Tietoturvallisuusliite –
HUS henkilötietojen käsittelijänä

1 Tämän dokumentin tarkoitus ja soveltaminen

#1 Tämä dokumentti on sopijapuolten välistä yhteistyötä koskevan sopimuksen liite, jolla sovitaan tietoturvallisuuteen, tietosuojaan, tilaajan aineiston käsittelyyn ja salassapitoon liittyvistä seikoista. Tätä dokumenttia sovelletaan sopimuksessa mainitun sopimusasiakirjojen soveltamisjärjestyksen mukaisesti. Tilaajan aineistoa koskevia ehtoja sovelletaan sopimuksen päättymisestä huolimatta niin kauan kuin HUSilla on hallussaan tilaajan aineistoa. Tässä liitteessä oleva viittaus sopimukseen tarkoittaa sopimusta ja kaikkia muita sen liitteitä, ellei erikseen ole toisin todettu.

2 Tässä liitteessä käytetyt määritelmät

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

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

#4 *HUS:* Helsingin ja Uudenmaan Sairaanhoitopiirin kuntayhtymä.

#5 *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.

#6 *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.

#7 *Tilaaja:* Organisaatio, jonka puolesta HUS käsittelee henkilötietoja.

3 Alihankkijat

#8 Tässä liitteessä sopijapuolelle ja sen palveluksessa oleville henkilöille asetetut velvoitteet koskevat myös sopijapuolen alihankkijoita ja niiden palveluksessa olevia henkilöitä siltä osin kuin ne osallistuvat sopimuksen kohteen toteuttamiseen. Sopijapuolen on tiedotettava alihankkijoille näistä velvoitteista, ja sopijapuoli vastaa siitä, että alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat niitä. Sopijapuoli 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 Ilmoitusvelvollisuus

#12 Sopijapuolen on ilmoitettava toiselle sopijapuolelle sellaisista sopijapuolen tietoon tulleista seikoista, jotka voivat olennaisesti vaikuttaa sopimuksen kohteeseen liittyvään tietoturvallisuuteen, ja niiden aiheuttamista toimenpiteistä ja mahdollisista seurauksista.

#13 Jos edellä mainittu ilmoitus koskee henkilötietojen tietoturvaloukkausta, ilmoitus on tehtävä ilman aiheetonta viivytystä. Ilmoituksessa on vähintään

- kuvattava tapahtunut 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 HUS ehdottaa tehtäväksi tietoturvaloukkauksen johdosta ja sen mahdollisten haittavaikutusten lieventämiseksi.

4.5 Tietoturvallisuuteen liittyvät tehtävät ja vastuut

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

4.6 Tietoturvaloukkaustilanteessa toimiminen

#15 Sopijapuolilla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen.

#16 Sopijapuolet ovat velvollisia auttamaan toisiaan tietoturvaloukkauksiin liittyvien vahinkojen minimoinnissa sekä asian selvittämisessä viranomaistahojen kanssa.

4.7 Sopijapuolten tietoturvallisuuteen liittyvät sisäiset ohjeet

#17 Sopijapuolilla voi olla erillisiä tietoturvallisuuteen liittyviä sisäisiä ohjeita. Sopijapuolten tulee noudattaa niitä siltä osin kuin ne eivät ole ristiriidassa sopimuksen kanssa.

5 Tilaajan aineisto

5.1 Käsitteleminen

#18 HUS noudattaa tilaajan aineistoa käsitellessään tietosuojalainsäädäntöä ja tilaajan antamia kohtuullisia ohjeita. Jos sopimuksen perusteella laaditaan tai käsitellään potilasasiakirjoja, sopijapuolet sitoutuvat laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjoja koskeva lainsäädäntö edellyttää.

5.2 Käyttötarkoitus

#19 HUS käyttää muuta kuin julkista tilaajan aineistoa vain sopimuksen kohteen toteuttamiseen ja vain sopimuksen kohteen toteuttamisen edellyttämässä laajuudessa. HUSin tulee huolehtia siitä, että tällaista aineistoa käsittelevät vain ne HUSin lukuun työskentelevät henkilöt, joiden työtehtäviin tilaajan aineiston käsittely kuuluu.

5.3 Varmistukset ja palautukset

#20 Jos sopijapuolet ovat sopineet tilaajan aineiston tallentamisesta HUSin hallinnassa olevaan järjestelmään tai laitteeseen, HUS huolehtii siitä, että tilaajan aineisto pystytään palauttamaan järjestelmän tai laitteen vikatilanteessa vastaavalla tavalla kuin järjestelmään tai laitteeseen tallennettava HUSin aineisto. Sopijapuolet sopivat tarvittaessa tarkemmin erikseen varmistusten toteuttamistavasta ja -frekvenssistä sekä varmistusten eheyden ja palautuskyvyn seurannasta.

5.4 Tietopyynnöt

#21 HUSin tulee pyrkiä ohjaamaan kolmansien osapuolten tekemät tilaajan aineistoa koskevat tietopyynnöt ilman aiheetonta viivytystä tilaajalle siltä osin kuin HUSilla ei ole lainsäädäntöön perustuvaa velvollisuutta itse vastata tietopyyntöön.

5.5 Tilaajan aineiston palauttaminen

#22 Jos ajan tasalla oleva tilaajan aineisto on tarpeen palauttaa tilaajalle sopimuksen tai käyttötarpeen päättyessä, sopijapuolet sopivat asiasta erikseen.

5.6 Tilaajan aineiston hävittäminen

#23 HUSilla on velvollisuus omalla kustannuksellaan tietoturvallisella tavalla hävittää mahdolliset jäljennökset tilaajan aineistosta sen jälkeen, kun tilaaja on kirjallisesti hyväksynyt tilaajan aineiston sopimuksen mukaisesti palautetuksi, tai jos sitä ei ole sopimuksen tai käyttötarpeen päättyessä tarpeen palauttaa. HUSilla ei ole velvollisuutta hävittää aineistoa siltä osin kuin HUS on velvollinen lain tai viranomaismääräyksen perusteella säilyttämään aineiston.

6 Henkilötietojen käsittely

6.1 HUSin oikeus käsitellä henkilötietoja

#24 Tilaaja on tietosuojalainsäädännön tarkoittama rekisterinpitäjä ja HUS henkilötietojen käsittelijä. Tilaaja vastaa siitä, että sillä on lainsäädännön mukainen ja tarvittaessa esimerkiksi rekisteröityjen suostumukseen perustuva oikeus luovuttaa henkilötiedot HUSin käsiteltäväksi. Tilaaja sitoutuu HUSin pyynnöstä esittämään oikeudesta kirjallisen selvityksen.

#25 HUSilla on oikeus käsitellä tilaajan aineistoon sisältyviä henkilötietoja

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

#26 Seuraavat seikat ilmenevät tarkemmin sopimuksesta 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).

#27 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

#28 HUS 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.

#29 Sopijapuolen on viipymättä ilmoitettava toiselle sopijapuolelle, jos se epäilee, että sopimus tai sopimuksen kohteen toteuttamisessa käytettävä ohjeistus tai käytäntö rikkoo tietosuojalainsäädäntöä.

6.3 Toimet tietosuojalainsäädännön vaatimusten noudattamisen turvaamiseksi

#30 Sopijapuolten tulee omalta osaltaan 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. Sopijapuolten tulee esimerkiksi omalta osaltaan huolehtia henkilötietojen asianmukaisesta suojaamisesta varmistaakseen niiden luottamuksellisuuden, eheyden ja saatavuuden sekä noudattaa sopimuksen kohteen toteuttamisessa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta.

#31 HUSin on nimettävä tietosuoja-asetuksen 37 artiklan mukaisesti tietosuojavastaava ja ilmoitettava hänen yhteystietonsa tilaajalle tai julkisilla verkkosivuillaan.

6.4 Muiden henkilötietojen käsittelijöiden käyttäminen

#32 HUS saa käyttää muina henkilötietojen käsittelijöinä sopimuksessa ja siihen liittyvässä dokumentaatiossa mainittuja alihankkijoita. HUSin on ilmoitettava tilaajalle muiden henkilötietojen käsittelijöiden lisäämisestä tai vaihtamisesta, jolloin tilaaja voi perustellusta syystä vastustaa tällaista muutosta. HUS vastaa siitä, että HUSin ja muun henkilötietojen käsittelijän välillä on tehty asianmukainen sopimus, joka täyttää tietosuojalainsäädännön velvoitteet.

6.5 HUSin avustamis- ja tiedonantovelvollisuus

#33 HUSin 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. HUSin tulee myös pyynnöstä tehdä tietosuoja-asetuksen 31 artiklan mukaista yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

#34 HUSin tulee antaa tilaajalle tiedot, jotka ovat tarpeen tietosuojalainsäädännössä asetettujen velvoitteiden noudattamisen osoittamista varten, ja ylläpitää niitä.

#35 HUSin tulee ilmoittaa tilaajalle henkilötietojen käsittelypaikat ja niiden muutokset, elleivät ne ilmene sopimuksesta tai siihen liittyvästä dokumentaatiosta.

6.6 Henkilötietojen käsittely ulkomailla

#36 HUS ei itse käsittele tilaajan aineiston sisältämiä henkilötietoja ETA-alueen ulkopuolella.

#37 Jos HUSin alihankkija käsittelee tilaajan aineiston sisältämiä henkilötietoja muualla ETA-alueen ulkopuolella kuin EU-komission listaamissa luotettavissa maissa, sopijapuolet huolehtivat siitä, että ennen henkilötietojen käsittelyn aloittamista solmitaan EU-mallilausekkeiden mukainen sopimus henkilötietojen käsittelystä. Vaihtoehtoisesti käsittely voi perustua muuhun tietosuojalainsäädännön mukaiseen perusteeseen.

#38 Jos EU-mallilausekkeiden mukaista sopimusta tai muuta perustetta ei myöhemmin pidettäisi riittävänä osoituksena tietosuojalainsäädännön velvoitteiden täyttämisestä tai jos käsittelymaa poistetaan luotettavien maiden listalta, sopijapuolten tulee ilman aiheetonta viivytystä ryhtyä toimenpiteisiin henkilötietojen käsittelyn saattamiseksi lainmukaiseksi.

7 Tietojärjestelmät, laitteet ja toimitilat

#39 Sopijapuolet vastaavat omien sopimuksen kohteen toteuttamiseen liittyvien tietojärjestelmiensä, laitteidensa ja tietoliikennejärjestelmiensä tietoturvallisuudesta sekä omien toimitilojensa, joissa käsitellään tai säilytetään luottamuksellisia tietoja, fyysisestä turvallisuudesta.

#40 Sopijapuolen lukuun työskentelevät henkilöt voivat päästä toisen sopijapuolen toimitiloihin, jos se on välttämätöntä sopimuksen kohteen toteuttamiseksi. Kyseisten henkilöiden tulee tällöin noudattaa toisen sopijapuolen osoittaman vastuuhenkilön antamia ja muita tiloissa yleisesti noudatettavia ohjeita.

#41 Jos sopijapuolen lukuun työskentelevät henkilö tarvitsee tunnukset toisen sopijapuolen tietojärjestelmiin, ne myönnetään tunnukset myöntävän sopijapuolen käyttövaltuuksien hallintamenettelyn mukaisesti. Sopijapuoli vastaa siitä, että sen lukuun työskentelevät henkilöt käyttävät toisen sopijapuolen tietojärjestelmiä vain työntekijän työtehtävien mukaiseen tarkoitukseen, vain sopimuksessa sovitussa laajuudessa ja noudattaen niiden käyttöön liittyviä ohjeita.

8 Salassapito

#42 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.

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

#44 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.

#45 Sopijapuolella on oikeus käyttää sopimuksen kohteen toteuttamisen yhteydessä hankkimaansa ammattitaitoa ja kokemusta.

#46 Sopijapuolella on salassapitoa koskevista ehdoista riippumatta velvollisuus noudattaa julkisuuslain (621/1999) mukaisia velvoitteitaan, jos julkisuuslakia sovelletaan sopijapuoleen.

9 Muita ehtoja

9.1 Jatkuvuussuunnitelmat ja valmiussuunnitelmat

#47 Sopijapuolet avustavat pyynnöstä toisiaan tarvittavien jatkuvuussuunnitelmien ja valmiussuunnitelmien tekemisessä.

9.2 Selosteiden laatiminen

#48 Tilaaja vastaa tarvittavan rekisteriselosteen, tietosuojaselosteen, käsittelytoimia koskevan selosteen, vaikutusten arvioinnin ja tietojärjestelmäselosteen laatimisesta sekä ennakkokuulemisen toteuttamisesta. HUS antaa tilaajalle niiden laatimisessa ja toteuttamisessa tarvittavat kohtuulliset tiedot.

9.3 Tarkastusoikeus

#49 Tilaajalla on tietosuojaan liittyvien menettelyiden tarkastamiseksi Julkisten hankintojen yleiset sopimusehdot palveluhankinnoissa JYSE 2014 – Palvelut kohdan 5 mukainen tarkastusoikeus. Tarkastusoikeuden käyttäminen ei saa vaarantaa HUSin tai kolmansien osapuolten tietoturvaa.

9.4 Sopimuksen muuttaminen tietoturvallisuuteen tai tietosuojaan liittyvästä syystä

#50 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.