Verohallinto
PL 325
00052 VERO

Valtiovarainministeriö
valtiovarainministerio@vm.fi

**LAUSUNTO**

8.12.2015

Viite / Diaarinumero
A74/00 00 01/2015

**VM136:00/2013**

**VEROHALLINNON LAUSUNTO KOSKIEN VALTIOVARAINMINISTERIÖN LAUSUNTOPYYNTÖÄ LUONNOKSESTA UUDEKSI TURVALLISUUSSOPIMUSMALLIKSI**

Valtiovarainministeriö on pyytänyt Verohallinnolta lausuntoa koskien luonnosta valtionhallinnon turvallisuussopimusmalliksi. Turvallisuussopimusmalli on ollut Valtion ICT-hankintojen tietoturvaohjeen (VAHTI 3/2011) liitteenä. Ohjeen antamisen jälkeen on uudistettu tietoturvallisuuteen ja tietosuojaan liittyvää lainsäädäntöä ja viranomaisohjeistusta.

Verohallinto toteaa turvallisuussopimusmallin päivittämisen hyväksi asiaksi ja vanhan sopimusmallin päivitystä kriittisesti tarvitsevaksi. Yhtenäinen turvallisuussopimusmalli antaa myös valtionhallinnon toimijoille yhtenäisen ja uskottavan kuvan toimittajan suuntaan sekä selkänojaa vaatia turvallisuussopimuksen täyttämiseksi siihen kriittisesti suhtautuvilta toimijoilta. Verohallinto haluaa kuitenkin tuoda esille muutamia havaintoja luonnoksesta Valtiovarainministeriön arvioitavaksi.

## Yleiset havainnot

Turvallisuussopimuspohjia on ICT-hankintojen ohjeen (VAHTI 3/2011) lisäksi myös Toimitilojen tietoturvaohjeessa (VAHTI 2/2013). Tässä yhteydessä kannattaisi kartoittaa myös näiden ohjeiden ajantasaisuuden tilanne. Lisäksi tämän uuden luonnoksen yhteydessä kannattaisi määrittää näiden kaikkien pohjien asema suhteessa uuteen pohjaan.

Nyt käytetyssä mallissa turvallisuussopimuksen käyttötapa on liittää se kunkin hankinnan liitteeksi. Tämä on useissa virastoissa ja hankinnoissa riittävä. Kuitenkin merkittävä osa virastoista suosii laajempaa turvallisuussopimuksen mallia, jossa etenkin kumppanuutta haettaessa, tehdään yrityksen kanssa yksi hankinnasta erillinen turvallisuussopimus joka määrittää toimittajan kyvykkyyden turvallisuuden hallintaan. Tämän jälkeen voidaan tehdä erillisiä hankintoja joissa kaikissa turvallisuussopimus on voimassa (ja joihin voidaan myös määritellä tarkentavia vaatimuksia turvallisuusasioille). Lausuntopyynnössä jää epäselväksi millaisella saatteella se jaellaan hallintoon, mutta siinä voisi tuoda esiin että myös vaihtoehtoiset toimintamallit voivat olla mahdollisia tai jopa tätä mallia toimivampia. Tällöin luonnollisesti pohja ei voi olla nyt luonnoksena oleva, pitäisikö tällaiselle toimintamallille laatia omansa?

Osa viranomaista käyttää turvallisuussopimuksia myös muuhun yhteistyöhön kuin hankintoihin, esim. varmistamaan että tiedon vastaanottaja ymmärtää yhteistyölle asetetut turvallisuusvaatimukset. Tämä sopimuspohja ei tue tuota mallia lainkaan. Tulisiko pohjaa muuttaa niin että se kattaa myös muun kuin hankintoihin liittyvän sopimisen?

**Yksityiskohtaiset havainnot**

Luvussa 1 on kuvattu yhteyshenkilöt. Olisiko yhteyshenkilöt hyvä kuvata erillisessä liitteessä jolloin niiden vaihtuminen ei aiheuttaisi sopimusmuutosta tai muuten rajata henkilöiden vaihtuminen sopimusmuutosten ulkopuolelle? Samalla kannattaisi nimetä varahenkilöt ja liittää tarkemmat yhteystiedot.

Luvussa 2.3 ja 2.6 määritetään Suojattava tieto. Tämä laajennus edelliseen pohjaan on hyvä. Luvussa 2.3 käytetään kuitenkin termiä "luottamuksellinen", se voisi olla hyvä vaihtaa esim. termiin "ei julkinen", koska termi on varattu yhteen turvallisuusluokkaan ja sekaannuksen vaara on ilmeinen. Yksi mahdollisuus tuoda lisäturvallisuutta on myös lisätä vaatimus että toimittajan on ennakkoon varmistettava tiedon julkisuus tilaajalta.

Luvussa 5.4 rajataan esim. turvallisuusselvitykset, toimittajien henkilöiden hyväksyntä ja turvallisuusohjeistus vasta suojaustasolle III. Tämä voisi olla hyvä laskea oletuksena STIV tasolle.

Luvussa 5.6 on hyvä ja tärkeä lisä. Verohallinto olettaa että Valtiovarainministeriö on varmistanut että se vaatimuksena on voimassa olevan lainsäädännön mukainen?

Luku 5.7 on ristiriitainen luvun 5.6 kanssa.

Luku 5.8 hävittämisen toimintamalli voisi olla hyvä konkretisoida tai määrittää pohjaan "asiakkaan hyväksymällä tavalla". Tähän tai tätä lukua ennen voisi kuvata myös asiakirjojen kirjaamisvelvoitteet; Voisi olla asianmukaista määrittää STIV tasolle että toimittajalla on kirjattuna tiedossa mitä asiakirjoja se on tilaajalta saanut ja STIII lisävaatimuksena yksittäisten asiakirjojen kirjaamisvelvoite. Tältä pohjalta myös luvun hävittämiskohtaan voitaisiin asettaa vaatimus joko asiakirjojen palauttamiseksi tilaajalle tai hävittämiseksi ja tiedon toimittaminen hävittämisestä tilaajalle.

Luku 5.11 osalta kannattaa arvioida onko se turha?

Luvussa 7.1 oli kirjoitusvirhe "sijaintimaineen".

Luvuissa 7.10-.12 tulisi käydä ilmi että toimittajan tulisi lähtökohtaisesti tuottaa palvelu salassa pidettävien tietojen osalta muusta toiminnasta eriytetyistä tiloista. Näin turvallisuustoimenpiteet voidaan mitoittaa vain palvelua tuottavaan joukkoon henkilöstöstä ja yrityksen toiminnasta. Tällä on toiminnan suunnittelun ja palvelun kustannusten kannalta keskeinen merkitys.

Luvussa 8 käsitellään paljon konkreettisia tietojärjestelmäturvallisuuden vaatimuksia. Luvussa pitäisi kuitenkin keskeisesti kuvata että tietojärjestelmä johon viranomaisen salassa pidettävää (tai Suojattavaa) tietoa viedään, tulee olla tilaajan hyväksymä ja turvallisuusratkaisuiltaan siihen vietävän suojaustason mukainen. Osa 8.2 luvun yksityiskohdista voidaan myös rajata edellä mainitun lisäyksen myötä pois ja ne olisi muutenkin hyvä määrittää esimerkeiksi, ei pois sulkevaksi vaatimuslistaksi.

Tulisiko luku 9 yhdistää luvun 8 vaatimuksiin ja nimetä yhdistetty luku tietojärjestelmävaatimuksiksi?

Luku 10 ei todellisuudessa ole tavallisissa hankinnassa relevantti ja saattaa vain aiheuttaa lisäkustannuksia. Kuitenkin mikäli jatkuvuuden kannalta palvelu on kriittinen, se ei nykymuodossa ole riittävän yksityiskohtainen. Tulisiko luku yksinkertaisesti poistaa sopimuksesta ja määrittää varautumiseen liittyvät asiat omissa sopimuksissaan tai liitteissään? Toinen vaihtoehto on tarkentaa kappaletta huomattavasti.

Luku 11 on huomattavan tarkka suhteessa muuhun sopimukseen. Tulisiko osa kappaleista poistaa sopimuksesta ja siirtää näistä vastaavien viranomaisten menettelyohjeisiin? Esim. luvut 11.4 ja 11.8 vaikuttaa täysin prosessiohjeelta, ei sopimuspohjaan kuuluvilta vaatimuksilta.

Luvussa 11.9 voi olla kannattavaa tarkentaa mitä tarkoitetaan ulkomaisella henkilöllä. Tarkoitetaanko ulkomaalaisella muun kuin Suomen kansalaista? Miten toimitaan esim. ulkomaisten henkilöiden osalta jotka ovat asuneet Suomessa koko ikänsä tai toisin päin?

Luku 12 on myös erittäin yksityiskohtainen ja osa luvuista kuuluu selvästi ohjaavan viranomaisen työohjeisiin eikä turvallisuussopimusprosessiin. Esimerkkeinä yksityiskohtaisista vaatimuksista luvut 12.2, 12.3. ja 12.5. Yleisempi tarkastusoikeuden kuvaus voisi olla kaikin puolin toimivampi.

Luku 12.1 rajoitus suoranaisen kilpailijan käytöstä on vaarallinen ja ehdotetaan poistettavaksi. Esim. suurilla IT-palvelutoimittajilla on hyvin laaja palvelutarjonta koskien myös mm. tietoturvakonsultointia ja voi olla vaikea löytää tarkastuskumppania joka ei olisi jollain sektorilla tällaisen toimittajan kilpailija. Luonnollisesti tilaajan on käytettävä järkeä tarkastuksia tehdessään.

Luvussa 12.6 on useita vaatimuksia koottuna yhteen lukuun. Kannattaisi arvioida että jos vaatimukset ovat relevantteja, ne kannattaisi jakaa erilleen. Osa vaatimuksista on myös esitetty jo muualla.

Luku 13.4 on kannattava määrittää laajemmin, tilaajalle tulee ilmoittaa myös muista asioista kuin uhkaavista yhteydenotoista tai uhkatilanteista. Esim. palvelussa tapahtuneet turvallisuustilanteen muutokset tai havaitut riskit ovat myös tärkeitä ilmoittaa.

Luvussa 14.2 voisi olla lisäys "Sopimussakko voidaan periä Toimittajalle maksettavista tulevista Pääsopimuksen mukaisista korvauksista."

Luvussa 14.3 voisi määritellä mitä tapahtuu kun laiminlyönnit ovat toistuvia ja toimittaja korjaa ne aina 14 vuorokauden kuluessa?

Luvussa 14.7 tulisi lisätä myös välillinen vahinko. Erityisesti tietoturvallisuuden osalta välittömän vahingon määrittäminen voi olla haastavaa ja suuri osa kustannuksista tulee välisistä vahingoista kuten virastojen henkilöstön ajankäytöstä, konsulttipalveluiden maksuista ongelmia selvitettäessä tai järjestelmien alasajosta ongelmatilanteiden selvityksen vuoksi.

Tietohallintojohtaja Markku Heikura

Turvallisuusjohtaja Samuli Bergström

**Verohallinto**
Tietohallintoyksikkö
Lintulahdenkuja 10
Helsinki

**www.vero.fi**
puh. 020 612 000
faksi 020 612 3595