

JHS 166 Julkisen hallinnon IT-hankintojen yleiset sopimusehdot

Liite 9. Erityisehtoja henkilötietojen käsittelystä (JIT 2015 – Henkilötiedot)

Versio: 1.1

Julkaistu: 6.9.2018

Voimassaoloaika: toistaiseksi

KÄYTTÖOHJE

Nämä erityisehdot on tarkoitettu käytettäväksi tilanteissa, joissa toimittaja käsittelee henkilötietoja tilaajan lukuun osana hankittavaa palvelua. Ehtoja ei ole tarkoitettu käytettäväksi sellaisenaan, vaan sopimukseen tulisi aina liittää niiden lisäksi kulloiseenkin palveluun soveltuvat erityisehdot sekä julkisen hallinnon IT-hankintojen yleiset sopimusehdot (*JIT 2015 – Yleiset ehdot*). Ehdot suositellaan otettavaksi soveltamisjärjestyksessä ennen muita erityisehtoja.

Sopimuksessa tulee tarvittaessa määritellä rekisterinpitäjä ja henkilötietojen käsittelijä sekä huomioida *EU:n yleisen tietosuoja-asetuksen (EU) 2016/679* vaatimukset henkilötietojen käsittelylle. Tilaaja toimii henkilötietojen käsittelyä ja tietosuoja koskevan lainsäädännön tarkoittamana rekisterinpitäjänä silloin, kun se määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Vaikka tilaaja tyypillisesti on palveluun liittyen henkilötietojen rekisterinpitäjä, on hyvä huomioida, että myös toimittajalla on sen omaan toimintaan liittyviä henkilötietoja, joita se saattaa hyödyntää palvelussa. Tällaisia ovat esimerkiksi toimittajan asiakasrekisteriin kuuluvat yhteystiedot. Nämä tiedot eivät kuulu tilaajan ohjeistuksen piiriin.

Sopimukseen on hyvä liittää asiakirja, josta käy konkreettisesti ilmi, mitä henkilötietoja käsitellään, miten ja mihin tarkoitukseen. *EU:n yleisen tietosuoja-asetuksen* 28 artiklan mukaan henkilötietojen käsittelyä on määritettävä sitovalla asiakirjalla, jossa vahvistetaan henkilötietojen käsittelyn tarkoitus, luonne, kohde, kesto, henkilötietojen tyypit ja rekisteröityjen ryhmät.

Sopijapuolet määrittelevät yhdessä sopimuksen kohteena olevalta palvelulta vaadittavan turvallisuuden tason. Turvallisuuden vaadittu taso voi perustua esimerkiksi tilaajan tekemään ja yhteisesti käsiteltyyn riskiarviointiin, käytettävissä olevaan teknologiaan ja teknisiin mahdollisuuksiin sekä käsiteltävien tietojen luonteeseen ja laatuun.

Tietosuoja-asetuksen mukaan rekisterinpitäjän tulee ennakolta hyväksyä käsittelijän käyttämät alihankkijat. Kirjallinen enakkolupa voidaan antaa yleisenä tai erityisenä. Toimittajan on lisäksi ilmoitettava tilaajalle kaikista alihankintaa koskevista suunnitelluista muutoksista. Tilaaja voi antaa kirjallisen hyväksynnän alihankkijakäsittelijöiden käyttöön esimerkiksi allekirjoittamalla sopimuksen, jossa alihankkijat on yksilöity.

Vahingonkorvauksista ja mahdollisesta rekisterinpitäjän ja käsittelijän välisestä regressioikeudesta on määrätty *JIT 2015 – Yleisissä ehdoissa*.

Tämä käyttöohje ei ole osa sopimusta.

Sisällys

1Soveltaminen.....	1
2Määritelmät.....	1
3Sopijapuolten roolit henkilötietojen käsittelyssä.....	2
4Toimittajan yleiset velvollisuudet.....	2
5Tilaaajan ohjeet.....	3
6Palveluhenkilöstö.....	3
7Alihankkijat, jotka käsittelevät henkilötietoja.....	3
8Palvelun paikka.....	4
9Tietoturvaloukkaukset.....	4
10Henkilötietojen käsittelyn päätyminen.....	4

1 Soveltaminen

(1) Näitä erityisehtoja noudatetaan julkisen hallinnon hankintayksikköjen ostaessa palvelua, jonka yhteydessä toimittaja toimii henkilötietojen käsittelijänä, jos näihin erityisehtoihin on viitattu sopimuksessa eikä näistä ole joiltakin osin sovittu kirjallisesti toisin.

(2) Näitä erityisehtoja käytetään yhdessä julkisen hallinnon IT-hankintojen yleisten sopimusehtojen kanssa. Ristiriitatilanteissa nämä erityisehdot pätevät vastaavilta kohdin ennen edellä mainittuja julkisen hallinnon IT-hankintojen yleisiä sopimusehtoja.

2 Määritelmät

Alla olevien erityisehtojen määritelmien lisäksi noudatetaan *JIT 2015 Yleisten ehtojen* määritelmiä.

käsittelijä

tietosuojalainsäädännössä tarkoitettu henkilötietoja käsittelevä taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun

rekisterinpitäjä

tietosuojalainsäädännössä tarkoitettu taho, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot

tietosuojalainsäädäntö

Euroopan unionin yleinen tietosuoja-asetus (EU) 679/2016 ja muut tietosuojasäädökset sekä tietosuojaviranomaisten määräykset

henkilötietojen tietoturvaloukkaus

tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin

tilaajan henkilötieto

henkilötieto, josta tilaaja vastaa rekisterinpitäjänä

3 Sopijapuolten roolit henkilötietojen käsittelyssä

(1) Tilaaja toimii rekisterinpitäjänä ja toimittaja henkilötietojen käsittelijänä, ellei sopimuksesta tai henkilötietojen käsittelyn tarkoituksesta muuta johdu. Sopimuksessa sovitaan sopijapuolten tarkemmat tehtävät ja vastuut henkilötietojen käsittelyn osalta.

(2) Henkilötietojen käsittelyn kohde ja kesto, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät, soveltuvat tietoturvatoinenpiteet, sekä toimittajan ja tilaajan yksityiskohtaisemmat velvollisuudet ja oikeudet kuvataan tarkemmin sopimuksessa, sen liitteissä tai tilaajan ohjeissa. Toimittaja noudattaa sopimuksessa, sen liitteissä ja ohjeissa olevia ehtoja.

4 Toimittajan yleiset velvollisuudet

(1) Toimittaja noudattaa voimassa olevaa tietosuojalainsäädännön edellyttämiä menettelytapoja ja henkilötietojen käsittelyä ja suojaamista koskevia säännöksiä. Toimittaja vastaa siitä, että palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön ja sopimuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta on säädetty.

(2) Toimittaja 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 henkilötietojen käsittelyyn käytettävien järjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus.

(3) Toimittaja ei käsittele eikä muulla tavoin hyödynnä sopimuksen perusteella käsittelemiään henkilötietoja muutoin kuin sopimuksen täyttämisen mukaisessa tarkoituksessa ja laajuudessa.

(4) Toimittaja nimeää tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön tilaajan henkilötietoihin liittyviä yhteydenottoja varten. Toimittaja ilmoittaa kirjallisesti tietosuojavastaavan tai yhteyshenkilön yhteystiedot tilaajalle.

(5) Toimittaja saattaa tilaajan saataville tämän pyynnöstä kaikki tiedot, jotka tilaaja tarvitsee rekisterinpitäjälle ja käsittelijälle 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. Toimittaja tekee nämä tehtävät sopimuksen mukaisilla hinnoilla, ellei toisin sovita.

(6) Toimittaja ilmoittaa tilaajalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Toimittaja ei itse vastaa näihin pyyntöihin. Toimittaja avustaa tilaajaa, jotta tilaaja pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyyntö voi edellyttää toimittajalta 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, toimittajalla

on oikeus laskuttaa tilaajaa sopimuksessa sovitulla hinnoilla, jos avustaminen aiheuttaa lisäkuluja toimittajalle. Toimittaja on velvollinen ennakolta ilmoittamaan tilaajalle mahdollisesti aiheutuvista lisäkuluista.

(7) Toimittaja sallii tilaajan tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin. Tarkastusmenettelyä koskevat tarkemmat ehdot ovat julkisen hallinnon IT-hankintojen yleisissä sopimusehdoissa (JIT 2015 – Yleiset ehdot) ja sopimuksessa.

5 Tilaajan ohjeet

(1) Toimittaja noudattaa tilaajan henkilötietojen käsittelyssä sopimuksessa ja näissä erityisehdoissa sovittuja ehtoja sekä tilaajan kirjallisia ohjeita. Tilaaja vastaa ohjeiden ylläpidosta ja saatavuudesta. Toimittaja ilmoittaa ilman aiheutonta viivytystä tilaajalle, jos tilaajan antamat ohjeet ovat puutteellisia tai jos toimittaja epäilee niitä lainvastaisiksi.

(2) Tilaajalla on oikeus muuttaa, täydentää ja päivittää toimittajalle antamia henkilö tietojen käsittelyä ja tietosuojaa koskevia ohjeita. Jos ohjeiden muutoksista aiheutuu sopimuksen mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovitaan sopimuksen mukaisessa muutoshallintamenettelyssä.

6 Palveluhenkilöstö

(1) Toimittaja varmistaa, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä tilaajan henkilötietoja, ovat sitoutuneet noudattamaan sopimuksessa sovittuja salassapitoehtoja tai heitä koskee lakisääteinen salassapitovelvollisuus.

(2) Toimittaja 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.

7 Alihankkijat, jotka käsittelevät henkilötietoja

(1) Jos toimittajan alihankkija käsittelee tilaajan henkilötietoja, alihankkijan käyttäminen edellyttää tilaajan ennakkoon kirjallisesti antamaa lupaa.

(2) Toimittaja tekee alihankkijan kanssa kirjallisen sopimuksen, jossa se sitouttaa käyttämänsä alihankkijat noudattamaan omalta osaltaan sopimuksessa toimittajalle asetettuja velvoitteita sekä tilaajan antamia kulloinkin voimassa olevia henkilötietojen käsittelyyn liittyviä ohjeita. Toimittaja varmistaa, että sopimuksen mukainen tilaajan tarkastusoikeus voidaan ulottaa alihankkijaan.

(3) Toimittaja vastaa käyttämänsä alihankkijan osuudesta kuin omastaan. Toimittaja vastaa siitä, että alihankkija noudattaa omalta osaltaan henkilötietojen käsittelijälle asetettuja velvoitteita.

(4) 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.

8 Palvelun paikka

(1) Ellei palvelun tuottamispaikasta ole toisin sovittu, toimittajalla 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.

(2) Jos sopijapuolet sopivat, että toimittajaa saa siirtää tilaajan henkilötietoja Euroopan talousalueen ulkopuolelle, sopijapuolet huolehtivat siitä, että henkilötietojen siirto toteutetaan lainsäädännön mukaisesti.

9 Tietoturvaloukkaukset

(1) Toimittaja ilmoittaa kirjallisesti tilaajalle tietoonsa tulleesta tilaajan henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä sovitusta palveluajasta riippumatta. Lisäksi toimittaja ilmoittaa tilaajalle ilman aiheetonta viivytystä muista palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.

(2) Toimittaja ilmoittaa kirjallisesti 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 yhteyshenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;

iii. kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja

iv. kuvaus toimenpiteistä, joita toimittaja ehdottaa tai joita se on jo toteuttanut tietoturvaloukkauksen johdosta, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

(3) Henkilötietojen tietoturvaloukkauksen havaittuaan toimittaja ryhtyy viipymättä sopimuksessa sovittuihin toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.

10 Henkilötietojen käsittelyn päättymisen

(1) Sopimuksen voimassaoloaikana toimittaja ei saa poistaa tilaajan lukuun käsittelemiään henkilötietoja ilman tilaajan nimenomaista pyyntöä.

(2) Sopimuksen päättyessä tai purkautuessa toimittaja palauttaa tilaajalle kaikki tilaajan puolesta käsitellyt henkilötiedot sekä kustannuksellaan hävittää omilta taltioiltaan mahdolliset kopiot henkilötiedoista, ellei toisin ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että toimittaja säilyttää henkilötiedot. Tilaajan henkilötietojen palauttamisesta tämän kappaleen mukaisesti ei toimittajalla ole oikeutta erillisveloitukseen, ellei toisin ole sovittu.