VAHTI

LAUSUMA

16.12.2014

Valtionhallinnon asiakkaiden tietojenkäsittely ja tiedon suojaaminen sille palveluita tuottavan toimittajan omissa sisäisissä tietojärjestelmissä

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän alaisuudessa toimiva tekninen jaosto on keskustellut usean eri toimittajan pyynnöstä otsikossa mainitusta asiasta. Toimittajat ovat pyytäneet valtionhallinnolta lausuntoa siitä, voivatko he siirtyä omassa sisäisessä toiminnassaan käyttämään Suomen ulkopuolella a) EU-alueella tai b) EU: ulkopuolella sijaitsevia palveluita.

Tämän linjauksen taustalla on suoritettu

a) riskienarviointi, joka koskee tietoliikenteen kulkemista Suomen rajojen ulkopuolella ja näihin tietoihin kohdistuvaa signaalitiedustelua ja muuta tiedusteluriskiä sekä

b) voimassa olevien turvallisuussopimusmallien ja tietoturvallisuuden ja varautumisen vaatimusten arviointi.

Tekninen jaosto toteaa seuraavaa:

Ei ole mahdollista antaa kannanottoa johonkin tiettyyn tekniseen ratkaisuehdotukseen siksi, että valtionhallinnon organisaatioiden sopimukset ottavat näihin asioihin kantaa hyvin eritasoisesti hankinta-ajankohdan ja hankittavan palvelun vaatimalla tavalla. Toimittajan tulee käydä läpi asiakkaiden kanssa tehdyt, voimassa olevat turvallisuussopimukset sekä muiden sopimusten vaatimukset ja varmistaa niiden vaikutus suunniteltuun ratkaisuun. Samoin toimittajan tulee huomioida se, tuleeko suunniteltu ratkaisu mahdollisesti myöhemmin vaikuttamaan siihen, pystyvätkö he täyttämään valtionhallinnon hankinnoissaan edellyttämiä vaatimuksia ja sopimuksia.

Valtionhallinto ei tällä hetkellä edellytä tiettyä toimintatapaa, tuotantomallia tai tuotantomaata toimittajan oman sisäisen toiminnan osalta, kunhan seuraavat sopimusten vaatimukset ja velvoitteet täyttyvät:

1) Toimittaja noudattaa voimassa olevia turvallisuussopimuksia, etenkin niitä kohtia, joissa määritetään velvoitteita palvelutuotannolle ja asiakkaan tietoaineistojen käsittelylle.

2) Osa valtionhallinnon organisaatioista edellyttää turvallisuus- tai palvelusopimuksessa (jäljempänä ”sopimus”), että joko a) kaikki

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

sen palvelutuotantoon liittyvä tieto tai b) kaikki salassa pidettävä tieto pitää käsitellä ja säilyttää Suomessa. Tällöin se ei saa kulkea edes tietoliikenteen osalta maan rajojen ulkopuolelle. Tällaisia vaatimuksia saattaa olla myös koko valtionhallinnolle tehdyissä yleisissä palveluhankinnoissa.

3) Valtionhallinnon salassa pidettäviä tietoja käsittelevät vain nimetyt asiakkaan hyväksymät henkilöt, joista on tehty turvallisuusselvitys. Turvallisuusselvityksen tekemisestä päättää turvallisuusselvityslain mukaisesti Suojelupoliisi tai pääesikunta. Suomen turvallisuusselvitystä vastaavan ulkomaisen turvallisuusselvityksen saaminen on pääsääntöisesti mahdollista vain niistä maista, joiden kanssa Suomella on sopimus turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta (tietoturvallisuussopimus, General Security Agreement, GSA). Tietoturvallisuussopimuksissa turvallisuusselvitystä edellytetään yleensä vain, mikäli henkilö saa pääsyoikeuden turvallisuusluokiteltuun tietoon tasolla LUOTTAMUKSELLINEN tai korkeampi. Mikäli yritys käsittelee tiloissaan turvallisuusluokiteltua tietoa, tulisi arvioida myös tarve yritysturvallisuusselvityksen (FSC, Facility Security Clearance[1]) tekemiseksi.

4) Osa valtionhallinnon organisaatioista edellyttää sopimuksissa, että myös ne henkilöt, joilla on mahdollisuus päästä asiakkaan salassa pidettäviin tietoihin, pitää nimetä ja turvallisuusselvittää. Tämä koskee esimerkiksi pääkäyttäjä (administrator) –tason käyttäjiä.

5) Mikäli toimittajan sähköposti-, työryhmä-, tiketöinti- tai muihin sen sisäiseen käyttöön tarkoitettuihin tietojärjestelmiin kertyy asiakkaan tuotantoon liittyvää tietoaineistoa, saatetaan kyseinen järjestelmä tulkita palvelutuotantoon liittyväksi tukijärjestelmäksi ja edellyttää, että se täyttää tietoturvallisuudeltaan ja varautumiseltaan sopimuksessa edellytetyt vaatimukset.

6) Mikäli sopimus mahdollistaa Suomen rajojen ulkopuolella olevien tietojärjestelmien käyttämisen osana palveluiden tuottamista, toimittajan tulee huolehtia palvelutuotannon jatkuvuuden ja huoltovarmuuden turvaamiseksi siitä, että sillä on käytettävissä tarvittavat tietojärjestelmät, palvelut ja tiedot esimerkiksi kansainvälisten tietoliikenneyhteyksien ollessa poikki.

7) Sopimuksen salliessa kansainvälisesti turvallisuusluokiteltujen tietojen siirron ulkomaille, tulee se tapahtua suojattuja yhteyksiä käyttäen siten, että tietojen luottamuksellisuus on turvattu esimerkiksi signaali-tiedustelua vastaan. Tämä edellyttää Kyberturvallisuuskeskuksen hyväksymän salaustuotteen käyttöä tällaisessa tiedonsiirrossa.

8) Mikäli henkilötietoja siirretään ulkomaille, toimittajan tulee varmistua henkilötietolain 5. luvun mukaisesta henkilötietojen suojaamisesta eli siitä, että kyseisessä maassa taataan riittävä tietosuojan taso. Mikäli tiedot siirretään muuhun kuin komission hyväksymään maahan (henkilötietolain 22 a§), toimittajan tulee varmistua henkilötietojen suojaamisesta esim. komission hyväksymiä mallisopimuslausekkeita käyttäen (henkilötietolain

[1] http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/kysymyksia_ja_vastauksia

23 §).

Kannanotto

VAHTI tekninen jaosto edellyttää, että toimittaja käsittelee kaiken valtionhallinnon asiakkaiden palvelutuotantoon liittyvän tiedon sopimusten mukaisesti ja täyttää lainsäädännön vaatimukset sekä sopimuksissa nimetyt, esimerkiksi palvelun tietoturvallisuutta ja ict-varautumista koskevat vaatimukset.

Erityistä huolellisuutta tulee kiinnittää siihen, että toimittaja ei siirrä asiakkaan tietoja ulkomaille turvallisuussopimusten vastaisesti esimerkiksi erilaisten tukijärjestelmien integraatiossa (esimerkiksi tiketöinti-, cmdb-, raportointi- tai hälytystietoja).

Jos valtionhallinnon asiakas on ylipäätään sallinut henkilötietojen käsittelyn Suomen ulkopuolella, ja mikäli toimittajan käyttämä tietojärjestelmä sijaitsee EU/ETA-alueen ulkopuolella, henkilötietojen käsittelyssä tulee noudattaa erityistä huolellisuutta. Mikäli EU/ETA-alueen ulkopuolisen tietojen tallennusmaan lainsäädännössä tai tiedonsaantioikeuksissa tapahtuu jotain sellaista joka vaarantaa viranomaisen luokitellun tiedon paljastumisen sivulliselle, toimittajan tulee olla yhteydessä asiakkaaseen neuvotellakseen tietojen palauttamisesta Suomeen/EU/ETA-alueelle.

Toimittajan tulee huolehtia siitä, ettei asiakkaiden salassa pidettäviä tietoja ylipäätään käsitellä sähköposteissa. Tietojen käsittelyä ohjaa ensi sijassa valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) sekä asiakkaiden sen perusteella antamat käsittelyohjeet.

Tekninen jaosto toteaa, että toimittajan tulee toteuttaa turvallisuus- ja muiden sopimusten mukaisten tietojen käsittely Suomessa sijaitsevassa tietojenkäsittely-ympäristössä niiden valtionhallinnon asiakkaiden osalta, jotka sitä edellyttävät. Erityistä huomiota tulee kiinnittää siihen, että näiden asiakkaiden tietoja ei päädy Suomen rajojen ulkopuolella sijaitseviin ympäristöihin, tai että ylläpitoa ei hoideta EU/ETA-alueen ulkopuolelta, mikäli tämä on sopimuksissa kielletty.

Mikäli toimittaja ei noudata sopimuksessa olevia vaatimuksia, tekninen jaosto suosittelee, että asiakas selvittää, syyllistyykö toimittaja tällöin sopimusrikkomukseen ja asiakas käynnistää tarvittaessa siihen liittyvät toimenpiteet.

Vaikka kaikissa voimassa olevissa sopimuksissa tietojen suojaamiseen ja käsittelyyn liittyviä vaatimuksia ei välttämättä ole riittävällä tarkkuudella määritelty, on selkeä suunta kuitenkin se, että ne tullaan tulevissa hankinnoissa sisällyttämään kaikkiin keskeisiin valtionhallinnon palvelusopimuksiin.

Lisätietoja:

Kimmo Rousku
Teknisen jaoksen puheenjohtaja
etunimi.sukunimi (at) valtori.fi
Puh. 050 566 2986

Aarne Hummelholm
Teknisen jaoksen varapuheenjohtaja
etunimi.sukunimi (at) vm.fi
Puh. 02955 30085