



15.12.2015

Valtiovarainministeriö
JulkiCT

VÄESTÖREKISTERIKESKUKSEN LAUSUNTO KOSKIEN PÄIVITETTYÄ TURVALLISUUSSOPIMUSMALLIA

Valtiovarainministeriö on pyytänyt lausuntoa valtionhallinnon turvallisuussopimusmallin luonnoksesta (v0.1.0) 23.11.2015. Turvallisuussopimusmalli on ollut Valtion ICT-hankintojen tietoturvaohjeen (Vahti 3/2011; VM/1982/00.00.00./2001) liitteenä.

Väestörekisterikeskus on ollut mukana jo sopimusmallin kommenteille tulleen version valmisteluvaiheessa VAHTI Ohjeaoston jäsenenä. Tämän lisäksi kiinnitämme huomiota seuraaviin seikkoihin:

Määritelmät

- ⇒ Pitäisikö lisätä määritelmiin "Poikkeama" ja "Tietojärjestelmä". Poikkeama keskeinen esimerkiksi kohdan 13.2 osalta.

Kaksisuuntaisuus

- Pitäisikö sopimuksesta tehdä tietyin osin kaksipuolinen. Esimerkiksi kohta 13.3:

"Toimittaja on viipymättä velvollinen ilmoittamaan Tilaajalle, mikäli Toimittajaan kohdistuu Tilaajaa mahdollisesti uhkaavia yhteydenottoja."

- ⇒ Tilaajan olisi myös hyvä sitoutua ilmoittamaan Toimittajalle, mikäli tähän kohdistuu Tilaajan tietoon tulleita uhkia.

Tai kohta 5.2 (ja 5.3):

"Toimittaja sitoutuu pitämään salassa Suojattavan tiedon eikä käytä taikka hyödynnä sitä muuhun kuin sovittuun tarkoitukseen ja ainoastaan siinä laajuudessa kuin se kulloinkin on tarpeen."





14.12.2015

- ⇒ Tilaaajan olisi myös hyvä sitoutua pitämään salassa Toimittajan salassa pidettävän tiedon.

Alihankkijat

Kohta 4.1: *"Mitä tässä sopimuksessa on sovittu Toimittajasta ja Toimittajan henkilöistä, sovelletaan myös alihankkijaan ja alihankkijan henkilöihin."*

- ⇒ Olisiko tässä hyvä tuoda esiin tila- ja tietojärjestelmäturvallisuuden soveltaminen myös alihankkijoihin?

Salassapito ja vaitiolovelvollisuus

Voisiko tähän liittää ehdon referenssien käytöstä, esimerkiksi uutena kohtana 5.12:

"Toimittaja ja sen alihankkijat saavat mainita referenssinä tehneensä työtä Tilaaajalle palveluiden tuottamisessa vain, jos asiasta on erikseen Tilaaajan kanssa kirjallisesti sovittu. Referenssioikeuden myöntäminen ei vapauta Toimittajaa sovituista salassapitovelvoitteista. Tilaaajalla on oikeus peruuttaa myöntämänsä referenssioikeus, jolloin Toimittaja lakkaa välittömästi käyttämästä referenssiä."

Tietosuoja

6.1: Pitäisikö olla maininta jo EU:n tietosuojasetuksesta, mikäli asetus on tullut voimaan ennen tämän sopimuksen voimaan tuloa.

Tilaaajan toimitilojen turvallisuus

7.7 b): Pitäisikö olla: *"joista on tehty henkilöturvallisuusselvitys, josta on saatu Tilaaajan hyväksyttävissä oleva tulos"*

Pitäisikö kohdassa 7 olla myös seuraavanlainen ehto:

"henkilöt, joille ei ole myönnetty oikeutta Suojattaviin tietoihin tai niitä sisältäviin järjestelmiin luvun X mukaisesti saavat oleskella tiloissa, joissa käsitellään Suojattavaa tietoa, ainoastaan valvonnan alaisina. Valvontaa muissa kuin IT-laitetiloissa ei edellytetä tapauksissa, joissa Suojattavia tietoja säilytetään tai käsitellään tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi."

Tietojärjestelmien hallinnan vaatimukset

8.1: Pitäisikö olla: *"... Suojattavaa tietoa sisältävän tietojärjestelmän toimivuutta, tietoturvallisuutta tai Suojattavia tietoja."*

Tarkastukset

12.6: *"Tilaaajan on ilmoitettava tahdostaan suorittaa tarkastus. Toimittaja voi ehdottaa uutta päivää tarkastukselle."*

- => Olisiko hyvä olla jotain päivämäärä-rajoitusta ainakin toimittajan uudelle ehdotukselle?



14.12.2015

12.8 : Pitäisikö olla maininta, että *"havaittujen kehityskohteiden toteuttamisesta ja niihin liittyvistä aikatauluista ja kustannuksista sovitaan erikseen."*

=> Tässä tarkoitetaan muita kuin poikkeamia ja niiden korjaamista

Sopimussakko ja vahingonkorvaukset

14.5: Pitäisikö olla: *"Ennen sopimussakon perimistä Tilaajan tulee ilmoittaa Toimittajalle kirjallisesti tämän sopimuksen rikkomuksesta. Jos Toimittaja tai Tilaaja sitä kirjallisesti pyytää, käsitellään rikkomus lisäksi Tilaajan ja Toimittajan välisissä neuvotteluissa."*

Soveltamisjärjestys

Mikä on Turvallisuuksopimuksen liitteiden pätemisjärjestys? Esimerkiksi Tilaajan tietoturva vaatimus vs Toimittajan tietoturvallisuuden kuvaus.

VRK:lla on lisäksi ollut käytössä seuraavat ehdot:

Sopimuksen allekirjoituksen jälkeen valmistuvat liitteet tulevat turvallisuuksopimuksen osaksi, kun molemmat osapuolet ovat ne toimivaltaisesti hyväksyneet.

Sopijapuolet tarkistavat yhdessä vähintään kerran (1) vuodessa turvallisuuksopimuksen ja sen liitteiden ajantasaisuuden.

Johtaja



Lea Krohns

Tietoturvapäällikkö



Pekka Ristimäki