Tietosuojavaltuutetun toimisto

Lausunto

29.11.2023 TSV/35/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Tietosuojavaltuutetun toimisto kiittää mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi. Laaja-alainen tietoturvallisuuden perustason nosto on pitkään odotettu kehityssuunta. Asianmukainen viestintäverkkojen ja tietojärjestelmien kyberturvallisuuden pohjataso edesauttaa ja tukee yleisen tietosuoja-asetuksen henkilötietojen käsittelijöiltä edellyttämää henkilötietojen käsittelyn suojaamista ja tietosuojavaltuutetun toimisto katsoo esityksen tavoitteiden olevan kannatettavia ja tärkeitä.

Soveltamisalaa koskevat huomiot

-

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

Ehdotetun lain kyberturvallisuuden riskienhallinnasta 11 § ja ehdotetun tiedonhallintalain 18 d § mukaisesti toimijan tai viranomaisen on ilmoitettava viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta, jolla voidaan tarkoittaa muun muassa poikkeamaa, joka voi aiheuttaa asianomaiselle toimijalle taloudellisia tappioita. Tämä voi asettaa merkittävyyden kynnyksen hyvin alhaiseksi, koska jo poikkeaman käsittelyyn kuluva työ voidaan katsoa tappioksi ja tämä voi ohjata toimijoita laatimaan viranomaisilmoituksia varmuuden vuoksi epätarkoituksenmukaisen alhaisella kynnyksellä.

Ehdotetun sääntelyn mukaan toimijan on tehtävä valvovalle viranomaiselle ensi-ilmoitus merkittävästä poikkeamasta 24 tunnin kuluessa poikkeaman havaitsemisesta. Tämä edellyttää toimijoilta, joilla ei ole ympärivuorokautista toimintaa, valmiutta epätyypillisiin työsuhteisiin tai

päivystysluonteiseen toimintaan. Asiaa olisi hyvä selkeyttää niin ettei toimijan tuleminen tietoiseksi merkittävästä poikkeamasta riippuisi siitä, tapahtuuko poikkeama virka-aikaan, yöllä tai pyhänä.

Ehdotetun kyberturvallisuuden riskienhallintalain 34 § mukaisesti valvovan viranomaisen on puolestaan ilmoitettava tietosuojavaltuutetulle laissa säädettyjä tehtäviä hoitaessaan tietoonsa saamista henkilötietojen tietoturvaloukkaukseen mahdollisesti johtavista seikoista. Pykälän perusteluissa rajataan ilmoitusvelvollisuuden piiristä pois yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat ja todetaan ettei velvollisuus koske tietosuojasääntelyn ja sähköisen viestinnän erityissääntelyn rajapinnoista johtuen teletoimintaa koskevia henkilötietojen tietoturvaloukkauksia. Yleisen tietosuoja-asetuksen 33 artiklan mukaan rekisterinpitäjän on ilmoitettava tietosuojan valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa sen ilmitulosta. On tärkeää ettei henkilötietojen tietoturvaloukkauksia koskevaan ilmoitusvelvollisuuteen jää aukkoja, mutta on myöskin syytä välttää ylimääräistä hallinnollista taakkaa, joten ilmoitusvelvollisuudesta voisi olisi hyvä säätää kattavasti suoraan pykälätasolla.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

Tietosuojavaltuutetun toimisto kiinnittää huomiota esitetyn kyberturvallisuuden riskienhallintalain 41 § 4 momenttiin, jonka mukaan seuraamusmaksua ei saa määrätä sille, jolle on määrätty samasta teosta yleisen tietosuoja-asetuksen 83 artiklassa tarkoitettu seuraamusmaksu. Euroopan tietosuojaneuvosto on sivunnut asiaa ohjeessaan 04/2022 tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen määräytymisestä. Sääntelyssä olisi hyvä ottaa selkeästi kantaa siihen, onko NIS2-direktiiviä tulkittava siten, että henkilötietojen käsittelyn turvallisuuteen liittyvistä puutteista määrättävät seuraamukset olisivat vain tietosuojavaltuutetun kollegion toimivallassa.

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Esitetyn tiedonhallintalain uuden 4 a luvun säännökset tarkoittaisivat viranomaisille nykyisiin tiedonhallintalain vaatimuksiin nähden osittain erilaisia velvoitteita sekä tietoturvallisuuden vähimmäisvaatimuksia ja ne saattavat edellyttää viranomaisen valmiustason nostamista. Tietosuojaviranomaisen osalta katsomme että esityksessä on asianmukaisesti arvioitu toimijalle ehdotuksesta aiheutuvat lisäresurssitarpeet.

Monet esitetyistä muutoksista edellyttävät hallinnonalojen palvelukeskuksilta uusia kyvykkyyksiä, kuten esimerkiksi tiedonhallintayksikkökohtaisia räätälöityjä selvityksiä sekä valvontatoimia. Näitä uusia kustannuksia ei välttämättä pystytä kattamaan valtion talousarvioin mukaisista määrärahoista ilman lisärahoitusta.

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Talus Anu
Tietosuojavaltuutetun toimisto

Karppinen Lauri
Tietosuojavaltuutetun toimisto