Yleinen tietoturvallisuusliite

1 Tämän dokumentin tarkoitus ja soveltaminen

#1 Tämä dokumentti on palvelusetelijärjestelmän sääntökirjan liite, jolla määritellään palvelusetelijärjestelmän tietosuojaan, tietoturvallisuuteen, HUSin (jäljempänä *tilaaja*) aineiston käsittelyyn ja salassapitoon liittyvät seikat. Tätä dokumenttia sovelletaan tietosuoja-asetuksen 28 artiklan tarkoittamana henkilötietojen käsittelyä koskevana sitovana oikeudellisena asiakirjana sen jälkeen, kun palveluntuottaja (jäljempänä *toimittaja*) on hyväksytty palvelusetelijärjestelmään. Tilaajan aineistoa koskevia ehtoja sovelletaan niin kauan kuin toimittajalla on hallussaan tilaajan aineistoa. Tässä dokumentissa olevat viittaukset sopimukseen tarkoittavat viittausta sääntökirjaan.

2 Määritelmät

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

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

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

#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.

3 Alihankkijat

#7 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. Toimittaja varmistaa, että sopimuksen mukainen auditointioikeus voidaan ulottaa myös alihankkijaan.

4 Yleiset velvollisuudet

4.1 Sopijapuolten velvollisuus noudattaa lainsäädäntöä

#8 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

#9 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

#10 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

#11 Sopijapuolten tulee määritellä organisaatiossaan tietoturvallisuuteen liittyvät tehtävät ja vastuut sekä nimetä riittävän kokeneet ja pätevät vastuuhenkilöt.

4.5 Sopijapuolten tietoturvallisuuteen liittyvät sisäiset ohjeet

#12 Sopijapuolten tulee noudattaa sisäisiä tietoturvallisuuteen liittyviä ohjeitaan siltä osin kuin ne eivät ole ristiriidassa sopimuksen tai tämän liitteen kanssa.

5 Tilaajan aineisto

5.1 Käsitteleminen

#13 Toimittaja noudattaa tilaajan aineistoa käsitellessään tilaajan antamia kohtuullisia ohjeita, samoin kuin omalta osaltaan tiedonhallintalain (906/2019) tietoturvallisuutta koskevaa sääntelyä. Jos toimittaja laatii tai käsittelee sopimuksen perusteella poti-

lasasiakirjoja, toimittaja sitoutuu laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjojen laatimisesta on erikseen säädetty ja tilaaja ohjeistaa. Myös muun muassa toimittajan laatimat potilasasiakirjat ovat tilaajan aineistoa.

5.2 Käyttötarkoitus

#14 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

#15 Tilaajalla saattaa olla tarve määritellä tilaajan aineistolle eri tietoturvallisuustasoja ja sen mukaisia erityisiä tietoturvatoimenpiteitä ja ohjeita. Jos tietoturvallisuustasoihin liittyvistä muutoksista aiheutuu toimittajalle lisäkustannuksia, eikä muutoksia ole hinnoiteltu sopimuksessa, sopijapuolet käsittelevät asian sopimuksen muutoshallintamenettelyn mukaisesti ja tilaaja voi tilata toimittajalta sopimuksen mukaisilla hinnoilla tarpeellisen määrän lisätyötä.

5.4 Tietopyynnöt

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

5.5 Tilaajan aineiston palauttaminen

#17 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

#18 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

#19 Henkilötietojen käsittelyyn sovelletaan myös muun muassa tilaajan aineistoa koskevia ehtoja.

6.1 Toimittajan oikeus käsitellä henkilötietoja

#20 Tilaaja on sosiaali- ja terveydenhuollon palvelusetelistä annetun lain (569/2009) mukaisesti tietosuojalainsäädännön tarkoittama rekisterinpitäjä ja toimittaja henkilötietojen käsittelijä.

#21 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 tietosuojalainsäädännön, tämän sopimuksen sekä tilaajan erikseen antamien dokumentoitujen ohjeiden mukaisesti.

#22 Seuraavat seikat ilmenevät tarkemmin sopimuksesta tai siihen liittyvästä muusta 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).

#23 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 tunteminen ja noudattaminen

#24 Toimittaja vakuuttaa, että se tuntee sopimuksen kohteena olevaa henkilötietojen käsittelyä koskevan tietosuojalainsäädännön, mukaan lukien muun muassa tietosuoja-asetuksen 28 ja 32 artiklassa henkilötietojen käsittelijälle asetetut velvollisuudet. Toimittajan tietosuojalainsäädännön vastaista menettelyä voidaan pitää olennaisena sopimusrikkomuksena.

#25 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

#26 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.

#27 Toimittajan on nimettävä tietosuojavastaava, jos tietosuoja-asetuksen 37 artikla niin edellyttää, tai muu tietosuojasta vastaava henkilö ja ilmoitettava hänen yhteystietonsa joko julkisilla verkkosivuillaan tai suoraan tilaajalle.

6.4 Muiden henkilötietojen käsittelijöiden käyttäminen

#28 Toimittaja saa käyttää muina henkilötietojen käsittelijöinä sopimuksessa mainittuja alihankkijoita. Toimittajan on ilmoitettava etukäteen kirjallisesti tilaajalle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, jolloin tilaaja voi perustellusta syystä vastustaa tällaisia muutoksia. Toimittaja vastaa siitä, että toimittajan ja muun henkilötietojen käsittelijän välillä on tehty asianmukainen sopimus, joka täyttää tietosuojalainsäädännön velvoitteet.

6.5 Toimittajan avustamis- ja tiedonantovelvollisuus

#29 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.

#30 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.

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

#32 Tilaaja vastaa tarvittavan tietosuojaselosteen, käsittelytoimia koskevan selosteen ja vaikutustenarvioinnin laatimisesta sekä ennakkokuulemisen toteuttamisesta. Toimittaja antaa tilaajalle niiden laatimisessa ja toteuttamisessa tarvittavat tiedot.

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

6.6 Henkilötietojen käsittely ulkomailla

#34 Jos sopimuksessa ei ole nimenomaisesti toisin sovittu, toimittaja tai toimittajan alihankkija ei saa käsitellä henkilötietoja ETA-alueen ulkopuolella.

#35 Jos toimittaja tai toimittajan alihankkija sopimuksen mukaan saa käsitellä henkilötietoja ETA-alueen ulkopuolella, toimittaja vastaa siitä, että henkilötietojen siirto ETA-alueen ulkopuolelle tapahtuu tietosuojalainsäädännön edellyttämällä tavalla.

#36 Jos toimittaja sopimuksen mukaisesti käsittelee henkilötietoja Yhdysvalloissa tai muualla ETA-alueen ulkopuolella kuin EU-komission listaamissa luotettavissa maissa, toimittaja sitoutuu solmimaan ennen henkilötietojen käsittelyn aloittamista tilaajan kanssa Euroopan komission hyväksymien vakiolausekkeiden mukaisen sopimuksen (Controller to Processor). Jos henkilötietojen käsittely tapahtuu toimittajan alihankkijan toimesta, toimittajan tulee solmia alihankkijansa kanssa vastaava sopimus (Processor to Processor). Toimittajan tulee tilaajan pyynnöstä esittää tilaajalle viimeksi mainittu sopimus.

#37 Vaihtoehtona vakiolausekkeiden mukaiselle sopimukselle toimittaja voi esittää selvityksen siitä, että toimittajaa tai alihankkijaa koskevat tietosuoja-asetuksen 47 artiklassa tarkoitetut sitovat säännöt (Binding Corporate Rules), jotka valvontaviranomainen on vahvistanut ja jotka soveltuvat kyseiseen käsittelyyn.

#38 Toimittaja sitoutuu siirtämään henkilötietojen käsittelyn omalla kustannuksellaan ETA-alueelle tai EU-komission listaamaan luotettavaan maahan ilman aiheetonta viivytystä, jos käsittelymaa poistetaan luotettavien maiden listalta. Samoin jos vakiolausekkeiden mukaista sopimusta tai edellä mainittuja sitovia sääntöjä ei myöhemmin pidettäisi riittävänä osoituksena tietosuojalainsäädännön velvoitteiden täyttämisestä, toimittaja sitoutuu yhteistyössä tilaajan kanssa viipymättä saattamaan henkilötietojen käsittelyn lainmukaiseksi.

6.7 Vahingonkorvaus

#39 Jos sopijapuoli on maksanut rekisteröidylle korvauksen tietosuojalainsäädännön rikkomisen johdosta aiheutuneesta vahingosta, on tällä sopijapuolella oikeus periä samaan tietojenkäsittelyyn osallistuneelta toiselta sopijapuolelta se osuus korvauksesta, joka vastaa tämän vastuuta aiheutuneesta vahingosta. Sopijapuolten keskinäinen vastuu määräytyy tietosuoja-asetuksen 82 artiklan mukaisesti. Sopimuksessa mahdollisesti olevia vastuunrajoitusehtoja ei sovelleta tämän kohdan perusteella maksettavaan korvaukseen.

7 Toimittajan ilmoitus- ja raportointivelvollisuudet

7.1 Ilmoitusvelvollisuus

#40 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 seurauk-

sista. 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.

#41 Jos edellä mainittu ilmoitus koskee henkilötietojen tietoturvaloukkausta, ilmoitus on tehtävä ilman aiheetonta viivytystä. Toimittajan tulee huomioida tilaajan velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle tietosuoja-asetuksen 33 artiklan mukaisessa 72 tunnin määräajassa esimerkiksi siten, että toimittaja tekee alustavan ilmoituksen heti saatuaan tiedon asiasta ja täydentää ilmoitusta sitä mukaan kuin saa lisätietoja. Ilmoituksessa on vähintään

- kuvattava tapahtunut henkilötietojen tietoturvaloukkaus todennäköisine seurauksineen
- ilmoitettava mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät
- kuvattava toimenpiteet, jotka on tehty tai jotka toimittaja ehdottaa tehtäväksi henkilötietojen tietoturvaloukkauksen johdosta ja sen mahdollisten haittavaikutusten lieventämiseksi.

#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

#48 Toimittaja vastaa siitä, että toimittajan lukuun työskentelevät henkilöt, joilla voi olla pääsy tilaajan luottamuksellisiin tietoihin, tilaajan tietojärjestelmiin tai itsenäisesti tilaajan toimitiloihin, ovat etukäteen allekirjoittaneet kirjallisen salassapitositoumuksen ja heillä on tehtäviinsä nähden riittävä tietoturvallisuusosaaminen. Toimittajan on tilaajan pyynnöstä esitettävä kohtuullinen selvitys kyseisen salassapitositoumuksen sisällöstä ja allekirjoittamisesta sekä henkilöiden tietoturvallisuusosaamisesta, kuten heidän saamastaan koulutuksesta. Tilaaja voi lisäksi edellyttää, että mainitut henkilöt suorittavat tilaajan tarjoaman tietoturvallisuuden verkkokoulutuksen.

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

- 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 tai tallenteita 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 lainsäädäntöön perustuvan henkilökohtaisen vastuun.

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

10 Toimitilat ja tietojärjestelmien käyttö

10.1 Toimittajan sisäinen tietoturva

#51 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

#52 Toimittaja vastaa siitä, että toimittajan toimitilat, joissa käsitellään tai säilytetään tilaajan luottamuksellisia tietoja, täyttävät seuraavat vaatimukset:

- Toimitilat on asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi.
- Toimitilojen tarkoituksenmukainen fyysinen turvallisuus on varmistettu tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden ja muiden vastaavien erityistilanteiden varalta.
- Toimitiloissa 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 Käyttö- ja kulkuoikeuksien hallinnointi

#53 Toimittaja ei saa antaa käyttöoikeuksia tilaajan aineistoon, järjestelmiin ja laitteisiin sekä niihin liittyviin loki-, hallinta- ja konfiguraatiotietoihin muille kuin niille toimittajan lukuun työskenteleville henkilöille, jotka tarvitsevat näitä oikeuksia työtehtäviensä suorittamiseen. Toimittaja pitää käyttöoikeuksista ja niiden perusteista ajantasaista luetteloa.

#54 Toimittaja ylläpitää ajantasaista luetteloa henkilöiden kulkuoikeuksista toimitiloihin, joissa on mahdollista päästä käsiksi tilaajan aineistoon, järjestelmiin ja laitteisiin.

#55 Toimittajan tulee poistaa tarpeettomat käyttö- ja kulkuoikeudet viipymättä esimerkiksi henkilön poistuessa toimittajan tai alihankkijan palveluksesta tai henkilön työtehtävien muuttuessa. Toimittajan tulee lisäksi tarkistaa aktiiviset käyttöoikeudet vähintään kerran vuodessa.

10.4 Pääsy tilaajan toimitiloihin

#56 Toimittajan lukuun työskentelevät henkilöt voivat päästä tilaajan toimitiloihin, jos se on välttämätöntä sopimuksen kohteen toteuttamiseksi. Toimittajan lukuun työskentelevien henkilöiden tulee tällöin noudattaa tilaajan osoittaman vastuuhenkilön antamia ja muita toimitiloissa yleisesti noudatettavia ohjeita sekä käyttää henkilökorttia.

10.5 Tilaajan tietojärjestelmien käyttö

#57 Jos toimittajan lukuun työskentelevä henkilö tarvitsee tunnukset tilaajan tietojärjestelmiin, ne myönnetään tilaajan käyttövaltuuksien hallintamenettelyn mukaisesti. Henkilön esimiehen tai toimittajan puolelta toimituksesta vastaavan henkilön tulee täyttää tilaajan tunnushakemuslomake sekä toimittaa se tilaajalle. Jos henkilöllä voi

olla pääsy arkaluonteisiin henkilötietoihin, tunnushakemuslomakkeessa on yksilöitävä henkilö suomalaisella henkilötunnuksella. Jos henkilöillä ei ole suomalaista henkilötunnusta, henkilöstä tulee ilmoittaa vastaava ulkomainen tunnus tai muu vastaava, tilaajan riittävästi yksilöiväksi katsoma tunniste. Jos henkilö ei halua antaa henkilötunnusta tai tunnistetta, toimittajan tulee osoittaa hänen tilalleen toinen henkilö, jolla on vastaava kokemus ja pätevyys.

Toimittajan on huolehdittava siitä, että tilaajan tietojärjestelmiin tunnukset saaneet, toimittajan lukuun työskentelevät henkilöt ovat tietoisia seuraavista seikoista ja noudattavat niitä:

- Tilaajan tietojärjestelmiä saa käyttää vain työntekijän työtehtävien mukaiseen tarkoitukseen, vain sopimuksen kohteen toteuttamiseksi tarvittavassa laajuudessa ja noudattaen tilaajan tietojärjestelmien käyttöön liittyviä ohjeita.
- Erityisesti seuraavat toimet ovat kiellettyjä, ellei niistä ole erikseen sovittu sopimuksessa:
    - tietojärjestelmien sisältämien potilastietojen ja muiden luottamuksellisten tietojen katselu ja käsittely ilman työtehtävien mukaista tarkoitusta
    - 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.

- 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

#58 Sopijapuolet pitävät toisiltaan saamansa luottamukselliset tiedot salassa eivätkä käytä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin ja sopimuksen edellyttämässä laajuudessa. Sopijapuolet vastaavat siitä, että kaikki niiden lukuun työskentelevät henkilöt ja alihankkijat noudattavat tätä määräystä. Tämä määräys on voimassa myös sopimuksen päättymisen jälkeen.

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

#60 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.

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

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

#63 Tilaajalla on velvollisuus noudattaa julkisuuslain (621/1999) mukaisia velvoitteitaan salassapitoa koskevista sopimusehdoista riippumatta.

12 Muita ehtoja

12.1 Auditoinnit

#64 Toimittajan tulee sallia tilaajan tai tilaajan valtuuttaman riippumattoman kolmannen osapuolen suorittamat tietoturvaa ja tietosuojaa koskevat auditoinnit sekä osallistua niihin.

#65 Auditoijana toimiva kolmas osapuoli ei voi olla toimittajan kilpailija auditoinnin kohteena olevien toimintojen osalta. Toimittaja voi edellyttää kolmannelta osapuolelta tämän sopimuksen mukaista salassapitovelvollisuutta vastaavan salassapitositoumuksen allekirjoittamista.

#66 Tilaajan tulee ilmoittaa kirjallisesti toimittajalle vähintään kaksi viikkoa etukäteen aikomuksestaan tehdä tai teettää auditointi. Auditointeja voidaan toteuttaa korkeintaan kaksi kertaa vuodessa.

#67 Ellei muualla sopimuksessa ole toisin sovittu, tilaaja vastaa auditoijana toimivan kolmannen osapuolen kustannuksista ja muilta osin sopijapuolet osallistuvat auditointiin omalla kustannuksellaan.

#68 Tämä alaluku 12.1 ei rajoita tilaajan muuta sopimukseen mahdollisesti perustuvaa tarkastusoikeutta.

12.2 Tämän liitteen muuttaminen tietoturvallisuuteen tai tietosuojaan liittyvästä syystä

#69 Tietoturvallisuuteen tai tietosuojaan liittyvän lainsäädännön tai viranomaismääräysten tai niiden tulkintaa koskevien ohjeiden tai suositusten muuttuessa sopijapuolet tekevät tarvittaessa vastaavat muutokset tähän liitteeseen siten kuin sopimuksessa on sovittu sopimusmuutosten tekemisestä.