

# TURVALLISUUSSOPIMUS

(MALLI v0.1.2)

19.11.2015

**[Tilaaaja]**

**ja**

**[Toimittaja]**

## SISÄLLYSLUETTELO

|    |                                                           |    |
|----|-----------------------------------------------------------|----|
| 1  | SOPIJAPUOLET .....                                        | 1  |
| 2  | MÄÄRITELMÄT .....                                         | 1  |
| 3  | SOPIMUKSEN KOHDE .....                                    | 2  |
| 4  | ALIHANKKIJAT .....                                        | 2  |
| 5  | SALASSAPITO JA VAITIOLOVELVOLLISUUS .....                 | 3  |
| 6  | TIETOSUOJA .....                                          | 4  |
| 7  | HALLINNOLLINEN JA FYYSINEN TIETOTURVALLISUUS .....        | 4  |
| 8  | TIETOJÄRJESTELMIEN HALLINNAN VAATIMUKSET .....            | 6  |
| 9  | OHJELMISTOTURVALLISUUS .....                              | 7  |
| 10 | JATKUVUUDEN VARMISTAMINEN .....                           | 7  |
| 11 | TURVALLISUUSSELVITYKSET .....                             | 8  |
| 12 | TARKASTUKSET .....                                        | 9  |
| 13 | RAPORTOINTI .....                                         | 10 |
| 14 | SOPIMUSSAKKO JA VAHINGONKORVAUS .....                     | 11 |
| 15 | SOPIMUSMUUTOKSET .....                                    | 12 |
| 16 | SOPIMUKSEN IRTISANOMINEN .....                            | 12 |
| 17 | SOPIMUKSEN VOIMASSAOLO .....                              | 13 |
| 18 | SOVELLETTAVA LAKI JA ERIKESKISYYKSIEN RATKAISEMINEN ..... | 13 |
| 19 | SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS .....        | 13 |
| 20 | SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET .....                | 14 |

## 1 SOPIJAPUOLET

### 1.1 Sopijapuolet ovat:

1. [nimi] (jäljempänä "Tilaaaja")

Osoite

Y-tunnus

Yhteyshenkilö:

2. [nimi] (jäljempänä "Toimittaja")

Osoite

Y-tunnus

Yhteyshenkilö:

1.2 Turvallisuuteen liittyvä viestintä käydään ensisijaisesti yhteyshenkilöiden välillä. Yhteyshenkilöt vastaavat turvallisuuden hallinnasta ja koordinoinnista, turvaongelmien raportoinnista, mahdollisten tarkastusten toteutuksesta sekä sovittujen korjaustoimenpiteiden toteutumisen seurannasta.

## 2 MÄÄRITELMÄT

2.1 **Henkilötieto** tarkoittaa kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

2.2 **Käsittely (tietojen käsittely)** tarkoittaa tietojen keräämistä, tallettamista, kopiointia, järjestämistä, käyttöä, lukemista, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita tietoihin kohdistuvia toimenpiteitä.

2.3 **Salassa pidettävä tieto** tarkoittaa kaikkea sellaista Tilaaajan asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä "julkisuuslaki") tai muussa lainsäädännössä, ja jonka Tilaaaja on tällaiseksi tiedoksi merkinnyt tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin.

Salassa pidettävällä tiedolla tarkoitetaan lisäksi kaikkea tuotteen toimituksen tai Palvelun yhteydessä käytettävää tai niihin sisältyvää taikka syntynyttä Tilaaajan aineistoa, jonka Toimittaja tietää tai sen voidaan kohtuudella olettaa tietävän olevan luottamuksellista. Tilaaajaan aineistoon sisältyy, tähän kuitenkaan rajoittumatta Tilaaajan henkilöstöön, asiakkaisiin, alihankkijoihin, prosesseihin, palveluihin, tiloihin, tietojärjestelmiin, tietokantoihin, ohjelmistoihin, rekistereihin, turvallisuus- ja varautumisjärjestelyihin sekä liikesalaisuuksiin sisältyvät tai niihin liittyvät tiedot sekä niiden muotoilu, rakenne ja metatieto.

Salassa pidettäväksi tiedoksi ei katsota sellaista tietoa, joka on julkisesti saatavilla tai jonka sopijapuoli on saanut tietoonsa laillisella tavalla kolmannelta sopijapuolelta ilman sitä koskevaa salassapitovelvoitetta.

- 2.4 **Palvelu** tarkoittaa sitä palvelua, josta Tilaaja ja Toimittaja ovat sopineet Pääsopimuksessa. Mitä tässä sopimuksessa on sovittu Palvelusta, sovelletaan soveltuvien osien lisäksi Pääsopimuksessa sovittuun tavarahankintaan.
- 2.5 **Pääsopimus** tarkoittaa kohdassa 3.1 yksilöityä Toimittajan ja Tilaajan välistä sopimusta liitteineen.
- 2.6 **Suojattava tieto tarkoittaa** Henkilötietoa ja/tai Salassa pidettävää tietoa. 
- 2.7 **Tekninen tukijärjestelmä** tarkoittaa pääosin Toimittajan omaan käyttöön tarkoitettua sähköposti-, tiketointi-, työryhmä-, toiminnanohjaus-, konfiguraationhallinta- tai vastaavaa tietojärjestelmää.
- 2.8 **Toimitila** tarkoittaa joko yksittäistä huonetta tai niistä muodostuvaa kokonaisuutta sekä tietoteknisiä laitetiloja.
- 2.9 **Tietotekninen laitetila** (IT-laitetila) tarkoittaa erityisesti konesalia, palvelinhotellia, viestiasemaa, tietoverkon valvomo- tai hallintatilaa tai muuta erillistä teknistä tilaa.
- 2.10 **Vahti** tarkoittaa Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmää.

### 3 SOPIMUKSEN KOHDE

- 3.1 Toimittaja ja Tilaaja ovat tehneet Pääsopimuksen nro [XXX] [sopimuksen kohde] [pvm]. 
- 3.2 Tässä sopimuksessa sovitaan turvallisuusjärjestelyistä, salassapidosta, tietosuojasta ja tietoturvallisuudesta Palveluiden tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Tilaajan ja Toimittajan välisessä yhteistyössä.
- 3.3 Jos tämä sopimus on Pääsopimuksen liite, sopimusasiakirjojen soveltamisjärjestys määräytyy Pääsopimuksen ehtojen mukaisesti. Pääsopimuksessa sovittuja vastuunrajoituksia ei sovelleta tämän sopimuksen perusteella syntyviin vastuisiin, ellei asiasta ole nimenomaisesti toisin sovittu.
- 3.4 Ellei kohdasta 3.3 muuta johdu, tämän sopimuksen ehtoja sovelletaan ristiriitatilanteissa ennen Pääsopimuksen ehtoja. 
- 3.5 Viittaus "tähän sopimukseen" tarkoittaa aina myös viittausta tämän sopimuksen liitteisiin, ellei nimenomaisesti toisin ole todettu.

### 4 ALIHANKKIJAT

- 4.1 Mitä tässä sopimuksessa on sovittu Toimittajasta ja Toimittajan henkilöistä, sovelletaan myös alihankkijaan ja alihankkijan henkilöihin. Mitä tässä sopimuksessa sovitaan alihankkijasta, koskee myös sellaisia Toimittajan konserniyhtiöitä, jotka osallistuvat sovittuun Tilaajalle tuotettaviin Palveluihin.
- 4.2 Ellei Toimittajan käyttämiä alihankkijoita ole ilmoitettu Pääsopimuksessa, Toimittajan tulee hyväksyttää Tilaajalla sellainen alihankkija, jota se aikoo käyttää Suojattavan tiedon käsittelyssä tai jolla on pääsy Tilaajan toimitiloihin tai tietojärjestelmiin, joissa käsitellään Suojattavaa tietoa. 

- 4.3 Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tätä sopimusta myös käyttäessään alihankkijoita. Toimittajan on tiedotettava alihankkijalleen, että turvallisuusjärjestelyjen saattamisesta tämän sopimuksen edellyttämälle tasolle saattaa syntyä kustannuksia. Tilaaaja ei vastaa näistä kustannuksista.
- 4.4 Toimittaja vastaa alihankkijoiden toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän sopimuksen ehtojen mukaisesti 

## 5 SALASSAPITO JA VAITIOLOVELVOLLISUUS

- 5.1 Tällä sopimuksella ei poiketa lainsäädännön asettamista pakottavista velvoitteista. Tällaisia velvoitteita voi sopijapuolille aiheutua esimerkiksi viranomaisten toiminnan julkisuudesta annetusta laista (621/1999), valtioneuvoston asetuksesta tietoturvallisuudesta valtionhallinnossa (681/2010; jäljempänä tietoturvallisuusasetus) sekä muussa lainsäädännössä olevista salassapitoa ja julkisuutta koskevista säännöksistä.
- 5.2 Toimittaja sitoutuu pitämään salassa Salassa pidettävän tiedon eikä käytä taikka hyödynnä Suojattavaa tietoa muuhun kuin sovittuun tarkoitukseen ja ainoastaan siinä laajuudessa kuin se kulloinkin on tarpeen.
- 5.3 Toimittaja saa luovuttaa Suojattavia tietoja vain niille henkilöille, jotka tarvitsevat Suojattavia tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Toimittaja ohjeistaa ja kouluttaa  Suojattavan tiedon asianmukaisen käsittelyn henkilöille, jotka käsittelevät Suojattavaa tietoa.
- 5.4 Ellei toisin sovita, Toimittajan henkilön on täytettävä seuraavat edellytykset saadakseen oikeuden käsitellä Suojattavaa tietoa, joka on suojaustasotai turvallisuusluokiteltu tasolle III tai ylempi 
- a) Toimittaja on hyväksyttänyt henkilön Tilaaajalla etukäteen ja
- b) henkilöstä on tehty henkilöturvallisuusselvitys
- c) henkilö on tietoinen salassapitoa koskevista  velvoitteistaan.
- 5.5 Henkilöturvallisuusselvitystä ei edellytet Toimittajan henkilölle myönnetään käsittelyoikeus korkeintaan suojaus- tai turvallisuustason IV Suojattavaan tietoon, ellei Tilaaaja erikseen turvallisuusselvitystä vaadi.
- 5.6 Ellei Suojattavaa tietoa ole luokiteltu eikä Tilaaaja ole muutoin ohjeistanut Toimittajaa Suojattavan tiedon käsittelystä, Suojattavaa tietoa käsitellään kuin se olisi luokiteltu suojaustasolle IV.
- 5.7 Toimittaja toimittaa Tilaaajan pyynnöstä tiedon Toimittajan henkilöistä, jotka käsittelevät suojaustasolle [valitaan sopivat vaihtoehdot: II, III, IV] luokiteltuja Tilaaajan Suojattavia tietoja. 
- 5.8 Suojattavaa tietoa sisältävää asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi. Tarpeettomat tiedostot ja tulosteet tulee hävittää  olellisesti ja suojaustasoluokituksen edellyttämällä tavalla.

- 5.9 Toimittaja sitoutuu noudattamaan tämän sopimuksen liitteenä olevaa Tilaa-  
jan ohjeistusta Suojattavan tiedon käsittelystä.
- 5.10 Toimittaja vastaa siitä, että Toimittajan henkilö, joka käsittelee Suojatta-  
vaa tietoa, tekee Tilaaajan pyynnöstä salassapitositoumuksen tämän sopi-  
muksen liitteenä olevalle lomakkeelle  nen kuin hän aloittaa suorittamaan  
sopimuksen mukaista palvelutehtävää.
- 5.11 Toimittaja tiedostaa, että Suojattavan tiedon luvaton paljastaminen tai oi-  
keudeton käsittely saattaa olla rikoslain mukaan rangaistava teko.

## 6

### TIETOSUOJA

- 6.1 Toimittaja noudattaa julkisuuslaissa tarkoitettua hyvää tiedonhallintapaa  
sekä Henkilötietoja käsitellessään henkilötietolain (523/1999) edellyttämää  
hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä  
sekä muuta Toimittajaa koskevaa tietosuojalainsäädäntöä Pääsopimukseen  
liittyvän Palvelun tuottamisessa.
- 6.2 Mikäli toimitukseen tai osapuolen väliseen yhteistyöhön sisältyy Henkilötie-  
tojen käsittelyä, vastaavat sopijapuolet omista lakiin perustuvista velvoit-  
teistaan joko rekisterinpitäjänä tai Henkilötietojen käsittelijänä. Jos Toimit-  
taja käsittelee Henkilötietoja Tilaaajan toimeksiannosta, toimii Toimittaja  
Henkilötietojen käsittelijänä ja sitoutuu toimimaan sekä lain että erikseen  
annettavan Tilaaajan ohjeistuksen mukaisesti käsitellessään Henkilötietoja.  
Toimittaja myös sitoutuu toteuttamaan ne tekniset ja organisatoriset toi-  
menpiteet, joita tarvitaan Henkilötietojen suojaamiseksi luvattomalta tie-  
toihin pääsylvä tai tietojen tuhoutumiselta tai muuttumiselta. 
- 6.3 Ellei toisin ole sovittu, Toimittaja ei siirrä Henkilötietoja sovitusta palvelu-  
tuotannon paikasta, tai ellei tällaisesta paikasta ole sovittu, Euroopan talo-  
usalueelta sen ulkopuolelle tai mahdollista pääsyä Euroopan talousalueella  
oleviin Henkilötietoihin Euroopan talousalueen ulkopuolelta  toimittaja tie-  
dostaa tämän vaatimuksen koskevan myös erilaisia teknisiä tukijärjestel-  
miä, joita se saattaa hyödyntää Palvelujen tuotannossa.

## 7

### HALLINNOLLINEN JA FYYSINEN TIETOTURVALLISUUS

#### Yleiset vaatimukset

- 7.1 Toimittaja on velvollinen ilmoittamaan Tilaaajalle kaikki ne toimipisteet si-  
jaintimaineen, mistä Toimittaja tuottaa Palvelua ja/tai käsittelee Suojatta-  
vaa tietoa.
- 7.2 Tilaaaja on määrittänyt Palvelun hankinnan yhteydessä Palveluun sovellet-  
tavan valtionhallinnon tietoturvatason ja Palveluun liittyvät konkreettiset  
tietoturvavaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esi-  
tetty [Pääsopimuksen liitteessä X/tämän sopimuksen liitteessä X.]. Vaati-  
mukset täydentävät tämän sopimuksen mukaisia vaatimuksia, jotka aset-  
tavat vähimmäistason Palvelun tietoturvallisuudelle.
- 7.3 Mikäli Tilaaaja on luokitellut tai myöhemmin pääsopimuksen aikana luokitte-  
lee Suojattavia tietoja tietoturvallisuusasetuksen (681/2010) mukaisiin  
suojaustasoihin, Toimittaja sitoutuu noudattamaan luokiteltuja tietoja käsi-  
tellessään edellä mainitun asetuksen kyseiselle suojaustasolle asettamia

vaatimuksia. Ellei Suojattavaa tietoa ole luokiteltu eikä Tilaaja ole muutoin ohjeistanut Toimittajaa Suojattavan tiedon käsittelystä, Suojattavaa tietoa käsitellään kuin se olisi luokiteltu suojaustasolle IV.

### **Henkilöstölle asetettavat vaatimukset**

- 7.4 Toimittaja vastaa siitä, että sillä on nimetty tietoturavastaava ja että sen henkilöstö tuntee työrooliin kuuluvat vastuunsa tietoturvallisuuden osalta.
- 7.5 Toimittaja vastaa siitä, että sen henkilöstö on saanut asianmukaisen tietoturvalisluuskoulutuksen ja että sen henkilöstö on ohjeistettu ilmoittamaan välittömästi havaitsemistaan tai epäilemistään turvallisuuipoikkeamista ja -uhista.

### **Tilaajan toimitilojen turvallisuu**

- 7.6 Toimittaja vastaa siitä, ettei Tilaajan toimitilojen tai toiminnan turvallisuu vaaranu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän sopimuksen tai Pääsopimuksen vastaisen toiminnan johdosta.
- 7.7 Ellei toisin sovita, pääsyoikeus Tilaajan korotetulle tai korkealle turvallisuuastalolle määriteltuihin toimitiloihin annetaan vain niille Toimittajan henkilöille, jotka
- a) Toimittaja on hyväksyttänyt Tilaajalla etukäteen,
  - b) joista on tehty henkilöturvallisuuaselvitys ja
  - c) jotka ovat tietoisia tämän sopimuksen velvoitteista ja tiloissa liikkumisesta annetuista ohjeista.
- 7.8 Ellei toisin sovita, pääsyoikeus Tilaajan perustason turvallisuuastalolle määriteltuihin toimitiloihin annetaan vain niille Toimittajan henkilöille, jotka
- a) Toimittaja on hyväksyttänyt Tilaajalla etukäteen ja
  - b) jotka ovat tietoisia tämän sopimuksen velvoitteista ja tiloissa liikkumisesta annetuista ohjeista.

Tilaajalla on oikeus edellyttää henkilöturvallisuuaselvityksen tekemistä myös Tilaajan perustason tiloihin pääsevien henkilöiden osalta, ottaen huomioon henkilöturvallisuuaselvitysten tekemiselle laissa asetetut edellytykset.

- 7.9 Ellei toisin ole sovittu, henkilöillä on oltava Tilaajan tiloissa liikkueissa näkyvillä tunniste, kuten Toimittajan tai Tilaajan myöntämä henkilö- tai vierailijakortti.

### **Toimittajan toimitilojen turvallisuu**

- 7.10 Ellei muuta ole sovittu, Toimittajan toimitilojen, joissa käsitellään Suojattavaa tietoa, tulee olla toimitiloissa käsiteltävän Suojattavan tiedon luokitus-tason asettamat vaatimukset huomioon ottaen asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi toimitiloihin ja siellä olevaan Suojattavaan tietoon. Ellei muuta ole

sovittu, Toimittajan toimitiloille asetettavia vaatimuksia ja niiden täyttymistä arvioidaan tämän sopimuksen voimaantulohetken mukaisen Vahti - Toimitilojen turvallisuusohje mukaisesti.

- 7.11 Ellei muuta ole sovittu, henkilöiden joilla on pääsy Toimittajan toimitiloihin, joissa käsitellään Suojattavaa tietoa, tulee olla kulunvalvonnan piirissä ja tunnistettavissa kulkuluvin tai henkilökohtaisesti tunnistamalla. Kulunvalvonta IT-laitetiloihin, joissa käsitellään Suojattavaa tietoa, on järjestettävä siten, ettei kukaan pääse saapumaan tai poistumaan tulematta rekisteröidyksi (sähköinen/kirjallinen loki tai vastaava)
- 7.12 Toimittajan tulee Tilaaajan pyynnöstä hyväksyttää Tilaaajalla kaikki henkilöt, joille on tarpeen myöntää pääsyoikeus yksinomaan Tilaaajan tarkoituksiin osoitettuun Toimittajan tila-tilassa käsitellään Suojattavaa tietoa. Tässä kohdassa tarkoitetuista henkilöistä on Tilaaajan niin vaatiessa teetettävä henkilöturvallisuusselvitys.

## 8

### TIETOJÄRJESTELMIEN HALLINNAN VAATIMUKSET

- 8.1 Toimittaja on Tilaaajan pyynnöstä velvollinen hyväksyttämään Tilaaajalla sellaiset henkilöt, jotka voivat tietojärjestelmän pääkäyttäjänä tai muut toimivaltuutensa huomioon ottaen vahingoittaa Suojattavaa tietoa sisältävän tietojärjestelmän toimivuutta tai tietoturvasuutta. Tilaaaja teettää tällaisista henkilöistä tarvittaessa henkilöturvallisuusselvityksen.
- 8.2 Toimittajan tulee huolehtia Palvelun osalta siitä, että:
- sen henkilöstön oikeudet ja valtuudet järjestelmissä, joissa käsitellään Suojattavaa tietoa, rajataan vain työtehtävien edellyttämään laajuuteen,
  - käyttö- ja pääsyoikeuksien hallinnassa noudatetaan "vähimpien oikeuksien" periaatetta,
  - käyttö- ja pääsyoikeuksien myöntämisen, muuttamisen ja poistamisen osalta noudatetaan prosessia, joka kattaa kaikki toimitilat, tietojärjestelmät ja palvelut, joissa käsitellään Suojattavaa tietoa.
  - mikäli käyttö- ja pääsyoikeuksia tarvitaan Tilaaajan tiloihin tai järjestelmiin, noudatetaan aina Tilaaajan hyväksymää prosessia,
  - käyttö- ja pääsyoikeuksia katselmoidaan säännöllisesti,
  - kaikki tietojärjestelmien käyttäjät (henkilöt ja muut järjestelmät) tunnistetaan yksilöllisesti ja käyttö valtuutetaan ennen kuin järjestelmien käyttö sallitaan (poikkeuksena julkiset tiedot ja järjestelmät),
  - käyttö- ja pääsyoikeudet ovat henkilökohtaisia,
  - myönnettyjä käyttö- ja pääsyoikeuksia ei jaeta, siirretä tai anneta toiselle,
  - myönnettyjä oikeuksia ei käytetä laajemmin kuin työtehtävien suorittaminen edellyttää,

- pääsynhallintajärjestelmien ohittaminen on estetty asianmukaisilla teknisillä järjestelyillä,
- pääsynvalvontatapahtumat tallennetaan lokiin ja niitä valvotaan poikkeamien varalta,
- Toimittajan edustajalla olevat Tilaajan avaimet, henkilökortit ja kulkuluvat palautetaan Tilaajalle sekä käyttäjätunnukset ja käyttöoikeudet poistetaan ilman viivytystä, kun työtarve poistuu,
- Sopimuksen päätyttyä Toimittaja palauttaa ilman viivytystä Tilaajalle tämän avaimet, henkilökortit, kulkuluvat, salausavaimet, lisenssit, kulkukoodit, käyttäjätunnukset, salasanat sekä muut tunnistautumisvälineet ja sulkee sopimuksen nojalla avatut tietoliikenne-, tietojärjestelmä-, tiedonsiirto- sekä etäkäyttöyhteydet.

## 9 OHJELMISTOTURVALLISUUS

9.1 Toimittaja vastaa Palvelun osalta siitä, että:

- sen toimittamiin tietojärjestelmäpalveluihin, ohjelmistokomponentteihin tai medioihin ei sisälly haittaohjelmia tai muuta tahallista haitallista toiminnallisuutta,
- se seuraa toimeksiantoon liittyviin ohjelmistoihin, kolmannen osapuolen komponentteihin ja sen osana oleviin valmisohjelmistoihin liittyviä tietoturvallisuustiedotteita, julkaistuja tietoturvapäivityksiä ja haavoittuvuuksia,
- se tiedottaa Tilaajaa viivytyksettä vastuullaan olevien toimeksiantoon liittyvien ohjelmistojen tietoturva haavoittuvuuksista sekä tietoturvapäivityksistä ja, mikäli haavoittuvuuteen ei ole vielä korjausta, ehdottaa muita haavoittuvuutta rajoittavia toimia,
- Tilaajan omistamia tai hallitsevia tietoja ei ilman Tilaajan erillistä kirjallista lupaa käytetä järjestelmäkehityksessä tai testauksessa.

## 10 JATKUVUUDEN VARMISTAMINEN

10.1 Tilaaja on määrittänyt ICT-varautumisvaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä X/tämän sopimuksen liitteessä X.]  vaatimukset täydentävät tämän sopimuksen mukaisia vaatimuksia, jotka asettavat vähimmäistason ICT-varautumiselle.

10.2 Palvelun jatkuvuuden varmistamiseksi Toimittaja vastaa siitä, että:

- sillä on asianmukaiset voimassaolevat suunnitelmat, järjestelyt ja vakuutukset  pimentansa jatkuvuuden varmistamiseksi ja keskeytyksiltä suojautumiseksi,
- jatkuvuuden varmistamisen toimenpiteet ja suunnitelmat ovat koulutettu, harjoiteltu ja otettu käyttöön palvelutuotannossa,
- Palvelun saatavuuden ja häiriöstä tai vikatilanteesta toipumisen (ml. varmuuskopioinnin) prosessit sekä niiden tekniset toteutukset ovat

suunniteltu siten, että palautumisvalmius vastaa sovittuja jatkuvuusvaatimuksia.

## 11 TURVALLISUUSSELVITYKSET

- 11.1 Ellei toisin ole sovittu, tämän sopimuksen tarkoittamalla turvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain (726/2014) mukaista yritysturvallisuusselvitystä ja henkilöturvallisuusselvitystä taikka niitä vastaavia, Suomen kansallisen turvallisuusviranomaisen (National Security Authority, NSA) kautta hankittua ja ulkomaan turvallisuusviranomaisen myöntämää yritysturvallisuustodistusta ja henkilöturvallisuustodistusta.

### Yritysturvallisuusselvitykset

- 11.2 Toimittaja antaa Tilaaajan niin edellyttäessä suostumuksensa siihen, että Toimittajasta voidaan hakea turvallisuusselvityslain mukainen yritysturvallisuusselvitys.
- 11.3 Ellei toisin sovita, ulkomaisella Toimittajalla, joka käsittelee Suojattavaa tietoa Suomen rajojen ulkopuolella, tulee olla yrityksen kotimaan turvallisuusviranomaisen myöntämä yritysturvallisuustodistus (Facility Security Clearance, FSC). Sikäli kuin Tilaaaja ei pidä turvallisuusselvityslain mukaista yritysturvallisuusselvitystä tarkoituksenmukaisena, Toimittaja toimittaa pyynnöstä ja vaikutusmahdollisuuksiensa puitteissa turvallisuusselvityslain 37 §:ssä säädetty tiedot Tilaajalle, jotta Tilaaaja voi suorittaa kohdan 11.6 mukaisen arvioinnin.
- 11.4 Suomessa tehtävien yritysturvallisuusselvitysten hakemisesta vastaa Tilaaaja. Toimittaja on yhteydessä Suomen NSA:han ulkomaisen alihankkijansa yritysturvallisuustodistusten hankkimiseksi. Tilaaaja on yhteydessä Suomen NSA:han ulkomaisen Toimittajan ja sen ulkomaisen alihankkijan yritysturvallisuustodistuksen hankkimiseksi.
- 11.5 Yritysturvallisuusselvityksen kustannusvastuusta on säädetty turvallisuusselvityslain (726/2014).
- 11.6 Tilaajalla on oikeus arvioida yritysturvallisuusselvityksen sisältö ja yrityksen tai sen vastuuhenkilöiden luotettavuus, yrityksen tietoturvallisuuden taso sekä kyky hoitaa Pääsopimuksen ja tämän sopimuksen mukaiset sitoumukset.

### Henkilöturvallisuusselvitykset

- 11.7 Tilaajalla on oikeus vaatia turvallisuusselvityslain tarkoitetu henkilöturvallisuusselvitys Toimittajan henkilöstä turvallisuusselvityslain mukaisessa laajuudessa. Toimittaja tiedostaa, että henkilöturvallisuusselvityksen kohteena voivat olla muutkin kuin Suojattavaa tietoa käsittelevät henkilöt. Toimittaja vastaa turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta.
- 11.8 Toimittajan tulee toimittaa henkilöturvallisuusselvityksen kohteena olevan henkilön täyttämä ja allekirjoittama henkilöturvallisuusselvityshakemuslomake Tilaajalle henkilöturvallisuusselvityksen teettämistä varten. Lomakkeen tulee sisältää selvityksen kohteena olevan henkilön suostumus henkilöturvallisuusselvityksen tekemiseen. Jos henkilöturvallisuusselvitys tulee

tehtäväksi sellaisessa valtiossa, jonka lainsäädännön mukaan kyseessä olevan selvityksen tekeminen ei edellytä selvityksen kohteena olevan henkilön suostumusta, Toimittajan ei myöskään tämän kohdan nojalla tarvitse pyytää henkilöltä edellä mainittua suostumusta.

- 11.9 Ellei toisin sovita, ulkomaisilla Suojattavan tiedon käsittelyyn osallistuvilla Toimittajan henkilöillä tulee olla henkilöturvallisuustodistus (Personal Security Clearance, PSC). Sikäli kuin Tilaaja ei pidä turvallisuusselvityslain mukaista henkilöturvallisuusselvitystä tarkoituksenmukaisena, Toimittaja toimittaa vaikutusmahdollisuuksiensa puitteissa sellaiset tiedot Tilaajalle, että Tilaaja voi suorittaa kohdan 11.11 mukaisen arvioinnin.
- 11.10 Tilaaja vastaa Suomessa tehtyjen henkilöturvallisuusselvitysten kustannuksista. Mikäli henkilöturvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan henkilöstössä tapahtuu vaihdos tai Tilaajasta riippumaton lisäys, Toimittaja vastaa uuden henkilön henkilöturvallisuusselvityksen teettämisen kustannuksista. Toimittaja vastaa ulkomaisten henkilöturvallisuustodistusten kustannuksista.
- 11.11 Tilaajalla on oikeus hyväksyä tai olla hyväksymättä Toimittajan ehdottamia henkilöitä tämän sopimuksen tuottamiseen. Osana henkilön hyväksymistä arvioidaan henkilöturvallisuusselvityksen sisältö ja Toimittajan on viivytyksettä ja veloituksetta vaihdettava henkilö, jota Tilaaja ei hyväksy kyseiseen tehtävään. Toimittaja vastaa uuden henkilön perehdyttämisen aiheuttamista kuluista. Korvaavan henkilön on oltava osaamiseltaan vähintään samantasoinen kuin korvattava henkilö.

## 12 TARKASTUKSET

- 12.1 Tilaajalla tai Tilaajan määräämällä kolmannella taholla (joka ei ole Toimittajan suoranainen kilpailija) on oikeus tarkastaa etukäteen ilmoitettuna ajankohtana Toimittajan turvallisuusjärjestelyt tätä sopimusta sekä Pääsopimusta koskevilta osin.
- 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 kolmantena (3) päivänä Tilaajan kirjallisesta ilmoituksesta, ilmoituspäivää laskematta.
- 12.3 Selvyyden vuoksi todetaan, että kohdan 12.1 mukainen tarkastus voidaan lain edellytysten täyttyessä suorittaa myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011, jälj. auditointilaki) mukaisena arviointina tai valtiovarainministeriön teettämänä selvityksenä. Tämän kohdan mukaisen tarkastuksen toteuttamisesta päättää yksinomaan Tilaaja, ellei kyse ole auditointilain 5 §:n tarkoittamasta valtiovarainministeriön teettämästä selvityksestä.
- 12.4 Sopijapuolet pyrkivät myötävaikuttamaan tarkastuksen suorittamiseen siten, ettei tarkastustoimenpiteistä aiheudu kohtuutonta haittaa Toimittajan palvelutuotannolle tai sovitulle palvelutasolle.
- 12.5 Ellei turvallisuusselvityslaista tai auditointilaista muuta johdu tai elleivät sopijapuolet ole toisin sopineet, Tilaaja vastaa kohtien 12.1 ja 12.2 mukaisen tarkastusten ja arviointien ja todistuksen antamisesta aiheutuvista

maksuista, kuten tarkastajan työkustannuksesta. Selvyiden vuoksi todetaan, että Toimittaja vastaa kaikista niistä kuluista ja kustannuksista, joita sille aiheutuu tarkastuksiin käytetystä työajasta, havaittujen puutteiden korjaamisesta ja kuluista, jotka aiheutuvat Palvelun saattamiseksi sovittujen vaatimusten mukaisiksi.

- 12.6 Tilaaajan on ilmoitettava tahdostaan suorittaa tarkastus. Toimittaja voi ehdottaa uutta päivää tarkastukselle. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainituista määräajoista riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tietoturvalisua tai Toimittajan salassapitovelvoitteita muita asiakkaita kohtaan.
- 12.7 Toimittajan tulee huolehtia sopimusjärjestelyin siitä, että Tilaaajalla on mahdollisuus tarkastaa Toimittajan alihankkijan turvallisuusjärjestelyt.
- 12.8 Jos tarkastuksessa havaitaan, ettei Toimittajan toiminta täytä sovittuja vaatimuksia, Toimittaja laatii viipymättä aikataulutetun suunnitelman tilanteen korjaamiseksi. Ellei sopijapuolten hyväksymästä suunnitelmasta muuta johdu, Toimittajan tulee korjata tarkastuksessa havaitut puutteet viivytyksestä Tilaaajan kirjallisesta ilmoituksesta. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvallisuudelle, on korjattava heti tai Tilaaajan asettamassa aikataulussa. Tilaaaja ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.
- 12.9 Mikäli tarkastuksessa havaitaan, ettei Toimittajan toiminta täytä sovittuja vaatimuksia ja Tilaaaja edellyttää virheen korjaamisen todentamiseksi uusintatarkastusta, Toimittaja korvaa Tilaaajalle uusintatarkastuksesta aiheutuneet kustannukset.
- 12.10 Tilaaajalla on oikeus luovuttaa muille viranomaisille tieto siitä, että tämän luvun mukainen tarkastus on suoritettu ja siitä, ovatko Toimittajan turvallisuusjärjestelyt todettu vaatimusten mukaisiksi. Tilaaajalla ei kuitenkaan ole ilman Toimittajan lupaa oikeutta luovuttaa tietoa tarkastuksen yksityiskohdista havainnoista, ellei pakottavasta lainsäädännöstä muuta johdu.

## **13 RAPORTOINTI**

- 13.1 Toimittaja on velvollinen ilmoittamaan Tilaaajalle, jos Toimittajan tämän sopimuksen kannalta keskeisissä toiminnoissa tai sopimukseen liittyvissä turvallisuusjärjestelyissä tapahtuu muutoksia.
- 13.2 Toimittaja valvoo tämän sopimuksen edellyttämän turvallisuustason toteutumista ja vaatimuksen mukaisuutta toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Tilaaajalle viivytyksestä sekä aloittaa korjaustoimet ensi tilassa.
- 13.3 Tilaaaja seuraa turvallisuuden kaikkiin osa-alueisiin liittyviä muutoksia ja ilmoittaa Toimittajalle muutostarpeista.
- 13.4 Toimittaja on viipymättä velvollinen ilmoittamaan Tilaaajalle, mikäli Toimittajaan kohdistuu Tilaaajaa mahdollisesti uhkaavia yhteydenottoja tai uhkailanteita.

## 14 SOPIMUSSAKKO JA VAHINGONKORVAUS

*(Ohje: Muokkaa sopimussakon määrä hankinnan kohteeseen ja siihen liittyviin riskeihin soveltuvaksi.)*

- 14.1 Tilaajalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän sopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa.
- 14.2 Sopimussakon määrä jokaista salassapitovelvoitteen rikkomusta kohden on suurin seuraavista: (i) 10.000 euroa tai (ii) 1,5 % Pääsopimuksen tai siihen liittyvän sopimuksen toimituksen arvosta taikka (iii) 1,5 % Pääsopimuksen tai siihen liittyvän sopimuksen toistuvaismaksujen laskennallisesta 12 kuukauden hinnasta. Muissa turvallisuussopimuksen rikkomustilanteissa sopimussakon määrä jokaista rikkomusta kohden on 10.000 euroa.
- 14.3 Tilaajalla ei ole oikeutta saada sopimussakkoa, jos Toimittaja korjaa turvallisuusvelvoitteen rikkomuksen tai laiminlyönnin 14 vuorokauden kuluessa siitä, kun se on havainnut rikkomuksen tai laiminlyönnin. Oikeus sopimussakkoon kuitenkin säilyy, jos rikkomus tai laiminlyönti on luonteeltaan sellainen, että siitä on aiheutunut Tilaajalle vahinkoa.
- 14.4 Jos Toimittaja samalla teolla rikkoo useita tämän sopimuksen velvoitteita, se katsotaan kuitenkin vain yhdeksi sopimussakkoon oikeuttavaksi rikkomukseksi.
- 14.5 Ennen sopimussakon perimistä Tilaajan tulee ilmoittaa Toimittajalle kirjallisesti tämän sopimuksen rikkomuksesta. Jos Toimittaja sitä kirjallisesti pyytää, käsitellään rikkomus lisäksi Tilaajan ja Toimittajan välisissä neuvotteiluissa.
- 14.6 Sopimussakko ei rajoita Tilaajan oikeutta saada Toimittajalta vahingonkorvausta siltä osin kuin rikkomuksesta Tilaajalle aiheutunut vahinko ylittää sopimussakon määrän.
- 14.7 Sopijapuolella on oikeus saada vahingonkorvausta toisen sopijapuolen sopimusrikkomuksesta aiheutuneesta välittömästä vahingosta.
- 14.8 Jos sopijapuolella on velvollisuus suorittaa viivästys-, palvelutaso- tai muuta sopimussakkoa tai hyvitystä, on sopijapuolella velvollisuus suorittaa lisäksi vahingonkorvausta siltä osin kuin vahingon määrä ylittää viivästys-, palvelutaso- tai muut sopimussakot tai hyvitykset.
- 14.9 [OHJE: Tämä kohta voi soveltua vain jos Tilaaja on Palvelukeskus: Välittömiksi vahingoiksi katsotaan myös sellaiset Tilaajaosapuolena olevan julkisen hallinnon palvelukeskuksen tai sen asiakkaan välittömät vahingot, jotka aiheutuvat Toimittajan sopimusrikkomuksesta Toimittajan tuottaessa Palvelua julkisen hallinnon palvelukeskuksen välityksellä Tilaajan asiakasorganisaatioille.]
- 14.10 Tähän sopimukseen perustuva sopijapuolen vahingonkorvausvelvollisuus toiselle sopijapuolelle on mahdolliset viivästys-, palvelutaso- tai muut sopimussakot tai hyvitykset pois lukien yhteensä enintään Pääsopimuksen mukaisen toimituksen kokonaishintaa pääsopimuksen mukaisen toimituksen kokonaishintana pidetään sitä yhteenlaskettua arvonlisäverotonta hin-

taa, joka muodostuu Pääsopimuksen mukaisista tuotteiden ja Palveluiden toimituksista, lisätöistä ja jatkuvista palveluista laskettuna 12 kuukaudelle, ellei Pääsopimuksen sopimuskausi ole sitä lyhempi.

- 14.11 Sopijapuoli ei vastaa toisen sopijapuolen tietojen tai tiedostojen tuhoutumisesta, katoamisesta tai muuttumisesta ja tästä aiheutuneista kuluista, kuten tietojen ja tiedostojen uudelleen luomisen aiheuttamista kustannuksista. Tätä kohtaa ei kuitenkaan sovelleta, jos sopijapuolen velvollisuutena on Pääsopimuksen mukaan toisen sopijapuolen tietojen ja tiedostojen käytettävyydestä ja saatavuudesta huolehtiminen, ja sopijapuoli on rikkonut tätä velvollisuuttaan.
- 14.12 Tilaaaja ei vastaa vahingosta, joka Toimittajalle on aiheutunut tämän sopimuksen mukaisen tarkastustoimenpiteen suorittamisesta.
- 14.13 Sopijapuoli ei vastaa välillisestä vahingosta.
- 14.14 Näiden ehtojen mukaiset vahingonkorvausvelvollisuuden rajoitukset eivät koske tapausta, jossa sopijapuoli on aiheuttanut vahingon tahallisesti tai törkeällä huolimattomuudella tai rikkonut salassapitovelvollisuuden.

## 15 SOPIMUSMUUTOKSET

- 15.1 Turvallisuussopimuksen yhteyshenkilöt vastaavat tämän sopimuksen päivittämistarpeen seuraamisesta.
- 15.2 Tähän sopimukseen tai sen liitteisiin tehtävät muutokset tulee tehdä kirjallisesti ja molempien sopijapuolten vahvistaa allekirjoituksellaan. Tämän sopimuksen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

## 16 SOPIMUKSEN IRTISANOMINEN

- 16.1 Sopijapuoli voi irtisanoa tämän sopimuksen päättymään noudattaen Pääsopimuksessa sovittua irtisanomisaikaa. Sopijapuolella ei kuitenkaan ole oikeutta irtisanoa tätä sopimusta päättymään ennen Pääsopimuksen määräaikaisen sopimuskauden päättymistä.
- 16.2 Jos Toimittaja irtisanoa tämän sopimuksen, Tilaajalla on oikeus irtisanoa Pääsopimus.
- 16.3 Tilaaaja on oikeutettu irtisanomaan välittömästi päättymään tämän sopimuksen ja Pääsopimuksen, mikäli Toimittaja rikkoo tähän sopimukseen perustuvia sopimusvelvoitteitaan niin olennaisesti, ettei Tilaaajan voida kohtuudella edellyttää jatkavan sopimussuhdetta edes irtisanomisajan pituista aikaa. Lisäksi jos Toimittaja on rikkonut tätä sopimusta vähintään kolme kertaa siten, että Tilaajalle on syntynyt oikeus vaatia luvussa 14 tarkoitettua sopimussakkoa, Tilaajalla on aina oikeus irtisanoa välittömästi päättymään tämä sopimus ja Pääsopimus.
- 16.4 Tilaaaja on oikeutettu irtisanomaan välittömästi päättymään tämän sopimuksen ja Pääsopimuksen, mikäli Tilaajalla on tehdyn turvallisuusselvityksen tai muun tiedon perusteella perustellusti aiheutta epäily Toimittajan taikka sen johtohenkilön tai edustus-, päätös- tai valvontavaltaa käyttävien henkilöiden toimivan tavalla, 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.

- 16.5 Irtisanominen tulee tehdä kirjallisesti.
- 16.6 Irtisanominen ei poista velvollisuutta täyttää ennen irtisanomista syntyneitä tämän sopimuksen mukaisia velvoitteita.
- 16.7 Tämän sopimuksen päättymisestä huolimatta Toimittajan on maksettava päättymisen perusteena olevista rikkomuksista tämän sopimuksen mukaiset sanktiot.

## 17 SOPIMUKSEN VOIMASSAOLO

- 17.1 Tämä sopimus on voimassa niin kauan kuin Tilaaajan ja Toimittajan välinen Pääsopimus on voimassa.
- 17.2 Tämä sopimus tulee voimaan, kun kumpikin sopijapuoli on sen allekirjoittanut.
- 17.3 Tämän sopimuksen mukainen salassapitovelvollisuus on voimassa myös sen jälkeen kuin Tilaaajan ja Toimittajan välinen Pääsopimus on päättynyt.
- 17.4 Ellei Pääsopimuksessa ole toisin sovittu, Toimittaja palauttaa tämän sopimuksen päättyttyä 30 päivän kuluessa kaikki Tilaaajan Suojattavia tietoja sisältävät dokumentit, tallenteet ja muun materiaalin. Erikseen kirjallisesti niin sovittaessa Toimittaja voi myös tuhota edellä mainitun materiaalin. Tilaaajalla on oikeus tarkastaa tämän kohdan velvoitteiden noudattaminen luvun 12 mukaisesti myös sopimuksen päättyttyä.

## 18 SOVELLETTAVA LAKI JA ERIMIELISYYKSIEN RATKAISEMINEN

- 18.1 Tähän sopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintäsäännöksiä.
- 18.2 Tästä sopimuksesta aiheutuvat erimielisyydet pyritään ensisijaisesti ratkaista sopijapuolten välisin neuvotteluihin. Mikäli sopijapuolet eivät pääse sovinnolliseen ratkaisuun, erimielisyydet ratkotaan ensi asteessa Tilaaajan kotipaikan käräjäoikeudessa, ellei Pääsopimuksessa ole sovittu toisesta oikeuspaikasta. 

## 19 SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS

- 19.1 Tämä sopimus muodostuu tästä sopimusasiakirjasta ja seuraavista liitteistä:

|          |                                                                   |
|----------|-------------------------------------------------------------------|
| Liite 1  | Ohje Salassa pidettävien tietojen käsittelystä ja säilyttämisestä |
| [Liite 2 | Tietoturvallisuusvaatimukset (ja ICT-varautumisen vaatimukset)]   |

Liite 3 Salassapitositoumusmalli

Liite 4 [Toimittajan turvallisuudenhallinnan kuvaus [/Selvitys Palveluun liittyvistä tietoturvamenettelyistä]

Ohje: Liitteessä [1] kuvataan Tilaaajan hyväksymät menettelyt, määräykset ja ohjeet eri suojaustasoluokkiin kuuluvan tiedon, asiakirjojen ja muun tietoineiston käsittelystä. Liitteessä [2] esitetään Palveluun kohdistuvat tietoturva-, toimitila-, IT-laitetila-, ICT-varautumisvaatimukset yms. Nämä vaatimukset voivat olla myös Pääsopimuksen liitteenä.

Toimittaja vastaa liitteen [4] ylläpidosta. Liitteen tulee vastata voimassa olevaa tilannetta.

## 20 SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET

20.1 Tämä sopimus on laadittu kahtena (2) samasanaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]

[paikka ja aika]

[TILAAJA]

[TOIMITTAJA]

\_\_\_\_\_  
[allekirjoittaja]

\_\_\_\_\_  
[allekirjoittaja]