

Tietosuoja-asetuksen sopimusvaatimukset ja vaikutus tarjouspyynnön suunnitteluun

Uutta tukimateriaalia kunnan digitalisaatioon -seminaari
14.9.2017

Jukka Hämäläinen
Johtava lakimies, Hansel Oy
Jukka.hamalainen@hansel.fi

Aineistoa

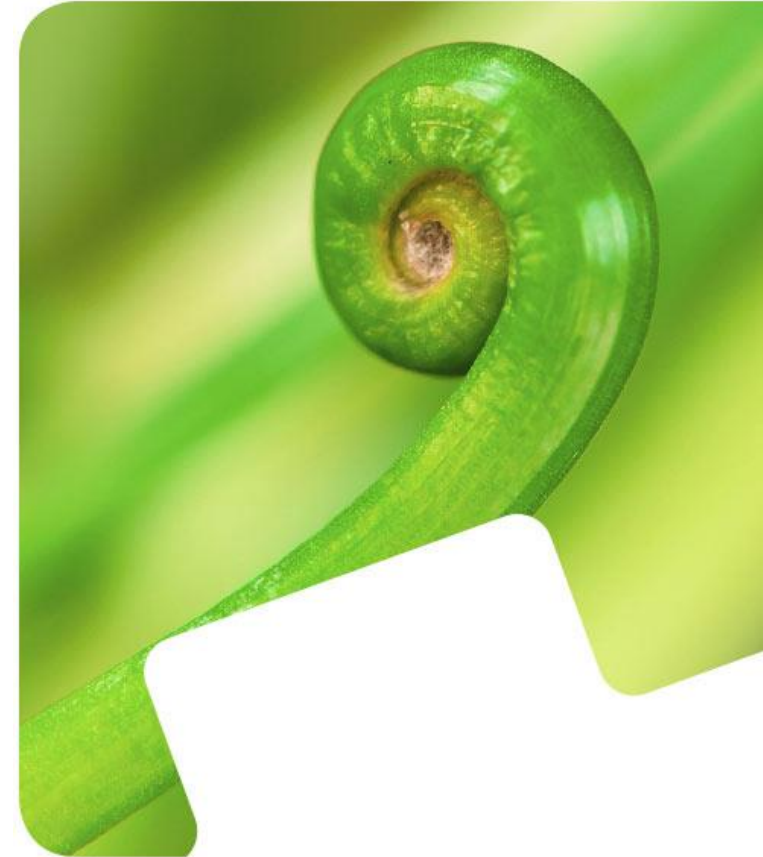
- Yleinen tietosuoja-asetus (EU) 2016/679
 - <http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1503654467343&uri=CELEX:32016R0679>
- Ohje 13.6.2017 on saatavilla netistä:
 - <https://www.hansel.fi/uutiset/tietosuojaopas-auttaa-huomioimaan-hankintojen-uude>
 - <https://www.kuntaliitto.fi/asiantuntijapalvelut/laki/tietosuoja>
 - Word-muotoinen liite "Henkilötietojen käsittelyn ehdot"
 - Liite on käännetty myös ruotsiksi
 - "Henkilötietojen luokkien ja rekisteröityjen määrittäminen" lisättäneen ohjeeseen
- TATTI-työryhmän mietintö
 - <https://julkaisut.valtioneuvosto.fi/handle/10024/80098>
- Tietosuojavaltuutetun ohjeistusta ja uutisia
 - <http://www.tietosuoja.fi/fi/index/euntietosuojaudistus.html>



Tietosuoja-asetuksen
huomioiminen
kilpailutettaessa julkisia
hankintoja

Tarjouspyynnön sisältö hankintalain 68 § :n mukaan

- 1) hankinnan kohteen määrittely tai hankekuvaus sekä hankinnan kohteeseen liittyvät muut laatuvaatimukset;
- 2) viittaus julkaistuun hankintailmoitukseen;
- 3) määräaika tarjosten tekemiselle;
- 4) osoite, johon tarjoukset on toimitettava;
- 5) kieli tai kielet, joilla tarjoukset on laadittava;
- 6) Tarjousasiakirjojen esittämistä ja muotoa koskevat muut vaatimukset;
- 7) kilpailullisessa neuvottelumenettelyssä neuvottelujen alkamispäivä sekä neuvotteluissa käytettävä kieli tai kielet;
- 8) ehdokkaiden tai tarjoajien taloudellista ja rahoituksellista tilannetta, teknistä soveltuvuutta ja ammatillista pätevyyttä koskevat ja muut vaatimukset sekä pyyntö täydentää yhteinen eurooppalainen hankinta-asiakirja ja luettelo asiakirjoista, joita ehdokkaan tai tarjoajan sekä tarjouskilpailun voittaneen tarjoajan on soveltuvuuden arviointia varten toimitettava;
- 9) kokonaistaloudellisen edullisuuden perusteet ja niiden suhteellinen painotus, kohtuullinen vaihteluväli tai poikkeuksellisissa tapauksissa vertailuperusteiden tärkeysjärjestys;
- 10) tarjosten voimassaoloaika;
- 11) keskeiset sopimusehdot;
- 12) muut tiedot, joilla on olennaista merkitystä hankintamenettelyssä ja tarjosten tekemisessä.



Ulkoisen palveluntuottajan rooli

- Tunnusmerkkejä -

Rekisterinpitäjä

- Päätösvalta henkilötietojen käyttämisen ja säilytyksen suhteen
- Vastaa käsittelyn oikeellisuudesta ja lainmukaisuudesta
- Vastaa rekisteröidyn oikeuksien toteutumisesta
- Suunnittelee tietojen käsittelyn ja luovutukset sekä näihin liittyvät yksityiskohdat
- Vastaa käsittelijän ohjeistamisesta

Käsittelijä

- Ei itsenäistä päätösvaltaa henkilötietojen käyttämisen ja säilytyksen suhteen
- Käsittelee tietoja vain sovitussa käyttötarkoituksessa
- Noudattaa rekisterinpitäjän ohjeita

→ Vaikka palveluntuottaja olisi käsittelijän roolissa, sillä saattaa lisäksi olla asiaan liittyviä omia henkilörekistereitä sen tuottaessa hankintasopimuksen mukaista palvelua.

Esim. asiakasrekisteri

28 artiklan sopimusvaatimukset, yleistä

- Rekisterinpitäjän **on laadittava** käsittelijän kanssa kirjallinen sopimus
 - Liitetään tarjouspyyntöön
- Sopimuksessa **on vahvistettava:**
 - Henkilötietojen käsittelyn kohde ja kesto
 - Käsittelyn luonne ja tarkoitus
 - Henkilötietojen tyyppi ja rekisteröityjen ryhmät
 - Rekisterinpitäjän velvollisuudet ja oikeudet
 - Rekisterinpitäjä **saa käyttää ainoastaan** sellaisia käsittelijöitä, joilla riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi



28 artiklan tarkemmat sopimusvaatimukset (1)

- **On sovittava**, että henkilötietojen käsittelijä
 - Käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen **ohjeiden** mukaisesti
 - Hankintayksikön laadittava kirjalliset ohjeet; vrt. tietoturvasojen käsittelysäännöt?
 - Käytännesäännöt
 - Varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan **salassapitovelvollisuutta**
 - Salassapitositoumus, ellei lakisääteistä salassapitovelvollisuutta
 - Varmistettava ulottuvuus henkilötietoihin



28 artiklan tarkemmat sopimusvaatimukset (2)

- **On sovittava**, että henkilötietojen käsittelijä
 - Toteuttaa kaikki 32 artiklassa vaaditut **tietoturvallisuustoimenpiteet**
 - Tarjouspyynnön vaatimusmäärittelyssä huomioon <> vrt. tietoturvasojen ja muiden VAHTI-ohjeiden vaatimukset?
 - Riskiarviointi
 - Tietojen eheys, käytettävyys, luottamuksellisuus, vikasietoisuus
 - Tietojen palauttaminen; pääsy tietoihin fyysisen tai teknisen vian sattuessa
 - Tietojen pseudonymisointi ja salausta
 - Tietoturvallisuuden ja toimenpiteiden jatkuva testaus ja arviointi
 - **Ei siirrä käsittelyä toiselle** käsittelijälle ilman rekisterinpitäjän kirjallista ennakkolupaa
 - Alkuperäinen käsittelijä säilyy tällöinkin vastuussa suhteessa rekisterinpitäjään
 - Toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla auttaa rekisterinpitäjää täyttämään velvollisuuden vastata **rekisteröidyn oikeuksia koskeviin pyyntöihin**
 - Tietojen irrottaminen, korjaaminen, siirtäminen, poisto, jne.

28 artiklan tarkemmat sopimusvaatimukset (3)

- **On sovittava**, että henkilötietojen käsittelijä
 - Auttaa rekisterinpitäjää varmistamaan, että tietoturvallisuuteen ja loukkauksista **ilmoittamiseen** liittyviä säädettyjä velvollisuuksia noudatetaan
 - Rekisterinpitäjällä 72 tunnin ilmoitusvelvollisuus viranomaiselle <> käsittelijältä tiedot nopeammin "ilman aiheetonta viivytystä" – 36 h
 - ilmoituksessa kuvattava:
 - Tapahtunut tietoturvaloukkaus
 - Rekisteröityjen ja henkilötietotyyppien ryhmät ja lukumäärät
 - Loukkauksen todennäköiset seuraamukset
 - Tehdyt toimenpiteet
 - Asetus ei tunne viikonloppuja, pyhäpäiviä, loma-aikoja...
 - Dokumentointivelvollisuus
 - Ilmoitusvelvollisuus rekisteröidyille ilman aiheetonta viivytystä (jos korkea riski)
 - Palvelun päätyttyä **poistaa tai palauttaa** kaikki henkilötiedot rekisterinpitäjälle ml. jäljennökset
 - Saattaa rekisterinpitäjän saataville kaikki ne tiedot, jotka tämä tarvitsee **osoitusvelvollisuuden toteuttamista** varten
 - Sallii rekisterinpitäjän tehdä **auditointeja** / tarkastuksia ja osallistuu niihin

Henkilötietojen käsittelyn ehdot

Versio 1.0 Toukokuu 2017

1 (4)

LIITE SOPIMUKSEEN NRO _____

Henkilötietojen käsittelyn ehdot

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitattut pääsopimuksen määräykset ja liitteet. Muokkaa tarvittaessa ennen ehtojen liittämistä tarjouspyyntöön. Poista tämä ohje.

1. Yleistä

- 1.1. Tämä sopimusliite "Henkilötietojen käsittelyn ehdot" on osa _____ sopimusta (Dnro _____), jäljempänä "Sopimus", jonka Tilaaaja on tehnyt Toimittajan kanssa.
- 1.2. Tässä sopimusliitteessä määritellään Tilaaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta ja lukuun Sopimuksessa olevien sopimusehtojen lisäksi.
- 1.3. Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä, ja lisäksi Osapuolet sitoutuvat saattamaan henkilötietojen käsittelyn ja tietosuojan EU:n yleisen tietosuoja-asetuksen (EU)2016/679 mukaiselle vaatimustasolle 25.5.2018 mennessä, jolloin tietosuoja-asetuksen soveltaminen alkaa.

Ks. lisäksi muut ohjeessa esitetyt sopimusehdot, jotka voit tarvittaessa sisällyttää pääsopimukseen.

Henkilötietojen käsittelyehto Versio 1.0 Toukokuu 2017 1 (4)

LIITE SOPIMUKSEEN NRO _____

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitattut pääsopimuksen määräykset ja liitteet. Muokkaa tarvittaessa ennen ehtojen liittämistä tarjouspyyntöön. Poista tämä ohje.

1. Yleistä

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

Tässä sopimusliitteessä määritellään Tilaaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta ja lukuun Sopimuksessa olevien sopimusehtojen lisäksi.

Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä, ja lisäksi Osapuolet sitoutuvat saattamaan henkilötietojen käsittelyn ja tietosuojan EU:n yleisen tietosuoja-asetuksen (EU)2016/679 mukaiselle vaatimustasolle 25.5.2018 mennessä, jolloin tietosuoja-asetuksen soveltaminen alkaa.

Toukokuu 2017 1 (4)

Henkilötietojen käsittelyehto Versio 1.0 Toukokuu 2017 1 (4)

LIITE SOPIMUKSEEN NRO _____

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitattut pääsopimuksen määräykset ja liitteet. Muokkaa tarvittaessa ennen ehtojen liittämistä tarjouspyyntöön. Poista tämä ohje.

1. Yleistä

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

Tässä sopimusliitteessä määritellään Tilaaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta ja lukuun Sopimuksessa olevien sopimusehtojen lisäksi.

Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä, ja lisäksi Osapuolet sitoutuvat saattamaan henkilötietojen käsittelyn ja tietosuojan EU:n yleisen tietosuoja-asetuksen (EU)2016/679 mukaiselle vaatimustasolle 25.5.2018 mennessä, jolloin tietosuoja-asetuksen soveltaminen alkaa.

Toukokuu 2017 1 (4)

Henkilötietojen käsittelyehto Versio 1.0 Toukokuu 2017 1 (4)

LIITE SOPIMUKSEEN NRO _____

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitattut pääsopimuksen määräykset ja liitteet. Muokkaa tarvittaessa ennen ehtojen liittämistä tarjouspyyntöön. Poista tämä ohje.

1. Yleistä

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

Tässä sopimusliitteessä määritellään Tilaaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta ja lukuun Sopimuksessa olevien sopimusehtojen lisäksi.

Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä, ja lisäksi Osapuolet sitoutuvat saattamaan henkilötietojen käsittelyn ja tietosuojan EU:n yleisen tietosuoja-asetuksen (EU)2016/679 mukaiselle vaatimustasolle 25.5.2018 mennessä, jolloin tietosuoja-asetuksen soveltaminen alkaa.

Toukokuu 2017 1 (4)

Henkilötietojen käsittelyehto Versio 1.0 Toukokuu 2017 1 (4)

LIITE SOPIMUKSEEN NRO _____

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitattut pääsopimuksen määräykset ja liitteet. Muokkaa tarvittaessa ennen ehtojen liittämistä tarjouspyyntöön. Poista tämä ohje.

1. Yleistä

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

Tässä sopimusliitteessä määritellään Tilaaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaaajan toimeksiannosta käsittelee henkilötietoja Tilaaajan puolesta ja lukuun Sopimuksessa olevien sopimusehtojen lisäksi.

Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa voimassaolevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä, ja lisäksi Osapuolet sitoutuvat saattamaan henkilötietojen käsittelyn ja tietosuojan EU:n yleisen tietosuoja-asetuksen (EU)2016/679 mukaiselle vaatimustasolle 25.5.2018 mennessä, jolloin tietosuoja-asetuksen soveltaminen alkaa.

Toukokuu 2017 1 (4)

Tarjouspyynnössä huomioitavaa

- Tietojärjestelmän vaatimusmäärittely
 - Toiminnalliset, tekniset, tietoturvallisuutta koskevat vaatimukset
 - Vahti-vaatimukset/Katakri-vaatimukset tp:n liitteenä
 - Vaatimusten toteutuminen varmistetaan myös myöhemmässä vaatimusten tarkennetussa määrittelyssä
- Tietojen sijainti
 - Järjestelmän sijaintimaa (palvelimet)
 - Ylläpito
 - Hallinta- ja valvontayhteydet
 - Tietojen siirron laillisuus
- Toiminnalliset prosessit ja yhteistyö sopimuskaudella
 - Vastuunjako, ilmoitusvelvollisuudet, menettelytavat, jatkuva testaus jne.
 - Häiriönhallinta
 - Dokumentointi, raportointi
- Salassapito ja vaitiolovelvollisuus
 - Turvallisuussopimus
 - Vaitiolositoumukset
 - Turvallisuusselvitykset



JIT 2015 ja tietosuoja-asetus

■ Yleiset ehdot

- 18(3) Yleisvelvoite noudattaa hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä.
- 18(4) Tietojen asianmukainen suojaaminen laittoman tai tapaturmaisen häviämisen tai hävittämisen varalta.
- 19 Tarkastusoikeus: Auditoinnin kohde laajasti määritelty

■ Palveluehdot

- 5(3) Henkilöstö: Pyynnöstä laadittava ja ylläpidettävä luettelo henkilöistä, joilla on pääsy tilaajan henkilötietoihin, tunnistamistietoihin ja salassa pidettäviin tietoaineistoihin.
- Tilaaja voi hakea palvelun tuottamiseen osallistuvista henkilöistä turvallisuusselvityksen JIT 2015 Yleisten ehtojen kohdan 18 (6) mukaisesti.
- 3(2) Toimittaja ilmoittaa tilaajalle etukäteen, mistä palvelua tuotetaan. Toimittajan on myös ilmoitettava tilaajalle etukäteen, jos paikka muuttuu.

■ Ohjelmistopalvelut (Palvelut verkon kautta)

- Tietojen siirtäminen Toimittajalle ja toimittajan vastuut
- Tietojen maantieteellinen sijainti



JYSE 2014 Palvelut ja tietosuoja-asetus

- 21.1 velvoittaa noudattamaan voimassaolevaa lainsäädäntöä sekä tilaajan ohjeita mm. tietosuojan osalta
- 21.3 Henkilötietolaissa (523/1999) tarkoitettuna rekisterinpitäjänä toimii tilaaja. Toimeksiantosuhteen päättyessä palveluntuottajan hallussa olevat toimeksiantosuhteeseen liittyvät henkilörekisterit luovutetaan tilaajalle.
- 21.5 Kielto luovuttaa ulkopuolisille henkilötietoja rekisterimuodossa
- 21.8 Tilaajan vaatiessa laadittava luettelo henkilöistä, joilla pääsy tietoihin
- 4.3 Palvelun tulee täyttää Euroopan unionin suoraan velvoittavien säädösten, Suomen lakien ja asetusten sekä viranomaisten antamat määräykset.
- 5.4 Tilaajan tarkastusoikeus



Muistilista

- **Selvitä**, mitä velvollisuuksia sinuun rekisterinpitäjänä kohdistuu (vaikka et ulkoistaisi mitään osaa toiminnasta)
- **Selvitä**, mitä velvollisuuksia asetus asettaa käsittelyn ulkoistajalle
- **Selvitä ja määrittele**, mitä henkilötietoja hankittavassa järjestelmässä tullaan käsittelemään ja miten
- **Pohdi**, mitkä tehtävät hoidat itse ja mitä palveluntarjoaja tekee
- **Listaa ja laadi** tarvittavat politiikat, ohjeistukset, prosessit, kuvaukset ja käytäntösäännöt
- **Liitä tarjouspyyntöön** vaatimusmäärittely ja varmista, että siinä on otettu huomioon myös tietosuoja
- **Liitä tarjouspyyntöön** sopimusehdot, joissa vyörytät palveluntarjoajalle ne velvollisuudet ja tehtävät, jotka sen tulee hoitaa, jotta käsittely on laillista, rekisterinpitäjän velvollisuudet voidaan täyttää ja rekisteröidyn oikeudet toteutuvat – vakioehtojen käyttö ei riitä täyttämään tätä vaatimusta.

