Yleinen tietoturvallisuus

1 Tämän asiakirjan tarkoitus ja soveltaminen

Tämä asiakirja on sopijaosapuolten välisen pääsopimuksen liite, jolla sovitaan sopimuksen kohteen tietosuojaan, tietoturvallisuuteen, tilaajan aineiston käsittelyyn ja salassapitoon liittyvistä seikoista. Tätä asiakirjaa sovelletaan pääsopimuksessa mainitun sopimusasiakirjojen soveltamisjärjestyksen mukaisesti, huomioiden kuitenkin mitä jäljempänä mainitaan mahdollisten pääsopimuksen vastuunrajoitusten soveltamisesta. Tilaajan aineistoa koskevia ehtoja sovelletaan pääsopimuksen päättymisestä huolimatta niin kauan kuin palveluntuottajalla on hallussaan tilaajan aineistoa.

2 Määritelmät

Luottamukselliset tiedot: Sopijaosapuolta 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.

Henkilötiedot: Määritelty tietosuoja-asetuksen 4 artiklassa.

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

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.

Tilaajan aineisto: Palvelun tai Tuotteen toimituksen yhteydessä käytettävät tai niihin sisältyvät tilaajan asiakirjat, kirjalliset tiedot, tietokannat ja ohjelmistot, sekä muu aineisto, jonka tilaaja on luovuttanut palveluntuottajalle 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.

3 Alihankkijat

Tässä liitteessä palveluntuottajalle ja palveluntuottajan palveluksessa oleville henkilöille asetetut velvoitteet koskevat myös palveluntuottajan mahdollisia alihankkijoita ja niiden palveluksessa olevia henkilöitä siltä osin kuin ne osallistuvat sopimuksen kohteen toteuttamiseen.Palveluntuottajan on tiedotettava alihankkijoille näistä velvoitteista, ja palveluntuottaja

vastaa siitä, että alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat niitä. Palveluntuottaja vastaa käyttämänsä alihankkijan osuudesta kuten omastaan.

4 Yleiset velvollisuudet

4.1 Sopijaosapuolten velvollisuus noudattaa voimassaolevaa lainsäädäntöä

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

4.2 Myötävaikutusvelvollisuus

Sopijaosapuolet pyrkivät kaikin käytettävissään olevin kohtuullisin keinoin myötävaikuttamaan sopimuksen kohteen toteuttamisessa korkeaan tietoturvallisuuden tasoon ja toisen sopijaosapuolen mahdollisuuteen omalta osaltaan ylläpitää sitä.

4.3 Huolellisuusvelvollisuus

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

4.4 Tietoturvallisuuteen liittyvät tehtävät ja vastuut

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

4.5 Sopijaosapuolten tietoturvallisuuteen liittyvät sisäiset ohjeet

Sopijaosapuolilla voi olla erillisiä tietoturvallisuuteen liittyviä sisäisiä ohjeita. Sopijaosapuolten tulee noudattaa niitä siltä osin kuin ne eivät ole ristiriidassa sopimuksen kanssa. Sopijaosapuolet pyrkivät mahdollisuuksien mukaan huomioimaan toistensa tietoturvallisuuteen liittyvät sisäiset ohjeet.

5 Tilaajan aineisto

5.1 Käsitteleminen

Palveluntuottaja 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 palveluntuottaja laatii tai käsittelee sopimuksen perusteella potilasasiakirjoja, palveluntuottaja sitoutuu laatimaan ne ja käsittelemään niitä siten kuin potilasas-

iakirjojen laatimisesta on erikseen säädetty ja tilaaja rekisterinpitäjänä ohjeistaa. ja tilaaja rekisterinpitäjänä ohjeistaa. Myös muun muassa palveluntuottajan laatimat potilasasiakirjat ovat tilaajan aineistoa.

5.2 Käyttötarkoitus

Palveluntuottaja saa käyttää tilaajan aineistoa vain sopimuksen kohteen toteuttamiseen ja vain sopimuksen kohteen toteuttamisen edellyttämässä laajuudessa. Palveluntuottajan tulee huolehtia siitä, että tilaajan aineistoa käsittelevät vain ne palveluntuottajan lukuun työskentelevät henkilöt, joiden työtehtäviin tilaajan aineiston käsittely kuuluu.

5.3 Tietopyynnöt

Palveluntuottajan tulee ohjata kolmansien osapuolten tekemät tilaajan aineistoa koskevat tietopyynnöt viipymättä tilaajalle.

5.4 Tilaajan aineiston palauttaminen

Sopimuksen tai käyttötarpeen päättyessä palveluntuottaja 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. Palveluntuottajalla ei ole oikeutta erillisveloitukseen tilaajan aineiston toimittamisesta tämän alaluvun 5.5 mukaisesti.

5.5 Tilaajan aineiston hävittäminen

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

6 Henkilötietojen käsittely

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

6.1 Palveluntuottajan oikeus käsitellä henkilötietoja

Tilaaja on tietosuojalainsäädännön mukainen rekisterinpitäjä ja palveluntuottaja on henkilötietojen käsittelijä.

Palveluntuottajalla 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.

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 ryhmä
- rekisterinpitäjän velvollisuudet ja oikeudet (siltä osin kuin niitä ei ole mainittu tässä liitteessä).

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

Palveluntuottaja sitoutuu noudattamaan henkilötietojen käsittelyssä voimassa olevaa tietosuojalainlainsäädäntöä ja sen perusteella annettuja viranomaismääräyksiä. Palveluntuottaja vakuuttaa tuntevansa esimerkiksi tietosuoja-asetuksen sisällön, mukaan lukien muun muassa 28 ja 32 artiklassa henkilötietojen käsittelijälle asetetut velvollisuudet. Palveluntuottajan tietosuojalainsäädännön vastaista menettelyä voidaan pitää olennaisena sopimusrikkomuksena.

Palveluntuottajan on viipymättä ilmoitettava tilaajalle, jos palveluntuottaja epäilee, että sopimus tai sopimuksen kohteen toteuttamisessa käytettävä ohjeistus tai käytäntö rikkoo tietosuojalainsäädäntöä.

6.3 Toimet tietosuojalainsäädännön vaatimusten noudattamisen turvaamiseksi

Palveluntuottajan 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.

Palveluntuottaja huolehtii esimerkiksi käsittelemiensä henkilötietojen asianmukaisesta suojaamisesta varmistaakseen niiden luottamuksellisuuden, eheyden ja saatavuuden sekä noudattaa sopimuksen kohteen toteuttamisessa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta.

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

6.4 Muiden henkilötietojen käsittelijöiden käyttäminen

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

6.5 Palveluntuottajan avustamis- ja tiedonantovelvollisuus

Palveluntuottajan 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. Palveluntuottajan tulee esimerkiksi avustaa tilaajaa tietosuoja-asetuksen 33 ja 34 artiklan edellyttämien ilmoitusten tekemisessä tietosuoja-asetuksen mukaisessa määräajassa valvontaviranomaiselle ja rekisteröidylle. Palveluntuottajan tulee myös pyynnöstä tehdä tietosuoja-asetuksen 31 artiklan mukaista yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

Palveluntuottajan tulee antaa tilaajalle kaikki tiedot, jotka ovat tarpeen tietosuojalainsäädännössä asetettujen velvoitteiden noudattamisen osoittamista varten. Palveluntuottajan tulee jatkuvasti ylläpitää mainittuja tietoja ja arvioida toimenpiteiden riittävyyttä.

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

Palveluntuottaja toteuttaa tämän alaluvun 6.5 mukaisen avustamis- ja tiedonantovelvollisuuden ilman erillistä korvausta.

6.6 Henkilötietojen käsittely ulkomailla

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

6.7 Vahingonkorvaus

Jos palveluntuottaja on toiminut tietosuoja-asetuksen tai muun tietosuojalainsäädännön tai sopimuksen vastaisesti ja tästä on aiheutunut tilaajalle välitöntä vahinkoa, on palveluntuottaja velvollinen korvaamaan kyseisen vahingon täysimääräisesti. Tilaajalle aiheutuneena välittömänä vahinkona pidetään muun muassa sellaista korvausta ja oikeudenkäyntikuluja korkoineen, jonka tilaaja on joutunut maksamaan rekisteröidylle palveluntuottajan 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 palveluntuottajasta johtuvan henkilötietojen tietoturvaloukkauksen vuoksi. Pääsopimuksessa tai muissa sopimusasiakirjoissa mahdollisesti olevia vastuunrajoitusehtoja ei sovelleta tämän kohdan perusteella maksettavaan korvaukseen.

Jos tilaajalle määrätään tietosuoja-asetuksen 83 artiklassa tarkoitettu hallinnollinen sakko ja sakon voidaan katsoa aiheutuneen kokonaan tai osittain palveluntuottajan tai sen alihankkijan tai niiden palveluksessa olevan henkilön menettelystä tai laiminlyönnistä, on palveluntuottaja 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 Palveluntuottajan ilmoitus- ja raportointivelvollisuudet

7.1 Ilmoitusvelvollisuus

Palveluntuottajan on ilman aiheetonta viivytystä ilmoitettava tilaajalle sellaisista palveluntuottajan 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. Palveluntuottajan tulee ilmoittaa tilaajalle vastuuhenkilö, jolta asiassa saa lisätietoja. Jos seikka liityy henkilötietoihin, palveluntuottajan on ilmoitettava asiaan liittyvien rekisteröityjen ryhmät ja arvioidut lukumäärät.

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

7.2 Määräajoin suoritettava raportointi

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

8 Tietoturvaloukkaustilanteessa toimiminen

Palveluntuottajalla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen.

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

Palveluntuottaja on velvollinen auttamaan tilaajaa tietoturvaloukkauksiin liittyvien vahinkojen minimoinnissa sekä asian selvittämisessä viranomaistahojen kanssa.

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

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

9 Palveluntuottajan henkilöstö

9.1 Henkilöstön salassapitovelvollisuus

Palveluntuottaja vastaa siitä, että palveluntuottajan lukuun työskentelevät henkilöt, joilla voi olla pääsy luottamuksellisiin tietoihin, ovat etukäteen allekirjoittaneet kirjallisen salassapitositoumuksen. Palveluntuottajan on tilaajan pyynnöstä esitettävä kyseinen salassapitositoumus tilaajalle.

Palveluntuottajan on huolehdittava siitä, että palveluntuottajan 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 palveluntuottajan lukuun työskenteleviä henkilöitä, jotka eivät työtehtäviensä perusteella tarvitse tilaajan aineistoa tietoonsa.
- Työntekijän on ilmoitettava tietoonsa tulleista tietoturvaa tai tietosuojaa vaarantavista seikoista tilaajalle tai palveluntuottajalle 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 palveluntuottajan 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.

Palveluntuottajan tulee lisäksi huolehtia siitä, että palveluntuottajan lukuun työskentelevät henkilöt ovat tietoinen myös muista mahdollisista sopimuksen mukaisista salassapitovelvoitteista, ja valvoa heidän toimintansa sopimuksenmukaisuutta.

9.2 Turvallisuusselvitys

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

Sopijaosapuoli vastaa itse kustannuksista, joita turvallisuusselvityksen teettämisestä sille aiheutuu. Tilaaja maksaa turvallisuusselvityksen teettämiseen liittyvät viranomaismaksut. Jos turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että palveluntuottajan henkilöstössä tapahtuu tilaajasta riippumaton muutos, palveluntuottaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.

10 Toimitilat ja tietojärjestelmien käyttö

10.1 Palveluntuottajan sisäinen tietoturva

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

10.2 Palveluntuottajan toimitilat

Palveluntuottaja vastaa siitä, että palveluntuottajan 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 palveluntuottajan henkilöistä

Palveluntuottajan 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. Palveluntuottaja pitää ajantasaista luetteloa vähintään seuraavista seikoista:

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

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

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

10.4 Pääsy tilaajan toimitiloihin

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

10.5 Tilaajan tietojärjestelmien käyttö

Jos palveluntuottajan 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. Palveluntuottajan 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

Sopijaosapuolet 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. Sopijaosapuolet vastaavat, että kaikki heidän palveluksessaan olevat samoin kuin alihankkijat noudattavat tätä määräystä. Tämä määräys on voimassa myös sopimuksen päättymisen jälkeen.

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

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.

Sopijapuolella on oikeus käyttää toimituksen yhteydessä hankkimaansa ammattitaitoa ja kokemusta.

Palveluntuottajalla ei ole oikeutta käyttää sopimusta referenssinä ilman tilaajan kirjallista lupaa.

12 Muita ehtoja

12.1 Tarkastusoikeus

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

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

12.3 Sopimuksen muuttaminen tietoturvallisuuteen tai tietosuojaan liittyvästä syystä ja lisätyöt

Tietoturvallisuuteen tai tietosuojaan liittyvän lainsäädännön tai sen tulkintaa koskevien suositusten, ohjeistusten tai määräysten muuttuessa sopijaosapuolet tekevät tarpeelliset sopimusmuutokset. Tilaajalla on oikeus tilata palveluntuottajalta sopimusmuutosten tai muiden henkilötietojen käsittelyä koskevien tilaajan ohjeistusten muutosten toteuttamiseksi tarpeellinen määrä lisätyötä.