Yleinen tietoturvallisuusliite

1 Tämän dokumentin tarkoitus ja soveltaminen

#1 Tämä dokumentti on palvelusetelijärjestelmän sääntökirjan liite, jolla määritellään palvelusetelijärjestelmän kohteen tietosuojaan, tietoturvallisuuteen, HUSin (jäljempänä tilaajan) aineiston käsittelyyn ja salassapitoon liittyvistä seikoista. Tätä dokumenttia sovelletaan sääntökirjassa mainitun soveltamisjärjestyksen mukaisesti, huomioiden kuitenkin mitä jäljempänä mainitaan mahdollisten sääntökirjan vastuunrajoitusten soveltamisesta. Tilaajan aineistoa koskevia ehtoja sovelletaan sääntökirjan mukaisen palvelusetelijärjestelyn päättymisestä huolimatta niin kauan kuin toimittajalla on hallussaan tilaajan aineistoa.

Tietoturvallisuusliitteen viittaukset sopimukseen/pääsopimukseen tarkoittavat viittausta sääntökirjaan.

2 Määritelmät

#2 *Luottamukselliset tiedot:* Sopijapuolta sekä sen toimintayksiköitä, sopimuskumppaneita tai muita yhteistyötahoja koskevat liike- ja ammattisalaisuudet, tiedot turvallisuus- ja valmiusjärjestelyistä sekä muut julkisuuslain (621/1999) mukaan salassa pidettävät tai muuten luottamuksellisiksi ja salassa pidettäviksi ymmärrettävät tiedot sekä henkilötiedot.

#3 *Henkilötiedot:* Määritelty tietosuoja-asetuksen 4 artiklassa.

#4 *Henkilötietojen käsittely:* Määritelty tietosuoja-asetuksen 4 artiklassa. Henkilötietojen käsittelynä pidetään esimerkiksi sitä, jos toimittajalla on mahdollisuus päästä näkemään henkilötietoja sopimuksen kohteen toteuttamisen yhteydessä.

#5 *Tietosuoja-asetus:* Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

#6 *Tilaajan aineisto:* Tuotteen toimituksen tai palvelun yhteydessä käytettävät tai niihin sisältyvät tilaajan asiakirjat, kirjalliset tiedot, tietokannat ja ohjelmistot, sekä muu aineisto, jonka tilaaja on luovuttanut toimittajalle tuotteen tai palvelun tuottamista varten, sekä lisäksi palvelua tai tuotetta käytettäessä syntynyt tilaajan tietoaineisto, tämän muotoilu, rakenne ja metatieto. Tietoaineiston rakenteella ei tarkoiteta tietosisällön tallennusteknistä rakennetta, vaan sen käsitteellistä muotoilua ja jäsennystä tilaajan tarkoitusta varten. Tietoaineisto voi olla tallennusteknisesti tiedostoissa, tietokannoissa tai muissa tallennusmuodoissa. Tässä määritelmässä tietosisällöllä ja tiedolla tarkoitetaan sekä raakatietoa että jalostettua tietoa.

#7 *Sopijapuolet:* HUS-kuntayhtymä/tilaaja ja palveluseteli palveluntuottaja

3 Alihankkijat

#8 Tässä liitteessä toimittajalle ja toimittajan palveluksessa oleville henkilöille asetetut velvoitteet koskevat myös toimittajan alihankkijoita ja niiden palveluksessa olevia henkilöitä siltä osin kuin ne osallistuvat sopimuksen kohteen toteuttamiseen.

Toimittajan on tiedotettava alihankkijoille näistä velvoitteista, ja toimittaja vastaa siitä, että alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat niitä. Toimittaja vastaa käyttämänsä alihankkijan osuudesta kuten omastaan.

4 Yleiset velvollisuudet

4.1 Sopijapuolten velvollisuus noudattaa lainsäädäntöä

#9 Sopijapuolet sitoutuvat noudattamaan tietoturvallisuudesta, tietosuojasta, julkisuudesta ja salassapidosta annettua lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomaismääräyksiä. Sopimuksella ei poiketa lainsäädännön sopijapuolelle asettamista pakottavista velvoitteista.

4.2 Myötävaikutusvelvollisuus

#10 Sopijapuolet pyrkivät kaikin käytettävissään olevin kohtuullisin keinoin myötävaikuttamaan sopimuksen kohteen toteuttamisessa korkeaan tietoturvallisuuden tasoon ja toisen sopijapuolen mahdollisuuteen omalta osaltaan ylläpitää sitä.

4.3 Huolellisuusvelvollisuus

#11 Sopijapuolet vastaavat siitä, että sopimuksen mukaiset tehtävät tehdään huolellisesti ja ettei tilaajan aineiston tai luottamuksellisten tietojen luottamuksellisuus, saatavuus tai eheys vaarannu sopijapuolten henkilöstön huolimattomuuden, virheellisten työtapojen tai muun sopimuksen vastaisen toiminnan johdosta.

4.4 Tietoturvallisuuteen liittyvät tehtävät ja vastuut

#12 Toimittajan tulee määritellä organisaatiossaan tietoturvallisuuteen liittyvät tehtävät ja vastuut sekä nimetä kokemukseltaan ja pätevyydeltään riittävät vastuuhenkilöt ja ilmoittaa heidän yhteystietonsa toiselle sopijapuolelle.

4.5 Sopijapuolten tietoturvallisuuteen liittyvät sisäiset ohjeet

#13 Sopijapuolilla voi olla erillisiä tietoturvallisuuteen liittyviä sisäisiä ohjeita. Sopijapuolten tulee noudattaa niitä siltä osin kuin ne eivät ole ristiriidassa sopimuksen kanssa. Sopijapuolet pyrkivät mahdollisuuksien mukaan huomioimaan toistensa tietoturvallisuuteen liittyvät sisäiset ohjeet.

5 Tilaajan aineisto

5.1 Käsitteleminen

#14 Toimittaja noudattaa tilaajan aineistoa käsitellessään julkisuuslaissa (621/1999) tarkoitettua hyvää tiedonhallintatapaa, tietosuojalainsäädännön edellyttämää hyvää tietojen käsittelytapaa, muuta tietojen suojaamista ja tietosuojaa koskevaa lainsäädäntöä sekä tilaajan antamia kohtuullisia ohjeita. Jos toimittaja laatii tai käsittelee sopimuksen perusteella potilasasiakirjoja, toimittaja sitoutuu laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjojen laatimisesta on erikseen säädetty ja tilaaja rekisterinpitäjänä ohjeistaa. Myös muun muassa toimittajan laatimat potilasasiakirjat ovat tilaajan aineistoa.

5.2 Käyttötarkoitus

#15 Toimittaja saa käyttää tilaajan aineistoa vain sopimuksen kohteen toteuttamiseen ja vain sopimuksen kohteen toteuttamisen edellyttämässä laajuudessa. Toimittajan tulee huolehtia siitä, että tilaajan aineistoa käsittelevät vain ne toimittajan lukuun työskentelevät henkilöt, joiden työtehtäviin tilaajan aineiston käsittely kuuluu.

5.3 Tietoturvallisuustasot

#16 Tilaajalla on oikeus määritellä tilaajan aineistolle eri tietoturvallisuustasoja ja sen mukaisia erityisiä tietoturvatoimenpiteitä ja ohjeita. Toimittaja käsittelee tilaajan aineistoa sen tietoturvallisuustason edellyttämällä tavalla. Jos tietoturvallisuustasojen muutokset aiheuttavat olennaisesti lisätyötä toimittajalle, sopijapuolet käsittelevät asian muutoshallintamenettelyn mukaisesti.

5.4 Tietopyynnöt

#17 Toimittajan tulee ohjata kolmansien osapuolten tekemät tilaajan aineistoa koskevat tietopyynnöt viipymättä tilaajalle.

5.5 Tilaajan aineiston palauttaminen

#18 Sopimuksen tai käyttötarpeen päättyessä toimittaja palauttaa ajan tasalla olevan tilaajan aineiston tilaajalle 14 päivän kuluessa tilaajan kirjallisesta pyynnöstä tietoaineiston avoimuusvaatimuksen mukaisesti. Tietoaineiston avoimuusvaatimuksella tarkoitetaan sitä, että tilaajan tietoaineisto on saatavissa yleisesti käytetyssä muodossa ja käsiteltävissä yleisesti käytössä olevilla tietojärjestelmillä ilman rojalteja ja lisenssimaksuja tai muita käsittelyä rajoittavia ehtoja. Toimittajalla ei ole oikeutta erillisveloitukseen tilaajan aineiston toimittamisesta tämän alaluvun 5.5 mukaisesti.

5.6 Tilaajan aineiston hävittäminen

#19 Toimittajalla on velvollisuus omalla kustannuksellaan tietoturvallisella tavalla hävittää mahdolliset jäljennökset tilaajan aineistosta sen jälkeen, kun tilaaja on kirjallisesti hyväksynyt tilaajan aineiston sopimuksen mukaisesti palautetuksi. Toimittaja tulee tilaajan pyynnöstä ilman erillisveloitusta esittää hävittämisestä kohtuullinen selvitys. Toimittajalla ei ole velvollisuutta hävittää aineistoa, jos toimittaja on velvollinen lain tai viranomaismääräyksen perusteella säilyttämään aineiston.

6 Henkilötietojen käsittely

#20 Tätä lukua 6 sovelletaan, jos toimittaja käsittelee sopimuksen perusteella henkilötietoja. Henkilötietojen käsittelyyn sovelletaan myös muun muassa tilaajan aineistoa koskeva ehtoja.

6.1 Toimittajan oikeus käsitellä henkilötietoja

#21 Tilaaja on tietosuojalainsäädännön mukainen rekisterinpitäjä ja toimittaja henkilötietojen käsittelijä.

#22 Toimittajalla on oikeus käsitellä tilaajan aineistoon sisältyviä henkilötietoja

- vain sopimuksessa mainitulla perusteella tai tilaajan kirjallisesti etukäteen antamalla luvalla
- vain siinä määrin ja niin kauan, kuin se on sopimuksen kohteen toteuttamiseksi välttämätöntä
- vain tämän sopimuksen sekä tilaajan erikseen antamien dokumentoitujen ohjeiden mukaisesti.

#23 Seuraavat seikat ilmenevät tarkemmin pääsopimuksesta, muista sopimuksen liitteistä tai muusta sopimukseen liittyvästä dokumentaatiosta:

- henkilötietojen käsittelyn kohde ja kesto
- henkilötietojen käsittelyn luonne ja tarkoitus
- henkilötietojen tyyppi
- rekisteröityjen ryhmät
- rekisterinpitäjän velvollisuudet ja oikeudet (siltä osin kuin niitä ei ole mainittu tässä liitteessä).

#24 Jos sopijapuoli katsoo, etteivät edellä mainitut tai muut tietosuojalainsäädännön edellyttämät seikat ilmene mainituista asiakirjoista riittävän täsmällisesti, sopijapuolella on oikeus edellyttää, että kyseiset seikat kirjataan osaksi sopimusasiakirjoja tai dokumentaatiota.

6.2 Tietosuojalainsäädännön noudattaminen

#25 Toimittaja sitoutuu noudattamaan henkilötietojen käsittelyssä voimassa olevaa tietosuojalainlainsäädäntöä ja sen perusteella annettuja viranomaismääräyksiä. Toimittaja vakuuttaa tuntevansa esimerkiksi tietosuoja-asetuksen sisällön, mukaan

lukien muun muassa 28 ja 32 artiklassa henkilötietojen käsittelijälle asetetut velvollisuudet. Toimittajan tietosuojalainsäädännön vastaista menettelyä voidaan pitää olennaisena sopimusrikkomuksena.

#26 Toimittajan on viipymättä ilmoitettava tilaajalle, jos toimittaja epäilee, että sopimus tai sopimuksen kohteen toteuttamisessa käytettävä ohjeistus tai käytäntö rikkoo tietosuojalainsäädäntöä.

6.3 Toimet tietosuojalainsäädännön vaatimusten noudattamisen turvaamiseksi

#27 Toimittajan tulee arvioida henkilötietojen käsittelyyn rekisteröityjen kannalta liittyvät riskit sekä toteuttaa riittävät tekniset ja organisatoriset toimet sen varmistamiseksi, että henkilötietojen käsittely täyttää tietosuojalainsäädännön vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Teknisistä ja organisatorisista toimista tulee laatia kirjallinen dokumentaatio, joka on pidettävä ajan tasalla. Toimittaja huolehtii esimerkiksi käsittelemiensä henkilötietojen asianmukaisesta suojaamisesta varmistaakseen niiden luottamuksellisuuden, eheyden ja saatavuuden sekä noudattaa sopimuksen kohteen toteuttamisessa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta.

#28 Toimittajan on nimettävä tietosuoja-asetuksen 37 artiklan mukaisesti tietosuojavastaava ja ilmoitettava hänen yhteystietonsa joko julkisilla verkkosivuillaan tai suoraan tilaajalle.

6.4 Muiden henkilötietojen käsittelijöiden käyttäminen

#29 Toimittaja ei saa käyttää muiden henkilötietojen käsittelijöiden palveluksia ilman tilaajan etukäteen kirjallisesti antamaa lupaa. Toimittajan on ilmoitettava etukäteen kirjallisesti tilaajalle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, jolloin tilaaja voi perustellusta syystä kieltää muutoksen. Toimittaja vastaa siitä, että toimittajan ja muun henkilötietojen käsittelijän välillä on tehty asianmukainen sopimus, joka täyttää tietosuojalainsäädännön velvoitteet.

6.5 Toimittajan avustamis- ja tiedonantovelvollisuus

#30 Toimittajan tulee avustaa tilaajaa täyttämään velvollisuuden vastata pyyntöihin, jotka koskevat tietosuojalainsäädännön mukaisten rekisteröidyn oikeuksien käyttämistä, sekä varmistamaan, että tietosuoja-asetuksen 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan. Toimittajan tulee esimerkiksi avustaa tilaajaa tietosuoja-asetuksen 33 ja 34 artiklan edellyttämien ilmoitusten tekemisessä tietosuoja-asetuksen mukaisessa määräajassa valvontaviranomaiselle ja rekisteröidylle. Toimittajan tulee myös pyynnöstä tehdä tietosuoja-asetuksen 31 artiklan mukaista yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

#31 Toimittajan tulee antaa tilaajalle kaikki tiedot, jotka ovat tarpeen tietosuojalainsäädännössä asetettujen velvoitteiden noudattamisen osoittamista

varten. Toimittajan tulee jatkuvasti ylläpitää mainittuja tietoja ja arvioida toimenpiteiden riittävyyttä.

#32 Toimittajan tulee oma-aloitteisesti ilmoittaa tilaajalle henkilötietojen käsittelypaikat ja niiden muutokset, elleivät ne selvästi ilmene sopimuksesta tai tilaajan käytettävissä olevasta dokumentaatiosta.

#33 Toimittaja toteuttaa tämän alaluvun 6.5 mukaisen avustamis- ja tiedonantovelvollisuuden ilman erillistä korvausta.

6.6 Henkilötietojen käsittely ulkomailla

#34 Jos pääsopimuksessa tai soveltamisjärjestyksessä tämän liitteen yläpuolella olevissa liitteissä ei ole nimenomaisesti toisin todettu, toimittaja ei saa käsitellä tilaajan aineiston sisältämiä henkilötietoja ETA-alueen ulkopuolella.

#35 Jos toimittaja pääsopimuksen tai soveltamisjärjestyksessä tämän liitteen yläpuolella olevan liitteen mukaan saa käsitellä tilaajan aineiston sisältämiä henkilötietoja ETA-alueen ulkopuolella, toimittajan tulee kirjallisesti ilmoittaa tällaisen henkilötietojen käsittelyn aloittamisesta tilaajalle viimeistään 30 päivää ennen suunniteltua aloitusajankohtaa.

#36 Jos toimittaja käsittelee henkilötietoja Yhdysvalloissa tai muissa kuin EU-komission listaamissa luotettavissa maissa, toimittaja sitoutuu siihen, että se solmii ennen henkilötietojen käsittelyn aloittamista tilaajan kanssa erillisen EU-mallilausekkeiden mukaisen sopimuksen henkilötietojen käsittelystä. Jos EU-mallilausekkeiden mukaista sopimusta ei myöhemmin pidettäisi riittävänä osoituksena tietosuojaa koskevan lainsäädännön velvoitteiden täyttämisestä, toimittaja sitoutuu yhdessä tilaajan kanssa viipymättä saattamaan henkilötietojen käsittelyn lainmukaiseksi.

#37 Toimittaja sitoutuu siirtämään henkilötietojen käsittelyn ETA-alueelle tai luotettavaan maahan ilman aiheetonta viivytystä, jos käsittelymaa poistetaan luotettavien maiden listalta. Siirrosta ei saa aiheutua tilaajalle ylimääräisiä kustannuksia.

#38 Toimittaja takaa saman tietoturvan ja tietosuojan tason riippumatta henkilötietojen käsittelymaasta.

6.7 Vahingonkorvaus

#39 Jos toimittaja on toiminut tietosuoja-asetuksen tai muun tietosuojalainsäädännön tai sopimuksen vastaisesti ja tästä on aiheutunut tilaajalle välitöntä vahinkoa, on toimittaja velvollinen korvaamaan kyseisen vahingon täysimääräisesti. Tilaajalle aiheutuneena välittömänä vahinkona pidetään muun muassa sellaista korvausta ja oikeudenkäyntikuluja korkoineen, jonka tilaaja on joutunut maksamaan rekisteröidylle toimittajan tietosuoja-asetuksen tai muun tietosuojalainsäädännön tai sopimuksen vastaisen toiminnan seurauksena, sekä asiaan liittyviä tilaajan omia kohtuullisia selvittely-, asianajo- ja oikeudenkäyntikuluja korkoineen. Tilaajalle aiheutuneena välittömänä vahinkoja pidetään myös esimerkiksi niiden toimenpiteiden kustannuksia, jotka tilaaja on joutunut tekemään tai teettämään toimittajasta johtuvan henkilötietojen tietoturvaloukkauksen vuoksi. Pääsopimuksessa tai muissa sopimusasiakirjoissa mahdollisesti olevia

vastuunrajoitusehtoja ei sovelleta tämän kohdan perusteella maksettavaan korvaukseen.

#40 Jos tilaajalle määrätään tietosuoja-asetuksen 83 artiklassa tarkoitettu hallinnollinen sakko ja sakon voidaan katsoa aiheutuneen kokonaan tai osittain toimittajan tai sen alihankkijan tai niiden palveluksessa olevan henkilön menettelystä tai laiminlyönnistä, on toimittaja velvollinen korvaamaan tilaajalle hallinnollisen sakon euromäärän siltä osin kuin se on katsottavissa edellä mainitusta menettelystä tai laiminlyönnistä johtuvaksi. Pääsopimuksessa tai muissa sopimusasiakirjoissa mahdollisesti olevia vastuunrajoitusehtoja ei sovelleta tämän kohdan perusteella maksettavaan korvaukseen.

7 Toimittajan ilmoitus- ja raportointivelvollisuudet

7.1 Ilmoitusvelvollisuus

#41 Toimittajan on ilman aiheetonta viivytystä ilmoitettava tilaajalle sellaisista toimittajan tietoon tulleista seikoista, jotka voivat vaikuttaa sopimuksen kohteeseen liittyvään tietoturvallisuuteen, ja niiden aiheuttamista toimenpiteistä ja mahdollisista seurauksista. Velvollisuus koskee muun ohella tietoturvariskejä, muutoksia turvajärjestelyissä, toteutuneita tietoturvaloukkauksia tai niiden yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia, palvelunestohyökkäyksiä sekä muita vastaavia poikkeamia, jotka ovat omiaan nostamaan riskiä tilaajan aineiston luottamuksellisuudelle, eheydelle ja saatavuudelle. Toimittajan tulee ilmoittaa tilaajalle vastuuhenkilö, jolta asiassa saa lisätietoja. Jos seikka liityy henkilötietoihin, toimittajan on ilmoitettava asiaan liittyvien rekisteröityjen ryhmät ja arvioidut lukumäärät.

#42 Toimittajan tulee ilmoittaa tilaajalle tietoturvaan liittyvässä dokumentaatiossa tapahtuneet muutokset ja toimittaa viipymättä tilaajalle ajan tasalla oleva dokumentaatio.

7.2 Määräajoin suoritettava raportointi

#43 Toimittaja seuraa sopimuksen mukaisen tietoturvallisuustason toteutumista säännöllisesti ja suunnitelmallisesti. Toimittaja kirjaa mahdolliset poikkeamat ja raportoi ne tilaajalle viipymättä sekä aloittaa korjaustoimet ensi tilassa.

8 Tietoturvaloukkaustilanteessa toimiminen

#44 Toimittajalla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen.

#45 Toimittaja huolehtii häiriötilanteiden hallinnasta sopimuksen mukaisesti siten, että ongelman rajaus ja korjaus suoritetaan viipymättä yhteisesti sovittujen menettelytapojen mukaisesti.

#46 Toimittaja on velvollinen auttamaan tilaajaa tietoturvaloukkauksiin liittyvien vahinkojen minimoinnissa sekä asian selvittämisessä viranomaistahojen kanssa.

#47 Toimittaja saa veloittaa tietoturvaloukkauksen sille aiheuttamasta lisätyöstä sopimuksen mukaisen hinnan, jos kaikki seuraavat edellytykset toteutuvat:

- tietoturvaloukkaus ei aiheudu toimittajan vastuulla olevasta syystä
- toimittajan virhe tai laiminlyönti ei ole myötävaikuttanut tietoturvaloukkauksen tapahtumiseen
- toimittajan toimenpiteet eivät sisälly mahdolliseen jatkuvan palvelun veloitukseen.

9 Toimittajan henkilöstö

9.1 Henkilöstön salassapitovelvollisuus

#48 Toimittaja vastaa siitä, että toimittajan lukuun työskentelevät henkilöt, joilla voi olla pääsy luottamuksellisiin tietoihin, ovat etukäteen allekirjoittaneet kirjallisen salassapitositoumuksen. Toimittajan on tilaajan pyynnöstä esitettävä kyseinen salassapitositoumus tilaajalle.

#49 Toimittajan on huolehdittava siitä, että toimittajan lukuun työskentelevät henkilöt ovat tietoisia seuraavista seikoista ja ovat sitoutuneet niitä noudattamaan:

- Työntekijä saa käyttää tilaajan aineistoa vain työtehtäviensä mukaiseen tarkoitukseen ja vain siinä laajuudessa kuin työtehtävien hoitaminen edellyttää. Työntekijällä ei ole oikeutta käyttää tilaajan aineistoa muuhun kuin edellä mainittuun tarkoitukseen.
- Työntekijän on pidettävä tilaajan aineisto salassa, eikä sitä saa luovuttaa tai muulla tavalla paljastaa sivullisille. Salassapitovelvollisuus on voimassa pysyvästi. Salassapitovelvollisuus ei koske julkista aineistoa.
- Sivullisina pidetään muun muassa sellaisia toimittajan lukuun työskenteleviä henkilöitä, jotka eivät työtehtäviensä perusteella tarvitse tilaajan aineistoa tietoonsa.
- Työntekijän on ilmoitettava tietoonsa tulleista tietoturvaa tai tietosuojaa vaarantavista seikoista tilaajalle tai toimittajalle viipymättä.
- Työntekijän tulee käsitellä tilaajan aineistoa sisältäviä asiakirjoja ja tallenteita huolellisesti ja riittävästä tietoturvasta huolehtien. Tilaajan aineistoa sisältäviä asiakirjoja ei saa viedä pois tilaajan tai toimittajan toimitiloista, elleivät työntekijän työtehtävät sitä nimenomaisesti edellytä.
- Työntekijän pitää palauttaa tai hävittää hallussaan olevat asiakirjat ja tallenteet luotettavasti ja riittävästä tietoturvasta huolehtien työtehtäviensä mukaisen käyttötarpeen päätyttyä.
- Tietojärjestelmien käytöstä kertyy lokitietoa, jota tarpeen mukaan seurataan.
- Salassapitovelvollisuuden rikkominen saattaa aiheuttaa työntekijälle lainsäädännön mukaisen henkilökohtaisen vastuun.

#50 Toimittajan tulee lisäksi huolehtia siitä, että toimittajan lukuun työskentelevät henkilöt ovat tietoinen myös muista mahdollisista sopimuksen mukaisista salassapitovelvoitteista, ja valvoa heidän toimintansa sopimuksenmukaisuutta.

9.2 Turvallisuusselvitys

#51 Tilaajalla on oikeus edellyttää turvallisuusselvityslain (726/2014) mukaisen turvallisuusselvityksen tai tasoltaan vastaavan ulkomaisen turvallisuusselvityksen teettämistä toimittajan lukuun työskentelevistä henkilöistä, joilla saattaa olla pääsy tilaajan luottamuksellisiin tietoihin. Toimittaja vastaa turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta ja siitä, että henkilö antaa turvallisuusselvityksen teettämiseksi tarvittavat tiedot. Jos turvallisuusselvityksen kohteena oleva henkilö kieltäytyy selvityksestä, toimittajan tulee tarjota tilalle toinen henkilö, jolla on vastaava kokemus ja pätevyys.

#52 Sopijapuoli vastaa itse kustannuksista, joita turvallisuusselvityksen teettämisestä sille aiheutuu. Tilaaja maksaa turvallisuusselvityksen teettämiseen liittyvät viranomaismaksut. Jos turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että toimittajan henkilöstössä tapahtuu tilaajasta riippumaton muutos, toimittaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.

10 Toimitilat ja tietojärjestelmien käyttö

10.1 Toimittajan sisäinen tietoturva

#53 Toimittaja varmistaa omien sopimuksen kohteen toimittamiseen käyttämiensä tietojärjestelmien, laitteiden ja tietoliikennejärjestelmien tietoturvan. Toimittaja käyttää sopimuksen kohteen toteuttamiseen vain sellaisia tietojärjestelmiä, laitteita ja tietoliikennejärjestelmiä, joiden tietoturvariskejä toimittaja pystyy valvomaan ja hallitsemaan, ja joiden tietoturva on mahdollista auditoida. Jos toimittajan sopimuksen kohteen toteuttamiseksi käyttämä laite liitetään tietoverkkoon, siinä on oltava ajantasainen haittaohjelmasuojaus.

10.2 Toimittajan toimitilat

#54 Toimittaja vastaa siitä, että toimittajan tilat, joissa käsitellään tai säilytetään luottamuksellisia tietoja, täyttävät seuraavat vaatimukset:

- Tilat on asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi.
- Tilojen tarkoituksenmukainen fyysinen turvallisuus on varmistettu tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden ja muiden vastaavien erityistilanteiden varalta.
- Tiloissa ei oleskele ilman valvontaa henkilöitä, joiden työtehtäviin luottamuksellisten tietojen käsittely ei kuulu, ellei luottamuksellisia tietoja säilytetä siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

10.3 Luettelo toimittajan henkilöistä

#55 Toimittajan on toteutettava sopimuksen kohde siten, että käyttöoikeudet tilaajan järjestelmiin ja tilaajan aineistoon sekä niihin liittyviin loki-, hallinta- ja konfiguraatiotietoihin annetaan vain henkilöille, jotka tarvitsevat näitä oikeuksia

työtehtäviensä suorittamiseen. Toimittaja pitää ajantasaista luetteloa vähintään seuraavista seikoista:

- kenellä on pääsy järjestelmään
- mitkä oikeudet henkilöllä on
- millä perusteella oikeus on annettu.

#56 Toimittaja ylläpitää ajantasaista luetteloa henkilöiden kulkuoikeuksista tiloihin, joissa on mahdollista päästä käsiksi tilaajan järjestelmiin tai tilaajan aineistoon.

#57 Toimittajan tulee poistaa tarpeettomat käyttöoikeudet ja kulkuoikeudet viipymättä esimerkiksi henkilön poistuessa toimittajan tai alihankkijan palveluksesta tai henkilön työtehtävien muuttuessa. Toimittajan tulee lisäksi tarkistaa aktiiviset käyttöoikeudet vähintään kerran vuodessa ja tilaajan pyynnöstä raportoida tarkistuksen tuloksista.

10.4 Pääsy tilaajan toimitiloihin

#58 Toimittajan palveluksessa olevat henkilöt voivat päästä tilaajan toimitiloihin, jos se on välttämätöntä sopimuksen kohteen toteuttamiseksi. Toimittajan palveluksessa olevien henkilöiden tulee tällöin noudattaa tilaajan osoittaman vastuuhenkilön antamia ja muita tiloissa yleisesti noudatettavia ohjeita sekä käyttää henkilökorttia.

10.5 Tilaajan tietojärjestelmien käyttö

#59 Jos toimittajan lukuun työskentelevät henkilö tarvitsee tunnukset tilaajan tietojärjestelmiin, ne myönnetään tilaajan käyttövaltuuksien hallintamenettelyn mukaisesti. Henkilön esimiehen tulee täyttää ja allekirjoittaa tilaajan tunnushakemuslomake sekä toimittaa se sopimuksen yhdyshenkilölle. Toimittajan on huolehdittava siitä, että kyseinen henkilö on tietoinen seuraavista seikoista ja noudattaa niitä:

- Tilaajan tietojärjestelmiä saa käyttää vain työntekijän työtehtävien mukaiseen tarkoitukseen, vain sopimuksessa sovitussa laajuudessa ja noudattaen tilaajan tietojärjestelmien käyttöön liittyviä ohjeita.
- Erityisesti seuraavat toimet ovat kiellettyjä, ellei niistä ole erikseen sovittu pääsopimuksessa tai sen muissa liitteissä:
    - järjestelmien käyttö- tai hallintaoikeuksien lisäämiseen tähtäävä toiminta
    - järjestelmien tietoliikenneyhteyksien käyttäminen yhdyskäytävänä läpikulkuun tilaajan tietoliikenneverkon muihin osiin tai sen ulkopuolelle
    - järjestelmien tai tietoliikenteen hyödyntäminen tilaajan tietoliikenteen tai palveluiden rakenteen tai niiden yksityiskohtien tai tietojen selvittämiseen
    - ohjelmien asentaminen
    - muu kuin työtehtävien edellyttämä tietojenkäsittely sekä rekisterien ja lokitietojen katselu tai käyttäminen.
- Työntekijän on huolehdittava tilaajan antamista henkilökohtaisista tunnuksista, salasanoista ja muista autentikointivälineistä siten, että ne eivät joudu muiden käsiin tai tietoon.

- Tilaajalla on tarvittaessa oikeus rajoittaa työntekijän käyttöoikeuksia tai peruuttaa ne.

11 Salassapito

#60 Sopijapuolet pitävät toisiltaan saamansa luottamukselliset tiedot salassa eivätkä käytä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin ja sopimuksen edellyttämässä laajuudessa. Tilaajalla on kuitenkin velvollisuus noudattaa julkisuuslain (621/1999) mukaisia velvoitteitaan. Sopijapuolet vastaavat, että kaikki heidän palveluksessaan olevat samoin kuin alihankkijat noudattavat tätä määräystä. Tämä määräys on voimassa myös sopimuksen päättymisen jälkeen.

#61 Salassapitovelvollisuus ei koske tietoa, joka on yleisesti saatavilla tai julkista tai jonka sopijapuoli on saanut laillisesti haltuunsa muuten kuin toiselta sopijapuolelta.

#62 Sopijapuoli palauttaa tai toisen sopijapuolen suostumuksella hävittää tietoturvallisesti toisen sopijapuolen luottamuksellisen aineiston sopimuksen tai käyttötarpeen päättyessä. Aineistoa ei saa hävittää, jos laki tai viranomaisten määräykset vaativat säilyttämistä.

#63 Sopijapuolella on oikeus käyttää toimituksen yhteydessä hankkimaansa ammattitaitoa ja kokemusta.

#64 Toimittajalla ei ole oikeutta käyttää sopimusta referenssinä ilman tilaajan kirjallista lupaa.

12 Muita ehtoja

12.1 Tarkastusoikeus

#65 Tilaajalla on Julkisten hankintojen yleiset sopimusehdot palveluhankinnoissa JYSE 2014 – Palvelut kohdan 5 mukainen tarkastusoikeus, joka voi koskea esimerkiksi sopimuksen mukaisen tietosuojan, tietoturvallisuuden, tilaajan aineiston käsittelyn tai salassapidon toteuttamista.

12.2 Selosteiden laatiminen

#66 Tilaaja vastaa tarvittavan rekisteriselosteen, tietosuojaselosteen, käsittelytoimia koskevan selosteen, vaikutusten arvioinnin ja tietojärjestelmäselosteen laatimisesta sekä ennakkokuulemisen toteuttamisesta. Toimittaja antaa tilaajalle niiden laatimisessa ja toteuttamisessa tarvittavat tiedot ilman erillistä korvausta.

12.3 Sopimuksen muuttaminen tietoturvallisuuteen tai tietosuojaan liittyvästä syystä ja lisätyöt

#67 Tietoturvallisuuteen tai tietosuojaan liittyvän lainsäädännön tai sen tulkintaa koskevien suositusten, ohjeistusten tai määräysten muuttuessa sopijapuolet tekevät tarpeelliset sopimusmuutokset. Tilaajalla on oikeus tilata toimittajalta

sopimusmuutosten tai muiden henkilötietojen käsittelyä koskevien tilaajan ohjeistusten muutosten toteuttamiseksi tarpeellinen määrä lisätyötä.