

Riihimäen kaupunki
Henkilötietojen käsittelyn ehdot ja käsittelytoimien kuvaus

I Osa: 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.

Tilaaaja on rekisterinpitäjä. Palveluntuottaja noudattaa henkilötietojen käsittelijänä tämän sopimuksen liitteenä olevia ehtoja henkilötietojen käsittelystä.

II Osa: Henkilötietojen käsittelyn ehdot

1. Yleistä

1.1. Tämä sopimusliite ”Henkilötietojen käsittelyn ehdot” on osa _____ sopimusta (Dnro _____), jäljempänä ”Sopimus”, jonka Tilaaaja on tehnyt Palveluntuottajan kanssa.

1.2. Tässä sopimusliitteessä määritellään Tilaaajaa ja Palveluntuottajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Palveluntuottaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta. Näissä ehdoissa kuvatuista Palveluntuottajan toimenpiteistä ja velvollisuuksista ei suoriteta erillistä korvausta, ellei toisin ole näissä ehdoissa tai pääsopimuksessa sovittu.

2. Osapuolten roolit henkilötietojen käsittelyssä

2.1. Käsiteltäessä henkilötietoja Tilaaaja on rekisterinpitäjä ja Palveluntuottaja on henkilötietojen käsittelijä (jäljempänä myös ”käsittelijä”), ellei henkilötietojen käsittelyn tarkoituksesta muuta johdu. ”Tilaaajan henkilötiedoilla” tarkoitetaan näissä ehdoissa henkilötietoja, joista Tilaaaja 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 Tilaaajan ohjeistuksessa. Palveluntuottaja sitoutuu noudattamaan Sopimuksessa, käsittelytoimien kuvauksessa ja ohjeistuksessa olevia ehtoja ja kuvauksia. Tilaaaja vastaa ohjeistuksen ylläpidosta ja saatavuudesta.

2.3. Jos kohdan 2.2 mukaista käsittelytoimien kuvausta ei ole tehty tai se on puutteellinen, Tilaaaja 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 Käsitteijänä 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.
- 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 ylläpitämiseen 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.
- 3.7. Palveluntuottaja sallii Tilaajan aloitteesta suoritettavat auditoinnit ja osallistuu ja avustaa niissä ilman erillistä korvausta. Mikäli Tilaaja tai Tilaajan valtuuttama auditoija suorittaa tarkastuksen, vastaa Tilaaja tekemänsä tai teettämänsä auditoinnin kustannuksista.

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 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 antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Jos ohjeiden muutoksista aiheutuu sopimuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovi-
taan 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. Palveluntuottaja vastaa henkilöstönsä ajantasaisesta henkilötietojen käsittelyn osaamisesta ja siihen liittyvästä tietosuojasta ja –turvasta.

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 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 Tilaaajalle etukäteen. Ilmoituksessa tulee kuvata, miten alihankkija käsittelee Tilaaajan henkilötietoja tietosuojalainsäädännön mukaisesti. Tilaaajalla on oikeus perustellusta syystä vastustaa ehdotettua alihankkijaa.

7. Palvelun paikka

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

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

8. Tietoturvaloukkaukset

8.1. Palveluntuottajan on ilmoitettava Tilaaajalle kirjallisesti tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä. Lisäksi Palveluntuottaja sitoutuu ilmoittamaan Tilaaajalle ilman aiheetonta viivytystä muista palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Ilmoitus tehdään sopimuksessa määritellylle sopimusyhteyshenkilölle sekä tietosuojavastaavalle (tietosuojavastaavan yhteystiedot <https://www.riihimaki.fi/tietosuoja/>). Palveluntuottaja ei anna tietoja muille tahoille kuin rekisterinpitäjälle.

8.2. Palveluntuottajan on annettava Tilaaajalle 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 henkilötiedoista, ellei muuta ole sovittu. Tilaajan henkilötiedot toimitetaan Tilaajalle pyydettyssä muodossa (paperi / erikseen sovittu sähköinen muoto). Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

10. Sanktiot

10.1. Palveluntuottaja on velvollinen korvaamaan kaikki henkilötietojen käsittelystä Tilaajalle syntyneet välittömät vahingonkorvaukset ja muu kulut, jotka aiheutuvat palveluntuottajan virheellisestä menettelystä tai laiminlyönnistä.

Palveluntuottaja on velvollinen maksamaan sopimussakkoa aiheuttamastaan tietosuojaloukkauksesta alla olevan taulukon mukaisesti. Ennen sakon langettamista Tilaaja pyytää kirjallisen selvityksen tietosuojaloukkauksesta Palveluntuottajalta.

| Tietosuojarikkomuksen laajuus | sopimussakko |
|---|---------------------|
| tahaton yksittäinen tietosuojaloukkaus (vähäinen riski rekisteröidyille) | enintään 300 € |
| toistuva, useita rekisteröityjä koskeva tai laiminlyönnistä johtuva tietosuojaloukkaus (mahdollinen riski rekisteröidyille) | enintään 1000 € |
| tahallinen tai laaja tietosuojaloukkaus (riski rekisteröidyille) | enintään 5000 € |

Lisäksi olennainen tai toistuva palveluntuottajan aiheuttama tietosuojaloukkaus voi olla sopimuksen purkuperuste.

KÄSITTELYTOIMIEN KUVAUS

1. Osapuolet

Tilaaaja:

Palveluntuottaja:

2. Dokumentin tarkoitus

Tilaaaja on tehnyt Palveluntuottajan kanssa 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.

- x [ohje: kirjoita tähän, mitä rekisteröityjen ryhmiä Palveluntuottaja käsittelee, esim. Tilaaajan työntekijät]
- x [ohje: täydennä tähän, mitä henkilötietoja Palveluntuottaja käsittelee. Esim. Tilaaajan työntekijän nimi ja käyttäjätunnus]
- x
- x

4. Käsittelyn luonne ja tarkoitus

Osapuolet ovat sopineet, että Palveluntuottaja...

Ohje: kirjoita tähän, miksi ja miten Palveluntuottaja käsittelee kyseisiä henkilötietoja. Esimerkiksi Tilaaaja tilaa Palveluntuottajalta tietokoneiden asennuspalvelua, minkä vuoksi Palveluntuottajan on käsiteltävä Asiakkaan käyttäjien tietoja tietokoneiden käyttäjäkohtaisen asennuksen loppuunsaattamiseksi.

5. Henkilötietojen käsittelyn kesto

Palveluntuottaja käsittelee tässä liitteessä yksilöityjä henkilötietoja seuraavan ajan: _____

Ohje Tilaaajalle: kuvaa tähän henkilötietojen käsittelyn kesto Palveluntuottajalla. Esimerkiksi tiettyjen laitteiden asennustoimien ajan, minkä jälkeen Palveluntuottaja palauttaa / tuhoaa henkilötiedot. Tai vaihtoehtoisesti sopimuskauden ajan.

Tietoturvan ja tietosuojan ohjeistus – Vähimmäisvaatimukset palveluntuottajalle

Tilaja edellyttää Palveluntuottajalta tietoturvallista toimintatapaa ja toimittaa tarvittaessa tarkempia ohjeita sen toteuttamiseksi. Seuraavassa asiaan liittyviä vähimmäisvaatimuksia, jotka palveluntuottajan tulee täyttää. Palveluntuottajan tulee pyytää Tilajalta ohjeistuksen tarkennusta niiltä osin, kuin ohjeistus ei ole riittävän kattavaa.

1. FYYSINEN TURVALLISUUS

Palveluntarjoaja vastaa siitä, että tilat joissa säilytetään Tilajan henkilötietoja ja niiden käsittelyyn käytettäviä laitteita, ovat asianmukaisesti suojatut. Tilojen pääsynhallinta on asianmukaisesti rajoitettua ja tilojen fyysinen turvallisuus, kuten palo-, varkaus- ja vesivahinkojen uhka on tiedostettu ja riittävät suojaustoimet on tehtynä.

2. PÄÄSYNHALLINTA

Palveluntarjoaja vastaa siitä, että sähköisten tietovälineiden pääsynhallinnasta on huolehdittu riittävän turvallisella ja tarvittaessa moninkertaisella tunnistamiskäytännöllä. Tietovälineiden sisältämiin Tilajan henkilötietoihini ei tule olla pääsyä muilla kuin asianmukaisesti koulutetuilla tietojen käsittelijöillä, jotka toteuttavat Tilajan antamaa tehtävää.

3. TIETOJEN TALLENNUS

Palveluntarjoaja vastaa siitä, että Tilajan henkilötietoja ei tallenneta EU:n alueen ulkopuolella sijaitsevaan tallennuspaikkaan (EU:n rajat ylittäviä pilvipalveluja ei käytetä) muutoin kuin Tilajan kirjallisella suostumuksella. Sähköisessä muodossa olevista tiedoista muodostetaan varmuuskopioita, mikäli se on tarpeen Tilajan henkilötietojen tallessa pysymisen varmistamiseksi. Varmuuskopiot säilytetään asianmukaisesti suojattuna. Tilajan valinnan mukaan Tilajan henkilötiedot joko tuhoetaan tai toimitetaan Tilajalle tietoturvallisella tavalla välittömästi käyttötarkoituksen ja säilytysvelvoitteen päätyttyä. Palveluntarjoaja ei saa säilyttää Tilajan tietoja, joiden säilytykseen ei ole perustetta.

4. PÄÄTELAITE- JA VERKKOTURVALLISUUS

Palveluntuottaja vastaa siitä, että tietojen käsittelyssä käytettävä laitteisto on asianmukaisesti suojattu virus- ja haittaohjelmien aiheuttamia uhkia vastaan. Langattomat verkkoyhteydet ovat vahvasti salattuja ja kaikki verkkoyhteydet palomuurilla suojattuja. Henkilötietoja ei siirretä suojaamattomia yhteyksiä käyttäen (suojaamaton sähköposti, http, tms.).

5. HALLINNOLLINEN JA ORGANISATORINEN TIETOSUOJA

Palveluntuottajalla on nimettynä tietosuojasta vastaava yhteyshenkilö. Palveluntuottajalla on jatkuvuuden hallinnan suunnitelmat häiriötilanteiden varalle sekä toimintaohjeet tietoturva- ja tietosuojapoikkeamien varalle. Henkilötietoja käsittelevät henkilöt ovat saaneet riittävästi koulutusta henkilötietojen käsittelystä, käytössä olevan tietojärjestelmän käytöstä, tietoturvallisesta toimintatavasta ja tietosuojasta. Henkilötietojen käsittelyä seurataan asiattoman tietojenkäsittelyn havaitsemiseksi ja kaikista tietosuojai- tai tietoturvapoikkeamista sekä vakavista epäilyistä ilmoitetaan Tilajalle viipymättä. Palveluntuottaja voi käyttää Tilajan henkilötietojen käsittelyyn tietojärjestelmäpalvelua varmistuttuaan, että sen käyttöön liittyvät sopimukset ovat tietosuojalainsäädännön ja Tilajan vaatimusten mukaisia sekä tietojärjestelmätoimittaja on Tilajan hyväksymä.