

Henkilötietojen käsittelyn ohjeet

Henkilötietojen Käsittelijälle

V A A S A .

Henkilötietojen käsittelyn ohjeet

Henkilötietojen Käsittelijän velvollisuudet

Henkilötietojen Käsittelijän velvollisuus on noudattaa voimassa olevaa tietosuojalainsäädäntöä, henkilötietojen käsittelysopimusta (DPA) mahdollisine liitteineen ja Rekisterinpitäjän kirjallisia ohjeita. Käsittelijällä on velvollisuus ilmoittaa ilman aiheetonta viivytystä Rekisterinpitäjälle, jos Rekisterinpitäjän ohjeistus on voimassa olevan tietosuojalainsäädännön vastaista. Käsittelijän tulee noudattaa henkilötiedon käsittelyssä tietosuoja-asetuksessa (679/2016, EU, artikla 5) määriteltyjä peruseriaatteita ja Käsittelijälle määriteltyjä velvoitteita (679/2016, EU, artikla 28).

Henkilötietojen Käsittelijä varmistaa, että jokainen sen alaisuudessa toimiva henkilö, jolla on pääsy Rekisterinpitäjän henkilötietoihin, on tietoinen henkilötietojen käsittelyyn liittyvistä ohjeista, velvoitteista ja salassapitoehdoista sekä käsittelee niitä ainoastaan sopimuksen, voimassa olevan tietosuojalainsäädännön ja näiden ohjeiden mukaisesti.

Henkilötietojen Käsittelijä dokumentoi sen noudattamat henkilötietojen käsittelyyn liittyvät menettelyt, ja saattaa Rekisterinpitäjän pyytäessä Rekisterinpitäjän saataville kaikki tarvittavat ja kohtuulliset tiedot, jotka osoittavat, että Käsittelijä on noudattanut tämän sopimusliitteen ja sovellettavan tietosuojalainsäädännön mukaisia velvollisuuksiaan.

Käsittelijä saattaa Rekisterinpitäjän saataville tämän pyynnöstä kaikki tiedot, jotka Rekisterinpitäjä tarvitsee Rekisterinpitäjälle ja Henkilötietojen Käsittelijälle säädettyjen velvollisuuksien noudattamisen osoittamista varten (osoitusvelvollisuus), ja osallistuu pyydettyäessä sovitulla tavalla Rekisterinpitäjän vastuulla olevien kuvausten ja muiden dokumenttien, kuten vaikutustenarvioinnin, laatimiseen ja ylläpitämiseen sekä tietosuoja-asetuksen mukaisen ennakkuulemisen suorittamiseen.

Käsittelijä nimeää ja ilmoittaa kirjallisesti tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön liitteeseen Rekisterinpitäjälle tarvittavia yhteydenottoja varten.

Kaikkiin henkilötietoja sisältäviin tietojärjestelmiin kirjaudutaan henkilökohtaisella tunnuksella. Omia tunnuksia ei saa antaa kenenkään toisen käyttöön. Käyttöoikeuksia myönnetään vain niille henkilöille, jotka tarvitsevat niitä työtehtäviensä suorittamiseksi, ja vain siinä laajuudessa kuin se on työtehtävien vuoksi tarpeen. Mikäli työtehtävät muuttuvat tai henkilö lähtee pois sopimuskumppanin palveluksesta, on



Yksikkö

PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

käyttöoikeudet välittömästi poistettava, ellei niiden säilyttämiselle ole perustetta. Kun käyttöoikeuksia myönnetään, on käyttäjien sitouduttava siihen, että he käyttävät käyttöoikeuksiaan vain työtehtäviin eivätkä käy katsomassa sellaisia henkilötietoja, joita eivät työssään tarvitse. Erityisen tarkka tulee olla myönnettäessä käyttöoikeuksia järjestelmiin, jotka sisältävät erityisiä henkilötietoryhmiä / salassa pidettäviä henkilötietoja.

Henkilötietojen Käsittelijän ja sen alihankkijoiden/alikäsittelijöiden tilojen tulee olla asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin salassa pidettäviin tietoihin. Henkilötietojen Käsittelijän on aina huolehdittava, etteivät henkilötiedot joudu asiattomien saataville riippumatta siitä, käsitelläänkö tietoja tietojärjestelmissä, paperilla, kuvina, keskustelemalla puhelimessa tai kasvokkain. Tarpeettomiksi tulleet tiedot hävitetään tietoturvallisesti.

Sopimuksen mukaisen palvelun sisällön mukaan tulee Käsittelijän ottaa huomioon ja noudattaa viranomaisen asiakirjavaatimusten ja lainmukaisuuden (mm. asiakirjojen luovuttaminen, säilytysajat, arkistointi) sekä hyvän tiedonhallintatavan toteutuminen.

Alihankkijat/Alikäsittelijät

Henkilötietojen käsittelijän Alihankkijat/Alikäsittelijät toimivat myös Henkilötietojen Käsittelijöinä Rekisterinpitäjän puolesta ja lukuun, ja näin ollen käsittelevät henkilötietoja sopimuksen, voimassa olevan tietosuojalainsäädännön ja näiden ohjeiden mukaisesti.

Käsittelijä tai sen Alihankkija/Alikäsittelijä ei käsittele eikä muulla tavoin hyödynnä sopimuksen perusteella käsittelemiään henkilötietoja muutoin kuin sopimuksen täyttämisen mukaiseen tarkoitukseen ja silloinkin ainoastaan tarkoituksen edellyttämässä laajuudessa ja Rekisterinpitäjän antaman ohjeistuksen mukaisesti.

Henkilötietojen Käsittelijän tulee varmistaa, että sopimuksen mukainen Rekisterinpitäjän tietosuojan auditointi ja tarkastusoikeus voidaan ulottaa tarvittaessa myös alihankkijaan/alikäsittelijään. Tarkastusmenettelyä koskevat tarkemmat ehdot sovitaan erikseen tapauskohtaisesti.

Tekniset ja organisatoriset toimenpiteet

Käsittelijä toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla se varmistaa, että Rekisterinpitäjän henkilötietojen käsittely tapahtuu sopimuksen vaatimusten sekä alalla yleisesti käytettyjen ja sovittujen käytäntöjen mukaisesti. Toimenpiteiden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä käsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus. Näitä toimenpiteitä ovat muun muassa:



Yksikkö

PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

- kyky palauttaa nopeasti henkilötietojen saatavuus ja pääsy henkilötietoihin fyysisessä tai teknisessä häiriötilanteessa,
- tietoturvatöiden tehokkuuden valvonta, testaaminen, tutkiminen ja arviointi tietojenkäsittelyn turvallisuuden varmistamiseksi,
- henkilötietojen käsittelyn minimointi,
- järjestelmän suojaaminen tietomurtoja, tunkeutumisyrityksiä ja verkkohyökkäyksiä vastaan,
- muut tekniset toimet, kuten virustorjunta ja palomuurit sekä käyttöoikeushallinta ja toimitilojen kulunvalvonta,
- järjestelmään kuuluvien ohjelmistokomponenttien tietoturvapäivityksien asentaminen säännöllisesti ja riittävän nopeasti,
- se, että järjestelmä täyttää lainsäädännön lokien säilyttämiselle asettamat vaatimukset,
- henkilöstön koulutus ja perehdytys henkilötiedon käsittelyyn ja vaitiolovelvollisuuteen sekä
- riittävistä ja asiantuntevista henkilöstöresursseista huolehtiminen.

Henkilötietojen tietoturvaloukkaukset

Henkilötietojen Käsittelijä sitoutuu ilmoittamaan Rekisterinpitäjälle ja tämän tietosuojavastaavalle ilman aiheetonta viivytystä kirjallisesti tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta sekä muista mahdollisista palvelun häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Henkilötiedon käsittelijän on annettava Rekisterinpitäjälle ja tietosuojavastaavalle vähintään seuraavat tiedot tietoturvaloukkauksesta:

- tapahtuneen tietoturvaloukkauksen kuvaus, mukaan lukien asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat tiedossa;
- tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;
- kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja
- kuvaus toimenpiteistä, joita Henkilötiedon käsittelijä ehdottaa tai joita se on jo toteuttanut tietoturvaloukkauksen takia, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Henkilötietojen tietoturvaloukkauksen havaittuaan Henkilötiedon käsittelijä ryhtyy viipymättä sopimuksessa sovittuihin toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.

Rekisteröityjen pyynnöt



Yksikkö

PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Käsittelijä ilmoittaa Rekisterinpitäjän tietosuojavastaavalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Käsittelijä ei itse vastaa näihin pyyntöihin. Käsittelijä avustaa Rekisterinpitäjää, jotta Rekisterinpitäjä pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyyntöt voivat edellyttää Käsittelijältä esimerkiksi avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen.

Henkilötietojen siirrot

Ellei palvelun tuottamispaikasta ole toisin sovittu, Henkilötietojen Käsittelijällä ja sen Alihankkijalla/Alikäsittelijällä on oikeus käsitellä Rekisterinpitäjän henkilötietoja ainoastaan Euroopan talousalueella. Mitä Sopimuksessa ja näissä ohjeissa sovitaan henkilötietojen käsittelystä, koskee se myös pääsyn mahdollistamista Rekisterinpitäjän henkilötietoihin esimerkiksi hallinta- ja valvontayhteyden välityksellä.

Jos sopijapuolet erikseen sopivat, että Käsittelijä tai sen Alihankkija/Alikäsittelijä saa käsitellä Rekisterinpitäjän henkilötietoja Euroopan talousalueen ulkopuolella, sopijapuolet huolehtivat yhdessä siitä, että henkilötietojen käsittely toteutetaan voimassa olevan lainsäädännön mukaisesti. Käsittelijän tulee kirjallisesti ilmoittaa tällaisen käsittelyn aloittamisesta Rekisterinpitäjälle viimeistään 30 päivää ennen suunniteltua aloitusajankohtaa.

Tiedonsiirroissa on varmistettava GDPR:n vaatimuksia vastaava tietosuojan taso. Rekisterinpitäjän on Käsittelijän avustuksella varmistettava, ettei tietosuojasetuksen takaamaa henkilötietojen suojan tasoa vaaranneta, kun tietoja siirretään Euroopan talousalueen ulkopuolelle. Siirrossa on varmistettava, että tietojen vastaanottajalla on oikeus siirrettävien henkilötietojen käsittelyyn.

Kun kansainväliset henkilötietojen siirrot ja niihin käytettävä siirtooperuste ([Siirto tietosuojan riittävyttä koskevan päätöksen perusteella](#) | [Tietosuojavaltuutetun toimisto](#)) on määritelty, tietoja siirtävien rekisterinpitäjän ja henkilötietojen käsittelijöiden on tarkistettava tapauskohtaisesti, taataanko siirrettäville henkilötiedoille kolmannen maan lainsäädännössä ja/tai käytännössä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa. Tiedonsiirroissa USA:n organisaation on oltava sertifioitunut Tietosuojakehykseen, jonka lisäksi käytössä on oltava EU:n komission lausekkeet sekä mahdolliset lisäsuojatoimet tulee olla käytössä.

Jos käytetty siirtooperuste ei riitä takaamaan EU:n vaatimuksia vastaavaa tietosuojan tasoa, sitä voidaan tietyissä tilanteissa täydentää tapauskohtaisesti arvioituilla täydentävillä suojatoimilla → [Tiedonsiirtovälineitä täydentävät suojatoimet](#) | [Tietosuojavaltuutetun toimisto](#). Jos myöskään soveltuvia täydentäviä suojatoimia ei löydy riittävän tietosuojan takaamiseksi, ei siirtoa voi tehdä.



Yksikkö

PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Käsittelijä sitoutuu siirtämään henkilötietojen käsittelyn Euroopan talousalueelle ilman aiheutonta viivästystä, jos henkilötietojen käsittelyn lainmukaisuus Euroopan talousalueen ulkopuolisessa käsittelypaikassa vaarantuu tai osoittautuu tietosuojalainsäädännön velvoitteiden vastaiseksi. Käsittelijä vastaa siirrosta aiheutuneista kustannuksista.

Käsittelijä takaa saman tietoturvan ja tietosuojan tason riippumatta henkilötietojen käsittelymaasta.

Henkilötiedon poistaminen tai palauttaminen rekisterinpitäjälle käsittelypalvelujen päättyessä toteutetaan erikseen sovitulla tavalla. Käsittelijän tulee myös poistaa niistä hallussaan olevat kopiot ja varmistaa tiedon poistaminen myös alihankkijoiden/alikäsittelijöiden osalta.

Erityiset henkilötietoryhmät ja salassa pidettävät henkilötiedot

Tietosuoja-asetuksessa (art. 9) on määritelty erityiset henkilötietoryhmät, joiden käsittelylle on asetetut tiukemmat perusteet. Erityisiä henkilötietoja ovat rotu, etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, joita käytetään henkilön tunnistamiseksi, terveyttä koskevat tiedot sekä henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Myös Julkisuuslaki (621/1999, § 24) määrittelee rekisterinpitäjän salassa pidettäviä tietoja, joiden käsittelyssä tulee noudattaa erityistä huolellisuutta. Tällöin tiedon luovuttamisen perusteet ovat erittäin rajalliset.

Rekisterinpitäjän tietosuojavastaavan yhteystiedot

Rekisterinpitäjän tietosuojavastaava: Tanja Markkula, tietosuojavastaava@vaasa.fi, puh. 040 5634 101



Yksikkö

PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi