

Tietosuojavastaava, Hankintatoimisto

1.10.2019

Saate

SAATE – PÄIJÄT-HÄMEEN HYVINVOINTIKUNTAYHTYMÄN KÄYTTÄMÄ GDPR-LIITE SOPIMUKSIIN

Päijät-Hämeen hyvinvointikuntayhtymän (PHHYKY) sopimukseen liitettävä **GDPR-liite täydentää** yhtymässä käytössä olevaa **palvelutuotannon tietoturvaluussitoutumusta** (4. versio 1.10.2019) 25.5.2018 voimaan astuneen EU:n tietosuojasetuksen (GDPR) osalta.

GDPR-liitettä **käytetään palvelutuotannon tietoturvaluussitoutumuksen lisäksi siinä tapauksessa, että palvelutuotantoon liittyy henkilötietojen käsittelyä**. Palvelutuotannon tietoturvaluussitoutumus pätee sellaisenaan sopimuksen liitteenä.

Hyvinvointiyhtymän käyttämä GDPR-liite on pienin muutoksin käyttöön otettu Kuntaliiton julkaisu Henkilötietojen käsittelyn ehdot (versio 4.0 maaliskuu 2018)¹.

Kuntaliiton GDPR-liitteeseen kuuluu myös **henkilötietojen käsittelyä koskeva tarkempi lisäliite, Käsittelytoimien kuvaus** (Liite 1 Henkilötietojen käsittelyn ehtoihin).

Rekisterinpitäjän tulee aina kulloinkin olla tietoinen palvelutuotantoon kuuluvaan toimintaan liittyvästä **henkilötietojen käsittelystä**². Palveluntuottajan edellytetään täyttävän henkilötietojen käsittelyä koskevan lisäliitteen yhteistyössä tilaajan (rekisterinpitäjän) kanssa ilman erillistä korvausta siten, että tilaaja hyväksyy sen sisällön laadultaan ja tarkkuudeltaan riittäväksi. Rekisterinpitäjä vastaa tarvittavan selosteen henkilötietojen käyttämisestä laatisemisesta sekä korkean riskin tapauksissa myös vaikutusten arvioinnin laatisemisestä. Toimittaja antaa rekisterinpitäjälle niiden laatisemisessa ja toteuttamisessa tarvittavat tiedot ja avun ilman erillistä korvausta.

Henkilötietoja ei saa siirtää eikä tallentaa ETA-alueen ulkopuolelle (Vrt. Kuntaliiton julkaisu, kohta 7, Palvelun paikka). Tämä koskee myös etäyhteydessä tapahtuvaa tietojenkäsittelyä ETA-alueen ulkopuolelta huolimatta siitä, että henkilötiedot ovat tallennettuina ETA-alueen sisällä ja huolimatta siitä, että henkilötietoja siirretään salattuina. Palveluntuottajan tietojenkäsittelyn ja siihen liittyvien tukitoimintojen (esimerkiksi help desk -toimintojen) on tapahduttava kokonaisuudessaan ETA-alueen sisällä. Poikkeuksen tähän muodostaa kohdan 7.2 ehdot sekä EU:n ja USA:n välinen nk. Privacy Shield -tietosuojajärjestely niiltä osin, mitä siinä on yksityiskohtaisesti sovittu.

¹ <https://www.kuntaliitto.fi/sites/default/files/media/file/henkilotietojen-kasittelyn-ehdot-v4-liite-ohjeeseen-tietosuojasetuksen-huomioiminen-kilpailutettaessa-julkisia-hankintoja.docx>

² Vrt. Palvelutuotannon tietoturvaluussitoutumus, Kohta 1 (Salassapito), kolmas kappale.

HENKILÖTIETOJEN KÄSITTELYN EHDOT

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.

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. Myös mahdolliset muutokset on ilmoitettava kirjallisesti Tilaajalle.

3.5. Palveluntuottaja saattaa Tilaajan saataville tämän pyynnöstä kaikki tiedot, jotka Tilaaja tarvitsee rekisterinpitäjälle ja Palveluntuottajalle säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja osallistuu pyydettyä sovittulla tavalla Tilaajan vastuulla olevien kuvausten ja muiden dokumenttien, kuten vaikutustenarvioinnin, laatimiseen ja ylläpitämiseen sekä tietosuojasetuksen mukaisen ennakkokuulemisen suorittamiseen. Palveluntuottaja tekee nämä tehtävät sopimuksen mukaisella palvelulle määritellyllä hinnalla.

3.6. Tilaaja vastaa rekisterinpitäjänä kaikkiin niihin rekisteröityjen pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Palveluntuottaja ei itse vastaa näihin pyyntöihin, vaan ohjaa rekisteröityä oikeuksiensa käyttämisessä. (Kts. <https://www.phhyky.fi/fi/asiakkaalle/tietosuoja/>) Palveluntuottaja avustaa myös 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. Palveluntuottaja tekee nämä tehtävät sopimuksen mukaiselle palvelulle määritellyllä hinnalla, ellei toisin sovita.

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 sovittuja ehtoja sekä Tilaajan kirjallisia ohjeita. Tilaaja vastaa ohjeiden ylläpidosta ja saatavuudesta. Palveluntuottaja ilmoittaa ilman aiheutonta 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 henkilö tietojen käsittelyä ja tietosuojaa koskevia ohjeita. Jos ohjeiden muutoksista aiheutuu sopimuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovitaan erikseen.

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 asetettu ja velvoitteita sekä Tilaajan antamia kulloinkin voimassa 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 Palveluntuottaja 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 palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Ilmoitus tehdään sopimuksessa määritellylle sopimusyhteystietokentälle sekä tietosuojavastaavalle (yhteystiedot löytyvät <https://www.phhyky.fi/fi/asiakkaalle/tietosuoja/>).

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 toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.

9. Henkilötietojen käsittelyn päätyminen

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 henkilö- tiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

KÄSITTELYTOIMIEN KUVAUS

1. Sopimusosapuolet

Sopimus:	
Tilaaaja (rekisterinpitäjä):	Päijät-Hämeen hyvinvointikuntayhtymä /
Palveluntuottaja (henkilötietojen käsittelijä):	
Palveluntuottajan tietosuojavastaava:	

2. Dokumentin tarkoitus

Tilaaaja on tehnyt Palveluntuottajan kanssa yllä mainitun Sopimuksen, joka koskee sellaista palvelua, jossa Palveluntuottaja toimii Tilaaajan ylläpitämään henkilörekisteriin 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 henkilörekisteriin kuuluvia henkilötietoja:

4. Käsittelyn luonne ja tarkoitus

Osapuolet ovat sopineet, että Palveluntuottaja

--

5. Henkilötietojen käsittelyn kesto

Palveluntuottaja käsittelee tässä liitteessä yksilöityjä henkilötietoja seuraavan ajan: