Tietoturvallisuusliite –
HUS henkilötietojen käsittelijänä

v1.0

1 Tämän dokumentin tarkoitus ja soveltaminen

#1 Tämä dokumentti on sopijapuolten välistä yhteistyötä koskevan sopimuksen liite, jolla sovitaan henkilötietojen käsittelyyn liittyvistä seikoista, tietoturvasta ja salassapidosta. Tätä dokumenttia sovelletaan sopimuksessa mainitun sopimusasiakirjojen soveltamisjärjestyksen mukaisesti.

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 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.

#6 *Yhteistyötä koskeva sopimus:* Sopijapuolten välinen sopimus, jonka perusteella HUS käsittelee henkilötietoja.

#7 *Sopimus:* Ks. *Yhteistyötä kokeva sopimus*.

#8 *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.

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

3 Alihankkijat

#10 Tässä liitteessä HUSille ja HUSin palveluksessa oleville henkilöille asetetut velvoitteet koskevat myös HUSin alihankkijoita ja niiden palveluksessa olevia henkilöitä siltä osin kuin ne osallistuvat sopimuksen kohteen toteuttamiseen. HUSin on tiedotettava alihankkijoille näistä velvoitteista, ja HUS vastaa siitä, että alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat niitä. HUS vastaa käyttämänsä alihankkijan osuudesta kuten omastaan.

4 Yleiset velvollisuudet

4.1 Sopijapuolten velvollisuus noudattaa lainsäädäntöä

#11 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

#12 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

#13 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

#14 Sopijapuolen on ilman aiheetonta viivytystä ilmoitettava toiselle sopijapuolelle sellaisista sopijapuolen tietoon tulleista olennaisista seikoista, jotka voivat vaikuttaa sopimuksen kohteeseen liittyvään tietoturvallisuuteen, ja niiden aiheuttamista toimenpiteistä ja mahdollisista seurauksista. Tällaiset seikat voivat koskea muun ohella tietoturvariskejä, muutoksia turvajärjestelyissä, toteutuneita tietoturvaloukkauksia tai niiden yrityksiä, paikkaamattomia järjestelmähaavoittuvuuksia, palvelunestohyökkäyksiä sekä muita vastaavia poikkeamia, jotka ovat omiaan nostamaan tietoturvallisuuteen kohdistuvaa riskiä. Jos seikka liittyy henkilötietoihin, HUSin on pyrittävä ilmoittamaan tilaajalle asiaan liittyvien rekisteröityjen ryhmät ja arvioidut lukumäärät.

4.5 Tietoturvallisuuteen liittyvät tehtävät ja vastuut

#15 Sopijapuolten tulee määritellä organisaatiossaan tietoturvallisuuteen liittyvät tehtävät ja vastuut sekä nimetä kokemukseltaan ja pätevyydeltään riittävät vastuuhenkilöt ja ilmoittaa heidän yhteystietonsa toiselle sopijapuolelle tai julkisilla verkkosivuillaan.

4.6 Tietoturvaloukkaustilanteessa toimiminen

#16 Sopijapuolilla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen.

#17 HUS huolehtii häiriötilanteiden hallinnasta siten, että ongelman rajaus ja korjaus suoritetaan ilman aiheetonta viivytystä ohjeistuksen mukaisesti.

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

4.7 Sopijapuolten tietoturvallisuuteen liittyvät sisäiset ohjeet

#19 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

#20 HUS 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 sopimuksen perusteella laaditaan tai käsitellään potilasasiakirjoja, sopijapuolet sitoutuvat laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjoja koskeva lainsäädäntö edellyttää.

5.2 Käyttötarkoitus

#21 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 Tietoturvallisuustasot

#22 Jos tilaaja haluaa määritellä tilaajan aineistolle eri tietoturvallisuustasoja ja sen mukaisia erityisiä tietoturvatoimenpiteitä ja ohjeita, sopijapuolet neuvottelevat tarvittavista sopimusmuutoksista sopimuksen kohteen toteuttamiseksi uusien tietoturvallisuustasojen edellyttämällä tavalla.

5.4 Varmistukset ja palautukset

#23 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.

5.5 Tietopyynnöt

#24 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.

5.6 Tilaajan aineiston palauttaminen

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

5.7 Tilaajan aineiston hävittäminen

#26 Jos tilaajan aineisto on sopimuksen mukaisesti palautettu tilaajalle ja HUS ei ole sopimuksen, lain tai viranomaismääräyksen perusteella velvollinen säilyttämään jäljennöstä siitä, HUSin tulee omalla kustannuksellaan tietoturvallisella tavalla hävittää mahdolliset jäljennökset.

6 Henkilötietojen käsittely

6.1 HUSin oikeus käsitellä henkilötietoja

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

#28 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 tämän sopimuksen ja lainsäädännön sekä tilaajan erikseen antamien dokumentoitujen ohjeiden mukaisesti.

#29 Seuraavat seikat ilmenevät tarkemmin sopimuksesta, 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).

#30 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

#31 HUS sitoutuu noudattamaan henkilötietojen käsittelyssä voimassa olevaa tietosuojalainlainsäädäntöä ja sen perusteella annettuja viranomaismääräyksiä. HUS vakuuttaa tuntevansa esimerkiksi tietosuoja-asetuksen sisällön, mukaan lukien muun muassa 28 ja 32 artiklassa henkilötietojen käsittelijälle asetetut velvollisuudet.

#32 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

#33 Sopijapuolten 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. Esimerkiksi HUSin tulee huolehtia käsittelemiensä henkilötietojen asianmukaisesta suojaamisesta varmistaakseen niiden luottamuksellisuuden, eheyden ja saatavuuden sekä noudattaa sopimuksen kohteen toteuttamisessa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta.

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

6.4 Muiden henkilötietojen käsittelijöiden käyttäminen

#35 HUSin tulee ilmoittaa tilaajalle etukäteen, jos se käyttää henkilötietojen käsittelyssä alihankkijaa, ellei alihankkijan käyttäminen ilmene sopimuksesta tai siihen liittyvästä dokumentaatiosta. HUS vastaa siitä, että HUSin ja alihankkijan välillä on tehty asianmukainen sopimus, joka täyttää tietosuojalainsäädännön velvoitteet.

6.5 HUSin avustamis- ja tiedonantovelvollisuus

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

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

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

6.6 Henkilötietojen käsittely ulkomailla

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

#40 Jos HUSin alihankkija käsittelee tilaajan aineiston sisältämiä henkilötietoja Yhdysvalloissa tai muualla ETA-alueen ulkopuolella kuin EU-komission listaamissa luotettavissa maissa, sopijapuolet huolehtivat siitä, että ennen henkilötietojen käsittelyn aloittamista solmitaan tarvittava EU-mallilausekkeiden mukainen sopimus henkilötietojen käsittelystä.

#41 Jos EU-mallilausekkeiden mukaista sopimusta ei myöhemmin pidettäisi riittävänä osoituksena tietosuojaa koskevan lainsäädännön 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

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

#43 Sopijapuolen palveluksessa olevat 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.

#44 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

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

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

#47 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.

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

#49 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

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

9.2 Selosteiden laatiminen

#51 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

#52 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 ja lisätyöt

#53 Tietoturvallisuuteen tai tietosuojaan liittyvän lainsäädännön tai sen tulkintaa koskevien suositusten, ohjeistusten tai määräysten muuttuessa sopijapuolet tekevät tarpeelliset sopimusmuutokset ja toteuttavat ne.