

HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVA SOPIMUS

OSAPUOLET

Tilaaaja:

Toimittaja:

yhdessä “**Osapuolet**” ja erikseen “**Osapuoli**”.

SOPIMUKSEN TAUSTA JA TARKOITUS

Tämä sopimus on Osapuolten xx päivätyn työterveyshuollon palveluita koskevan sopimuksen (“Pääsopimus”) liitteenä X ja siten osa Pääsopimusta ja Osapuolia sitova.

Tässä Sopimuksessa määritellään Tilaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuoja koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan lukuun Tilaaajan toimiessa Rekisterinpitäjänä. Toimittajan ja Toimittajan edustajien, Toimittajan alihankkijat mukaan lukien, tulee noudattaa tämän Sopimuksen ehtoja Pääsopimuksen mukaisia palveluita toimittaessaan.

Tällä Henkilötietosopimuksella varmistetaan turvallisuusjärjestelyistä, salassapidosta ja tietoturvallisuudesta sopimalla, että henkilötietojen käsittely tapahtuu Pääsopimuksen mukaisessa palvelutuotannossa kulloinkin voimassa olevan lainsäädännön mukaisesti henkilötietojen koko elinkaaren ajan.

Toimittajan tulee noudattaa kulloinkin voimassa olevaa henkilötietojen käsittelyä ja tietosuoja koskevaa kotimaista lainsäädäntöä, EU:n yleistä tietosuoja-asetusta (679/2016) ja muita sovellettavaksi tulevia eurooppalaisia tai ulkomaisia tietosuojalakeja muutoksineen sekä tietosuojaviranomaisten määräyksiä ja ohjeita (yhdessä “Tietosuojalainsäädäntö”) kaikissa käsittelytoimenpiteissä. Toimittajan tulee myös noudattaa Tilaaajan tietosuojakäytännöistä tai muista Tilaaajan Toimittajalle kirjallisesti välitetyistä ohjeista johtuvia velvollisuuksia kaikissa käsittelytoimenpiteissä. Osapuolet ovat sopineet seuraavista seikoista:

- a) Osapuolten roolit
- b) Henkilötietojen käsittelyn tarkoitus ja luonne;
- c) Rekisteröityjen ryhmät ja henkilötietojen tyypit

EU:n yleisen tietosuoja-asetuksen (679/2016) 28 artiklan mukaisesti.

1. MÄÄRITELMÄT

Tässä sopimuksessa sovelletaan EU:n yleisen tietosuoja-asetuksen 4 artiklan mukaisia määritelmiä, ja lisäksi täydentävästi seuraavia määritelmiä:

“Tilaaajan Henkilötiedot” tarkoittavat mitä tahansa henkilötietoja, joita Toimittaja käsittelee Tilaaajan lukuun Osapuolten välisen sopimuksen perusteella.

“Henkilötiedot” tarkoittavat tietoja liittyen tunnistettavaan tai tunnistettavissa olevaan luonnolliseen henkilöön.

“Turvatoimenpiteet” tarkoittavat teknisiä ja organisatorisia toimenpiteitä, jotka ovat tarpeen Tietojen turvallisuuden varmistamiseksi, mukaan lukien erilaiset tekniset ja organisatoriset toimenpiteet.

“Palvelut” tarkoittavat palveluita, joita Toimittaja toimittaa Tilaajalle Osapuolten välisen Pääsopimuksen mukaisesti.

”Pääsopimus” tarkoittaa Osapuolten välillä xx allekirjoitettua työterveyspalveluita koskevaa sopimusta.

2. OSAPUOLTEN ROOLIT

Tilaaajan henkilöstön henkilötiedoista (”Tilaaajan henkilötiedot”) muodostuu työterveyshuollon asiakkuusrekisteri (”TTH:n asiakkuusrekisteri”). Tilaaajaan työ- tai muussa toimeksiantosuhteessa oleva työterveyshuollon palveluita käyttävä luonnollinen henkilö on tietosuojasetuksen tarkoittama rekisteröity.

Tilaaaja toimii TTH:n asiakkuusrekisterin osalta Rekisterinpitäjänä. Toimittaja toimii henkilötietojen käsittelijänä, kun se hyödyntää kyseisen rekisterin tietosisältöä Pääsopimuksen mukaisia Palveluita tuottaessaan.

Toimittajalle muodostuu oma erillinen rekisterinsä TTH:n asiakkuusrekisteriin kuuluvien henkilöiden terveystiedoista (”potilasrekisteri”), jolta osin Toimittaja on rekisterinpitäjä. Tässä Sopimuksessa ei säädetä potilasrekisteriä koskevista velvoitteista.

Mikäli Toimittaja hyödyntää kolmannen tahon tarjoamia palveluja (”alihankinta”) tai ryhmittymän jäsentä Tilaaajan henkilötietojen käsittelyssä, toimii myös kyseinen alihankkija tai ryhmittymän jäsen tietosuojasetuksen tarkoittamana henkilötietojen käsittelijänä suhteessa Tilaaajaan ja TTH:n asiakkuusrekisteriin.

Tilaaaja määrittelee tarvittaessa yhdessä Toimittajan kanssa henkilötietojen käsittelyn kohteen, luonteen ja tarkoituksen sekä henkilötietojen tyypit ja rekisteröityjen ryhmät käsittelytoimien selosteessa (”käsittelyseloste”), joka on tämän Henkilötietosopimuksen liitteenä. Toimittajan velvollisuutena on täyttää etenkin käsittelyselosteen kohdat 3–5. Tällä yhteistyövelvollisuudella ei tarkoiteta tietosuojasetuksen mukaista yhteisrekisterinpitäjyyttä, vaan sitä, miten Toimittaja Pääsopimuksen ja Henkilötietosopimuksen mukaisessa kokonaisuudessa huolehtii omalta osaltaan Tilaaajan henkilötietojen asianmukaisesta suojaamisesta.

Toimittajalla tulee olla myös oma henkilötietojen käsittelijän seloste käsittelytoimista, jota sen tulee noudattaa Tilaaajan Henkilötietoja käsitellessään. Tilaaajan henkilötietoja ei silti saa käsitellä tämän Henkilötietosopimuksen tai Tilaaajan kirjallisten ohjeiden kanssa ristiriitaisella tavalla vetoamalla Toimittajan omaan käsittelyselosteeseen, ellei Tilaaajan käsittelyseloste tai ohjeistus ole arvioitavissa ilmeisellä tavalla lainvastaiseksi

Tilaaaja vastaa käsittelyselosteen ja antamiensa kirjallisten ohjeiden tietosisällöstä, päivityksestä sekä saatavuudesta. Toimittaja on velvollinen avustamaan Tilaaajaa näiden laatimisessa ja päivittämisessä, mikäli käsittelyseloste tai kirjalliset ohjeet ovat puutteelliset tai Toimittaja epäilee niiden olevan ristiriidassa tietosuojalainsäädännön velvoitteiden kanssa.

Tilaaaja vastaa Rekisterinpitäjänä siitä, että rekisteröityjen henkilötietoja käsitellään lainmukaisella tavalla, mikä on myös pystyttävä osoittamaan. Toimittaja on velvollinen avustamaan Tilaaajaa osoitusvelvollisuuden noudattamisen toteen näyttämisessä esimerkiksi koostamalla kaikki sellaiset tiedot, joista henkilötietojen lainmukaisesti tapahtunut käsittely ilmenee.

Tilaaaja vastaa siitä, että rekisteröidyt voivat käyttää tietosuojasetuksessa mainittuja oikeuksiaan. Toimittaja on velvollinen avustamaan Tilaaajaa näissä toimenpiteissä.

Toimittajan ja sen henkilöstön on noudatettava tämän Henkilötietosopimuksen ehtoja Pääsopimuksen mukaisia Palveluita tuottaessaan siltä osin, kuin palvelutuotantoon kuuluu henkilötietojen käsittelyä.

3. TIETOJEN KÄSITTELYÄ KOSKEVAT YLEISET VELVOLLISUUDET

Toimittaja saa käsitellä Tilaaajan lukuun Henkilötietoja ainoastaan tämän Sopimuksen ja Tilaaajan antamien kirjallisten ohjeiden mukaisesti.

Toimittaja ei saa ilman Tilaaajan etukäteistä kirjallista suostumusta käyttää Tilaaajan Henkilötietoja mihinkään muuhun tarkoitukseen kuin Osapuolten sopimien Palveluiden toimittamiseen.

Toimittaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla se varmistaa, että Tilaaajan Henkilötietojen käsittely tapahtuu sopimuksen vaatimusten ja sovitujen käytäntöjen mukaisesti. Toimittajan tulee myös ottaa käyttöön asianmukaiset toimintatavat sen varmistamiseksi, ettei Henkilötietoja säilytetä pidempään kuin on tarpeen. Toimittajan vastuulla on huolehtia, että kaikki Henkilötiedot, joita Toimittaja käsittelee Pääsopimuksen mukaisten Palveluiden toimittamisen yhteydessä, ovat asianmukaisia, olennaisia, kohtuullisia, täsmällisiä ja ajantasaisia.

Henkilötietojen käsittelyssä tulee huomioida terveydenhuollon ja sairaanhoidon palvelujen tuottamista koskevan aineellisen lainsäädännön velvoitteet. Toimittajan tietojärjestelmän tulee täyttää sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa (9.2.2007/159, ”asiakastieto-laki”) asetut edellytykset, kun Tilaaajan henkilötietoja käsitellään kyseisessä tietojärjestelmässä. Tähän sisältyy muun ohella Toimittajan velvollisuus pitää erillistä lokirekisteriä asiakastietojen käytön ja tietojen luovutuksen seuraamiseksi.

Toimittajan tulee suorittaa kaikki tässä sopimuksessa sovitut tehtävät ilman erillistä veloitusta, ellei erikseen ole toisin kirjallisesti sovittu.

Toimittajan tulee varmistaa, että Toimittaja ja Toimittajan henkilöstö (mukaan lukien Toimittajan alihankkijoiden henkilöstö):

- käsittelee Henkilötietoja vain Tilaaajan antamien kirjallisten ohjeiden mukaisesti;
- ilmoittaa Tilaaajalle, mikäli se epäilee Tilaaajan ohjeistuksen rikkovan Tietosuojalainsäädäntöä;
- ryhtyy teknisiin ja organisatorisiin toimenpiteisiin henkilötietojen käsittelyn lainmukaisuuden varmistamiseksi sekä torjuakseen Henkilötietojen tahattoman tai tahallisen katoamisen, muutoksen, tuhoutumisen tai vahingoittumisen;
- avustaa Tilaaajaa Tietosuojalainsäädännön mukaisten lainsäädännöllisten tai muun sääntelyn mukaisten Tilaaajan vastuiden noudattamisen toteennäyttämässä;
- avustaa Tilaaajaa varmistamaan, että tietosuojasetuksen 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan;
- antaa Tilaaajalle kaikki sellaiset tiedot, jotka Tilaaaja tarvitsee täyttääkseen rekisteröityjen oikeudet tai noudattaakseen tietosuojaviranomaisten tiedonantoja ja pyyntöjä;
- varmistaa, että Henkilötietoja käsittelevät henkilöt ovat sitoutuneet salassapitovelvollisuuteen tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;
- ilmoittaa viipymättä Tilaaajalle kaikista rekisteröityjen, tietosuojavaltuutetun tai muun viranomaisen tiedusteluista;
- varmistaa järjestelmien ja palveluiden, joissa Henkilötietoa säilytetään tai käsitellään, luottamuksellisuuden, eheyden, saatavuuden ja palautettavuuden;
- toteuttaa tarvittavat Turvatoimenpiteet ja ylläpitää niitä jatkuvasti.

Toimittaja eivätkä sen mahdolliset alihankkijat eivät saa käsitellä Henkilötietoja Euroopan Unionin tai Euroopan Talousalueen ulkopuolisessa maassa ilman Tilaaajan nimenomaista suostumusta.

Työterveyshuoltopalveluiden tarjouspyyntö, Liite 7

Mikäli Palveluiden tarjoaminen tapahtuu tai Henkilötietoja muuten käsitellään Euroopan Unionin tai Euroopan Talousalueen ulkopuolisessa maassa Tilaajan antaman nimenomaisen suostumuksen perusteella, Toimittajan on varmistettava Tietosuojalainsäädännön noudattaminen kaikkien tiedon- siirtojen yhteydessä. Osapuolet sitoutuvat tekemään asianmukaiset, EU:n mallisopimusehtojen mukaiset sopimusjärjestelyt, kun Henkilötietoja siirretään kolmansiin maihin.

Toimittaja saa käsitellä Tilaajan henkilötietoja vain siinä laajuudessa, joka on välttämätöntä Pääsopimuksen mukaisten Palvelujen tuottamisessa, ja vain sen ajan, mitä Pääsopimuksen mukaisia Palveluja tuotetaan tai mitä laissa muutoin säädetään. Muunlainen Tilaajan henkilötietojen hyödyntäminen taikka vaitiolo- tai salassapitovelvollisuuden rikkominen ei ole sallittua.

Tilaajan henkilötietoja saavat käsitellä vain sellaiset Toimittajan henkilöstön jäsenet, joilla on siihen asianmukainen työhön liittyvä peruste. Toimittajan henkilöstön tulee olla tietoisia henkilötietojen käsittelyyn liittyvistä lainsäädännön velvoitteista sekä Tilaajan käsitte-lyselosteesta ja kirjallisista ohjeista.

Toimittajan on tehtävä vaitiolo- ja salassapitovelvollisuutta koskeva sopimus kaikkien henkilöstönsä jäsenten kanssa, jotka käsittelevät Tilaajan henkilötietoja. Vaitiolo- ja salassapitovelvollisuutta koskeva sopimus on tehtävä vain siltä osin, kuin Toimittajan henkilöstöä ei koske lakisääteinen salassapitovelvollisuus käsittelemiensä Tilaajan henkilötietojen osalta.

Toimittajalla ei ole oikeutta luovuttaa Tilaajan henkilötietoja fyysisinä kopioina taikka sähköisen tiedonsiirron tai teknisen käyttöyhteyden avulla kolmannelle ilman Tilaajan suostumusta, ellei lain- säädäntö nimenomaisesti salli tällaista tietojen luovuttamista.

Toimittajan on avustettava Tilaajaa tarvittaessa tietosuoja-asetuksen tarkoittamassa vaikutustenvaikutuksen tekemisessä ja ennakkokuulemisen suorittamisessa sekä näihin liittyvien asiakirjojen laatimisessa.

Mikäli Toimittaja havaitsee henkilötietojen käsittelyn kannalta keskeisiä riskejä tai muutoksia jo tunnistetuissa riskeissä, Toimittaja on velvollinen ilmoittamaan näistä seikoista Tilaajalle.

Kaikki tässä Henkilötietosopimuksessa olevat Toimittajaan tai Toimittajan henkilöstöön kohdistuvat ehdot koskevat identtisesti laajuudessa ilman erillistä mainintaakin myös Toimittajan mahdollisesti käyttämiä alihankkijoita tai ryhmittymän jäseniä sekä näiden molempien henkilöstöä.

4. TEKNISET JA ORGANISATORISET TOIMENPITEET

Toimittajan on suojattava Tilaajan henkilötiedot vahingossa tapahtuvalta tai lainvastaiselta tuhoamiselta, häviämiseltä, muuttamiselta sekä luvattomalta luovuttamiselta ja turvattava, etteivät ulkopuoliset kolmannet tahot pääse käsiksi kyseisiin tietoihin (”tietoturvaloukkaus”). Suojauksen turvallisuustason tulee olla korkea ottaen huomioon se, että Toimittaja käsittelee säännönmukaisesti myös erityisiin henkilötietoryhmiin kuuluvia terveystietoja.

Toimittajan tulee tietoturvan varmistamiseksi sekä tietoturvaloukkausten estämiseksi toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla taataan Tilaajan henkilötietojen jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä palautettavuus fyysisen tai teknisen vian satuttua. Tähän sisältyy myös velvollisuus säännöllisesti testata, tutkia ja arvioida teknisten ja organisatoristen toimenpiteiden riittävyys ja tehokkuus tarvittaessa tietosuoja-asetuksen tarkoittamaa hyväksytyä sertifiointimekanismia noudattamalla.

Tekniset toimenpiteet liittyvät esimerkiksi Toimittajan hyödyntämiin käyttö- ja tietojärjestelmiin ja ohjelmistoihin eli järjestelmäturvallisuuteen, tiedonsiirtoon ja -välittämiseen sekä näihin liittyviin salaustekniikoihin, erilaisiin ohjelmisto- ja komponenttipäivityksiin, päätelaitteiden suojaamiseen ja muihin vastaaviin tietoteknisiin tai tiedonhallinnollisiin ratkaisuihin, joiden tarkoituksena on tieto- turvan säilyttäminen, ylläpito ja parantaminen.

Organisatoriset toimenpiteet liittyvät Toimittajan hallinnollisiin ja fyysisiin tietoturvaratkaisuihin. Hallinnollisia keinoja ovat esimerkiksi laadunvarmistusjärjestelmät ja mahdolliset sertifiointit, henkilöstön säännöllinen kouluttaminen sekä salassapito- ja vaitiolovelvollisuutta koskevat sopimusehdot niin yritysten kuin luonnollisten henkilöiden kanssa tehtävissä sopimuksissa ja muut vastaavat ratkaisut. Fyysisiä keinoja ovat esimerkiksi Toimittajan toimitilojen turvallisuus ja kulkuoikeuksien kontrollointi sekä työntekijöiden että Toimittajalle tukitoimintoja tuottavien yhteistyökumppanien osalta, joiden avulla Toimittaja estää tarpeettoman ja luvattoman kulun toimitiloissaan.

Toimittajan on estettävä pääsy salassa pidettäviin Tilaajan henkilötietoihin, olipa kyse sitten fyysisistä asiakirjoista tai niiden kopiosta taikka sähköisistä tietojärjestelmistä, pilvipalveluista tai vastaavista tietoteknisistä tai tiedonhallinnollisista ratkaisuista.

Toimittajan on käytettävä tietoturvallisia ratkaisua Tilaajan henkilötietoja sisältävien asiakirjakopioiden, tiedostojen, metatietojen ja muiden vastaavien tuhoamisessa siltä osin, kuin kyse on tarpeettoman aineiston tuhoamisesta, ja Toimittaja on oikeutettu tuhoamaan kyseisen aineiston Tilaajan käsittelyselosteen tai muiden kirjallisten ohjeiden perusteella.

5. REKISTERÖITYJEN OIKEUKSIEN TOTEUTTAMINEN

Tämä kappaleen velvollisuudet koskevat yksistään Tilaajan TTH:n asiakkuusrekisteriä ja sen sisältämiin tietoihin kohdistuvia rekisteröityjen tekemiä pyyntöjä. Tässä kappaleessa Toimittajalle asetettuja velvollisuuksia ei sovelleta Toimittaja omaan potilasrekisteriin ja rekisteröityjen siihen kohdistamiin pyyntöihin, vaikka pyynnöntehtijänä olisi Tilaajan palveluksessa oleva rekisteröity.

Toimittajan tulee auttaa Tilaajaa teknisten ja organisatoristen toimenpiteiden avulla siinä, että Rekisterinpitäjä voi toteuttaa kaikki rekisteröityjen oikeudet esimerkiksi tekemällä Tilaajan henkilötietoihin oikaisuja, poistoja tai käsittelyn rajoittamista koskevia toimenpiteitä tai auttamalla rekisteröityä omien henkilötietojensa siirtämisessä järjestelmästä toiseen.

Toimittajan tietosuojavastaava toimii tarvittaessa rekisteröityjen oikeuksien toteuttamiseen liittyvissä asioissa yhteyshenkilönä ja antaa Tilaajalle asiantuntija-apua, ellei Toimittaja ole osoittanut tätä nimenomaista tehtävää oman organisaationsa puitteissa jollekulle toiselle henkilölle. Siinä tilanteessa kyseinen henkilö vastaa edellä mainituista tehtävistä. Toimittaja on tällöin velvollinen ilmoittamaan kyseisen henkilön yhteystiedot Tilaajalle.

Mikäli Toimittaja vastaanottaa rekisteröidyltä oikeuksiensa käyttämistä koskevan pyynnön, Toimittajan on ilmoitettava siitä Tilaajalle viipymättä ja viimeistään kahden työpäivän kuluessa pyynnön saapumisesta. Toimittajan tulee pyyntöä vastaanottaessaan pyrkiä varmistamaan rekisteröidyn henkilöllisyys tai antamaan ohjeita rekisteröidylle siitä, miten tämä voi osoittaa henkilöllisyytensä.

Toimittajan tulee organisoida toimintansa siten, että Tilaaja pystyy vastaamaan rekisteröityjen pyyntöihin kuukauden kuluessa pyynnön vastaanottamisesta riippumatta siitä, onko pyyntö saapunut Toimittajalle vai Tilaajalle.

Toimittajan tulee luetteloida kaikki rekisteröityjen pyynnöstä tehdyt toimenpiteet. Dokumentoinnista tulee ilmetä ajankohtien lisäksi, mitä on pyydetty, mitä tietoa on mahdollisesti muutettu, oikaistu tai poistettu, ja mille kaikille tahoille tästä on ilmoitettu.

6. HENKILÖTIETOJEN SIIRTÄMINEN

Toimittaja ei saa käsitellä Tilaaajan henkilötietoja Euroopan unionin tai Euroopan talousalueen ulko- puolisessa maassa ilman Tilaaajan nimenomaista suostumusta.

Käsittelyllä tarkoitetaan tässä kohtaa esimerkiksi palvelinten sijaintimaata, pilvipalvelujen tallennuspaikkaa ja vastaavia teknisiä tai tiedonhallinnollisia ratkaisuja, joiden avulla Tilaaajan henkilötiedot siirtyvät Euroopan unionin tai talousalueen maantieteellisen alueen ulkopuolelle. Sama koskee esimerkiksi pääsyn sallimista Tilaaajan henkilötietoihin teknisen etäyhteyden avulla kyseisen maan- tieteellisen alueen ulkopuolella olevista paikoista.

Mikäli Tilaaajan henkilötietoja käsiteltäisiin Euroopan unionin tai Euroopan talousalueen ulkopuolisessa maassa Tilaaajan antaman nimenomaisen suostumuksen perusteella, Toimittajan on varmistettava lainsäädännön noudattaminen kaikkien tiedonsiirtojen yhteydessä.

Osapuolet sitoutuvat tekemään asianmukaiset, tämän Henkilötietosopimuksen sekä EU:n mallisopimusehtojen mukaiset sopimusjärjestelyt, kun Tilaaajan henkilötietoja siirretään kolmansiin maihin.

7. AUDITOINNIT

Tilaaajalla on oikeus järjestää auditoinnit Henkilötietojen käsittelytoimintoihin liittyen Toimittajan tiloissa kustannuksellaan. Auditointien yhteydessä selvitetään, täyttyvätkö tämän Sopimuksen ja Pääsopimuksen mukaisesti Henkilötietojen käsittelystä asetetut vaatimukset, turvatoimenpiteet, suojan taso ja turvallisuus. Tarkastuksen yhteydessä voidaan myös arvioida Toimittajan ja sen alihankkijoiden tämän Sopimuksen ja Pääsopimuksen noudattamista. Toimittaja takaa Tilaaajalle samat oikeudet suhteessa Toimittajan alihankkijoihin. Mahdolliset Tilaaajan suorittamat tarkastukset eivät rajoita Toimittajan tai sen alihankkijoiden tämän Sopimuksen tai Pääsopimuksen mukaisia velvollisuuksia ja vastuita.

8. TIETOTURVALOUKKAUKSET

Toimittajan tulee ilman aiheetonta viivästystä ilmoittaa Tilaaajalle kirjallisesti kaikista Tilaaajan Tietoihin kohdistuneista tietoturvaloukkauksista ("Tietoturvaloukkaus"). Toimittajan Tietoturvaloukkausta koskevan Tilaaajalle tekemän ilmoituksen tulee sisältää vähintään:

- a) kuvaus Tietoturvaloukkauksen luonteesta;
- b) asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat tiedossa;
- c) tietoturvaloukkauksen tehneen toimijan tunnistaminen sekä niiden osapuolten tiedot, jotka ovat saaneet pääsyn, tarkastelleet, käyttäneet tai vastaanottaneet tietoa Tietoturvaloukkauksen johdosta;
- d) kuvaus korjaavista toimenpiteistä, jotka Toimittaja on suorittanut tai tulee suorittamaan Tietoturvaloukkausten ennaltaehkäisemiseksi jatkossa;
- e) kuvaus tietoturvaloukkauksen todennäköisistä seurauksista
- f) kuvaus Toimittajan suorittamista toimista haittavaikutusten minimoimiseksi ja lieventämiseksi.

Toimittajan on dokumentoitava kaikki Tietoturvaloukkaukset, mukaan lukien kuhunkin Tietoturvaloukkaukseen liittyvät tosiseikat, vaikutukset ja tehdyt korjaavat toimenpiteet. Tilaaajan tulee pystyä dokumentaation perusteella varmistamaan Tietosuojalainsäädännön noudattaminen.

9. KOLMANSIEN OSAPUOLIEN KÄYTTÄMINEN TIETOJEN KÄSITTELYSSÄ

Toimittajalla on oikeus käyttää alihankkijaa Henkilötietojen käsittelyssä. Toimittaja on velvollinen ilmoittamaan Tilaajalle kaikista suunnitelluista muutoksista, jotka koskevat muiden Henkilötietojen käsittelijöiden lisäämistä tai vaihtamista ja annettava Tilaajalle mahdollisuus vastustaa tällaisia muutoksia.

Mikäli Toimittajan käyttää alihankkijaa Tilaajan Tietoihin sisältyvien Henkilötietojen käsittelyyn, tulee Toimittajan noudattaa seuraavia ehtoja:

- a) Toimittajalla ja sen alihankkijalla on kirjallinen sopimus;
- b) kirjallinen sopimus velvoittaa alihankkijan noudattamaan samoja velvollisuuksia, sitoumuksia ja kuvauksia, jotka tämän Sopimuksen, sen liitteiden ja sen perusteella annettujen ohjeiden sekä Tietosuojalainsäädännön mukaan soveltuvat Toimittajaan; ja
- c) Tilaajalla on samat oikeudet alihankkijaa kohtaan kuin Toimittajaa kohtaan.

Toimittaja vastaa alihankkijoidensa toimista ja laiminlyönneistä suhteessa Tilaajaan kuin omista toimistaan ja laiminlyönneistään.

10. HENKILÖTIETOJEN POISTAMINEN JA PALAUTTAMINEN TILAAJALLE

Toimittaja ei saa poistaa Tilaajan lukuun käsittelemiään Henkilötietoja ilman Tilaajan nimenomaista pyyntöä. Tilaajalla on oikeus, milloin tahansa, saada kirjallisella pyynnöllä Toimittajan käsittelemät Henkilötiedot tai ote tai kopio niistä.

Toimittajan tulee palauttaa Tilaajalle tai, mikäli Tilaaja niin päättää, tuhota Tilaajan Henkilötiedot Tilaajan pyynnöstä tämän Sopimuksen päättymisen yhteydessä taikka kun Tilaajan Henkilötietojen käsittely ei ole enää tarpeen palveluiden toimittamista varten. Mikäli Henkilötiedot palautetaan Tilaajalle ja ellei toisin ole sovittu, Henkilötiedot tulee palauttaa Tilaajalle muodossa, jossa Henkilö- tiedot alun perin toimitettiin Toimittajalle Tilaajan toimesta. Mikäli Toimittajan tulee Tilaajan pyynnöstä tuhota Henkilötiedot, tuhoaminen tulee varmentaa kohtuullisen ajan kuluessa siitä, kun tuhoaminen on tehty.

Toimittaja ei saa poistaa Henkilötietoja, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Toimittaja säilyttää henkilötiedot.

11. YHTEISTYÖVELVOITE

Toimittajan velvollisuutena on tehdä yhteistyötä Tilaajan kanssa tietosuojalainsäädännön mukaisten velvoitteiden toteuttamiseksi. Toimittaja avustaa tarpeen mukaan Tilaajaa rekisteröityjen oikeuksien toteuttamisessa Tilaajan ohjeiden mukaan, ja toimittaa Tilaajalle viipymättä selkaiset tiedot käsittelystä, joita Tilaaja tarvitsee täyttääkseen velvoitteensa suhteessa rekisteröityyn.

12. VASTUU

Toimittaja sitoutuu maksamaan sopimussakkoa Tilaajalle yhteensä 20 000 euroa / rikkomus, joka on seurausta Toimittajan tai Toimittajan alihankkijan tähän sopimukseen kohdistuvasta sopimusrikkomuksesta ja/tai Tietosuojalainsäädännön rikkomisesta. Lisäksi Toimittaja on velvollinen korvaamaan Tilaajalle Toimittajan rikkomuksesta aiheutuneen välittömän vahingon. Toimittaja on velvollinen korvaamaan myös välillisen vahingon, mikäli rikkomus johtuu Toimittajan tahallisuudesta tai törkeästä huolimattomuudesta.

Mikäli valvontaviranomainen langettaa sakkoja, joiden perusteena on Henkilötietojen käsittelyä koskevien määräysten rikkominen, vastaa sakoista aina yksin se Osapuoli, jolle sakot on määrätty.

Työterveyshuoltopalveluiden tarjouspyyntö, Liite 7

Se Osapuoli joka on maksanut rekisteröidylle korvauksen tietosuojalainsäädännön rikkomisen johdosta aiheutuneesta vahingosta, on oikeus, sovittujen vastuunrajoitusten rajoittamatta, periä toiselta Osapuolelta tämän vahingonkorvausvastuuta vastaava osuus. Osapuolen vastuu rekisteröidylle aiheutuneesta vahingosta määräytyy EU:n yleisen tietosuoja-asetuksen 82 artiklan mukaan.

Muilta osin Sopimuksen rikkomisen osalta tai tietosuoja-asetukseen liittyvään muuhun vaatimukseen liittyvä vastuu määritellään Osapuolten välisessä Palvelusopimuksessa. Väilisiä vahinkoja ei korvata.

13. VOIMASSAOLO

Tämä Sopimus on voimassa, kunnes Toimittaja on lopettanut Tilaajan Tietojen ja Henkilötietojen käsittelyn Osapuolten välisen Pääsopimuksen perusteella ja suorittanut käsittelyn päättämiseen liittyvät velvollisuudet.

X __.__.2023

X __.__.2023

Liite 1: HENKILÖTIETOJEN KÄSITTELYTOIMIEN SELOSTE**1. KÄSITTELYPERUSTE, LUONNE, TARKOITUS JA KESTO**

Rekisterinpitäjän lukuun tapahtuva henkilötietojen käsittely perustuu:

- Rekisteröidyn suostumukseen (tietosuoja-asetuksen 6 artiklan 1 a kohta); ja/tai
- Rekisterinpitäjän lakisääteiseen velvoitteeseen (tietosuoja-asetuksen 6 artiklan 1 c kohta).

Rekisterinpitäjällä on lakisääteinen velvollisuus järjestää työterveyshuolto työntekijöilleen. Henkilötietojen käsittelyn tarkoitus liittyy tähän Pääsopimuksen mukaisiin velvoitteisiin, joista Tilajana oleva Rekisterinpitäjä ja Toimittaja ovat keskenään sopineet.

Rekisterinpitäjän työntekijöiden ja asiakkaiden henkilötietoja käsitellään vain siinä laajuudessa kuin Pääsopimuksen mukaisten Palvelujen tuottamiseksi on tarpeen. Henkilötietoja käsitellään vain sen ajan, kun Pääsopimus on voimassa, ellei erikseen muuta sovita esimerkiksi Rekisterinpitäjän tekemän tietojen tuhoamispyynnön seurauksena.

2. REKISTERÖITYJEN RYHMÄT JA HENKILÖTIETOJEN TYYPIT

Toimittaja käsittelee Rekisterinpitäjän pyynnöstä Asiakkuusrekisteriin kuuluvia henkilötietoja.

Käsiteltävät henkilötietojen tyypit ovat:

- Rekisteröityjen yksilöintitiedot, kuten nimi, henkilötunnus ja ammattinimike
- Erityisiin henkilötietoryhmiin kuuluvat rekisteröityjen terveystiedot, joita ovat terveydentilaa koskevat tiedot, sairauspoissaolotiedot ja mahdolliset työkykyä koskevat lääkärintodistukset ja -lausunnot
- *Muut tiedot [täydennetään].*

3. ALIHANKKIJAT

Toimittaja käyttää Rekisterinpitäjän henkilötietojen käsittelyssä alihankkijoita seuraavien tehtävien suorittamisessa:

- *[Täydennetään, jos käytetään alihankintaa]*
- *[Poistetaan, jos ei käytetä alihankintaa]*

4. KUVAUS TEKNISISTÄ JA ORGANISATORISISTA TOIMENPITEISTÄ

Toimittaja hyödyntää seuraavia teknisiä keinoja henkilötietojen käsittelyssä ja suojaamisessa:

- *[Täydennetään]*

Toimittaja hyödyntää seuraavia organisatorisia keinoja henkilötietojen käsittelyssä ja suojaamisessa:

- *[Täydennetään]*

5. HENKILÖTIETOJEN KÄSITTELYPAIKKA

Toimittaja käsittelee Rekisterinpitäjän henkilötietoja seuraavissa paikoissa:

- *[Täydennetään]*