



Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja

Sisällys

1. Johdanto	3
1.1 Taustaksi	3
1.2 Henkilötietojen käsittelyn ulkoistaminen julkisena hankintana	3
2. Yleistä tietosuojaa-asetuksesta ja henkilötietojen käsittelystä	5
2.1 Tietosuojaa-asetuksen soveltaminen (artiklat 1-3)	5
2.2 Määritelmät (artikla 4)	5
2.3 Henkilötietojen lainmukainen käsittely	6
2.3.1 Henkilötietojen käsittelyä koskevat periaatteet (artikla 5)	6
2.3.2 Käsittelyn lainmukaisuus (artiklat 6-11)	6
3. Rekisteröidyn oikeudet	8
3.1 Avoin informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten (artikla 12)	8
3.2 Toimitettavat tiedot (artiklat 13-14)	8
3.3 Rekisteröidyn oikeus saada pääsy tietoihin (artikla 15)	9
3.4 Oikeus tietojen oikaisemiseen (artikla 16)	9
3.5 Henkilötietojen oikaisua, poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus (artikla 19)	9
3.6 Oikeus siirtää tiedot järjestelmästä toiseen (artikla 20)	9
3.7 Vastustamisoikeus (artikla 21)	10
4. Rekisterinpitäjän velvollisuudet	11
4.1 Rekisterinpitäjän vastuu (artikla 24)	11
4.2 Sisäänrakennettu ja oletusarvoinen tietosuojaa (artikla 25)	11
4.3 Tietosuojavastaavan nimittäminen, asema ja tehtävät (artiklat 37-39)	11
5. Henkilötietojen käsittely	13
5.1 Henkilötietojen käsittelijä (artikla 28)	13
5.2 Tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa (artikla 29)	13
5.3 Käsittelyn turvallisuus (artikla 32)	13
5.4 Tietoturvaloukkauksesta ilmoittaminen (artiklat 33-34)	14
5.5 Tietosuojaa koskeva vaikutustustenarviointi ja ennakkokuuleminen (artiklat 35-36)	14
6. Henkilötietojen siirrot kolmansiin maihin	15
6.1 Siirtoja koskeva yleinen periaate (artikla 44)	15
6.2 Siirto tietosuojan riittävyttä koskevan päätöksen perusteella (artikla 45)	15
6.3 Siirto asianmukaisia suojatoimia soveltaen (artikla 46)	16
6.4 Yritystä koskevat sitovat säännöt (artikla 47)	16
6.5 Eritystilanteita koskevat poikkeukset (artikla 49)	16
7. Oikeussuojaa ja seuraamukset	17
7.1 Oikeussuojaa	17
7.2 Vastuu ja oikeus korvauksen saamiseen (artikla 82)	17
7.3 Hallinnolliset sakot ja muut seuraamukset (artikla 83)	17
Liite: Henkilötietojen käsittelyn ehdot	18

1. Johdanto

1.1 Taustaksi

Henkilötietojen käsittelyä (tietosuojaa) koskeva lainsäädäntö uudistui Euroopan unionin yleisen tietosuojasetuksen tultua voimaan toukokuussa 2016. Asetus tulee sovellettavaksi kahden vuoden siirtymäajan jälkeen 25.5.2018 alkaen.

Tämän ohjeen tarkoituksena on antaa tietoa tietosuojaan liittyvistä asioista erityisesti julkisia hankintoja tekeville organisaatioille. Keskeisenä teemana on henkilötietojen käsittelyn lainmukaisuuden varmistaminen tilanteissa, joissa ulkoinen sopimuskumppani tulee käsittelemään henkilötietoja hankintasopimuksen perusteella. Tietosuojavaltuutettu tulee ennen asetuksen soveltamisen aloittamista antamaan yksityiskohtaisempaa ohjeistusta sen soveltamisesta. Tämä ohjeistus sekä valmisteilla olevan kansallisen tietosuojalain säännökset tullaan soveltuvin osin huomioimaan tämän asiakirjan päivityksessä. Lisätietoja tietosuojavaltuutetun ohjeistuksesta saa osoitteesta tietosuoja.fi.

Tässä ohjeessa kuvataan tietosuojasetuksen keskeiset velvoitteet hankintojen suunnittelun tueksi. Luettavuutta on yritetty parantaa karsimalla varsin yksityiskohtaista säädöstekstiä. Ohjeeseen on lisäksi kirjattu mallilausekkeita sopimuksia varten. Ohjeen liitteenä on yksityiskohtaiset ehdot henkilötietojen käsittelyä koskeviin sopimuksiin. Jos hankintayksikkö ei ole varma mallilausekkeen soveltuvuudesta yksittäiseen hankintaan, on suositeltavaa varata hankintamenettelyyn osallistuvilla yrityksillä tilaisuus kommentoida tietosuojaan liittyviä ehtoja ja vaatimuksia esimerkiksi teknisen vuoropuhelun yhteydessä.

Tietosuojaa koskevat mallilausekkeet ja -vaatimukset kannattaa sisällyttää hankinta-asiakirjoihin jo hankinnan alkuvaiheessa, jotta tarjoajat voivat arvioida niiden vaikutuksen tarjouksensa laadinnassa. Edellä lausuttu koskee myös neuvottelumenettelyjä; jos kilpailutukseen osallistuu ehdokkaita ETA-alueen ulkopuolelta, heille on suureksi hyödyksi, jos hankintayksikkö jo osallistumispyynnössä saattaa tietäväksi henkilötietojen käsittelyn edellytykset.

Ohje on laadittu valtion yhteishankintayksikkö Hansel Oy:n, Kuntaliiton, Julkisten hankintojen neuvontayksikön ja KL-Kuntahankinnat Oy:n yhteistyönä.

1.2 Henkilötietojen käsittelyn ulkoistaminen julkisena hankintana

Tässä ohjeessa on pyritty kuvaamaan sitä varsin yleistä tilannetta, että rekisterinpitäjänä toimiva viranomaistaho (hankintayksikkö, tilaaja) ulkoistaa erilaisia henkilötietojen käsittelytehtäviä palveluntarjoajille (sopimustoimittajille). Ulkoistamisen myötä palveluntarjoajat ovat lähtökohtaisesti rekisterinpitäjän lukuun henkilötietoja käsitteleviä tahoja. Toisin sanoen, jos palveluntarjoajalla ei ole itsenäistä päättösvaltaa henkilötietojen säilytyksen ja käyttämisen suhteen, palveluntarjoaja toimii rekisterinpitäjän lukuun henkilötietojen käsittelijänä.

Ulkoistamistilanteesta on erotettava ne tilanteet, joissa palveluntarjoaja itse toimii rekisterinpitäjänä tuottaessaan hankintasopimuksen mukaista palvelua. Esimerkiksi matkatoimistoilla voi olla matkavarauksjärjestelmä, jota hankintayksikön työntekijät käyttävät työmatkojen varaamiseen. Tällaisessa tilanteessa matkatoimisto vastaa rekisterinpitäjänä henkilörekisterin lainmukaisuudesta. Matkavarauksjärjestelmä voi olla toisaalta yhteinen jonkun toisen palveluntarjoajan (esim. lentoyhtiön) kanssa, jolloin rekisterinpitäjän vastuu koskee molempia palveluntarjoajia.

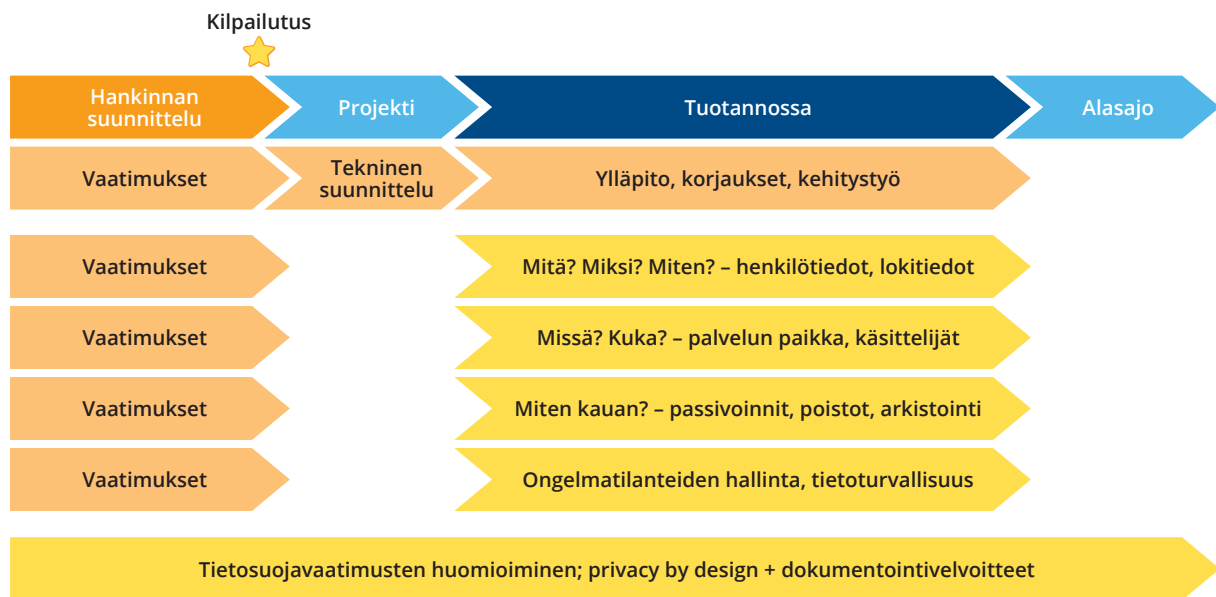
Rekisterinpitäjä vastaa henkilötietojen lainmukaisesta käsittelystä, joten tässä ohjeessa ei ole katsottu välttämättömäksi käsitellä rekisterinpitäjän vastuuta samassa laajuudessa kuin henkilötietojen käsittelijän vastuuta.

Kun henkilötietojen käsittelyä koskevia tehtäviä annetaan sopimusperusteisesti palvelutuottajalle, on välttämätöntä huolehtia siitä, että henkilötietojen käsittelyä koskevat ehdot on sopimusveloittein saatettu käsittelijän tietoisuuteen. Jos käsittelijä ryhtyy esimerkiksi käsittelemään henkilötietoja muussa kuin sovitussa käyttötarkoituksessa, sille voisi syntyä tältä osin rekisterinpitäjän vastuu tai käsittely saattaisi olla lainsäädännön vastaista.

Rekisterinpitäjän on siis ennen hankintamenettelyn aloittamista tapauskohtaisesti arvioitava, missä roolissa palvelutuottaja tulee hankinnassa olemaan. On huomattava, että palvelutuottaja voi toimia sekä rekisterinpitäjänä että käsittelijänä. Hankinnan perusteella hankintayksikön on määriteltävä ne tässäkin

ohjeessa kuvatut velvollisuudet, jotka palvelutuottajalle kuuluvat, ja otettava ne osaksi hankinta-asiakirjoja. On myös huomattava, että jo pelkästään rekisterinpitäjän ja henkilötietojen käsittelijän väliseen rajanvetoon liittyy oikeudellista epävarmuutta lainsäädännön tulkinnanvaraisuuden vuoksi. Hankintasopimuksen ehdoilla voidaan pyrkiä vaikuttamaan siihen, kuinka eri toimijoiden asemaa tulkitaan.

Rekisterinpitäjän velvollisuutena on suunnitella tietojen käsittely ja luovutukset sekä näihin liittyvät yksityiskohdat, kuten käyttöoikeuspolitiikka, tietojen saatavuus ja säilytysajat. Tietojen käsittely tulee suunnitella jo hyvissä ajoin ennen mahdollisen kilpailuttamisen aloittamista, jotta kaikki tarpeelliset velvoitteet voidaan huomioida myös hankintasopimuksissa. Arvioinnin apuna voidaan käyttää esimerkiksi alla olevassa kuvassa esitettyjä kysymyksiä.



Kuva 1. Tietojärjestelmän elinkaari ja tietosuojavaatimukset

2. Yleistä tietosuojasetuksesta ja henkilötietojen käsittelystä

2.1 Tietosuojasetuksen soveltaminen (artiklat 1-3)

Tietosuojasetusta sovelletaan automaattiseen henkilötietojen käsittelyyn. Asetusta sovelletaan myös muussa kuin automaattisessa muodossa tapahtuvaan henkilötietojen käsittelyyn silloin, kun käsiteltävät henkilötiedot muodostavat rekisterin tai sen osan.

Asetusta sovelletaan aina kun henkilötietoja käsitellään organisaation EU:n alueella sijaitsevan toimipaikan toiminnan yhteydessä, riippumatta siitä, suoritetaanko itse käsittely unionin alueella. Lisäksi asetusta sovelletaan tietyissä tilanteissa myös EU:n ulkopuolelle sijoittuneisiin organisaatioihin. Asetusta sovelletaan esimerkiksi unionissa olevia henkilöitä koskevien tietojen käsittelyyn, jos käsittely liittyy tavaroiden tai palveluiden tarjoamiseen näille henkilöille tai näiden henkilöiden käyttäytymiseen.

Koska asetuksen soveltamisala on varsin laaja, sen asettamat vaatimukset tulevat vaikuttamaan suureen osaan julkisia hankintoja, kun niiden kohteena olevissa palveluissa käsitellään henkilötietoja.

Asetusta ei sovelleta

- henkilötietojen käsittelyyn, joka on yksinomaan henkilökohtaista tai kotitaloutta koskevaa ja joka ei ole sidoksissa mihinkään ammatilliseen tai kaupalliseen toimintaan (esim. kirjeenvaihto tai osoitteiston pitäminen sekä sosiaalinen verkostoituminen)
- unionin oikeuden soveltamisalaan kuulumattomiin perusoikeuksien ja -vapauksien suojeluun liittyviin kysymyksiin, kuten kansallista turvallisuutta koskeviin toimiin
- henkilötietojen käsittelyyn kun jäsenvaltio toteuttaa unionin yhteiseen ulko- ja turvallisuuspolitiikkaan liittyviä toimia
- henkilötietojen käsittelyyn, jota viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia

varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

2.2 Määritelmät (artikla 4)

Tietosuojasetuksen henkilötiedon määritelmä on henkilötietolain määritelmää yksityiskohtaisempi. Määritelmään sisältyy esimerkkejä henkilötiedoksi määriteltävistä tiedoista.

Asetuksen mukaan henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön eli ihmiseen liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella.

Henkilötieto voi määritelmän mukaan olla esimerkiksi paikkatieto, joka kertoo jotakin tietystä henkilöstä; kuva, joka yhdistettynä esimerkiksi osoitetietoihin kertoo jotakin tietystä henkilöstä tai tämän elinolosuhteista; IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään; tai käyttäjätunnus.

Henkilötiedon käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Esimerkkejä tietojen käsittelystä ovat tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Henkilörekisteri on mikä tahansa jäsenneiltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty,

hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Esimerkiksi lokirekisteri, käyttäjärekisteri ja jäsenrekisteri ovat henkilörekistereitä.

Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

2.3 Henkilötietojen lainmukainen käsittely

2.3.1 Henkilötietojen käsittelyä koskevat periaatteet (artikla 5)

Henkilötietojen käsittelyssä on aina noudatettava tietosuoja-asetuksessa määriteltyjä peruseriaatteita:

- henkilötiedot on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi ("**lainmukaisuus, kohtuullisuus ja läpinäkyvyys**")
- henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla ("**käyttötarkoitussidonnaisuus**")
- henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään ("**tietojen minimointi**")
- henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä ("**täsmällisyys**")
- henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten ("**säilytyksen rajoittaminen**")
- henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia ("**eheys ja luottamuksellisuus**").

Rekisterinpitäjä on vastuussa ja sen on myös käytännössä pystyttävä osoittamaan, että sekä rekisterinpitäjä että käsittelijä noudattavat henkilötietojen käsittelyn peruseriaatteita (osoitusvelvollisuus). Rekisterinpitäjä ei voi ulkoistaa tätä vastuutaan. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjä toteuttaa yllä mainittuja periaatteita käytännön tasolla esimerkiksi siten, että se määrittelee periaatteiden käytännön toteutuksen hankinnan kohteena olevassa palvelussa. Rekisterinpitäjän eli tilaajan velvollisuuksiin kuuluu siten hankinnassa varmistaa, että palveluntuottaja toteuttaa periaatteet käytännössä rekisterinpitäjän ohjeistuksen ja vaatimusten mukaisesti.

2.3.2 Käsittelyn lainmukaisuus (artiklat 6-11)

Rekisterinpitäjä ja käsittelijä saavat käsitellä henkilötietoja ainoastaan tietosuoja-asetuksessa säädetyllä perusteella (6 art.). Muussa tapauksessa henkilötietojen käsittely on laitonta. Henkilötietoja saa asetuksen mukaan käsitellä jos

- rekisteröity on antanut **suostumuksensa** henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
- käsittely on tarpeen sellaisen **sopimuksen täytäntöön panemiseksi**, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä
- käsittely on tarpeen **rekisterinpitäjän lakisääteisen veloitteen noudattamiseksi**;
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön **elintärkeiden etujen suojaamiseksi**
- käsittely on tarpeen **yleistä etua** koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle **kuuluvan julkisen vallan käyttämiseksi**
- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen **oikeutettujen etujen** toteuttamiseksi, paitsi milloin henkilötietojen suoja edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Rekisterinpitäjä on vastuussa siitä, että henkilötietoja ei käsitellä siten, että niistä ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisiä tai biometrisiä tietoja, joista henkilö voidaan yksiselitteisesti tunnistaa, terveyttä koskevia tietoja taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevia tietoja.

Edellä mainittujen erityisten henkilötietojen käsittelystä on säädetty eräitä poikkeuksia tietosuojasetuksen 9 artiklassa. Poikkeukset liittyvät lähinnä tilanteisiin, joissa turvataan rekisteröidyn itsensä oikeuksia tai tilanteisiin, joissa käsittely on tarpeen tärkeää yleistä etua koskevasta syystä. Rekisterinpitäjä on vastuussa siitä, että kyseisiä tietoja käsitellään asetuksen poikkeussäännöksen mukaisesti.

Tarjouspyynnön vaatimusmäärittelyn ja hankintasopimuksen ehtojen yhteydessä on mietittävä, voiko palveluntuottaja toimia erityisten henkilötietojen käsittelijänä ja millaisin varmistuksin, sekä millaisia resursseja ja toimia tämä vaatii hankintayksiköltä ja järjestelmältä, jossa tietoja käsitellään.

3. Rekisteröidyn oikeudet

3.1 Avoin informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten (artikla 12)

Rekisterinpitäjän on suunniteltava toimintansa siten, että se voi pyynnöstä toimittaa rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Tietosuoja-asetuksen mukaan tiedot on pystyttävä esittämään tiiviisti esitetystä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa.

Tiedot on toimitettava pääsääntöisesti kirjallisesti. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on myös pääsääntöisesti toimitettava sähköisesti. Tiedot voidaan pyynnöstä antaa myös suullisesti, jos rekisteröidyn henkilöllisyydestä on voitu luotettavalla tavalla varmistua.

Rekisteröidyn informoinnille ja toteutettaville toimenpiteille on asetettu määräaikoja. Tiedot on annettava ilman aiheutonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietäen edellytyksin jatkaa. Asiaa on syytä huomata myös viranomaisten toiminnan julkisuudesta annetun lain (621/1999; julkisuuslaki) mukaiset säännökset viranomaisen asiakirjojen luovuttamisesta. Jos tietopyyntö koskee henkilötietojen käsittelyä koskevien tietojen lisäksi myös viranomaisen asiakirjaa, tulee jälkimmäisen osalta noudatettavaksi julkisuuslain mukaiset lyhyemmät määräajat (14 pv).

Samaa yhden kuukauden määräaikaa noudatetaan tilanteissa, joissa rekisterinpitäjä ei tule antamaan rekisteröidylle tietoja tämän henkilötietojen käsittelyä tai ei muutoin toteuta toimenpiteitä rekisteröidyn pyynnön perusteella. Tietojen pyytäjälle on samalla ilmoitettava oikeudesta käyttää oikeussuojakeinoja, esimerkiksi mahdollisuudesta tehdä valitus valvontaviranomaiselle.

Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän muut toimet rekisterinpitäjän oikeuksien toteuttamiseksi ovat pääsääntöisesti maksuttomia. Rekisterinpitäjä voi kuitenkin periä kohtuullisen maksun toimenpiteistään tai kieltäytyä

pyynnön toteuttamisesta, jos rekisteröidyn pyyntö voidaan osoittaa kohtuuttomaksi tai ilmeisen perusteettomaksi. Kohtuuttomaksi tietopyynnöksi voitaisiin asetuksen mukaan katsoa esimerkiksi tapaukset, joissa rekisteröity tekisi toistuvia tietopyyntöjä ilmeisen perusteettomasti.

Edellä lausuttu tarkoittaa, että hankintayksikön on kilpailutuksen vaatimuksilla varmistettava, että henkilötiedot ovat irrotettavissa tietojärjestelmästä ja liitettävissä rekisteröidylle toimitettavaan vastaukseen. Irrotettavuus tulisi toteuttaa mahdollisuuksien mukaan automatisoidusti siten, että vältetään manuaalista tietojen keräämistä järjestelmän eri osista.

3.2 Toimitettavat tiedot (artiklat 13-14)

Tietosuoja-asetuksessa on yksityiskohtaisesti kuvattu ne henkilötiedon käsittelyyn liittyvät tiedot, jotka rekisterinpitäjän tulee toimittaa rekisteröidylle henkilötiedot saatuaan. Käytännössä kyse on rekisteriselosteesta tai vastaavanlaisesta dokumentaatiosta.

Tiedot on ilmoitettava rekisteröidylle, ellei asetukselta muuta johdu. Tietoja ei esimerkiksi tarvitse antaa, jos rekisteröity on jo saanut nämä tiedot tai jos tiedot ovat salassa pidettäviä. Tietoja ei myöskään tarvitse antaa, jos tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa.

Jos henkilötiedot saadaan rekisteröidyltä itseltään, rekisteröidylle ilmoitettavat tiedot toimitetaan, kun henkilötiedot kerätään. Jos henkilötiedot saadaan muulta lähteeltä, rekisterinpitäjän on toimitettava asetuksessa mainitut tiedot rekisteröidylle kohtuullisessa ajassa, mutta viimeistään kuukauden kuluessa.

Jos henkilötietoja käytetään viestintään asianomaisen rekisteröidyn kanssa ja tiedot on saatu muulta lähteeltä kuin rekisteröidyltä itseltään, tiedot on toimitettava viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran. Jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, tiedot on toimitettavat viimeistään silloin, kun näitä tietoja luovutetaan ensimmäisen kerran.

Hankintayksikön tulee tarjouspyynnössä esittää tarvittaessa vaatimukset siitä, kuinka tiedonantovelvollisuus toteutetaan mahdollisimman automaattisesti.

3.3 Rekisteröidyn oikeus saada pääsy tietoihin (artikla 15)

Rekisteröidyllä on kohtuullisin väliajoin oikeus saada pääsy henkilötietoihin, joita hänestä on kerätty. "Kohtuullista väliaikaa" ei ole asetuksessa määritelty. Kaikilla rekisteröidyillä olisi siten oltava oikeus tietää ja saada ilmoitus erityisesti henkilötietojen käsittelyn tarkoituksista, ja jos mahdollista, käsittelyajasta, henkilötietojen vastaanottajista, käsiteltävien henkilötietojen automaattisen käsittelyn logiikasta sekä kyseisen käsittelyn mahdollisista seurauksista.

Rekisterinpitäjän pitää pyynnöstä ilmoittaa, käsittelee se kysyjää koskevia henkilötietoja. Jos henkilötietoja käsitellään, rekisteröidylle on annettava jäljennös rekisterissä olevista tiedoista, ellei ole lakisääteisiä perusteita olla antamatta pyydettyä tietoa.

Rekisteröidyn tiedonsaantioikeus koskee myös hänen henkilötietoihinsa kohdistuneita käsittelytoimia. Voidakseen informoida rekisteröityä niistä on rekisterinpitäjän pidettävä lokia tietojen käsittelytoimista: kuka tietoja on käsitelty, mitä tietoja on käsitelty ja milloin niitä on käsitelty.

Tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Rekisterinpitäjän olisi varmistuttava sellaisen rekisteröidyn henkilöllisyydestä, joka haluaa saada pääsyn tietoihin erityisesti verkkopalvelujen ja verkkotunnistetietojen yhteydessä. Esimerkiksi vahva sähköinen tunnistautuminen täyttäneen edellä kuvatun tarpeen rekisteröidyn tunnistamiseen luotettavasti.

3.4 Oikeus tietojen oikaisemiseen (artikla 16)

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheutonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Rekisteröidyllä on lähtökohtaisesti oikeus saada puutteelliset henkilötiedot täydennettyä, esimerkiksi toimittamalla rekisterinpitäjälle lisäselvitystä.

Hankintayksikön on huolehdittava, että järjestelmässä, jossa henkilötietoja käsitellään, tulee olla mahdollista korjata tietoja. Tiedon korjaamisesta tulee jäädä lokimerkintä.

3.5 Henkilötietojen oikaisua, poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus (artikla 19)

Tietosuoja-asetuksen mukaan rekisterinpitäjä on velvollinen ilmoittamaan tehdyistä henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle, jolle henkilötietoja on luovutettu, paitsi jos ilmoittaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisterinpitäjän on myös pyynnöstä ilmoitettava rekisteröidylle, keille tietoja on luovutettu.

Käytännössä rekisterinpitäjä voi esimerkiksi velvoittaa palveluntarjoajan/henkilötietojen käsittelijän ilmoittamaan suoraan tietojen vastaanottajalle niistä henkilötietojen oikaisuista, poistoista tai rajoituksista, jotka se on tehnyt sopimuksen mukaisesti.

Jotta rekisterinpitäjä voi asetuksen vaatimusten mukaisesti ilmoittaa rekisteröidylle tietojen luovutuksista, on tietojen käsittelyyn käytetystä tietojärjestelmästä tai muuten voitava selvittää, kenelle mitkäkin tiedot on luovutettu ja milloin.

3.6 Oikeus siirtää tiedot järjestelmästä toiseen (artikla 20)

Rekisteröidyllä on oikeus saada itselleen häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle. Tiedot on toimitettava jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Rekisteröidyllä on myös oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu.

Siirtämisoikeuden käyttö edellyttää, että käsittely perustuu rekisteröidyn suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti.

Kun rekisteröity käyttää tätä oikeuttaan, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.

Tämän vuoksi hankintayksikkö voi asettaa hankinnassa vaatimuksen, jonka mukaan palveluntuottajan on huolehdittava siitä, että järjestelmässä olevat henkilötiedot ovat sellaisessa teknisessä muodossa, että ne ovat vaivattomasti siirrettävissä järjestelmästä toiseen ja että siirrosta ei aiheudu hankintayksikölle lisäkustannuksia.

3.7 Vastustamisoikeus (artikla 21)

Rekisteröidyllä on oikeus vastustaa käsittelyä suoramarkkinointitarkoituksissa ja eräissä muissa tietosuoja-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa.

Käytännössä hankintayksikön on vaadittava tarjouspyynnössä, että rekisteriin voidaan merkitä suoramarkkinointikielto ja muu artikkelissa mainittu tietojen käsittelykielto.

4. Rekisterinpitäjän velvollisuudet

4.1 Rekisterinpitäjän vastuu (artikla 24)

Rekisterinpitäjä on tietosuoja-asetuksen mukaan vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan asetuksen vaatimuksia.

Toimenpiteet mitoitetaan riskiarvioinnin perusteella, jossa otetaan huomioon mm. käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit. Toimenpiteitä on arvioitava ja tarkistettava säännöllisesti ja ne on päivitettävä tarvittaessa.

Edellä kuvattujen toimenpiteiden toteuttaminen on lainsäädännön mukaan rekisterinpitäjän vastuulla. Jos rekisterinpitäjä on ulkoistanut käsittelytehtäviä, sen on sopimuksilla varmistettava, että palveluntuottaja huolehtii sovituista toimenpiteistä rekisterinpitäjän ohjeiden mukaisesti. Pystyäkseen osoittamaan, että riittävät toimenpiteet on toteutettu, rekisterinpitäjän ja palveluntuottajan tulee huolellisesti dokumentoida sovitut ja toteutetut toimenpiteet. Dokumentaatio tulee pitää ajan tasalla. Toimenpiteiden riittävyttä tulee arvioida yhteisesti säännöllisin väliajoin.

4.2 Sisäänrakennettu ja oletusarvoinen tietosuoja (artikla 25)

Tietosuoja-asetuksen mukaan rekisterinpitäjän on varmistettava, että henkilötietojen käsittelyyn käytettävä järjestelmä täyttää ns. sisäänrakennetun ja oletusarvoisen tietosuojan (privacy by design) vaatimuksen. Asetuksen mukaan rekisterinpitäjän on sekä käsittelyn suunnittelussa että itse käsittelyn osalta toteutettava tehokkaasti asetuksessa säädettyjen tietosuojaperiaatteiden täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että käsittely vastaa asetuksen vaatimuksia ja että rekisteröidyn oikeuksia suojataan. Tällaisia toimenpiteitä ovat esimerkiksi

- tiedon pseudonymisointi, tiedon minimointi
- tarvittavat suojatoimet
- koulutus, ohjeistus, määräykset, sitoumukset, tilivalvonta, omavalvonta
- prosessit, käytännesäännöt, sertifikaatit
- salausrakenteet, auditoinnit, etäkäyttöyhteydet, tekniset rajoitukset, valvontajärjestelmät.

Tarvittavia toimia arvioitaessa tulee huomioida uusin tekniikka ja toteuttamiskustannukset sekä käsittelyn aiheuttamat riskit rekisteröidyn oikeuksille ja vapauksille, käsittelyn luonne ja laajuus huomioon ottaen.

Rekisterinpitäjä voi arvioida ja määrittellä nämä toimenpiteet itse tai yhdessä palveluntuottajan kanssa. Kilpailutusvaiheessa rekisterinpitäjän tulee varmistua siitä, että palveluntuottaja on sopimuksellisesti sitoutunut siihen, että hankittava tietojen käsittelyjärjestelmä tai -palvelu täyttää sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset. Rekisterinpitäjän velvollisuuksien ja rekisteröidyn oikeuksien toteutuminen on huomioitava ja varmistettava jo tietojärjestelmän määrittelyssä ja toteutuksessa.

Sopimusehto:

Toimittaja noudattaa voimassa olevan henkilötietolainsäädännön edellyttämää hyvää tietojen käsittelytapaa ja henkilötietojen suojaamista koskevia säännöksiä. Toimittaja vastaa siitä, että palvelu on kulloinkin voimassa olevan henkilötietolainsäädännön ja tämän sopimuksen vaatimusten mukainen, ottaen erityisesti huomioon, mitä on säädetty sisäänrakennetusta ja oletusarvoisesta tietosuojasta.

4.3 Tietosuojavastaavan nimittäminen, asema ja tehtävät (artiklat 37-39)

Joissain organisaatioissa on aina nimitettävä tietosuojavastaava. Tietosuojavastaava on nimitettävä aina kun

- käsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin
- rekisterinpitäjän tai käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen seuraamista
- rekisterinpitäjän tai käsittelijän ydintehtävät muodostuvat arkaluonteisten tietojen laajamittaisesta käsittelystä tai rikostuomioihin liittyvien tietojen laajamittaisesta käsittelystä.

Tietosuojavastaava voi olla yhteinen konsernitasolla ja viranomaiset voivat nimittää yhteiset tietosuojavastaavat.

Tietosuojavastaava on riippumaton ja raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle.

Sopimusehto:

Jos sopijapuoli on velvollinen nimeämään tietosuojavastaavan, sopijapuoli ilmoittaa kirjallisesti tietosuojavastaavan yhteystiedot toiselle sopijapuolelle.

5. Henkilötietojen käsittely

5.1 Henkilötietojen käsittelijä (artikla 28)

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suoja-toimet asianmukaisten teknisten ja organisaattoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuojasetuksen vaatimukset.

Henkilötietojen käsittelijän vastuu on määritettävä sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään. Sopimuksessa on määriteltävä vähintään käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

Sopimusehto:

Toimittaja noudattaa henkilötietojen käsittelijänä tämän sopimuksen liitteenä olevia ehtoja henkilötietojen käsittelystä.

Toimittaja ei saa käyttää henkilötietojen käsittelyyn alihankkijan palveluja ilman Tilaajan antamaa kirjallista ennakkolupaa.

5.2 Tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa (artikla 29)

Henkilötietoja saa käsitellä vain rekisterinpitäjän ohjeiden mukaisesti, ellei lainsäädännöstä muuta johdu.

Sopimusehto:

Toimittaja ei käytä taikka muulla tavoin hyödynnä sopimuksen perusteella käsittelemiään henkilötietoja muuhun kuin sopimuksen täyttämisen mukaiseen tarkoitukseen ja silloinkin ainoastaan tarkoituksen edellyttämässä laajuudessa ja tilaajan antaman ohjeistuksen mukaisesti.

5.3 Käsittelyn turvallisuus (artikla 32)

Tietosuojasetus velvoittaa riskilähtöisen turvallisuustason arviointiin ja tietoturva-vaatimusten asettamiseen. Koko käsittelyn ja henkilötietojen elinkaaren aikana on arvioitava prosessien, käsittelyn ja järjestelmien turvallisuustaso. Arvioinnissa kiinnitetään huomiota mm. käsittelyn luonteeseen ja laajuuteen. Asetuksen mukaan sekä rekisterinpitäjä että henkilötietojen käsittelijä arvioivat turvallisuustason riittävyyttä.

Rekisterinpitäjän on, jo ennen tarjouspyynnön tekemistä, määriteltävä henkilötietojen käsittelylle asianmukainen turvallisuustaso ja asetettava teknisiä ja organisatorisia vaatimuksia kyseisen turvallisuustason saavuttamiseksi. Asetus määrittelee toimet turvallisuustason arvioimiseksi sekä ohjeistaa vaatimustenasettelua. Rekisterinpitäjä ei voi siirtää tätä vastuuta.

Riskilähtöisen turvallisuustason arvioinnissa tulee kiinnittää huomiota käsittelyn sisältämiin riskeihin, jotka voivat erityisesti liittyä siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvaan tai laittomaan tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai henkilötietoihin pääsyyn.

Käytännössä turvallisuustason arvioinnissa voidaan huomioida mm.

- hankinnan kohteena olevassa palvelussa tai järjestelmässä käsiteltävien tietojen suojaustasoluokittelu, sekä
- hankinnan kohteena olevan palvelun tai järjestelmän oma luokittelu, jolloin arvioidaan mm.
 - > millaisia tietoja käsitellään
 - > onko luottamuksellisuus, käytettävyys vai eheys keskeisenä vaatimuksena
 - > käsittelyn, palvelun tai järjestelmän merkitys organisaation ydintoiminnalle
 - > käsittelyn, palvelun tai järjestelmän merkitys asiakkaille tai muulle toimintaverkostolle
 - > käsittelyn, palvelun tai järjestelmän merkitys yhteiskunnalle ja välillisille asiakkaille.

Turvallisuustason määrittely johtaa tietoturva- ja tietosuojavaatimusten asettamiseen. Asetuksen mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, joita voivat asetuksen mukaan olla esimerkiksi:

- henkilötietojen pseudonymisointi ja salaus
- kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuesssa
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Tukena vaatimusten asettamisessa voidaan myös käyttää VAHTI-tietoturvasoivaatimuksia.

Vaatimukset, tai asetuksen kielellä toimenpiteet, otetaan tarjouspyynnön ja mahdollisen tietoturvasopimuksen liitteeksi, sekä sisällytetään tarvittavin osin suoraan sopimukseen.

Sopimusehto:

Toimittaja huolehtii tämän sopimuksen perusteella käsittelemiensä henkilötietojen asianmukaisesta suojaamisesta omien käytäntöjensä, sopimuksen vaatimusten ja tilaajan kirjallisen ohjeistuksen mukaisesti varmistaa henkilötietojen luottamuksellisuuden, eheyden ja saatavuuden.

Sopimusehto:

Toimittaja dokumentoi sovitut ja toteutetut toimenpiteet ja huolehtii siitä, että dokumentaatio on ajan tasalla. Sopijapuolet arvioivat edellä tarkoitettuja teknisiä ja organisatorisia toimenpiteitä ja niiden riittävyttä säännöllisesti.

5.4 Tietoturvaloukkauksesta ilmoittaminen (artiklat 33-34)

Tietosuoja-asetuksen mukaan rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle 72 tunnin kuluessa loukkauksen ilmitulosta. Asetuksen 33 artiklasta ilmenee

vaatimukset valvontaviranomaiselle tehtävän ilmoituksen sisällölle.

Ilmoitusta ei tarvitse kuitenkaan tehdä tilanteissa, joissa loukkaus ei todennäköisesti aiheuttaisi rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä. Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivästyä saatuaan loukkauksen tietoonsa.

Tämän lisäksi rekisterinpitäjän on ilmoitettava rekisteröidylle henkilötietojen tietoturvaloukkauksesta, mikäli loukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidyn oikeuksille ja vapauksille. Ilmoitus vastaa keskeiseltä sisällöltään valvontaviranomaiselle annettavaa ilmoitusta.

Ilmoitusta ei tarvitse tehdä, jos rekisterinpitäjä on toteuttanut toimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu tai jos ilmoitus vaatisi kohtuutonta vaivaa, jolloin ilmoituksen sijaan käytetään julkista tiedonantoa tai muuta vastaavaa toimenpidettä.

Rekisterinpitäjän on sopimuksen määräyksillä varmistettava, että se saa palveluntuottajalta viivytystä riittävät tiedot tietoturvaloukkauksesta ja sen vaikutuksista, jotta rekisterinpitäjä voi täyttää oman 72 tunnin ilmoitusvelvollisuutensa valvontaviranomaiselle. Tällaisesta toimittajan ilmoittamisvelvollisuudesta on ehto liitteessä 1.

5.5 Tietosuoja koskeva vaikutustenarviointi ja ennakkokuuleminen (artiklat 35-36)

Asetuksen mukaan rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista arvioitava suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojalle. Tällainen vaikutustenarviointi on tehtävä, jos käsittely, etenkin uutta teknologiaa käytettäessä, todennäköisesti aiheuttaa korkean riskin luonnollisen henkilön oikeuksille ja vapauksille.

Jos vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin ja rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi, rekisterinpitäjän on ennen käsittelyn aloittamista kuultava valvontaviranomaista. Valvontaviranomainen voi esimerkiksi antaa rekisterinpitäjälle kirjalliset ohjeet käsittelylle.

Rekisterinpitäjän pitää sisällyttää em. ohjeiden mukaiset toimet sopimukseen siltä osin kuin niiden mukaiset toimenpiteet ovat palveluntuottajan vastuulla.

6. Henkilötietojen siirrot kolmansiiin maihin

6.1 Siirtoja koskeva yleinen periaate (artikla 44)

Henkilötietojen siirron ETA-alueen ulkopuolelle voi toteuttaa ainoastaan, jos rekisterinpitäjä ja henkilö-tietojen käsittelijä noudattavat tietosuoja-asetukses-sa vahvistettuja edellytyksiä.

Siirrot kolmansiiin maihin aktualisoituvat esim. pilvipalvelun käytön yhteydessä. Pilvipalvelut saattavat käyttää ETA:n ulkopuolella sijaitsevia palvelimia. Pilvipalvelun tietojenkäsittelylaitteisto voi olla ETA:n ulkopuolisen palveluntarjoajan hallinnassa. Molemmissa näissä tapauksissa henkilötietojen siirtojen pilvipalveluun täytyy tapahtua asetuksen kolmansia maita koskevien sääntöjen mukaisesti.

Hankintayksikön tulee tarjouspyynnössä ottaa kantaa siihen, voidaanko henkilötietoja käsitellä ETA:n ulkopuolella. On hyvä muistaa, että käsittely tulkitaan laajasti ja että esimerkiksi etäyhteydellä tapahtuva pääsy tai tietojen tallentaminen ETA:n ulkopuolella olevaan pilvipalveluun täyttää käsittelyn tunnusmerkit. Jos tietoja käsitellään näissä ns. kolmansissa maissa, hankintayksikön on sopimuksessa todettava, mikä on lainmukainen peruste tietojen siirtoon sekä veloitettava palveluntuottaja ja sen alihankkijat sitoutumaan EU:n tietosuoja-asetuksen noudattamiseen komission mallilausekkein, vakiosopimusehdoin tai muilla asetuksessa määritellyillä suojatoimilla.

Sopimusehto:

Toimittaja käsittelee henkilötietoja ainoastaan sovitulla palvelutuotantoalueella. Mitä tässä sopimuksessa sovitaan henkilötietojen käsittelystä, koskee myös pääsyn mahdollistamista henkilötietoihin esimerkiksi hallinta- ja valvontayhteyden välityksellä.

Toimittajalla on oikeus käsitellä henkilötietoja ainoastaan Euroopan talousalueella (EU-jäsenvaltiot, Islanti, Norja ja Liechtenstein), elleivät sopijapuolet ole sopineet henkilötietojen käsittelyn tapahtuvan ainoas-

taan Suomessa eikä tämän sopimuksen mukaisista vaatimuksista muuta johdu. Muut kuin edellä mainitut valtiot ovat jäljempänä tarkoitettuja "kolmansia maita".

Toimittaja voi käsitellä henkilötietoja kolmansissa maissa ainoastaan, jos käsittelystä on sovittu kirjallisesti Tilaajan kanssa ja käsittely täyttää tietosuoja-asetuksen V luvun mukaiset käsittelyn edellytykset.

Tämän kohdan mukaisessa tarkoituksessa sopijapuolet toimivat yhteistyössä varmistaa ne asianmukaiset toimenpiteet, joiden perusteella tietojen käsittely kolmansissa maissa täyttää tietosuoja-asetuksen vaatimukset. Toimittaja ei ole oikeutettu veloittamaan kuluja ja kustannuksia, joita sille voi aiheutua tietojenkäsittelyn saattamiseksi tietosuoja-asetuksen vaatimusten mukaiseksi tai tämän kohdan mukaisesta yhteistyöveloitteesta.

Huomaa, että tämän asiakirjan liitteenä olevissa ehtoissa on myös henkilötietojen siirtämiseen liittyviä ehtoja. Tekstejä on hyvä verrata toisiinsa ja tehdä harkinta siitä, määrätäänkö asiasta varsinaisissa sopimusehdoissa vai liitteen 1 mukaisissa ehtoissa.

6.2 Siirto tietosuojan riittävyttä koskevan päätöksen perusteella (artikla 45)

Henkilötietojen siirto voidaan toteuttaa kolmanteen maahan ilman erityistä lupaa, jos komissio on päättänyt, että kyseinen kolmas maa varmistaa riittävän tietosuojan tason.

Artiklassa 45 säädetään komission toimivallasta antaa edellä mainittuja päätöksiä. Kolmansiiin maihin rinnastetaan myös kolmannen maan tietty alue tai kolmannen maan sektori sekä kansainväliset järjestöt.

Komissio julkaisee Euroopan unionin virallisessa lehdessä ja verkkosivustollaan luettelon niistä kolmansista maista, joiden osalta se on päättänyt, että tietosuojan taso on tai ei enää ole riittävä. Tällä hetkellä

luettelo on löydettävissä osoitteesta: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

6.3 Siirto asianmukaisia suojatoimia soveltaen (artikla 46)

Jos komissio ei ole tehnyt 45 artiklan mukaista päätöstä riittävän tietosuojan tasosta kolmannessa maassa, rekisterinpitäjä tai käsittelijä voi siirtää henkilötietoja kolmanteen maahan, jos kyseinen rekisterinpitäjä tai käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.

Asetuksessa luetellaan ne asianmukaiset suojatoimet, joihin ei tarvita valvontaviranomaiseen lupaa:

- viranomaisten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen sopimus
- valvontaviranomaisen hyväksymät yritystä koskevat sitovat säännöt
- komission antamat tietosuojaa koskevat vakio-lausekkeet
- tietosuojaa koskevat vakio-lausekkeet, jotka tietosuojaviranomainen on vahvistanut ja komissio hyväksynyt
- hyväksytyt käytännesäännöt ja sopimus yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän kanssa - näissä on turvattava asianmukaisten suojatoimien soveltaminen ja rekisteröityjen oikeudet
- hyväksytty sertifiointimekanismi ja sopimus yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän kanssa - näissä on turvattava asianmukaisten suojatoimien soveltaminen ja rekisteröityjen oikeudet.

Lisäksi on suojatoimet, jotka voidaan toteuttaa toimivaltaisen valvontaviranomaisen luvalla. Näitä voivat olla erityisesti seuraavat:

- rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön rekisterinpitäjän, henkilötietojen käsittelijän tai vastaanottajan väliset sopimuslausekkeet
- säännökset, jotka sisällytetään viranomaisten välisiin hallinnollisiin järjestelyihin ja joihin sisältyy rekisteröityjen täytäntöönpanokelpoisia ja tehokkaita oikeuksia.

6.4 Yritystä koskevat sitovat säännöt (artikla 47)

Yritysten, jotka säännönmukaisesti siirtävät henkilötietoja eri maissa sijaitsevien konsernin osien välillä, on hyvä laatia yrityksiä koskevat sitovat säännöt, jotka tietosuojaviranomainen vahvistaa. Tarjoajayritykseltä voidaan tietyissä tilanteissa vaatia esimerkiksi tällaisten sääntöjen olemassaoloa ja noudattamista, jos henkilötietoja sopimuksen mukaan käsitellään kolmansissa maissa.

6.5 Erityistilanteita koskevat poikkeukset (artikla 49)

Tietojen siirto kolmansiin maihin on mahdollinen, jos EU:n komissio on tehnyt kyseistä kolmatta maata koskeva päätöksen tietosuojan riittävästä tasosta. Jos tällaista päätöstä ei ole tehty, eikä ole vahvistettu kyseistä yritystä sitovia sääntöjä, siirto kolmansiin maihin voidaan kuitenkin toteuttaa satunnaisesti tietosuojasetuksessa säädettyjen edellytysten täytyessä, ellei tietojen luovuttamista ole nimenomaisesti muussa lainsäädännössä rajoitettu tärkeän yleisen edun vuoksi. Rekisterinpitäjän on huolehdittava siitä, että siirron lainmukaisuuden arviointi ja tehdyt suojatoimet dokumentoidaan asianmukaisesti.

7. Oikeussuoja ja seuraamukset

7.1 Oikeussuoja

Tulevassa kansallisessa tietosuojalaissa ehdotetaan perustettavaksi tietosuojavirasto, joka toimii tietosuojasetuksessa tarkoitettuna valvontaviranomaisena. Jos rekisterinpitäjä kieltäytyy toteuttamasta toimenpiteitä rekisteröidyn pyynnöstä, rekisteröity voi viedä asian tietosuojaviraston käsiteltäväksi.

Tietosuojavirasto voi myös tietosuojasetuksen nojalla toteuttaa omia tarkastuksia ja antaa niiden tulosten perusteella esimerkiksi varoituksia tai rekisterinpitäjän toimintaa koskevia määräyksiä, taikka määrätä hallinnollisia sakkoja.

Tietosuojaviraston päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen. Valitusoikeus on asianosaisilla.

7.2 Vastuu ja oikeus korvauksen saamiseen (artikla 82)

Tietosuojasetuksen mukaan henkilöllä, jolle on aiheutunut tietosuojasetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta joko rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjä ja kaikki käsittelijät ovat siis yhteisvastuussa käsittelyn lainmukaisuudesta suhteessa rekisteröityyn. Korvauksen suorittanut osapuoli voi periä aiheetta maksamansa osuuden muilta yhteisvastuullisilta sen mukaisesti, mikä kunkin vastuulla oleva osuus vahingosta oli.

Rekisterinpitäjällä on lähtökohtaisesti ns. ankara vastuu. Rekisterinpitäjä on siis aina vastuussa vahingosta, joka on aiheutunut sellaisesta henkilötietojen käsittelystä, joka ei ole ollut tietosuojasetuksen mukaista. Rekisterinpitäjä vapautuu vastuusta vain, jos se pystyy osoittamaan, että tapahtuma oli sen vaikutusmahdollisuuksien ulkopuolella.

Henkilötietojen käsittelijän vastuu on toissijaista. Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut tietosuojasetuksessa käsittelijälle nimennomaisesti asetettuja velvoitteita tai rekisterinpitäjän lainmukaista ohjeistusta. Käsittelijän tulee siten pystyä osoittamaan, että se on noudattanut edellä tarkoitettuja velvoitteita ja ohjeita.

Hankintasopimukseen voidaan ottaa määräys, jonka mukaan käsittelijän tulee ilmoittaa rekisterinpitäjälle, jos tämän antama ohjeistus on puutteellinen tai jos käsittelijä epäilee sitä lainvastaiseksi. Tällainen ehto on kirjattu liitteeseen 1.

7.3 Hallinnolliset sakot ja muut seuraamukset (artikla 83)

Rekisteröidylle suoritettavan vahingonkorvauksen lisäksi rekisterinpitäjä ja henkilötietojen käsittelijä voivat joutua maksamaan hallinnollisia sakkoja tietosuojasetuksen rikkomisen perusteella. Hallinnollisen sakon määrä voi olla enintään 20 000 000 euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Hallinnollisten sakkojen ohella tai niiden sijasta valvontaviranomaisilla on käytettävissään useita muita keinoja rekisterinpitäjien ohjaamiseen ja lainvastaisen käsittelyn lopettamiseen. Tällaisia keinoja ovat esimerkiksi huomautus tai varoitus rekisterinpitäjälle, määräys saattaa käsittely lain mukaiseksi annettussa määräajassa, määräys korjata lainvastainen tilanne tai oikaista virheelliset tiedot, käsittelyrajoitusten asettaminen sekä määräys tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle.

LIITE _____ SOPIMUKSEEN NRO _____

Henkilötietojen käsittelyn ehdot

OHJE HANKINTAYKSIKÖLLE: Tarkista tämän ohjeen ehdot sekä tässä viitatussa 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 Tilaaja on tehnyt Toimittajan kanssa.
- 1.2. Tässä sopimusliitteessä määritellään Tilaajaa ja Toimittajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat sopimusehdot, joiden mukaisesti Toimittaja Tilaajan toimeksiannosta käsittelee henkilötietoja Tilaajan 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.

2. Osapuolten roolit henkilötietojen käsittelyssä

- 2.1. Tilaaja toimii henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön tarkoituksena rekisterinpitäjänä, silloin kun se määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Osapuolet ymmärtävät, että rekisterinpitäjänä Tilaaja saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää voimassaolevan henkilötietojen käsittelyyn ja tietosuojaan liittyvän lainsäädännön vaatimukset ja 25.5.2018 alkaen EU:n yleisen tietosuoja-asetuksen vaatimukset, ja että sillä varmistetaan rekisteröidyn oikeuksien suojeleminen.
- 2.2. Toimittaja toimii henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön tarkoituksena henkilötietojen käsittelijänä, joka käsittelee Tilaajan henkilötietoja Tilaajan puolesta ja lukuun. Toimittajan Sopimuksen ja tämän sopimusliitteen mukaisesti käyttämät alihankkijat, jotka osallistuvat Tilaajan henkilötietojen käsittelyyn, toimivat myös henkilötietojen käsittelijöinä Tilaajan puolesta ja lukuun. Ryhmittymän ollessa Toimittajana tämän sopimusliitteen velvoitteet koskevat kaikkia ryhmittymän jäseniä, ja ryhmittymän käyttämiä alihankkijoita, jotka osallistuvat henkilötietojen käsittelyyn.
- 2.3. Tilaaja sitoutuu huolehtimaan henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön mukaisista rekisterinpitäjän velvollisuuksista.
- 2.4. Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän ja käsittelijän velvollisuudet ja oikeudet kuvataan Sopimuksessa, sopimuksen mukaisen palvelun aikana laadittavassa ja Toimittajaa sitovassa dokumentaatioissa tai muussa Tilaajan ohjeistuksessa. Toimittaja sitoutuu noudattamaan Sopimuksessa, dokumentaatioissa ja ohjeistuksessa olevia henkilötietojen käsittelyä koskevia ehtoja ja kuvauksia. Tilaaja vastaa ohjeistuksen ylläpidosta ja saatavuudesta.

LIITE _____ SOPIMUKSEEN NRO _____

- 2.5. Jos kohdan 2.4 mukaista kuvausta ei ole tehty tai se on puutteellinen, Tilaaja laatii tai täydentää kuvausta tarvittaessa yhteistyössä Toimittajan kanssa. Toimittajan on ilmoitettava Tilaajalle, jos tämän antama ohjeistus on puutteellinen tai jos Toimittaja epäilee sitä lainvastaiseksi.
- 2.6. Toimittaja osallistuu Tilaajan pyynnöstä tietojärjestelmäselosteen laatimiseen. Toimittaja suorittaa vaatimuksen mukaiset tehtävät Sopimuksen mukaisilla henkilötyöhinnoilla, ellei toisin ole sovittu.

3. Alihankkijat, jotka käsittelevät henkilötietoja

- 3.1. Toimittaja ei saa käyttää henkilötietojen käsittelyyn alihankkijan palveluja ilman Tilaajan antamaa kirjallista ennakkolupaa. Toimittajan on tiedotettava Tilaajalle kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat henkilötietojen käsittelijöinä toimivien alihankkijoiden lisäämistä tai vaihtamista, ja annettava Tilaajalle mahdollisuus vastustaa tällaisia muutoksia.
- 3.2. Siltä osin kuin Toimittaja käyttää toiminnassaan alihankkijoita, jotka käsittelevät henkilötietoja, alihankintaan sovelletaan Sopimuksen lisäksi tässä sopimusliitteessä kuvattuja ehtoja.
- 3.3. Toimittaja ja sen alihankkijat, jotka henkilötietojen käsittelijöinä käsittelevät Tilaajan henkilötietoja Tilaajan puolesta ja lukuun, sitoutuvat kaikki tässä sopimusliitteessä kuvattuihin henkilötietojen käsittelijää koskeviin velvollisuuksiin. Toimittajalla on velvollisuus sopimuksilla sitouttaa käyttämänsä alihankkijat noudattamaan tämän sopimusliitteen ehtoja.
- 3.4. Toimittaja on vastuussa mahdollisista Tilaajan henkilötietoja käsittelevien Toimittajan alihankkijoiden Sopimuksen, tämän sopimusliitteen tai sovellettavan lainsäädännön taikka EU:n yleisen tietosuojasetuksen rikkomisista tai laiminlyönneistä kuin omistaan. Jos tietojen käsittelyä suorittava alihankkija ei täytä tietosuojavelvoitteitaan, Toimittaja on edelleen täysimääräisesti vastuussa suhteessa Tilaajaan. Jos Tilaaja perustellusti katsoo, että Toimittajan alihankkija ei täytä tietosuojavelvoitteitaan, Tilaajalla on oikeus vaatia Toimittajaa vaihtamaan alihankkijaa.

4. Henkilötietojen käsittelijän yleiset velvollisuudet

- 4.1. Henkilötietojen käsittelijä käsittelee henkilötietoja Sopimuksen ja Tilaajan antamien ohjeiden mukaisesti.
- 4.2. Henkilötietojen käsittelijä sitoutuu varmistamaan, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.
- 4.3. Sen lisäksi, mitä Sopimuksessa on sovittu henkilötietojen suoja, tietoturvallisuutta ja tietojen salassapitoa koskevista vaatimuksista, henkilötietojen käsittelijä sitoutuu toteuttamaan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn turvallisuuden varmistamiseksi ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit sekä noudattamaan Tilaajan ohjeita ja mahdollisia Tilaajan ohjeiden päivityksiä.
- 4.4. Henkilötietojen käsittelijän on myös toteutettava toimenpiteet sen varmistamiseksi, että jokainen henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan Sopimuksen ja Tilaajan ohjeiden mukaisesti.

LIITE _____ SOPIMUKSEEN NRO _____

- 4.5. Henkilötietojen käsittelijä sitoutuu ilman aiheetonta viivästystä ilmoittamaan Tilaajalle kaikista rekisteröityjen pyynnöistä, jotka koskevat voimassaolevan lainsäädännön sekä EU:n yleisen tietosuoja-asetuksen mukaisten rekisteröidyn oikeuksien käyttämistä.
- 4.6. Henkilötietojen käsittelijä sitoutuu avustamaan Tilaajaa asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, jotta Tilaaja pystyy täyttämään velvollisuutensa vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Henkilötietojen käsittelijä ymmärtää, että näiden oikeuksien käyttämistä koskevat pyynnöt voivat edellyttää siltä avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa ja/tai henkilötietojen siirtämisessä järjestelmästä toiseen. Ellei näiden tehtävien ole sovittu sisältyvän Sopimuksen mukaisiin palveluihin ja niistä veloittaviin maksuihin, Toimittajalla on oikeus veloittaa kohtuulliset työkustannukset Sopimuksessa sovitulla henkilötyöhinnolla.
- 4.7. Toimittajan on huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan automaattisesti irrottaa järjestelmästä siirrettäväksi toiseen järjestelmään.
- 4.8. Henkilötietojen käsittelijä sitoutuu tarvittaessa avustamaan Tilaajaa EU:n yleisen tietosuoja-asetuksen mukaisen tietosuoja koskevan vaikutustenarvioinnin tekemisessä, mahdollisessa ennakkokuulemisessa ja mahdollisen tietosuoja koskevan sertifiointin hankkimisessa. Toimittajalla on oikeus veloittaa kohtuulliset työkustannukset Sopimuksessa sovitulla henkilötyöhinnolla.
- 4.9. Henkilötietojen käsittelijä sitoutuu Tilaajan valinnan mukaan poistamaan tai palauttamaan käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki Tilaajan henkilötiedot Tilaajalle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot. Tilaaja voi antaa tältä osin tarkempia ohjeita henkilötietojen käsittelijälle.
- 4.10. Henkilötietojen käsittelijä ei saa siirtää henkilötietoja EU:n tai ETA-alueen ulkopuolelle. Henkilötietojen siirtäminen kolmansiin maihin voidaan tehdä asianmukaisella siirtosopimuksella noudattaen EU-komission kulloinkin voimassa olevia mallilausekkeita ja/tai muita tuolloin voimassa olevia henkilötietojen siirtoa koskevia vaatimuksia.
- 4.11. Henkilötietojen käsittelijä saattaa Tilaajan saataville kaikki tiedot, jotka ovat tarpeen tässä sopimusliitteessä kuvattujen velvollisuuksien noudattamisen osoittamista varten, ja sallii Tilaajan valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin. Auditointia koskevat tarkemmat ehdot ovat Sopimuksessa.

5. Henkilötietojen käsittelijän erityiset velvollisuudet

- 5.1. Toimittajalla on oltava valmius asettaa ja hallinnoida tietojen luovutuksia koskevia rajoituksia, jollaisia voi aiheutua esimerkiksi väestötietolain mukaisesta rekisteröidyn turvakiellosta. Toimittajan tulee pystyä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan Tilaajan vaatimalla tavalla. Rekisteröidyn henkilötietojen rajoittaminen ei saa johtaa muiden rekisterissä olevien luonnollisten henkilöiden henkilötietojen rajoittamiseen, ellei Tilaajan ja Toimittajan kesken kirjallisesti toisin sovita.
- 5.2. Ellei toisin sovita, Toimittaja on velvollinen ylläpitämään luetteloa rekisteröityjen henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista. Luettelo on luovutettava pyydettyä Tilaajalle. Tilaaja

LIITE _____ SOPIMUKSEEN NRO _____

jan pyynnöstä Toimittajan on luovutettava luettelossa mainittuja tietoja Tilaajan pyytämässä laajuudessa Tilaajan yksilöimille kolmansille tahoille.

6. Tietoturvaloukkaukset


- 6.1. Henkilötietojen käsittelijän on ilmoitettava kirjallisesti henkilötietojen tietoturvaloukkauksesta Tilaajalle ilman aiheetonta viivytystä saatuaan sen tietoonsa ja viimeistään 36 tunnin kuluessa. Lisäksi Toimittaja sitoutuu ilmoittamaan Tilaajalle muista Toimittajan tuottaman palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Ilmoitus on tehtävä edellä mainitussa määräajassa, ellei Sopimuksessa tai sen liitteissä ole sovittu lyhyemmästä määräajasta.
- 6.2. Henkilötietojen käsittelijän on annettava Tilaajalle vähintään seuraavat tiedot tietoturvaloukkauksesta:
 - 1) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;
 - 2) ilmoitettava tietosuojavastaava tai muu vastuuhenkilö, jolta voi saada asiassa lisätietoja;
 - 3) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset; sekä
 - 4) kuvattava toimenpiteet, joita kyseinen henkilötietojen käsittelijä ehdottaisi tai joita se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

7. Muita vaatimuksia

- 7.1. Tilaajalla on oikeus muuttaa, täydentää ja päivittää Toimittajalle antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Nämä ohjeet voivat olla henkilötietojen käsittelyä tai tietosuojaa koskeviin teknisiin tai organisatorisiin toimenpiteisiin liittyviä muutoksia, täydennyksiä tai päivityksiä. Toimittaja tekee tarvittavat muutostyöt Tilaajan ohjeiden mukaisesti. Jos Tilaajan ohjeet aiheuttavat Toimittajalle olennaisia muutostöitä (yli yksi (1) henkilötyöpäivää), lisäkustannuksista sovitaan erikseen hintaliitteen mukaisesti. Toimittaja ja muut henkilötietojen käsittelijät sitoutuvat noudattamaan näitä muutettuja, täydennettyjä tai päivitettyjä ohjeita.
- 7.2. Osapuolet ymmärtävät, että Sopimuksessa ja sen liitteissä käsitellään myös tietosuojaa koskevia aiheita.
- 7.3. Toimittaja sitoutuu reagoimaan viimeistään 72 tunnin kuluessa Tilaajan yhteydenotosta ja vastamaan viimeistään yhden (1) viikon kuluessa Tilaajan tietosuojaa koskeviin ilmoituksiin, reklamaatioihin tai muihin viesteihin, pois lukien EU:n yleisen tietosuojasetuksen mukaiset tietoturvaloukkaukset, joihin sovelletaan Sopimuksessa ja edellä tässä liitteessä määritettyjä määräaikoja.
- 7.4. Jos Toimittaja laiminlyö tai rikkoo tätä sopimusliitettä, sovellettavaa lainsäädäntöä tai EU:n yleistä tietosuojasetusta, Toimittajan korvausvastuu on määritelty Sopimuksen lisäksi sovellettavassa lainsäädännössä. Lisäksi tällainen laiminlyönti tai rikkomus muodostaa Sopimuksessa tarkoitetun olennaisen sopimusrikkomuksen, jonka seurauksena Tilaajalla on halutessaan oikeus turvautua Sopimuksessa määriteltyihin oikeussuojakeinoihin.

LIITE _____ SOPIMUKSEEN NRO _____

- 7.5. Osapuolet ymmärtävät, että Sopimusta ja tätä sopimusliitettä tehtäessä tietosuojaa koskeva lainsäädäntö on muutostilassa. Jos kyseiseen lainsäädäntöön tai sitä tai sen tulkintaa koskeviin suosituksiin, ohjeistuksiin tai määräyksiin tulee muutoksia, jotka vaikuttavat Tilaaajan asemaan tai velvollisuuksiin tai tässä sopimusliitteessä määriteltyihin velvollisuuksiin tai vastuisiin, tätä sopimusliitettä voidaan tarvittaessa niiltä osin tarkistaa. Jos tähän sopimusliitteeseen tehdään sellaisia muutoksia, joista aiheutuu Toimittajalle olennaisia lisäkustannuksia (yli yksi (1) henkilötyöpäivää), niiden korvaamisesta voidaan sopia erikseen Sopimuksen hintaliitteen hintojen mukaisesti. Toimittaja ja muut henkilötietojen käsittelijät sitoutuvat noudattamaan kyseistä tarkistettua sopimusliitettä.

A photograph of a wooden desk in a bright, sunlit room. On the desk, there is a white mug, a blue notebook, a white tablet, a red pencil, a white smartphone, a set of colored pencils, and a white mouse. The background is a blurred view of green foliage and a wooden fence, suggesting an outdoor or semi-outdoor setting.

Versio 1.0 Toukokuu 2017

Työryhmä

Katariina Huikko, Julkisten hankintojen neuvontayksikkö
Jukka Hämäläinen, Hansel Oy
Pauliina Juntunen, KL-Kuntahankinnat Oy
Karolina Lehto, Hansel Oy
Ida Sulin, Kuntaliitto ry