyn mukaisesti nyt Valviralle esitettävän määräyksenantovaltuuden ja asiakastietolaissa THL:lle säädettyjen määräyksenantovaltuuksien suhdetta tulee esityksen jatkovalmistelussa selkiyttää. Vaikka valtuuden asiayhteys olisi eri, voi olla lain soveltamisen kannalta vaikeaselkoista, mikäli määritelmällisesti määräyksenantovaltuudet vaikuttavat päällekkäisiltä. Lisäksi terveydenhuollon palvelunantajan voi olla haastavaa toteuttaa poikkeamailmoituksiin liittyvää menettelyä, mikäli yhteen tapahtumaan sovelletaan samanaikaisesti osin päällekkäistä sääntelyä. Tältä osin on syytä huomioida, että esimerkiksi hyvinvointialueet ovat sosiaali- ja terveydenhuollon palvelunantajia, jolloin tietyissä tilanteissa voi olla käytännössä haastavaa erotella ilmoitusmenettelyyn liittyvä toimintatapa kyseessä olevasta toiminnasta riippuen.

KANSANELÄKELAITOS
PL 78, 00381 Helsinki
Puhelin 020 634 11
etunimi.sukunimi@kela.fi

FOLKPENSIONSANSTALTEN
PB 78, 00381 Helsingfors
Telefon 020 634 11
fornamn.efternamn@kela.fi

Yleisesti ottaen esityksen jatkovalmistelussa voisi olla perusteltua selvittää, onko kansallista soveltamisalaa tai asiaan kuluvan kansallisen sääntelyn soveltamisalaa mahdollista laajentaa tavalla, joka mahdollistaisi poikkeamailmoitusmenettelyihin yhdenmukaiset toimintatavat. Lisäksi tässä yhteydessä voisi olla tarpeen arvioida, tulisiko vastaavia velvoitteita soveltaa esimerkiksi myös toimijoihin, joiden rekisterinpidossa on terveydenhuollon potilastietoja, mutta joita ei määritelmällisesti katsota direktiivin soveltamisalaan kuuluviksi. Jatkovalmistelussa tulee myös varmistua siitä, ettei ilmoitusmenettelyihin sovellettava lainsäädäntö muodostu käytännön soveltamisen kannalta liian vaikeaselkoiseksi ja monimutkaiseksi.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Luonnoksessa laiksi kyberturvallisuuden riskienhallinnasta käytetään 30 §:ssä käsitettä turvallisuusauditointi. Kyseisessä kohdassa ei kuitenkaan määritellä, mitä vaatimuskehikkoa vasten auditointi tehtäisiin. Kyseistä kohtaa tulisi selvyyden vuoksi tarkentaa ja lisäksi arvioida, tulisiko auditoinnin sijaan käyttää käsitettä arviointi, koska lain tasolla esitetyt vaatimukset ovat melko yleisellä tasolla.

Kela on eduskunnan alainen itsenäinen julkisoikeudellinen laitos, jonka tehtävistä säädetään laissa Kansaneläkelaitoksesta (731/2001). Kelan sosiaaliturvaa koskevista tehtävistä ja sosiaali- ja terveydenhuollon tiedonhallintapalveluja koskevista tehtävistä säädetään eri laeissa. Kela kuuluu julkisen hallinnon tiedonhallinnasta annetun lain (tiedonhallintalaki, 906/2019) soveltamisalan piiriin, mutta kyseisen lain 18 §:n nojalla annettu asetus asiakirjojen turvallisuusluokittelusta ei koske Kelaa.

Kela tekee laajaa yhteistyötä valtionhallinnon kanssa turvallisuuteen ja varautumiseen liittyvissä kysymyksissä. Turvallisen, selkeän ja sujuvan tietojenvaihdon ja -käsittelyn varmistamiseksi Kela katsoo, että tiedonhallintalain (906/2019) 18 §:n tulisi koskea myös Kelaa.

Matti Koskinen

Turvallisuusjohtaja

Henri Burtsov

Tietoturvayksikön päällikkö