Posti Oy

Lausunto

30.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Posti pitää ehdotetun sääntelyn tavoitetta EU:n yhteisen sekä jäsenvaltioiden kansallisen kyberturvallisuuden tason vahvistamisesta kriittisten sektoreiden osalta yhteiskunnan toimivuuden kannalta tärkeänä. Posti kannattaa linjausta, jonka mukaan kansallinen täytäntöönpano tehtäisiin direktiivin edellyttämän vähimmäistason mukaisesti ja välttäen kansallista lisäsääntelyä. Kyberturvallisuutta koskevan sääntelyn laajentuessa kokonaan uusille toimialoille on olennaista myös vahvistaa yhteistyötä valvovien viranomaisten ja yritysten välillä.

Viittaamme sääntelyn yleisten huomioiden osalta myös Elinkeinoelämän keskusliitto EK:n lausuntoon.

Soveltamisalaa koskevat huomiot

NIS2-direktiivissä on posti- ja kuriiripalvelut listattu uusina kyberturvallisuussääntelyn soveltamisalaan kuuluvina toimialoina. Luonnoksen liitteessä II tämä on ehdotettu täytäntöönpantavaksi sanamuodolla ”kuriiripalvelun tarjoajat ja postilain 2 §:n 1 momentin 2 kohdassa tarkoitetun postipalvelun tarjoajat”.

Posti pitää valitettavana, että luonnoksessa soveltamisalan määrittely on jäänyt tulkinnanvaraiseksi erityisesti posti- ja kuriiritoiminnan osalta. Lakiluonnoksessa tai sen perusteluissa ei ole käytännössä lainkaan avattu kuriiripalvelun tarjoajan määritelmää. Tämä on merkittävä kysymys sen kannalta, mitä yrityksiä lopulta lainsäädäntö koskee. Posti toivoo tähän selkeämpää kansallista kannanottoa.

Postipalvelujen osalta liitteessä on viitattu postilain 2 §:ään, joka koskee kaikkia osoitteellisten kirjeiden tai yleispalveluun kuuluvien postipakettien palvelua. Toisin sanoen kyberturvallisuuslain soveltamisalaan kuuluisivat tämän perusteella kaikki postilaissa tarkoitetut postiyritykset. Kuitenkin lakiluonnoksen yleisperusteluissa (s. 59) on esitetty, että soveltamisalassa olisikin postipalveluiden osalta nimenomaan yleispalvelun tarjoajan palvelut eli käytännössä lähinnä Posti Oy. Tähän on päädytty kirjoittamalla perusteluihin postilähetyksen määritelmä postilaista poikkeavasti siten, että sillä tarkoitettaisiin ”nimenomaan yleispalvelun tarjoajan kuljetettavaa valmista lähetystä, joka on osoitettu jollekin vastaanottajalle”.

Postiyritykseksi on Liikenne- ja viestintäviraston ylläpitämän postitoimintarekisterin mukaan ilmoittautunut tällä hetkellä yhteensä 15 toimijaa. Postilain 11 luvussa olevat varautumista koskevat säännökset edellyttävät jo nykyisin kaikilta postiyrityksiltä varautumista siihen, että postitoiminta voi jatkua mahdollisimman häiriöttömästi valmiuslaissa tarkoitetuissa poikkeusoloissa sekä normaaliolojen häiriötilanteissa. Kyberturvallisuussääntelyn tavoitteiden kannalta Posti katsoo tarkoituksenmukaiseksi, että kaikki postiyritykset ovat yhdenmukaisesti sääntelyn piirissä. Jos lakiluonnoksessa tarkoitus ei ole ollut rajata sääntelyn soveltamista postin yleispalveluun, niin ehdotuksen perusteluja tulee korjata. Posti huomauttaa myös, että Posti-konsernissa postiyrityksenä toimivan yrityksen toiminimi on ollut 1.1.2023 alkaen Posti Jakelu Oy (aiemmin Posti Oy).

Riskienhallintavelvoitetta koskevat huomiot

Lakiluonnoksen yksityiskohtaisissa perusteluissa 2 §:n 10 kohdassa eli keskisuuren toimijan määritelmän kohdalla on todettu, että "liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta eikä arviointia tule rajata vain liitteessä I tai II tarkoitetun toiminnan laajuuteen. Arviointi tehdään toimijakohtaisesti”.

Vastaavasti kyberturvallisuuden riskienhallintavelvoitetta koskevassa 7 §:ssä säädetään riskienhallintavelvoitteesta seuraavasti:

"Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuuden riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin."

Ehdotuksista jää tulkinnanvaraiseksi, kohdistuuko velvollisuus riskienhallintaan vain liitteessä 1 ja 2 määriteltyyn toimintaan, vai onko tarkoitettu sen koskevan laajasti myös toimijan muuta liiketoimintaa. Säännöksen yksityiskohtainen perustelu viittaa jälkimmäiseen tulkintavaihtoehtoon: ”pykälässä säädettäisiin soveltamisalaan kuuluvien toimijoiden yleisestä velvoitteesta”. Posti katsoo, että sääntelyä tulisi täsmentää niin, että velvoitteet rajoittuvat vain siihen toimintaan, joka on NIS2-direktiivissä nimenomaan mainittu.

Oikeushenkilökohtaisen tarkastelun ei pitäisi estää konsernirakenteessa toimivien yritysten järjestävän ICT- ja kyberturvallisuustoimintojaan keskitetysti esimerkiksi konsernin emoyhtiössä.

Kyberturvallisuuden riskienhallinnan toimenpiteet perustuvat NIS2-direktiivin 21 artiklaan ja ne on 9 §:n pykälätekstissä asianmukaisesti muotoiltu. Sama koskee yleisperustelujen lukua 2.5, jossa on siteerattu NIS2-direktiivin 21 artiklaa. Kuitenkin 9 §:n yksityiskohtaisissa perusteluissa on listattu vaatimuksia ja annettu esimerkkiluetteloita, jotka ovat mielestämme liian yksityiskohtaisia ja toisaalta tulkinnanvaraisia. Esimerkkinä tällaisesta voidaan mainita kohdan 11 kyberhygieniakäytäntöjä selittävät yksityiskohtaiset perustelut. Perustelutekstien valossa velvoitteen edellyttämien toimenpiteiden käytännön tulkinnat voivat johtaa toimijoiden kannalta ennalta-arvaamattomiin vaatimuksiin. Perusteluja tulisi lain jatkovalmistelussa täsmentää niin, että sääntely jättää toimijoille liikkumavaraa itse päättää, millaisilla keinoilla sen toiminnassaan tunnistamat riskit voidaan parhaiten hallita.

Raportointivelvoitetta koskevat huomiot

Poikkeamailmoituksia koskevat säännökset lähtevät siitä, että soveltamisalaan kuuluvien toimijoiden tulee raportoida merkittävästä poikkeamasta valvovalle viranomaiselle hyvin tiukoissa määräajoissa. Ilmoitusvelvollisuuden aktualisoitumisen tulisi sen vuoksi olla mahdollisimman yksiselitteistä.

Merkittävän poikkeaman kriteereinä on ensinnäkin vakava toimintahäiriö palveluissa. Myös tilanne, jossa poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa, edellyttää ilmoitusta. Lisäksi raportti tulisi tehdä, jos asianomaiselle toimijalle aiheutuu taloudellisia tappioita. Viimeksi mainitun edellytyksen kohdalla jää epäselväksi, milloin toimijan omien taloudellisten tappioiden katsottaisiin täyttävän merkittävän poikkeaman kriteerin, vai voisivatko aivan vähäisetkin taloudelliset tappiot edellyttää poikkeaman ilmoittamista. Säännöstä tulisi täsmentää niin, että taloudellisten tappioiden tulisi olla huomattavia, jotta raportointivelvoite syntyy.

Valvontaa koskevat huomiot

Viittaamme Elinkeinoelämän keskusliitto EK:n lausuntoon.

Seuraamusmaksua koskevat huomiot

Viittaamme Elinkeinoelämän keskusliitto EK:n lausuntoon.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei lausuttavaa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei lausuttavaa.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Lakiehdotuksen vaikutuksia eri toimialojen yrityksiin ei valmisteluvaiheessa ole kattavasti arvioitu. Komissio on arvioinut, että NIS2-direktiivin mukaisilla velvoitteilla olisi ensimmäisten toimeenpanovuosien aikana jopa 25 % korottava vaikutus kyberturvallisuuteen liittyviin IT-kustannuksiin, jos velvoitteiden kohteena oleva toimija ei ole kuulunut NIS1-direktiivin soveltamisalaan. Posti toteaa, että yrityksen on vaikea tehdä tarkkaa vaikutusarviointia, kun säännöksen soveltamisen yksityiskohdat ovat vielä toistaiseksi osittain epäselviä, mutta kustannusvaikutus voi olla erittäin merkittävä.

Muut huomiot ja avoin palaute esityksestä

Viittaamme Elinkeinoelämän keskusliitto EK:n lausuntoon.

Rokkanen Päivi
Posti Oy - Posti Group Oyj