Valtionhallinnon tietoturvallisuussopimusmalli

Versio: 1.0 / 7.6.2016

Julkaistu: 8/2016 osana VAHTi-tukimateriaalikokonaisuutta

Voimassaoloaika: toistaiseksi

KÄYTTÖOHJE

Yleisesti sopimuksen käytöstä

Valtionhallinnon tulosyksiköille (tilaaja) suositellaan näiden sopimusehtojen käyttämistä IT-hankintojen yhteydessä. Tietoturvallisuussopimus on tarkoitettu käytettäväksi etenkin tietojärjestelmien toimitusten ja niihin liittyvien jatkuvien palvelujen hankinnoissa. Sopimusta voidaan käyttää myös asiantuntijapalveluiden hankinnassa.

Tämän sopimuksen tavoitteena on huolehtia siitä, että valtionhallinnon tulosyksiköitä sitovat vaatimukset salassa pidettävien tietojen käsittelystä ja tietoturvallisuudesta ulotetaan myös valtionhallinnolle palveluja tuottavaan yksityiseen osapuoleen. Tavoitteen täyttäminen vaatii siten laajempaa ehtokokonaisuutta kuin mistä on sovittu julkishallinnon käyttämissä yleisissä sopimusehdoissa (JIT- ja JYSE-ehdot), joissa on käsitelty esimerkiksi Toimittajan liike- ja ammattisalaisuuksien salassapitovelvoitteet.

Tietoturvallisuussopimuksen ehdoilla täydennetään hankintaa koskevaa sopimusta (pääsopimus), jossa kuvataan mm. sopimuksen osapuolet, kohde, toimituksen tai palvelun sisältö ja sopimuksen kohteelle asetetut vaatimukset.

Sopimusrakenne on aina suunniteltava huolellisesti. Tämän sopimuksen ehtoja voidaan hankintakohtaisesti muokata kulloiseenkin tilanteeseen soveltuvaksi. Täydentämistä tai erityistä harkintaa vaativat kohdat on erikseen merkitty harmaalla korostuksella. Poista korostus lopullisesta sopimustekstistä.

Vaihtoehtoisesti tämän sopimuksen ehdoista voidaan poiketa pääsopimuksen ehdoilla. Tällöin pääsopimuksesta tulee selkeästi ilmetä, mistä ehdoista on sovittu turvallisuussopimuksen ehdoista poikkeavasti ja tarkastettava ehtojen soveltamisjärjestys. Tilaajan tulee kiinnittää huomiota ”Ellei toisin ole sovittu,” -alkaviin kohtiin tarjouspyynnön valmistelussa ja ottaa niihin selkeästi kantaa tarjouspyynnössä, jos ehdon pääsäännöstä on tarkoitus poiketa.

Tietoturvallisuussopimus on hankintakohtainen, joten se ei sovellu käytettäväksi yleisenä, kaikkea tilaajan ja toimittajan välistä turvallisuusyhteistyötä koskevana sopimuksena. Hankintakohtaisuus johtuu ennen kaikkea siitä, että hankinnan kohteen tietoturvallisuusvaatimukset eroavat toisistaan erilaisissa IT-hankkeissa.

Näissä ehdoissa on pyritty käyttämään vastaavaa terminologiaa kuin julkisen hallinnon IT-hankintojen sopimusehdoissa (JIT 2015).

Ehtokohtaiset käyttöohjeet

Ohessa esitetään kustakin luvusta keskeiset havainnot.

1. Sopijapuolet

Tietoturvallisuussopimuksessa sovitaan sopimuksen yhteyshenkilöistä. Jos tietoturvallisuussopimuksen yhteyshenkilöille halutaan antaa erityisiä vastuita, tulisi nämä vastuut määritellä Yhteyshenkilöt-liitteellä. Tarkasta, että yhteyshenkilöiden määritelty vastuu kohdassa 1.2 vastaa tahtotilaanne.

2. Määritelmät

Asiakastiedon määritelmä on sopimuksen keskeisiä määritelmiä. Asiakastietoa on määritelmän mukaan henkilötiedot sekä tiedot oikeushenkilöistä. Henkilötietojen suojaan kohdistuu lainsäädännöllisiä velvoitteita. Oikeushenkilön tietoihin ei sitä vastoin sovelleta henkilötietoja koskevaa lainsäädäntöä. Tässä sopimuksessa sekä henkilötietojen että oikeushenkilötietojen käsittelyyn kohdistuu yhtenäisiä vaatimuksia, jonka vuoksi käytetään pääsääntöisesti yhteistä Asiakastiedon määritelmää.

Tilaajan aineiston määritelmä kattaa kaiken sopimuksen mukaisessa toiminnassa käytetyn tilaajan aineiston, olipa se salassa pidettävää tai julkista esimerkiksi julkisuuslain perusteella. Sopimuksen lähtökohtana on varmistaa tilaajan aineiston luottamuksellisuus, eheys ja saatavuus pääsopimuksen mukaisessa palvelutuotannossa siitä riippumatta, onko tilaajan aineisto salassa pidettävää tietoa.

3. Sopimuksen tavoite ja kohde

Sopimuksen kohta 3.1 on täydennettävä pääsopimuksen tiedoilla.

Tietoturvallisuussopimus voidaan liittää pääsopimuksen osaksi. Tällöin sen tulisi olla soveltamisjärjestyksessä ensimmäinen liite. Vaihtoehtoisesti tietoturvallisuussopimus voi olla pääsopimuksesta erillinen sopimusdokumentti, jolloin sen ehdot saavat etusijan suhteessa pääsopimukseen.

4. Alihankkijat

Alihankkijoiden käyttäminen ja heidän soveltuvuutensa selvitetään pääsääntöisesti palveluja koskevan hankintamenettelyn aikana. Jos

Toimittaja on hyväksytyssä tarjouksessa ilmoittanut soveltuvat alihankkijat, Tilaajan tulee lähtökohtaisesti katsoa tällaiset alihankkijat hyväksytyiksi kohdan 4.2 mukaisesti.

Alihankkijamuutokset ovat sallittuja sopimuskaudella ainoastaan hankintalain sallimissa rajoissa. Sen vuoksi alihankkijoiden vaihtaminen ei ole yksinomaan toimittajan harkinnassa. Lisäksi tilaaja voi rajoittaa alihankkijavaihdoksia esimerkiksi turvallisuuteen liittyvistä syistä.

Jos sopimuksen kohteena on valmisohjelmistohankinta, tietoturvallisuussopimuksen velvoitteiden ulottamista valmisohjelmistotoimittajaan on syytä arvioida kriittisesti, sillä valmisohjelmistotoimittaja ei välttämättä käsittele Tilaajan salassa pidettävää aineistoa. Esimerkiksi tarkastusoikeuden käyttäminen tai vaatimukset toimittajan toimitiloille voivat johtaa siihen, ettei ohjelmistotalo katso voivansa niihin sitoutua.

Sopimuksen alihankintaa koskevaan lukuun voidaan lisätä ehto, jossa valmisohjelmiston toimittajan velvoitteita rajataan esimerkiksi seuraavasti:

> *Jos Toimittajan alihankkijan tehtävänä on ainoastaan toimittaa sovittu valmisohjelmisto, tällaiseen alihankkijaan sovelletaan tämän sopimuksen ehtoja lukuun ottamatta kohtia* ***Virhe. Viitteen lähdettä ei löytynyt.*** *(luettelo toimittajan henkilöistä), 8.1 (Henkilöiden hyväksyttäminen tilaajalla), lukua 10 (Jatkuvuuden varmistaminen), lukua 11 (turvallisuusselvitykset), lukua 12 (tarkastukset), lukua 14 (sopimussakko ja vahingonkorvaus).*

5 Salassapito ja vaitiolovelvollisuus

Luvussa on asetettu Toimittajalle kielto hyödyntää tai luovuttaa tilaajan aineistoa muussa kuin sopimuksen mukaisessa tarkoituksessa. Vaatimus koskee näin ollen kaikkea tilaajaan aineistoa riippumatta siitä, onko aineisto salassa pidettävää.

Salassa pidettävän aineiston osalta tässä luvussa on keskeiset ehdot. Salassa pidettävää saavat käsitellä ainoastaan asetetut kriteerit täyttävät toimittajan henkilöt. STIV-suojaustason aineiston käsittelyn osalta ei ole välttämätöntä vaatia henkilöturvallisuusselvitystä, mutta käytännössä useat viranomaiset edellyttävät sellaista.

Tilaaja voi edellyttää myös erityisen luettelon ylläpitämistä niistä henkilöistä, joilla on oikeus käsitellä salassa pidettävää aineistoa. Tilaaja erikseen harkitsee ne tilanteet, joissa luettelon ylläpitäminen on tarkoituksenmukaista.

Kohdassa 5.9 on mainittu tilaajan ohjeistus salassa pidettävän tiedon käsittelystä. Useimmilla viranomaisilla on tällainen ohje käytössään ja

hankintavaiheessa se tulisi toimittaa tarjoajille tarjouspyynnön osana. Liite on olennainen osa tätä tietoturvallisuussopimusta.

6 Tietosuoja

Kohdissa 6.1 ja 6.2 on poikkeuksellisesti käytetty määritelmänä ”Henkilötietoa” ”Asiakastiedon” sijaan. Syynä on henkilötietolain soveltamisalan rajoittuminen henkilötietojen suojaan. Henkilötiedon määritelmä on yleisesti tunnettu ja henkilötietolaissa määritelty.

7 Hallinnollinen ja fyysinen tietoturvallisuus

Luvun kohdassa 7.2 sovitaan sopimukseen liitettävien tietoturvavaatimusten noudattamisesta. Tietoturvavaatimuksina on usein käytetty Valtion tieto- ja viestintekniikkalaitos Valtorin ylläpitämää vaatimusluetteloa, jossa vaatimukset on jaoteltu perustason, korotetun tason ja korkean tason vaatimuksiin. Vaatimukset on kussakin hankinnassa asetettava siten, että ne soveltuvat hankinnan kohteeseen ja vastaavat suunniteltua tietoturvan tasoa. Hankintamenettelyissä vaatimukset ja tietoturvallisuussopimus on liitettävä tarjouspyyntöön.

Tietoturvavaatimukset voidaan teknisesti liittää osaksi pääsopimuksen muuta vaatimusmäärittelyä tai ottaa tietoturvallisuussopimuksen liitteeksi. Joka tapauksessa harmaalla korostettua sopimuskohtaa on muokattava. Jos erillisiä tietoturvavaatimuksia ei ole otettu osaksi sopimuksia, tietoturvallisuussopimus määrittää tietoturvallisuuden vähimmäistason. Sen vuoksi tietoturvallisuussopimuksessa on eräitä yksityiskohtaisia sopimusehtoja.

Kohdassa 7.3 Toimittaja on velvoitettu noudattamaan tietoturva-asetuksen (681/2010) mukaisia käsittelysääntöjä. Käsittelysäännöt perustuvat voimassa olevan asetuksen 4 lukuun. Pääasiassa asetuksen velvoitteet tulevat jo sovituksi muualla tässä sopimuksessa ja sen liitteenä olevissa tietoturvallisuusvaatimuksissa, mutta erityisesti asetuksen 15-21 §:n velvoitteet on syytä saattaa sopimusehdolla Toimittajan noudatettavaksi.

Kohdassa 7.4 viitataan toimittajan ylläpitämään turvallisuudenhallinnan kuvaukseen. Sikäli kuin turvallisuudenhallinnan kuvausta edellytetään, hankintamenettelyssä tulisi asettaa kuvaukselle tietyt reunaehdot ja pyytää sellainen toimitettavaksi osana tarjousta.

Kohdissa 7.6-7.10 on käsitelty tietojen kansainvälistä käsittelyä. Henkilötietojen käsittely toisissa maissa on mahdollista henkilötietolain säätämissä rajoissa. Tässä sopimuksessa sääntely on ulotettu sopimuksella myös oikeushenkilön tietoihin. Tilaaja voi esimerkiksi huoltovarmuus- tai muista turvallisuussyistä rajoittaa myös muun tilaajan

aineiston siirtämistä Suomen rajojen ulkopuolelle. Asiaa koskevat ehdot tulisi kuvata jo hankintamenettelyn aikana.

8 Tietojärjestelmien hallinnan vaatimukset

Kohta 8.1 perustuu turvallisuusselvityslain säännöksiin ja kohdan tarkoituksena on saattaa tilaajan kontrollin piiriin ko. kohdan mukaisia tehtäviä suorittavat henkilöt, vaikkeivat nämä työtehtävissään käsittelisi tilaajan salassa pidettäviä tietoja.

Tässä luvussa asetetaan lisäksi vähimmäisvaatimukset toimittajan vastuulla olevien palveluympäristöjen osalta. Vaatimukset täydentyvät usein hankinnan kohteelle asetettujen tietoturvavaatimusten myötä.

9 Ohjelmistoturvallisuus

Tässä luvussa asetetaan vähimmäisvaatimukset ohjelmistoturvallisuudelle. Vaatimukset täydentyvät usein hankinnan kohteelle asetettujen tietoturvavaatimusten myötä.

10 Jatkuvuuden varmistaminen

Kohdassa 10.1 on viitattu erillisiin, hankinnan kohteeseen liittyviin ICT-varautumisvaatimuksiin.

ICT-varautumisvaatimuksina on usein käytetty Valtion tieto- ja viestintekniikkalaitos Valtorin ylläpitämää vaatimusluetteloa, jossa vaatimukset on jaoteltu perustason, korotetun tason ja korkean tason vaatimuksiin. Vaatimukset on kussakin hankinnassa asetettava siten, että ne soveltuvat hankinnan kohteeseen ja vastaavat suunniteltua varautumisen tasoa. Hankintamenettelyissä vaatimukset ja tietoturvallisuussopimus on liitettävä tarjouspyyntöön.

Tämän sopimuksen jatkuvuutta koskevat vaatimukset kohdassa 10.2 muodostavat siten vähimmäistason ja ne perustuvat Huoltovarmuuskeskuksen Sopiva-suosituksiin. Sopiva-suosituksissa on myös lisävaatimuksia ja niihin voi tutustua osoitteessa http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/

11 Turvallisuusselvitykset

Sopimus kattaa turvallisuusselvityslain mukaisesti sekä yritysturvallisuusselvitykset että henkilöturvallisuusselvitykset.

Kohta 11.2 on tarkoitettu täyttävän turvallisuusselvityslain 4 §:n 2 momentin mukaisen tiedottamisvelvollisuuden julkisissa hankinnoissa,

silloin kun tämä sopimus on osa tarjouspyyntöä. On suositeltavaa lisäksi ilmoittaa yritysturvallisuusselvityksen mahdollisuudesta lisäksi tarjouspyyntöasiakirjassa tai hankinnan kohteen kuvauksessa.

Yritysturvallisuusselvityksen teettäminen edellyttää erillistä toimittajan antamaa suostumusta. Jos toimittaja ei anna suostumustaan selvityksen teettämiselle, tilaajalle syntyy oikeus irtisanoa tietoturvallisuussopimus ja pääsopimus.

Käytännön haasteena on ilmennyt turvallisuusselvitysten teettäminen silloin, kun palvelussa ei käsitellä turvallisuusluokiteltua tietoa ja toimittaja tai sen työntekijä on ulkomaalainen. Tällöin ei voida välttämättä toteuttaa turvallisuusselvitysmenettelyä Kansallisen turvallisuusviranomaisen välityksellä. Tästä syystä tietoturvallisuussopimukseen on otettu ehdot vaihtoehtoisesta menettelytavasta, jossa toimittaja voisi omatoimisesti esittää vastaavaa selvitystä kuin mistä on säädetty turvallisuusselvityslaissa.

Jos yritysturvallisuusselvityksen perusteella havaitaan sellaisia ilmiöitä, joiden ehkäisemiseksi yritysturvallisuusselvitys lain mukaan tehdään, on tilaajalla oltava käytettävissään sopimukseen perustuvat oikeuskeinot riskin poistamiseksi. Irtisanomisoikeudesta tällä perusteella sovitaan luvussa 16.

Kohta 11.6 asettaa kustannusvastuun yritysturvallisuusselvityksistä toimittajalle. Ehto perustuu turvallisuusselvityslain 60 §:n 1 momenttiin, jonka mukaan kustannuksista vastaa selvityksen kohde, jos selvitys on laadittu viranomaisen hakemuksesta. Näitä ehtoja käyttävät muutkin julkisoikeudelliset toimijat kuin viranomaiset, joten kustannusvastuun osalta on syytä sopia yhdenmukaisesti kaikkien julkishallinnon toimijoiden osalta.

12 Tarkastukset

Tilaaja voi suorittaa joko itsenäisesti tai kolmannen osapuolen toimesta tietoturvallisuusauditointeja milloin tahansa sopimuksen aikana ilmoittamalla siitä etukäteen toimittajalle. Käytännössä auditointeja suorittavat toimeksiannon perusteella Viestintävirasto, sen akkreditoimat yritykset taikka muut auditointeihin erikoistuneet yritykset. Tilaajan tulisi keskustella toimittajan kanssa tarkastuksen toteuttajasta ja vaikka sopimuksen mukaan tilaajalla on harkintavalta tarkastajan valinnasta, toimittajan suoranaisia kilpailijoita ei tulisi tarkastuksessa käyttää.

Julkishallinnon toimijaan voi kohdistua auditointeja EU-lainsäädännön perusteella. Tarkastusoikeus voi olla yllätystarkastuksen luonteinen, jolloin ei voida soveltaa kohtuullisia aikoja ennakkoilmoittamiselle. Tällaisissa tapauksissa tilaajan on laadittava tietoturvallisuussopimukseen poikkeusehto. Ehto voi olla esimerkiksi seuraava:

Kohta 12.2: Jos tarkastusvaatimuksen esittää Tilaajalle sellainen kolmas osapuoli, jolla on lainsäädäntöön perustuva oikeus tarkastaa Tilaajan toimintaa ja tietojärjestelmiä Palveluiden piiriin kuuluvilta osin, Toimittajan on järjestettävä tarkastusmahdollisuus viimeistään kolmantena (3) työpäivänä Tilaajan kirjallisesta ilmoituksesta, ilmoituspäivää laskematta.

Tarkastuksen käytännön toteutukseen on perusteltua laatia tarkastussuunnitelma ja katselmoida se toimittajan kanssa.

13 Raportointi ja viestintä

Toimittajan tulee noudattaa sopimuksessa asetettuja vähimmäisvaatimuksia. Käytännössä tietoturva- ja ICT-varautumisvaatimuksista aiheutuu tarkempia raportointivelvoitteita toimittajalle. Tilaajan tulisi tehdä hankintamenettelyn aikana arvio raportointivelvollisuuksien laajuudesta, jotta vältytään päällekkäisiltä ja ylimääräisiä kustannuksia aiheuttavilta raportointivelvoitteilta.

14 Sopimussakko ja vahingonkorvaus

Tässä luvussa on erityisesti korostettu Tilaajan harkintaa sopimussakon määrän asettamisessa. Sopimussakko tulisi asettaa kohtuulliselle tasolle ottaen huomioon salassa pidettävän tiedon merkitys, sopimuksen arvo ja muu yhteistyön luonne.

Sopimussakon osalta on erotettu salassapitovelvoitteiden rikkominen ja muut turvallisuussopimuksen rikkomistilanteet.

Kohdan 14.4. mukaan toimittajalla on mahdollista korjata menettelyään turvallisuusvelvoitteiden rikkomus- ja laiminlyöntitilanteissa välttääkseen sopimussakon. Sanottu ei koske salassapitovelvoitteen rikkomista.

Vahingonkorvauksen osalta on sovittu vastuunrajoituksista. Vahingonkorvausvelvollisuus koskee lähtökohtaisesti välittömiä vahinkoja. Vastuurajoituksen sopimuskauden yhteenlaskettu kattohinta on sidottu pääsopimuksen mukaiseen toimitukseen. Ehdoissa on tarkennettu toimituksen kokonaishinnan määrittäviä elementtejä. Kokonaishinta sisältää sopimuksen mukaiset tuotteet, palvelut (esim. toimitusprojektin) sekä jatkuvat palvelut. Myös lisätyöt, kuten muutoshallinnan työ sisältyy kokonaishintaan.

Jos tietoturvallisuussopimuksen tilaajaosapuolena on esimerkiksi valtionhallinnon palvelukeskus, voidaan tietoturvallisuussopimukseen kirjata ehto siitä, että välittömien vahinkojen piiriin sisältyy vahingot, jotka aiheutuvat palvelukeskuksen asiakkaille näiden hankkiessa palvelua palvelukeskukselta, mutta joita tuotetaan palvelukeskuksen ja toimittajan väliseen sopimukseen perustuen. Esimerkkiehto voi olla seuraava:

Kohta 14.8: Tilaajalle aiheutuneiksi välittömiksi vahingoiksi katsotaan myös sellaiset Tilaajan asiakkaan välittömät vahingot, jotka aiheutuvat Toimittajan sopimusrikkomuksesta sen tuottaessa Palvelua Tilaajan alihankkijana Tilaajan asiakasorganisaatioille ja joista Tilaaja on asiakkaisiinsa nähden korvausvelvollinen.

15 Sopimusmuutokset

Jos sopimuksen liitteitä halutaan muuttaa ilman erillistä muutossopimusta, asiasta voidaan sopia kohdassa 15.2.

16 Sopimuksen irtisanominen

Tietoturvallisuussopimuksen irtisanomisaika on sama kuin pääsopimuksella. Jos pääsopimuksessa ei olisi poikkeuksellisesti sovittu irtisanomisaikaa, tämän sopimuksen irtisanomisaika on kolme kuukautta.

Tietoturvallisuussopimus ei ole vapaasti irtisanottavissa ennen kuin pääsopimuksen mukainen määräaikainen sopimuskausi on kulunut.

Erityisinä irtisanomisperusteina on mainittu Toimittajan kieltäytyminen yritysturvallisuusselvityksestä tai siihen liittyvien selvitysten toimittamisesta. Toisena erityisenä irtisanomisperusteena on yritysturvallisuusselvityksen perusteella ilmennyt vakava epäluottamus toimittajan toimintaan. Irtisanomisperusteet perustuvat turvallisuusselvityslain 1 §:ään, jonka mukaan lain tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä.

19 Sopimusasiakirjat ja niiden pätemisjärjestys

Tässä yhteydessä korostetaan liiteasiakirjojen tärkeyttä. Tilaajalla tulisi olla käytössään ohje salassa pidettävien tietojen käsittelystä. Liitteenä 3 olevat tietoturvavaatimukset voidaan halutessa liittää tähän sopimukseen, jos niitä ei oteta osaksi pääsopimuksen liiteluetteloa.

Tämä käyttöohje ei ole osa sopimusta.