

15.12.2015

STM/4163/2015

Valtiovarainministeriö / kirjaamo
valtiovarainministerio@vm.fi

Viite VM:n lausuntopyyntö 19.11.2015 Vm 136:00/2013

STM:N LAUSUNTO VALTIONHALLINNON TURVALLISUUS SOPIMUSMALLIN LUONNOKSESTA

Valtiovarainministeriö on pyytänyt lausuntoa valtionhallinnon turvallisuusso-
pimusmallin luonnoksesta. Sosiaali- ja terveysministeriö esittää lausuntonaan
seuraavaa.

Turvallisuus sopimusmalliin on tehty useita hyviä parannuksia. Yleisenä huo-
miona todettakoon, että sopimusmallissa tulisi edellyttää Toimittajan taloudel-
lisen aseman vaikutuksen arviointi liittämällä luottoluokitusta koskevat tiedot
tarjous sopimukseen tai varsinaiseen sopimukseen. Tällä varmistettaisiin välil-
listen vahinkojen minimointi esim. valmistumisen viivästyminen, kustannusten
kohoaminen, toimittajan vaihtuminen jne. Erityisen merkitseväksi tämä muo-
dostuu laajoissa ja pitkäkestoisissa hankkeissa, joissa keskeytymisen riskit kas-
tavat.

Yksityiskohtaiset kommentit:

kohta 3.2 Tässä sopimuksessa sovitaan turvallisuusjärjestelyistä, salassapidos-
ta, tietosuojasta ja tietoturvallisuudesta Palveluiden tuottamisessa sekä kaikessa
Pääsopimukseen liittyvässä Tilaaajan ja Toimittajan välisessä yhteistyössä.

Lause on tarpeen muotoilla uudestaan.

kohta 3.3. Jos tämä on pääsopimuksen liite, sopimusasiakirjojen soveltamisjär-
jestys määräytyy Pääsopimuksen ehtojen mukaisesti.

*Tarpeellinen täsmennys siitä, että tämä sopimus voi olla pääsopimuksen liite.
Maininta tästä puuttui nykyisestä turvallisuus sopimuksesta.*

kohta 5.4 Ellei toisin sovita, Toimittajan henkilön on täytettävä seuraavat edel-
lytykset saadakseen oikeuden käsitellä Suojattavaa tietoa, joka on suojaustaso-
tai turvallisuusluokiteltu tasolle III tai ylempi.

*Tuo "ylempi" sana tässä yhteydessä olisi parempi korvata joko sanalla korke-
ampi tai sitten selvyiden vuoksi mainita kaikki seuraavat tasot.*

kohta 5.4.B henkilöstä on tehty henkilöturvallisuus selvitys

*Suppea vai perus? Mikä määrittää minkä tason selvitys tehdään? Se pitää kui-
tenkin toimittajalle perustella samalla kun esitätetään henkilöturvallisuus sel-
vityslomake täydennettäväksi ja allekirjoitettavaksi.*



kohta 5.4.C henkilö on tietoinen salassapitoa koskevista velvoitteistaan
Tarkoittaako vaitiolositoumuksen allekirjoittamista?

kohta 5.5. Henkilöturvallisuusselvitystä ei edellytetä,...
Hyvä lievennys aiempaan sopimukseen.

kohta 7.1.

Toimittaja on velvollinen ilmoittamaan Tilaajalle kaikki ne toimipisteet sijaintimaineen, mistä....

Lause on korjattava kieliopillisesti. Lisäksi miten ja missä vaiheessa ilmoitus tulee tehdä? Vai tuleeko olla tämän sopimuksen liitteenä? Koskeeko suojattava tieto kaikkia suojaustasoja?

kohta 7.2

Tilaaja on määrittänyt Palvelun hankinnan yhteydessä Palveluun sovellettavan valtionhallinnon tietoturvatason...

Aina ei pystytä sanomaan onko palvelun tuottamisessa käsiteltävä tieto tai asiakirja perus- vai korotetun tietoturvatason menettelyitä edellyttävä tieto/asiakirja. Asiakirjoissa ei ole yleensä merkintää vaadittavasta tietoturvasasta, joten hankaluus on jos esim. ST III tason tietoa/asiakirjoja on eri tietoturvasoilla. Millaisia selvittäviä menettelyitä tämä käytännössä edellyttää sekä tilaajalta ja toimittajalta?

kohta 8.2

Toimittajan tulee huolehtia Palvelun osalta siitä, että käyttö- ja pääsyoikeuksien myöntämisen, muuttamisen ja poistamisen osalta noudatetaan prosessia, joka kattaa kaikki toimitilat, tietojärjestelmät ja palvelut, joissa käsitellään Suojattavaa tietoa.

Lauseen merkitys jää epäselväksi.

kohta 8.2.

Toimittajan tulee huolehtia Palvelun osalta siitä, että Sopimuksen päätyttyä Toimittaja palauttaa ilman viivytystä Tilaajalle tämän avaimet, henkilökortit, kulkuluvat, salausavaimet, lisenssit, kulkukoodit, käyttäjätunnukset, salasanaat sekä muut...

Näistä ainakin kulkukoodit ja käyttäjätunnukset ovat sellaisia, ettei niissä 'palauttaminen' pelkästään riitä, vaan pikemmin Tilaajan on suljettava oikeudet.

kohta 12.1

Tilaajalla tai Tilaajan määräämällä kolmannella taholla...

Voisiko olla: Tilaajalla tai Tilaajan määräämällä tai toimeksi saaneella kolmannella taholla...

kohta 13.3

Tilaaja seuraa turvallisuuden kaikkiin osa-alueisiin liittyviä muutoksia ja ilmoittaa Toimittajalle muutostarpeista.

Tulisiko tämä rajata koskemaan hallinnollista, palvelun ja järjestelmän toiminnan vaatimuksia sekä asiakirjojen tietoturva vaatimuksia? Ei voi välttämättä edellyttää tietoturva teknologian seuraamista.



kohta 14 Sopimussakko ja vahingonkorvaus

Ylivoimainen este (force majeure) lauseke on jäänyt tästä kappaleesta pois. Se on ollut nykyisessä turvallisuussopimuksessa mainittuna.

kohta 14.2.

Sopimussakon määrä jokaista salassapitovelvoitteen rikkomusta kohden on...
Rikkomusta olisi tarkennettava: mikä tarkkaan ottaen on salassapitovelvoitteen rikkominen? Tietovuoto? Miten muut sopimusrikkomukset esim. raportoimatta jättäminen: luetaanko ne salassapitovelvoitteen rikkomuksiksi?

kohta 19 Liite 3 Salassapitositoumusmalli

Vaitiolositoumus-termi on ollut Vahti 2/2010 ohjeessa. Onko termi muutettu tarkoituksella?

kohta 19 Liite 4

Toimittajan turvallisuudenhallinnan kuvaus

Tuleeko tälle jokin yhtenäinen malli/pohja? Kokemus on että muuten saadaan toimittajilta jotain ympäröyviä tietoturvapoliittikka selityksiä.

STM katsoo, että uuteen malliin on saatu paljon hyviä täsmennyksiä, mutta ehkä jokin lyhyt sopimusohje olisi vielä tarpeen. Varsinkin asiaa vähemmän tuntevalle on melko haasteellista ymmärtää näin laajaa ja osittain vaikeaselkoista ohjetta.

Osastopäällikkö, ylijhtaja


 Raimo Ikonen

Tietohallintopäällikkö


 Maarit Puhto

JAKELU

TIEDOKSI

