Tiedonhallintalautakunta
Informationshanteringsnämnden

6.5.2025 VN/28287/2023

Vastauksia 1.4.2025 webinaarista kyberturvallisuusvelvollisuuksien toimeenpanosta julkisessa hallinnossa esiin nousseisiin kysymyksiin

Tiedonhallintalautakunta järjesti yhdessä Liikenne- ja viestintäviraston kanssa tiistaina 1.4.2025 webinaarin kyberturvallisuusvelvollisuuksien toimeenpanosta julkisessa hallinnossa.

Webinaarin tarkoituksena oli esitellä tiedonhallintalain (906/2019) uudessa 4 a luvussa säädettäviä kyberturvallisuusvelvollisuuksia julkisen hallinnon viranomaisille sekä niiden vaikutuksia. Tilaisuudessa käytiin läpi kyberturvallisuusvelvollisuuksien ohjausta ja valvontaa sekä tiedonhallintaa ohjaavien viranomaisten roolia ja toimenpiteitä tiedonhallintalain vaatimusten toteuttamiseksi.

Webinaarissa nousi esiin kysymyksiä, joiden vastauksia on tarkennettu tässä muistiossa.

Mikä on 4 a luvun suhde tiedonhallintalain muuhun sääntelyyn?

Tiedonhallintalakia (906/2019) sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä. Tiedonhallintalain 3 §:n 3 momentissa sekä 4 ja 6 momenttien viimeisessä virkkeessä säädetään lain 4 a luvun soveltamisalasta.

Viranomaisten on syytä huomioida tiedonhallintalain säännösten soveltamisessa, että lain 4 a luku sisältää samansuuntaista sääntelyä muun tiedonhallintalain kanssa. Lisäksi kun tiedonhallintalain 4 a luvussa ja muualla tiedonhallintalaissa säädetty tulevat usein sovellettavaksi samanaikaisesti viranomaisen tietoaineistojen käsittelyyn, korostuu tarve arvioida eri säännösten soveltamista tapauskohtaisesti. Edelleen viranomaisten on hyvä myös muistaa, ettei tiedonhallintalain 4 a luvussa säädettyjen vaatimusten toteuttaminen muodosta perustetta jättää toteuttamatta muualla tiedonhallintalaissa säädettyjä velvollisuuksia.

Olettaen, että viranomainen toimii nykyisen tiedonhallintalain tietoturvavaatimusten mukaisesti, eli määrittää tietoturvatoimenpiteensä riskilähtöisesti ja on dokumentoinut toimintamallinsa tarkoituksenmukaisesti, riittääkö se täyttämään NIS2 vaatimuksen riskienhallintamallista?

Tiedonhallintalain 13 §:n 1 momentti velvoittaa tiedonhallintayksikön selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Tiedonhallintalain 13 a §:n 3 momentissa säädetään tiedonhallintayksikön velvollisuudesta selvittää sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit. Momentin jälkimmäinen virke edellyttää tiedonhallintayksikköä riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehtimaan, että sen

tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa.

Tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalain 4 luvussa säädettyjen vaatimusten ja menettelytapojen toteuttamista. Lautakunta ei voi arvioida tiedonhallintalain 4 luvussa tai 4 a luvussa säädettyjen vaatimusten toteuttamista. Liikenne- ja viestintävirasto on tiedonhallintalain 4 a luvun säännösten toteuttamista valvova viranomainen.

Liikenne- ja viestintäviraston näkemyksen mukaan tiedonhallintalain nykyiset tietoturvavaatimukset voi julkishallinnon toimialan osalta mieltää ns. perustason tietoturvakäytäntöinä, joiden päälle tiedonhallintalain uuden 4 a luvun mukaisia kyberturvallisuuden riskienhallintatoimenpiteitä voi alkaa rakentamaan.

Jos virastolla on käytössä ulkoistettu SOC-palvelu, voiko tämä toimittaa ensi-ilmoituksen viraston puolesta?

Tiedonhallintalaki ja sen perustelut lähtevät siitä, että toimija ilmoittaa merkittävästä poikkeamasta valvovalle viranomaiselle, jonka vuoksi se on lähtökohtana myös KTK:n luomassa kanavassa, jota kautta merkittävät poikkeamat pyydetään lähtökohtaisesti ilmoittamaan (https://eservices.traficom.fi/ContactForms/form/NIS2-Ilmoitus?langid=fi).
Varsinaista estettä ei liene ole kuitenkaan sille, että merkittävästä poikkeamasta ilmoittaisi palveluntarjoaja toimijan puolesta. Ilmoituksen oikeellisuus ja jatkokeskustelujen osapuolet täytyy varmistaa asianmukaisin valtuuksin.

KTK:n luomasta poikkeamailmoituskanavasta on esittelyvideo Youtube:ssa Fimean kyberturvallisuuswebinaarin yhteydessä, aloitus kohdassa 45:20: https://www.youtube.com/watch?v=3x8Al_uUxdE&t=745s

Saako lähettäjä merkittävästä poikkeamasta ilmoitettuaan ilmoituksen pdf:nä tai muussa muodossa omaan sähköpostiinsa?

Ei saa. Merkittävästä poikkeamasta ilmoittanut saa omaan sähköpostiinsa kuittauksen tehdystä ilmoituksesta, joka sisältää ainoastaan ilmoituksen yksilöivän asianumeron. Ilmoittajan on mahdollista tallentaa kopio ilmoituksesta pdf-muodossa itselleen.

Toimijaluetteloon ilmoittautumisen edellyttämästä suomi.fi valtuutuksesta.

Liikenne- ja viestintävirasto. Kyseessä oleva valtuus on 'Kyberturvallisuuteen liittyvien toimijatietojen ilmoittaminen - Tällä valtuudella valtuutettu voi valtuuttajan puolesta ilmoittaa ja ylläpitää kyberturvallisuuteen liittyviä toimijatietoja.'
Lisätietoja valtuutuksista saa parhaiten DVV:ltä: https://www.suomi.fi/ohjeet-ja-tuki/valtuudet/organisaation-puolesta-asiointi