

12.6.2019

Palvelutuotannon tietoturvallisuussitoumus

Sosiaali- ja terveystoimi

1. Salassapito ja vaitiolovelvollisuus

Heinolan kaupungille palveluja tuottavan yksityisen organisaation on noudatettava salassapitovelvollisuutta liittyen käsittelemiinsä asiakas- ja henkilötietoihin.

Salassapitovelvollisuus on lakisääteinen ja siitä säädetään EU:n tietosuoja-asetuksessa (GDPR), tietosuojalaissa, julkisuuslaissa sekä sosiaalihuollon ja terveydenhuollon lainsäädännössä.

Heinolan kaupungin sosiaali- tai terveydenhuollon asiakkaita koskevia salassa pidettäviä tietoja ei saa luovuttaa sivullisille palvelutuotannon aikana tai sen päätyttyä. Salassa pidettävillä tiedoilla tarkoitetaan myös sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja. Sivullisilla tarkoitetaan muita kuin asianomaisessa toimintayksikössä potilaan hoitoon tai asiakkaan asian hoitamiseen osallistuvia henkilöitä. Salassapito koskee myös harjoittelijoita tai muita henkilöitä, jotka toimivat terveyden- tai sosiaalihuollon järjestäjän tai tuottajan toimeksiannosta.

2. Käyttäjätunnus Heinolan kaupungin tietojärjestelmiin tai muihin resursseihin

Jos palveluntuottaja toiminnassaan tarvitsee käyttäjätunnuksia Heinolan kaupungin tietojärjestelmiin, siitä sovitaan rekisterinpitäjän edustajan valtuutuksen perusteella Heinolan tietohallinnon kanssa. Heinolan kaupungin asiakas- ja potilasjärjestelmien käyttöoikeudet annetaan vain tietoturvallisuussitoumuksen allekirjoittaneille henkilöille. Käyttäjätunnukset ovat aina henkilökohtaisia.

12.6.2019

3. Laitteiden ja ohjelmistojen asentaminen ja käyttö

Heinolan kaupungin sisäisiin tietoverkkoihin ei lähtökohtaisesti saa liittää palveluntuottajan omia laitteita tai ohjelmistoja. Näistä sovitaan erikseen Heinolan tietohallinnon kanssa.

4. Sähköpostin käyttö ja laskutusmerkinnät

Salassapidettäviä tietoja ei saa lähettää suojaamattomassa sähköpostissa. Laskulla ei lähtökohtaisesti saa näkyä asiakkaan henkilötunnusta. Vaadittaessa asiakkaan yksilöintiä, henkilötunnus tai ainakin syntymäaika tulee kuitenkin voida todentaa. Salassapidettäviä tietoja sisältävät asiakirjat kuten laskujen liitteet tulee lähettää salatulla sähköpostilla tai kirjeitse.

5. Seuraamukset tietoturvallisuuden vaarantamisesta ja potilas- ja asiakastietojen väärinkäytöstä

Potilas- tai asiakastietojärjestelmien tietojen lainvastainen käsittely tai tietosuojan rikkominen voi johtaa oikeudellisiin seuraamuksiin. Myös EU:n tietosuoja-asetuksessa säädetään mahdollisista sanktioista.

Olemme perehtyneet yllä oleviin palvelutuotantoon liittyviin Heinolan kaupungin tietoturvallisuusohjeisiin ja sitoudumme palveluntuottajaorganisaationa noudattamaan niitä. Palveluntuottajana vastaamme siitä, että työntekijämme toimivat tässä sitoumuksessa edellytetyllä tavalla. Lisäksi vastaamme ja huolehdimme siitä, että käyttämämme mahdolliset alihankkijat noudattavat tässä tietosuojasitoumuksessa esitettyjä periaatteita ja sääntöjä.

Paikka ja päiväys _____

Palveluntuottajaorganisaation nimi ja Y-tunnus _____

12.6.2019

Yhteys henkilön nimi ja ammattinimike* _____

Allekirjoitus ja nimen selvennys _____

*henkilö, jolla on kyseiseen palvelutuotantoon liittyvien sopimusten allekirjoitusoikeus

12.6.2019

Henkilötietojen käsittelyn ehdot

Sosiaali- ja terveystoimi

Sopimusehdot

Palveluntuottaja noudattaa voimassa olevan tietosuojalainsäädännön edellyttämiä menettelytapoja ja henkilötietojen käsittelyä ja suojaamista koskevia säännöksiä.

Palveluntuottaja vastaa siitä, että palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön ja sopimuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta on säädetty. Tilaaja on rekisterinpitäjä. Palveluntuottaja noudattaa henkilötietojen käsittelijänä tämän sopimuksen liitteenä olevia ehtoja henkilötietojen käsittelystä.

1. Yleistä

- 1.1. Tämä sopimusliite ”Henkilötietojen käsittelyn ehdot” on osa sopimusta, jonka Tilaaja on tehnyt Palveluntuottajan kanssa.
- 1.2. Tässä sopimusliitteessä määritellään Tilaajaa ja Palveluntuottajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Palveluntuottaja Tilaajan toimeksiannosta käsittelee henkilötietoja Tilaajan puolesta. Näissä ehdoissa kuvatuista Palveluntuottajan toimenpiteistä ja velvollisuuksista ei suoriteta erillistä korvausta, ellei toisin ole näissä ehdoissa sovittu.

2. Osapuolten roolit henkilötietojen käsittelyssä

- 2.1. Käsiteltäessä henkilötietoja Tilaaja on rekisterinpitäjä ja Palveluntuottaja on henkilötietojen käsittelijä (jäljempänä myös ”käsittelijä”), ellei henkilötietojen käsittelyn tarkoituksesta muuta johdu. ”Tilaajan henkilötiedoilla” tarkoitetaan näissä ehdoissa henkilötietoja, joista Tilaaja vastaa rekisterinpitäjänä.

12.6.2019

2.2. Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän ja käsittelijän velvollisuudet ja oikeudet kuvataan näiden ehtojen liitteessä 1 olevassa Käsittelytoimien kuvauksessa tai muussa Tilaajan ohjeistuksessa. Palveluntuottaja sitoutuu noudattamaan Sopimuksessa, käsittelytoimien kuvauksessa ja ohjeistuksessa olevia ehtoja ja kuvauksia. Tilaaja vastaa ohjeistuksen ylläpidosta ja saatavuudesta.

2.3. Jos kohdan 2.2 mukaista käsittelytoimien kuvausta ei ole tehty tai se on puutteellinen, Tilaaja laatii tai täydentää käsittelytoimien kuvausta tarvittaessa yhteistyössä Palveluntuottajan kanssa.

3. Palveluntuottajan yleiset velvollisuudet

3.1. Palveluntuottaja käsittelee henkilötietoja Sopimuksen ja Tilaajan antamien ohjeiden mukaisesti. Ryhmittymän ollessa Käsittelijänä tämän sopimusliitteen velvoitteet koskevat kaikkia ryhmittymän jäseniä, ja ryhmittymän käyttämiä alihankkijoita, jotka osallistuvat henkilötietojen käsittelyyn.

3.2. Palveluntuottaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla se varmistaa, että Tilaajan henkilötietojen käsittely tapahtuu sopimuksen vaatimusten ja sovittujen käytäntöjen mukaisesti. Toimenpiteiden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä käsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus.

3.3. Palveluntuottaja ei käsittele eikä muulla tavoin hyödynnä sopimuksen perusteella käsittelemiään henkilötietoja muutoin kuin sopimuksen täyttämisen mukaisessa tarkoituksessa ja laajuudessa.

3.4. Palveluntuottaja nimeää tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön Tilaajan henkilötietoihin liittyviä yhteydenottoja varten. Palveluntuottaja ilmoittaa kirjallisesti tietosuojavastaavan tai yhteyshenkilön yhteystiedot Tilaajalle.

12.6.2019

- 3.5. Palveluntuottaja saattaa Tilaajan saataville tämän pyynnöstä kaikki tiedot, jotka Tilaaja tarvitsee rekisterinpitäjälle ja Palveluntuottajalle säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja osallistuu pyydettyä sovitulla tavalla Tilaajan vastuulla olevien kuvausten ja muiden dokumenttien, kuten vaikutustenarvioinnin, laatimiseen ja yllä-pitämiseen sekä tietosuoja-asetuksen mukaisen ennakkokuulemisen suorittamiseen. Palveluntuottaja tekee nämä tehtävät sopimuksen mukaisilla hinnoilla, ellei toisin sovita.
- 3.6. Palveluntuottaja ilmoittaa Tilaajalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Palveluntuottaja ei itse vastaa näihin pyyntöihin. Palveluntuottaja avustaa Tilaajaa, jotta Tilaaja pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyyntöt voivat edellyttää Palveluntuottajalta esimerkiksi avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen. Ellei toisin ole sovittu, Palveluntuottajalla on oikeus laskuttaa Tilaajaa sopimuksessa sovitulla hinnoilla, jos avustaminen aiheuttaa lisäkuluja Palveluntuottajalle. Palveluntuottaja on velvollinen ennakolta ilmoittamaan Tilaajalle mahdollisesti aiheutuvista lisäkuluista.
- 3.7. Palveluntuottaja sallii Tilaajan tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin. Tarkastusmenettelyä koskevat tarkemmat ehdot ovat sopimuksessa.

4. Tilaajan ohjeet

- 4.1. Palveluntuottaja noudattaa Tilaajan henkilötietojen käsittelyssä sopimuksessa ja näissä erityisehdoissa sovitut ehtoja sekä Tilaajan kirjallisia ohjeita. Tilaaja vastaa ohjeiden ylläpidosta ja saatavuudesta. Palveluntuottaja ilmoittaa ilman

12.6.2019

aiheetonta viivytystä Tilaajalle, jos Tilaajan antamat ohjeet ovat puutteellisia tai jos Palveluntuottaja epäilee niitä lainvastaisiksi.

4.2. Tilaajalla on oikeus muuttaa, täydentää ja päivittää Palveluntuottajalle antamia henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Jos ohjeiden muutoksista aiheutuu sopimuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovitaan sopimuksen mukaisessa muutoshallintamenettelyssä.

5. Palveluhenkilöstö

5.1. Palveluntuottaja varmistaa, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä Tilaajan henkilötietoja, ovat sitoutuneet noudattamaan sopimuksessa sovittuja salassapitoehtoja tai heitä koskee lakisääteinen salassapitovelvollisuus.

5.2. Palveluntuottaja varmistaa, että jokainen sen alaisuudessa toimiva henkilö, jolla on pääsy Tilaajan henkilötietoihin, on tietoinen henkilötietojen käsittelyyn liittyvistä velvoitteistaan ja käsittelee niitä ainoastaan sopimuksen, näiden erityisehtojen ja Tilaajan ohjeiden mukaisesti.

6. Alihankkijat, jotka käsittelevät henkilötietoja

6.1. Siltä osin kuin Palveluntuottaja käyttää toiminnassaan alihankkijoita, jotka käsittelevät henkilötietoja, alihankintaan sovelletaan Sopimuksen lisäksi tässä sopimusliitteessä kuvattuja ehtoja.

6.2. Jos Palveluntuottajan alihankkija käsittelee Tilaajan henkilötietoja, alihankkijan käyttäminen edellyttää Tilaajan ennakkoon kirjallisesti antamaa lupaa.

6.3. Palveluntuottaja tekee alihankkijan kanssa kirjallisen sopimuksen, jossa se sitouttaa käyttämänsä alihankkijat noudattamaan omalta osaltaan sopimuksessa Palveluntuottajalle asetettuja velvoitteita sekä Tilaajan antamia kulloinkin voimassa

12.6.2019

olevia henkilötietojen käsittelyyn liittyviä ohjeita. Palveluntuottaja varmistaa, että sopimuksen mukainen Tilaajan tarkastusoikeus voidaan ulottaa alihankkijaan.

6.4. Palveluntuottaja vastaa käyttämänsä alihankkijan osuudesta kuin omastaan. Palveluntuottaja vastaa siitä, että alihankkija noudattaa omalta osaltaan henkilötietojen käsittelijälle asetettuja velvoitteita. Jos Tilaaja perustellusti katsoo, että Palveluntuottajan alihankkija ei täytä tietosuojavelvoitteitaan, Tilaajalla on oikeus vaatia Palveluntuottajaa vaihtamaan alihankkijaa.

6.5. Henkilötietojen käsittelyyn osallistuvan alihankkijan vaihtamisesta on ilmoitettava Tilaajalle etukäteen. Ilmoituksessa tulee kuvata, miten alihankkija käsittelee Tilaajan henkilötietoja tietosuojalainsäädännön mukaisesti. Tilaajalla on oikeus perustellusta syystä vastustaa ehdotettua alihankkijaa.

7. Palvelun paikka

7.1. Ellei palvelun tuottamispaikasta ole toisin sovittu, Palveluntuottajalla on oikeus käsitellä Tilaajan henkilötietoja ainoastaan Euroopan talousalueella. Mitä sopimuksessa ja näissä erityisehdoissa sovitaan henkilötietojen käsittelystä, koskee myös pääsyn mahdollistamista Tilaajan henkilötietoihin esimerkiksi hallinta- ja valvontayhteyden välityksellä.

7.2. Jos sopijapuolet sopivat, että Palveluntuottajaa saa siirtää Tilaajan henkilötietoja Euroopan talousalueen ulkopuolelle, sopijapuolet huolehtivat siitä, että henkilötietojen siirto toteutetaan lainsäädännön mukaisesti.

8. Tietoturvaloukkaukset

8.1. Palveluntuottajan on ilmoitettava Tilaajalle kirjallisesti tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä. Lisäksi Palveluntuottaja sitoutuu ilmoittamaan Tilaajalle ilman aiheetonta viivytystä muista

12.6.2019

palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.

8.2. Palveluntuottajan on annettava Tilaajalle vähintään seuraavat tiedot tietoturvaloukkauksesta:

- i. tapahtuneen tietoturvaloukkauksen kuvaus, mukaan lukien asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat tiedossa;
- ii. tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;
- iii. kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja
- iv. kuvaus toimenpiteistä, joita Palveluntuottaja ehdottaa tai joita se on jo toteuttanut tietoturvaloukkauksen johdosta, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

8.3. Henkilötietojen tietoturvaloukkauksen havaittuaan Palveluntuottaja ryhtyy viipymättä sopimuksessa sovittuihin toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.

9. Henkilötietojen käsittelyn päättymisen

9.1. Sopimuksen voimassaoloaikana Palveluntuottaja ei saa poistaa Tilaajan lukuun käsittelemiään henkilötietoja ilman Tilaajan nimenomaista pyyntöä.

9.2. Sopimuksen päättyessä tai purkautuessa Palveluntuottaja palauttaa Tilaajalle kaikki Tilaajan puolesta käsitellyt henkilötiedot sekä hävittää omilta taltioiltaan mahdolliset kopiot henkilötiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

12.6.2019

Käsittelytoimien kuvaus

Sosiaali- ja terveystoimi

1. Sopimuksen osapuolet

Sopimuksen nimi ja diaarinumero:

Sopimuksen voimassaoloaika:

Tilaaaja (rekisterinpitäjä): Heinolan kaupunki, sosiaali- ja terveyslautakunta

Palveluntuottaja (henkilötietojen käsittelijä):

Mahdollinen alihankkija:

Palveluntuottajan tietosuojavastaava:

2. Dokumentin tarkoitus

Tilaaaja on tehnyt Palveluntuottajan kanssa Sopimuksen, joka koskee sellaista palvelua, jossa Palveluntuottaja toimii Tilaaajan ylläpitämään henkilökisteriin kuuluvien henkilötietojen käsittelijänä. Tässä dokumentissa kuvataan käsittelytoimet, joita palveluntuottaja henkilötietojen käsittelijänä tekee Tilaaajan puolesta, henkilötietojen tyypit sekä käsiteltävät henkilötiedot. Henkilötietojen käsittelyssä on noudatettava Palveluntuottajan ja Tilaaajan välistä Sopimusta sekä Tilaaajan ohjeita.

3. Henkilötietojen tyypit ja rekisteröityjen ryhmät

Osapuolet ovat sopineet, että Palveluntuottaja käsittelee Tilaaajan puolesta

Sopimuksessa sovitun palvelun tuottamiseksi seuraavia Asiakkaan henkilökisteriin kuuluvia henkilötietoja:

Ohje: kirjoita tähän, mitä rekisteröityjen ryhmiä Palveluntuottaja käsittelee, esim. Tilaaajan työntekijät



12.6.2019

Ohje: täydennä tähän, mitä henkilötietoja Palveluntuottaja käsittelee. Esim. Tilaajan työntekijän nimi ja käyttäjätunnus jne.



12.6.2019

Käsittelyn luonne ja tarkoitus

Osapuolet ovat sopineet, että Palveluntuottaja:

Ohje: kirjoita tähän, miksi ja miten Palveluntuottaja käsittelee kyseisiä henkilötietoja.

4. Henkilötietojen käsittelyn kesto

Palveluntuottaja käsittelee tässä liitteessä yksilöityjä henkilötietoja seuraavan ajan:

Ohje Tilaajalle: kuvaa tähän henkilötietojen käsittelyn kesto Palveluntuottajalla. HUOM! Palveluntuottaja sopii yhdessä rekisterinpitäjän kanssa henkilötietojen toimittamisesta rekisterinpitäjälle tietoturvaisella tavalla.