



Hyrynsalmen kunta

Henkilötietojen käsittelyohje

Hyväksytty (khal § xx.xx.xxxx)

Sisällys

| | |
|--|----|
| 1 YLEISTÄ HENKILÖTIETOJEN KÄSITTELYSTÄ | 2 |
| 1.1 Käsittelyohjeen tausta | 2 |
| 1.2 Keskeiset käsitteet | 2 |
| 2 HENKILÖTIETOJEN KÄSITTELY | 4 |
| 2.1 Yleiset henkilötietojen käsittelyperiaatteet | 4 |
| 2.2 Tietojen julkisuus, salassapito ja vaitiolovelvollisuus | 5 |
| 2.3 Oikeus käsitellä henkilötietoja | 6 |
| 2.4 Arkaluontoisten tietojen käsittely | 7 |
| 2.5 Henkilötunnuksen käsittely | 8 |
| 2.6 Henkilötietojen hävittäminen tai siirtäminen arkistoon | 8 |
| 2.7 Rekisterinpitäjän osoitusvelvollisuus | 9 |
| 2.7.1 Osoitusvelvollisuuden toteuttaminen | 9 |
| 2.7.2 Seloste käsittelytoimista | 9 |
| 2.7.3 Tietosuojaseloste – rekisteröidyn informointi | 10 |
| 3. TIETOTURVA HENKILÖTIETOJEN KÄSITTELYSSÄ | 11 |
| 3.1 Tietojen suojaaminen | 11 |
| 3.2 Henkilötietojen tietoturvaloukkaus | 11 |
| 3.2.1 Henkilötietojen tietoturvaloukkauksen tunnistaminen | 11 |
| 3.2.2 Toiminta tietoturvaloukkaustilanteessa | 12 |
| 4 REKISTERÖIDYN OIKEUDET | 13 |
| 4.1 Oikeus saada tietoa henkilötietojen käsittelystä | 13 |
| 4.2 Oikeus saada pääsy tietoihin | 14 |
| 4.2.1 Tiedot, joihin rekisteröidyllä on oikeus | 14 |
| 4.2.2 Rekisteröidyn pyyntöön vastaaminen | 15 |
| 4.2.3 Rekisteröidyn tietopyynnöstä kieltäytyminen | 15 |
| 4.2.4 Rekisteröidyn henkilöllisyyden vahvistaminen | 16 |
| 4.3 Oikeus tietojen oikaisemiseen | 16 |
| 4.4 Oikeus tietojen poistamiseen | 17 |
| 4.5 Oikeus rajoittaa tietojen käsittelyä | 18 |
| 4.6 Oikeus siirtää tiedot järjestelmästä toiseen | 19 |
| 4.7 Oikeus vastustaa tietojen käsittelyä ja automaattista päätöksentekoa | 19 |

1 YLEISTÄ HENKILÖTIETOJEN KÄSITTELYSTÄ

1.1 Käsittelyohjeen tausta

Henkilötietojen käsittely tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.

Kaikessa henkilötietojen käsittelyssä on noudatettava tietosuojalainsäädäntöä. Henkilötietojen käsittelyä ohjaavat erityisesti EU:n yleinen tietosuoja-asetus (2016/679) ja tietosuojalaki (1050/2018). Työntekijää koskevaa henkilötietojen käsittelyä sääntelee yksityisyyden suojasta työelämässä annettu laki (2004/759). Lisäksi henkilötietojen käsittelystä säännellään Suomessa lukuisissa erityislajeissa. Lainsäädännön noudattamisen lisäksi rekisterinpitäjän on pystyttävä osoittamaan huomioineensa nämä velvoitteet toiminnassaan.

Organisaatio vastaa siitä, että sen työntekijöillä on käytössään riittävä tuki ja ohjeistus lainsäädännön huomioimiseksi. Jokainen työntekijä puolestaan vastaa omalta osaltaan henkilötietojen asianmukaisesta käsittelystä ja tietoturvan ja tietosuojan huomioimisesta arjen työtehtävissä. Tämä ohje on tarkoitettu Hyrynsalmen kunnan henkilökunnan käyttöön avuksi henkilötietojen käsittelyyn, yksityisyyden suojan toteuttamiseen ja rekisteröidyn oikeuksien toteuttamiseen. Tietoturvavastuut on käyty tarkemmin läpi Hyrynsalmen kunnan tietoturva- ja tietosuojapolitiikassa. Tiedonhallinnan vastuut on määritelty hallintosäännössä.

1.2 Keskeiset käsitteet

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella. Henkilötieto voi olla myös esimerkiksi paikkatieto, joka kertoo tietystä henkilöstä tai kuva, joka yhdistettynä esimerkiksi osoitetietoihin kertoo jotakin tietystä henkilöstä.

Esimerkkejä henkilötiedoista:

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.com
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- kiinteistötunnus
- paikannustiedot (esim. matkapuhelimen paikannustiedot)
- IP-osoite (jos liitettävissä tiettyyn käyttäjään)
- potilastiedot
- lemmikin eläinlääkärítiedot
- pseudonymisoidut tiedot = tiedot, joista henkilö on tunnistettavissa vain epäsuorasti

- Pseudonymisointi on tiedon suojaamistoimenpide, jota käytetään esim. tilanteissa, joissa yksilön tiedot korvataan jollain tunnisteella, mutta tunnisteen avulla tiedot voidaan myöhemmin vielä palauttaa ja yhdistää luonnolliseen henkilöön. Pseudonymisoitu tieto on edelleen henkilötieto ja siihen sovelletaan tietosuojasetusta.

Esimerkkejä tiedoista, jotka **eivät** ole henkilötietoja:

- yrityksen rekisteritunnus
 - yleinen sähköpostiosoite, kuten info@yritys.com.
 - anonymisoidut tiedot = henkilötietojen tunnistettavuus on poistettu siten, ettei tunnistaminen ole mahdollista edes yhdistämällä tiedot muualta saataviin tietoihin.
 - käsitellään mm. tilasto- ja tutkimustarkoituksia varten. Tietosuojasetus ei koske anonymisoituja henkilötietoja.
- **Erityistä (arkaluonteista) henkilötietoa** ovat tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot henkilön yksiselitteistä tunnistamista varten, terveyttä koskevat tiedot, henkilön seksuaalinen käyttäytyminen tai suuntautuminen. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.

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

Henkilötietojen käsittely tarkoittaa toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Henkilötietojen käsittelyä on siten tietojen

- kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen ja muokkaaminen tai muuttaminen
- haku, kysely, käyttö ja luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville
- yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen
- katseleminen tai haku sähköisestä järjestelmästä sekä
- pääsyn mahdollistaminen henkilötietoon esimerkiksi silloin kun henkilötiedon käsittely esim. palkanlaskenta ulkoistetaan rekisterinpitäjän ulkopuolelle

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi henkilö, jolla ei ole käsittelyoikeutta.

Henkilörekisteri on mikä tahansa jäsenneily henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietojoukko voi olla keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. *Samaan käyttötarkoitukseen kerätyt henkilötiedot kuuluvat samaan henkilörekisteriin, mutta voivat koostua erillisistä tietolähteistä.* Esimerkiksi potilasrekisterin tarkoitus on potilaan tutkimuksen ja hoidon järjestäminen, mutta sitä ylläpidetään erilaisilla tietojärjestelmillä, paperein, jne.

Osoitusvelvollisuudella tarkoitetaan, että organisaation on kyettävä osoittamaan, että se on huolehtinut tietosuoja-asetuksen edellyttämistä henkilötietojen käsittelyn periaatteista.

Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä on se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

Rekisteriseloste, tietosuojaseloste on dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetystä, avoimesta ja helposti ymmärrettävässä muodossa.

Rekisteröity on luonnollinen henkilö, jota henkilötieto koskee.

Tietosuoja tarkoittaa niitä toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietosuojapolitiikka on johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Tietoturva kattaa kaikki järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luotamuksellisuus. Tietoturva on riskienhallintaa ja osa yritysturvallisuutta.

2 HENKILÖTIETOJEN KÄSITTELY

2.1 Yleiset henkilötietojen käsittelyperiaatteet

Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen 5 artiklan mukaan seuraavia vaatimuksia:

1. Henkilötietojen käsittelyn on oltava lainmukaista, asianmukaista ja läpinäkyvää. Henkilötietojen käsittelyssä on noudatettava EU:n yleistä tietosuoja-asetusta ja muuta henkilötietojen käsittelyä koskevaa lainsäädäntöä. Käsittelylle on oltava peruste ja käsittelyn on oltava asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen. Läpinäkyvyys tarkoittaa, että rekisteröidyn tulee saada helposti ja ymmärrettävästi tiedot siitä, mitä henkilötietoja kerätään, mitä tarkoitusta varten, miten tietoja käsitellään ja millaisia oikeuksia rekisteröidyllä on ("**lainmukaisuus, kohtuullisuus ja läpinäkyvyys**");
2. Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa käsitellä myöhemmin alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla. Jos tietoja käytetään yleisen edun mukaista arkistointia, tieteellistä tai historiallista tutkimusta tai tilastollisia tarkoituksia varten käyttötarkoitussidonnaisuutta ei tarvitse olla ("**käyttötarkoitussidonnaisuus**");

3. Henkilötietojen on oltava asianmukaisia, olennaisia ja rajoittua siihen, mikä on tarpeellista suhteessa niiden käsittelytarkoitukseen ("**tietojen minimointi**");
4. Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän on kohtuullisin toimenpitein varmistettava, että käsittelyn tarkoitukseen nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä ("**täsmällisyys**");
5. Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. Rekisterinpitäjän on varmistettava esimerkiksi asetettujen määräaikojen avulla, ettei henkilötietoja säilytetä pidempään kuin on tarpeen. Tietoja voi kuitenkin säilyttää kauemmin, jos tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten edellyttäen, että tietosuoja-asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi. ("**säilytyksen rajoittaminen**");
6. 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 vastaa siitä, ja sen on pystyttävä osoittamaan se, että edellä mainittuja periaatteita on noudatettu ("**osoitusvelvollisuus**").

2.2 Tietojen julkisuus, salassapito ja vaitiolovelvollisuus

Tietosuojalain ja -asetuksen ohella tärkeimmät tiedon julkisuutta, salassapitoa ja vaitiolovelvollisuutta koskevat lait kunnassa ovat:

- laki viranomaisen toiminnan julkisuudesta (1999/621, "julkisuuslaki"), jossa säännellään mitkä viranomaisen asiakirjat ovat julkisia, oikeudesta saada tieto asiakirjasta, viranomaisen velvollisuudesta edistää tiedonsaantia sekä salassapidosta
- hallintolaki (2003/434), jossa määritellään hyvän hallinnon perusteet sekä säännellään mm. asian käsittelystä ja käsittelyn julkisuudesta
- kuntalaki (2015/410), jossa säännellään mm. kunnan viestinnästä, luottamushenkilöiden tiedonsaantioikeudesta, kokosten julkisuudesta, kunnan ilmoituksista ja päätösten tiedoksiannosta

Pääsääntöisesti kaikki viranomaiselle toimitetut asiakirjat ja tehdyt päätökset ovat julkisia. Valmisteluasiakirjojen osalta organisaatio voi käyttää harkintavaltaa tiedottamisen tai tietojen luovuttamisen osalta. Sisäiset muistiot tai esimerkiksi omat muistiinpanot eivät ole julkisia, eivätkä siten kuulu lainkaan julkisuuslain piiriin.

Viranomaisen palveluksessa oleva ja luottamustehtävää hoitava ei saa näyttää tai luovuttaa salassa pidettävää asiakirjaa eikä keskustella sen sisällöstä ulkopuolisten kanssa. Vaitiolovelvollisuus koskee paitsi salassa pidettävää asiakirjaa, myös muuta tietoa, jonka virkamies, työntekijä, harjoittelija jne. saa tietoonsa työtehtäviä hoitaessaan. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa senkään jälkeen, kun toiminta viranomaisessa tai tehtävän hoitaminen viranomaisen lukuun on päättynyt. Yleisimmät salassa pidettävät asiat koskevat erityisiä henkilötietoryhmiä, sosiaali- ja terveystietoja ja näihin liittyvää asiakkuutta, oppilashuoltoa tai kunnan liike- ja ammattisalaisuuksia.

Tietosuojalain 35 §:ssä säädetään vaitiolovelvollisuudesta: *”Joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta taikka toisen liikesalaisuudesta, ei saa oikeudettomasti ilmaista sivulliselle näin saamiaan tietoja eikä käyttää niitä omaksi tai toisen hyödyksi tai toisen vahingoksi.”*

Jokainen Hyrynsalmen kunnan työntekijä on hyväksynyt tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen, jonka perusteella on sitoutunut noudattamaan kunnassa noudatettavia määräyksiä ja ohjeita sekä olemaan paljastamatta salassa pidettäviä tai muuten luottamuksellista tietoa ulkopuoliselle työsuhteen aikana tai sen jälkeen.

2.3 Oikeus käsitellä henkilötietoja

Tietojen keräämisen ja käsittelyn tulee olla laillista ja rekisterinpitäjän toiminnan ja tehtävien kannalta asianmukaista. Henkilötietoja voidaan kerätä ja käsitellä vain tietosuojasetuksessa määriteltujen edellytysten mukaisesti.

Tietosuojasetuksen 6 artiklan mukaan henkilötietoja saa käsitellä ainoastaan, jos

- a) rekisteröity on antanut **suostumuksensa** henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
- b) käsittely on tarpeen sellaisen **sopimuksen täytäntöön panemiseksi**, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
- c) käsittely on tarpeen rekisterinpitäjän **lakisääteisen velvoitteen noudattamiseksi**;
- d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen **henkilön elintärkeiden etujen suojaamiseksi**;
- e) käsittely on tarpeen **yleistä etua** koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan **julkisen vallan käyttämiseksi**;
- f) 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. (Ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.)



Rekisteröityjen henkilötiedoista ei voi keskustella vapaasti kollegoidenkaan kanssa tai näyttää heihin liittyviä tai muuten salassa pidettäviä tietoja tietojärjestelmästä. Henkilötietojen käsittelylle, esimerkiksi tietojen katselulle, tulee aina löytyä myös henkilötietoja käsittelevän työntekijän työrooliin perustuva oikeus.

2.4 Arkaluontoisten tietojen käsittely

Niin sanottuihin erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Tällaisista tiedoista ilmenee henkilön

- rotu tai etninen alkuperä
- poliittisia mielipiteitä
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- terveyttä koskevia tietoja
- seksuaalinen suuntautuminen tai käyttäytyminen
- geneettisiä tai biometrisia tietoja henkilön tunnistamista varten

Erytyisiin henkilötietoryhmiin kuuluvia henkilötietoja saa käsitellä, kun kieltoon on säädetty poikkeus EU:n tietosuojasetuksessa tai erikseen unionin oikeudessa tai kansallisessa lainsäädännössä. Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Erytyisiä henkilötietoryhmiä voi käsitellä (tietosuojasetus 9 artikla), jos

1. rekisteröity on antanut nimenomaisen **suostumuksen** kyseisten henkilötietojen käsittelyyn;
2. käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn **velvoitteiden ja erityisten oikeuksien noudattamiseksi** työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla;
3. käsittely on tarpeen rekisteröidyn tai jonkun toisen henkilön **elintärkeiden etujen suojaamiseksi tilanteessa, jossa rekisteröity on fyysisesti tai juridisesti estynyt** antamasta suostumustaan;
4. henkilötietoja käsitellään poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän **säätiön, yhdistyksen tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä** ja ne suojataan asianmukaisesti. Käsittely voi koskea vain yhteisön jäseniä, entisiä jäseniä tai henkilöitä, joilla on yhteisöön säännölliset, yhteisön tarkoitukseen liittyvät yhteydet. Tietoja ei saa luovuttaa yhteisön ulkopuolelle ilman suostumusta;
5. käsittely koskee henkilötietoja, jotka **rekisteröity** on nimenomaisesti **saattanut julkiseksi** esimerkiksi julkaisemalla ne verkkosivuillaan;

6. käsittely on tarpeen **oikeusvaateen** laatimiseksi, esittämiseksi tai puolustamiseksi. Lisäksi käsittely on mahdollista aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään;
7. käsittely on tarpeen tärkeää **yleistä etua** koskevasta syystä;
8. käsittely on tarpeen **ennaltaehkäisevää terveydenhuoltoa, työterveydenhuoltoa, työkyvyn arviointia, lääketieteellisiä diagnooseja, terveys- tai sosiaalihuollollista hoitoa tai terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa** varten. Edellytyksenä on, että tietoja käsittelee vain ammattilainen tai henkilö, jolla on lakisääteinen salassapitovelvollisuus;
9. käsittely on tarpeen **kansanterveyteen liittyvän yleisen edun** vuoksi, kuten vakavilta rajat ylittäviltä terveysuhkilta suojautumiseksi tai terveydenhuollon, lääkevalmisteiden tai lääkinnällisten laitteiden korkeiden laatu- ja turvallisuusnormien varmistamiseksi; tai
10. käsittely on tarpeen **yleisen edun mukaista arkistointia, tieteellistä ja historiallista tutkimusta tai tilastointia** varten.

Arkaluonteiset tiedot ovat salassa pidettäviä, eikä niitä tule luovuttaa sivullisille. Henkilötietojen käsittelijän tulee käsitellä arkaluontoisia tietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä suorittaa käsittelytoimet niin, ettei rekisteröidyn yksityiselämän suoja vaarannu.

2.5 Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä rekisteröidyn antamalla suostumuksella tai jos käsittelystä säädetään laissa. Suostumus ei kuitenkaan yksin riitä, sillä henkilötunnuksen käsittelyn on aina täytettävä tarpeellisuusvaatimus. Henkilötietojen käsittelijän on huolehdittava siitä, ettei henkilötunnusta merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

2.6 Henkilötietojen hävittäminen tai siirtäminen arkistoon

Vanhentuneita, virheellisiä tai tarpeettomia henkilötietoja ei saa säilyttää. Tiedot, joita ei enää tarvita, hävitetään tai siirretään arkistoon säilytettäväksi tiedonohjaussuunnitelman mukaisesti. Lainsäädännössä on erityissäännöksiä henkilötietojen säilyttämisajoista, joita työnantajan on noudatettava. Tällaisia säännöksiä ovat esimerkiksi työsopimuslain, työaikalain ja kirjanpitolain mukaiset vanhentumisajat. Julkishallinnossa on lisäksi erityismääräyksiä työntekijöiden ja virkamiesten henkilötietojen säilyttämisestä. Tarpeettomat tiedot on tuhottava välittömästi säilytysajan kuluttua umpeen.

Tiedot tulee hävittää tietosuoja ja tietoturva varmistuen niin, että tiedot eivät joudu asiattomien käsiin. Lisäksi manuaaliset ja sähköiset asiakirjat tulee hävittää siten, että niitä ei enää voida yhdistää luonnolliseen henkilöön.

2.7 Rekisterinpitäjän osoitusvelvollisuus

2.7.1 Osoitusvelvollisuuden toteuttaminen

Henkilörekisterinpitäjän on kyettävä osoittamaan, että se noudattaa henkilötietojen käsittelyssä tietosuojalainsäädäntöä. Tämä edellyttää henkilötietojen käsittelytoimien, ohjeiden, koulutusten ja prosessien dokumentointia riittävän tarkalla tasolla, jotta tietosuojaviranomaiset pystyvät todentamaan tarvittaessa henkilötietojen käsittelyn lainmukaisuuden eri toiminnoissa. Lakisääteisten vaatimusten toteuttamisen lisäksi osoitusvelvollisuuden tarkoituksena on osoittaa rekisterinpitäjän kunnioittavan henkilötietojen käsittelyn kohteena olevien tietosuoja- ja tietoturvapoliittikalla, erilaisilla ohjeistuksilla kuten tällä ohjeella henkilötietojen käsittelyyn, sisäisen valvonnan ja riskien hallinnan ohjeilla, henkilötietojen tietoturvaloukkausten dokumentoinnilla sekä riskiarvioita ja toteutettuja toimenpiteitä koskevalla dokumentaatiolla.

2.7.2 Seloste käsittelytoimista

Rekisterinpitäjän on ylläpidettävä vastuullaan olevista käsittelytoimista selostetta eli henkilötietojen käsittelyn yleistä kuvausta. Seloste käsittelytoimista on tarkoitettu vain sisäiseen ja tietosuoja-
viranomaisen käyttöön. **Selosteen käsittelytoimista on sisällettävä kaikki seuraavat tiedot:**

1. rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
2. käsittelyn tarkoitukset: minkä rekisterinpitäjälle kuuluvan tehtävän/tehtävien hoitamiseksi tietoja käsitellään, mihin tietosuoja-asetuksen käsittelyperusteeseen käsittely perustuu
3. kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
4. henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan
5. tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainvälisille järjestöille
6. tietojen säilytysajat tai kriteerit, joilla säilyttämisajat määritellään
7. kuvaus käsittelyn turvallisuuteen liittyvistä teknisistä ja organisaatorisista turvatoimista: miten tiedot on suojattu organisaation ulkopuolisilta, miten käyttöoikeudet rajoitettu organisaation sisällä, miten tietojen käyttöä valvotaan.

2.7.3 Tietosuojaseloste – rekisteröidyn informointi

Rekisteröityjä täytyy informoida henkilötietojen käsittelystä. Tietosuojalailla 2018 kumotussa henkilötietolaissa (523/1999) säädettiin rekisteriselosteesta, joka täytyi laatia erikseen jokaisesta rekisteristä. Henkilötietolain nojalla rekisterinpitäjä on käytännössä voinut toteuttaa informointivelvoitetta laatimalla rekisteriselosteesta tietosuojaselosteen, jossa lisäksi kerrotaan rekisteröidyn oikeuksista.

Henkilötietolaista poiketen EU:n yleinen tietosuojasetus ei edellytä rekisteri- tai tietosuojaselosteen laatimista. Asetuksessa säädetään kuitenkin rekisterinpitäjän velvollisuudesta informoida rekisteröityjä. Informointiin voidaan käyttää edelleen käyttötarkoituksen mukaan ryhmiteltyjä selosteita, kunhan huolehditaan tietosuojasetuksen vaatimuksesta toimittaa tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Henkilötietojen käsittelytoimia koskevaa selostetta ei ole tarkoitettu käytettäväksi suoraan rekisteröidyn informointiin, mutta sitä voidaan hyödyntää rekisteröidyille suunnatun informaation tuottamisessa. **Selosteen käsittelytoimista sisältämien tietojen lisäksi rekisteröidyille on informoitava**

- jos käsittelyn perusteena on oikeutettu etu, tämän **edun yksilöinti** (artikla 6.1 (f))
- **rekisteröidyn oikeudet**: mitä oikeuksia käsittelyyn liittyy ja kuinka rekisteröity voi käyttää niitä
- jos käsittely perustuu suostumukseen (6.1.a artikla tai nimenomaiseen suostumukseen 9.2.a artikla), **tieto oikeudesta peruuttaa tämä suostumus** milloin tahansa
- tieto **oikeudesta tehdä valitus valvontaviranomaiselle**
- onko henkilötietojen antaminen **lakisääteinen tai sopimukseen perustuva vaatimus tai sopimuksen tekemisen edellyttämä vaatimus** sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset
- tiedot siitä, **mistä henkilötiedot on saatu** sekä tarvittaessa siitä, onko tiedot saatu yleisesti saatavilla olevista lähteistä
- tiedot **automaattisen päätöksenteon, ml. profiloinnin olemassaolosta**.

Tietosuojaselosteet kaikista organisaation rekisteristä on yksi osoitusvelvollisuutta toteuttava dokumentti. Keskeisimmät tietosuojaselosteet tietosuojasetuksen vaatimukset huomioivassa muodossa pidetään julkisesti saatavilla kunnan verkkosivuilla.

3. TIETOTURVA HENKILÖTIETOJEN KÄSITTELYSSÄ

3.1 Tietojen suojaaminen

Rekisterinpitäjän on suoritettava tarpeelliset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen häviämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelemiseltä.

Tietojen suojaamiseksi tulee huolehtia, että

- Tekninen suojaaminen on hoidettu kirjauduttaessa henkilötietojärjestelmiin käyttäjätunnuksin ja salasanoin.
- Tekninen tietoturva on kunnossa (palomuurit, virustorjunta, salausjärjestelmät, langattomat yhteydet ym.).
- Fyysinen tietoturva on kunnossa. Henkilötietoja sisältävät asiakirjat ja rekisterit säilytetään lukituissa kaapeissa ja tietojen säilytykseen käytetyt tilat pidetään lukittuina. Tietoja sisältäviä tulosteita ei säilytetä muiden nähtävillä. Tietokoneen näyttö on suojattu suojakalvolla tai sijoitettu siten, etteivät tiedot ole asiattomasti luettavissa. Tietokone lukitaan työhuoneesta poistuttaessa.
- Henkilökunnan tietoturvaroolit ja osaaminen ovat ajan tasalla. Työtehtäviensä vuoksi henkilötietoja käsittelevät on määritelty. Henkilöstö on saanut tarvittavan koulutuksen ja tuntee tietosuojavelvollisuutensa.

Tietosuoja-asetuksen 32 artiklan 4 kohta: ”Rekisterinpitäjän ja henkilötietojen käsittelevän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelevän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.”

- Sähköpostiviestintä toteutetaan turvallisesti. Luottamuksellisia tietoja ei lähetetä suojaamattomassa sähköpostissa.

3.2 Henkilötietojen tietoturvaloukkaus

3.2.1 Henkilötietojen tietoturvaloukkauksen tunnistaminen

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi

- hävinnyt tiedonsiirtoväline, kuten USB-tikku

- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

3.2.2 Toiminta tietoturvaloukkaustilanteessa

Rekisterinpitäjän on varauduttava mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet tietoturvaloukkaustilanteita varten. Tietoturvaloukkauksiin on pystyttävä reagoimaan mahdollisimman nopeasti. Rekisterinpitäjän täytyy arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille. Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä.

Toimenpiteet tietoturvaloukkaustilanteissa:

1. Kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet **dokumentoidaan** riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa. Tietoturvaloukkauksista raportoidaan osana sisäistä valvontaa.
2. Henkilötietojen tietoturvaloukkauksesta täytyy **ilmoittaa valvontaviranomaisena toimivalle tietosuojavaltuutetun toimistolle**, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheutonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksesta ensin rekisterinpitäjälle, jollei ole erikseen sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan tietosuojavaltuutetun toimistolle.
3. Henkilötietojen tietoturvaloukkauksesta on **ilmoitettava rekisteröidylle**, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisterinpitäjän on tällöin ilmoitettava asiasta ilman aiheutonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua esimerkiksi sulkemalla luottokorttinsa.

Ilmoitusta rekisteröidylle ei kuitenkaan vaadita, jos

- 1) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojaustoimenpiteet ja niitä on sovellettu henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin (erityisesti niitä, joiden avulla henkilötiedot muutetaan ulkopuolisille mahdolltomiksi ymmärtää, kuten salausta)
- 2) rekisterinpitäjä on tehnyt jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu

- 3) se vaatisi kohtuutonta vaivaa, koska ei esimerkiksi tiedetä, keitä rekisteröidyt ovat. Asiaa arvioidaan riskien mukaan. Jos rekisteröityihin ei voida ottaa yhteyttä henkilökohtaisesti, on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröityjä informoidaan yhtä tehokkaalla tavalla.

4 REKISTERÖIDYN OIKEUDET

4.1 Oikeus saada tietoa henkilötietojen käsittelystä

Rekisterinpitäjän on toimitettava tiedot henkilötietojen käsittelytoimista rekisteröidylle tiiviisti esitettyssä, läpinäkyvässä ja helposti ymmärrettävissä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tiedot on toimitettava kirjallisesti tai rekisteröidyn pyynnöstä suullisesti edellyttäen, että rekisteröidyn henkilöllisyys on vahvistettu muulla tavoin. Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien käyttämistä.

Informointi toteutetaan seuraavina ajankohtina:

- Kun tietoja kerätään rekisteröidyltä: tietojen keräämisen aikaan.
- Kun tietoja saadaan muualta kuin rekisteröidyltä itseltään: kohtuullisessa ajassa, viimeistään kuukauden kuluttua tietojen saamisesta.
- Kun tietoja, joita käytetään viestintään rekisteröidyn kanssa, saadaan muualta kuin rekisteröidyltä itseltään: viimeistään, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran.
- Kun tietoja, joita on tarkoitus luovuttaa toiselle vastaanottajalle, saadaan muualta kuin rekisteröidyltä itseltään: viimeistään, kun tietoja luovutetaan ensimmäisen kerran.

Informointia ei tarvitse tilanteissa, joissa:

1. rekisteröity on jo saanut kyseessä olevan informaation;
2. informoimatta jättäminen on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi;
3. tiedot on saatu muualta kuin rekisteröidyltä, ja informointi osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa.
 - Erityisesti, kun käsittely tapahtuu yleisen edun mukaisia arkistointitarkoituksia, tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, tai kun informoinnin toteuttaminen estäisi käsittelyn tarkoitusten saavuttamisen tai vaikeuttaisi sitä suuresti.
 - Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi, ainakin tarjoamalla henkilötietojen käsittelyä koskeva informaatio julkisesti saataville.

- Tietojen hankinnasta tai luovuttamisesta säädetään nimenomaisesti rekisterinpitäjään sovellettavassa lainsäädännössä, jossa vahvistetaan asianmukaiset toimenpiteet rekisteröidyn oikeutettujen etujen suojaamiseksi.
- Informoivia tietoja koskee laissa säädetty vaitiolovelvollisuus.
- Informointi aiheuttaa olennaista vahinkoa tai haittaa rekisteröidylle, eikä talletettavia tietoja käytetä rekisteröityä koskevaan päätöksentekoon.
 - Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi, ainakin tarjoamalla henkilötietojen käsittelyä koskeva informaatio kaikkien saataville, ellei tämä vaaranna informointivelvollisuuteen kohdistuvan rajoituksen tarkoitusta.

4.2 Oikeus saada pääsy tietoihin

4.2.1 Tiedot, joihin rekisteröidyllä on oikeus

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitteleeke tämä häntä koskevia henkilötietoja. Näin rekisteröidyllä on mahdollisuus arvioida ja varmistaa käsittelyn lainmukaisuus.

Jos rekisteröidyn tietoja käsitellään, rekisterinpitäjän on toimitettava hänelle jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.

Lisäksi rekisteröidyllä on oikeus saada seuraavat tiedot:

1. käsittelyn tarkoitukset
2. käsiteltävät henkilötietoryhmät
3. vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat tai kansainväliset järjestöt, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa
4. suoja-toimet, jos henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle
5. henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, säilytysajan määrittämiskriteerit
6. rekisteröidyn oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista tai henkilötietojen käsittelyn rajoittamista sekä oikeus vastustaa tällaista käsittelyä
7. oikeus tehdä valitus valvontaviranomaiselle
8. jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot

9. automaattisen päätöksenteon (ml. profilointi) mahdollinen käyttö, merkitykselliset tiedot käsittelyyn liittyvästä logiikasta, kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

4.2.2 Rekisteröidyn pyyntöön vastaaminen

Rekisterinpitäjän täytyy vastata rekisteröidylle ilman aiheetonta viivytystä, joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Vastauksessa rekisterinpitäjä kertoo toimenpiteistä, joihin se on pyynnön vuoksi ryhtynyt. Jos pyyntöjä on monta tai ne ovat monimutkaisia, rekisterinpitäjä voi ilmoittaa vastauksessaan, että se tarvitsee niiden käsittelyyn enemmän aikaa. Tällöin määrääikää voidaan perustellen jatkaa enintään kahdella kuukaudella. Rekisteröidyn pyynnöstä kieltäytymisestä on ilmoitettava rekisteröidylle viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Kieltäytyminen on perusteltava. Rekisterinpitäjän on myös kerrottava rekisteröidylle mahdollisuudesta tehdä valitus valvontaviranomaiselle sekä käyttää muita oikeussuojakeinoja.

Oikeuden käyttäminen on lähtökohtaisesti maksutonta. Rekisterinpitäjä voi kuitenkin periä rekisteröidyltä kohtuullisen, pyyntöön vastaamisesta aiheutuvien hallinnollisten kustannusten mukaisen maksun, jos tämä pyytää tietoista useampia jäljennöksiä. Rekisterinpitäjä voi periä pyynnön toteuttamisesta kohtuullisen maksun myös silloin, jos rekisteröidyn pyyntö on ilmeisen perusteeton tai kohtuuton. Vaihtoehtoisesti rekisterinpitäjä voi kieltäytyä pyynnöstä. Pyyntöjä voidaan pitää ilmeisen perusteettomina tai kohtuuttomina erityisesti, jos niitä esitetään toistuvasti.

4.2.3 Rekisteröidyn tietopyynnöstä kieltäytyminen

Rekisteröidyn oikeuden toteuttaminen on pääsääntö. Jos rekisterinpitäjä kieltäytyy rekisteröidyn pyynnöstä, sillä on oltava kieltäytymiselle lainmukainen peruste. Kieltäytymisperusteista säädetään yleisen tietosuoja-asetuksen 12 artiklassa, 15 artiklan 4 kohdassa sekä tietosuojalain 31 ja 34 pykälissä. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

Rekisterinpitäjä voi kieltäytyä rekisteröidyn pyynnöstä näissä tilanteissa:

1. Oikeus saada jäljennös tiedoista vaikuttaisi haitallisesti muiden oikeuksiin ja vapauksiin.
2. Rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti.
 - Rekisterinpitäjän on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Vaihtoehtoisesti rekisterinpitäjä voi periä pyynnön toteuttamisesta kohtuullisen maksun.
3. Tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta tai haitata rikosten ehkäisemistä tai selvittämistä.
4. Tiedon antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle tai rekisteröidyn tai jonkun muun oikeuksille.

5. Henkilötietoja käytetään valvonta- ja tarkastustehtävissä ja tiedon antamatta jättäminen on välttämätöntä Suomen tai Euroopan unionin tärkeän taloudellisen tai rahoitussellisen edun turvaamiseksi.

Oikeudesta saada pääsy tietoihin voi lisäksi tietyin edellytyksin poiketa tieteellisen tai historiallisen tutkimuksen tai tilastoinnin yhteydessä.

Jos kieltäytymisperuste koskee vain osaa tiedoista, on rekisteröidyllä oikeus saada tietää muut häntä koskevat tiedot.

Jos rekisterinpitäjä kieltäytyy rekisteröidyn pyynnöstä, sen on ilmoitettava siitä rekisteröidylle viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Rekisteröidylle on kerrottava kieltäytymisen syyt, ellei se vaaranna kieltäytymisen tarkoitusta. Rekisterinpitäjän on myös kerrottava rekisteröidylle tämän mahdollisuudesta tehdä valitus valvontaviranomaiselle sekä käyttää muita oikeus- suojakeinoja. Jos oikeuden toteuttamisesta kieltäydytään, pyydetty tiedot on annettava tietosuojavaltuutetulle rekisteröidyn pyynnöstä.

4.2.4 Rekisteröidyn henkilöllisyyden vahvistaminen

Rekisterinpitäjän on pystyttävä vahvistamaan tietosuojaoikeuksiaan käyttävän rekisteröidyn henkilöllisyys. Jos rekisterinpitäjällä on perusteltu syy epäillä pyynnön esittäjän henkilöllisyyttä, se voi pyytää tätä toimittamaan lisätietoja henkilöllisyyden vahvistamiseksi. Lisätietojen pyytäminen ei kuitenkaan saa johtaa kohtuuttomiin vaatimuksiin ja sellaisten henkilötietojen keräämiseen, jotka eivät ole olennaisia tai tarpeellisia. Jos rekisterinpitäjä ei pysty tunnistamaan rekisteröityä, sen on mahdollisuuksien mukaan ilmoitettava asiasta rekisteröidylle ja osoitettava, ettei henkilöllisyyttä voida vahvistaa.

Henkilötietoja saa säilyttää sellaisessa muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan kuin käsittelyn tarkoitusta varten on tarpeen. Jos rekisteröidyn tunnistamisen mahdollistavat henkilötiedot eivät ole tarpeellisia henkilötietojen käsittelyn tarkoituksen kannalta, tietosuojasetus ei velvoita rekisterinpitäjiä säilyttämään, hankkimaan tai käsittelemään tällaisia lisätietoja pelkästään tietosuojasetuksen noudattamiseksi.

4.3 Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee häntä koskevat epätarkat ja virheelliset henkilötiedot sekä oikeus saada puutteelliset henkilötiedot täydennettyä. Pyyntöön vastaamisvelvollisuudesta ja henkilöllisyyden toteamisesta on kerrottu tarkemmin edellä.

Kun rekisteröity on pyytänyt tietojaan oikaistavaksi, rekisterinpitäjä arvioi, ovatko oikaistavaksi pyytämät tiedot henkilötietojen käsittelyn tarkoituksen kannalta puutteellisia, epätarkkoja tai virheellisiä. Rekisterinpitäjän vastuulla on huolehtia siitä, että sen käsittelemät tiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset

toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Jos rekisterinpitäjä katsoo, että tiedot eivät rekisteröidyn esittämistä näkemyksistä huolimatta ole käsittelyn tarkoituksen kannalta epätarkkoja tai virheellisiä, ei tietoja tarvitse oikaista. Rekisterinpitäjän on tällöin annettava rekisteröidylle perusteltu vastaus siitä, miksi tietoja ei oikaista sekä kerrottava rekisteröidylle mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja. Jos rekisterinpitäjä ei pidä tietojen oikaisemista rekisteröidyn esittämään muotoon perusteltuna, on rekisteröidyllä huomioon ottaen tarkoitukset, joihin tietoja käsiteltiin, oikeus saada puutteelliset henkilötiedot täydennettyä muun muassa toimittamalla lisäselvitys.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen oikaisemisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää.

4.4 Oikeus tietojen poistamiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjä poistamaan itseään koskevat tiedot ilman aiheetonta viivytystä. Oikeus tunnetaan myös nimellä oikeus tulla unohdetuksi.

Rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, jos

1. henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin
2. rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta
3. rekisteröity vastustaa henkilötietojensa käsittelyä suoramarkkinoinnin tarkoituksiin tai käyttää vastustamisoikeuttaan muutoin, eikä käsittelyyn ole olemassa perusteltua syytä
4. henkilötietoja on käsitelty lainvastaisesti
5. henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen veloitteen noudattamiseksi
6. henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

Poistamisvelvollisuutta ei kuitenkaan ole, jos tietojen käsittely on tarpeen

1. sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi
2. rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen veloitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten
3. kansanterveyteen liittyvää yleistä etua koskevista syistä

4. yleisen edun mukaisia arkistointitarkoituksia tai tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, jos oikeus saada tiedot poistetuksi todennäköisesti estää kyseisen käsittelyn tai vaikeuttaa sitä suuresti
5. oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Pyyntöön vastaamisvelvollisuudesta ja henkilöllisyyden toteamisesta on kerrottu tarkemmin edellä.

Rekisterinpitäjä arvioi, täyttyvätkö edellytykset tietojen poistamiselle. Jos rekisterinpitäjä katsoo, että oikeutta saada tiedot poistetuksi ei ole, se voi kieltäytyä pyynnöstä. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen poistamisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää. Jos rekisterinpitäjä on julkistanut henkilötiedot ja se on velvollinen poistamaan tiedot rekisteröidyn pyynnöstä, sen on toteutettava kohtuulliset toimenpiteet ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt näitä poistamaan henkilötietoihin liittyvät linkit tai henkilötietojen jäljennökset tai kopiot. Kohtuullisiin toimenpiteisiin kuuluvat muun muassa tekniset toimenpiteet.

4.5 Oikeus rajoittaa tietojen käsittelyä

Rekisteröity voi pyytää rekisterinpitäjää rajoittamaan häntä koskevien henkilötietojen käsittelyä.

Oikeus on olemassa seuraavissa tilanteissa:

1. Rekisteröity kiistää henkilötietojen paikkansapitävyyden. Tällöin käsittelyä rajoitetaan ajaksi, jonka kuluessa rekisterinpitäjä voi varmistaa niiden paikkansapitävyyden.
2. Käsittely on lainvastaista, mutta rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista.
3. Rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
4. Rekisteröity on vastustanut henkilötietojen käsittelyä muuhun kuin suoramarkkinointitarkoitukseen, ja odotetaan sen todentamista, syrjäyttävätkö rekisterinpitäjän edut rekisteröidyn edut.

Käsittelyn rajoittaminen tarkoittaa, että rajoituksen alaisia henkilötietoja saa säilyttämisen lisäksi käsitellä vain

- rekisteröidyn suostumuksella
- oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi tai

- tärkeää unionin tai jäsenvaltion yleistä etua koskevista syistä.

Käsittelyä voidaan rajoittaa esimerkiksi siirtämällä valitut tiedot toiseen käsittelyjärjestelmään, esitämällä käyttäjien pääsy tietoihin tai poistamalla julkaistut tiedot verkkosivustolta. Jos käsittelyä on rajoitettu, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kuin käsittelyä koskeva rajoitus poistetaan. Rekisterinpitäjän on mahdollisuuksien mukaan ilmoitettava henkilötietojen käsittelyn rajoittamisesta jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Rekisterinpitäjän on ilmoitettava rekisteröidylle näistä vastaanottajista, jos rekisteröity sitä pyytää. Pyyntöön vastaamisvelvollisuudesta, pyynnöstä kieltäytymistä ja henkilöllisyyden toteamisesta on kerrottu tarkemmin edellä.

4.6 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle, jos

1. henkilötiedot koskevat rekisteröityä ja ovat hänen toimittamiaan
2. käsittely perustuu suostumukseen tai sopimukseen
3. käsittely suoritetaan automaattisesti
4. tietojen siirto ei vaikuta haitallisesti kolmansien osapuolten oikeuksiin ja vapauksiin.

Tiedot on oikeus saada siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista. Oikeus ei kata sellaisia tietoja, jotka rekisterinpitäjä on itse luonut rekisteröidyn toimittamien tietojen pohjalta (esim. terveyttä koskevat arviot) tai jotka on koostettu rekisteröidyn tarkkailusta muodostuneiden tietojen analysoinnista (kuten profilointi). Vastaanottavan rekisterinpitäjän vastuulla on varmistaa, että järjestelmästä toiseen siirrettävät tiedot ovat tarpeellisia uutta tietojenkäsittelyä ajatellen.

Rekisteröidylle on kerrottava oikeudesta siirtää tiedot ja siitä, mitä oikeus tarkoittaa tämän rekisterinpitäjän kohdalla. Kun rekisteröity käyttää oikeuttaan siirtää tietoja järjestelmästä toiseen, se ei rajoita minkään muun tietosuojasetuksessa annetun oikeuden käyttöä. Rekisteröity voi edelleen käyttää rekisterinpitäjän palvelua ja hyötyä siitä myös tietojen siirron jälkeen. Tietojen siirtäminen järjestelmästä toiseen ei automaattisesti käynnistä tietojen poistamista rekisterinpitäjän järjestelmästä eikä vaikuta alkuperäiseen säilytysaikaan. Rekisteröity voi käyttää oikeuksiaan niin kauan kuin rekisterinpitäjä käsittelee tietoja. Rekisteröidyn pyyntöön vastaamista, pyynnöstä kieltäytymistä ja henkilöllisyyden tunnistamista koskee edellä esitetty.

4.7 Oikeus vastustaa tietojen käsittelyä ja automaattista päätöksentekoa

Kun tietoja käsitellään yleistä etua koskevan tehtävän suorittamiseksi, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmannen osapuolten oikeutettujen etujen

toteuttamiseksi, rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perustelulla vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Tällöin tietojen käsittely on lopetettava, paitsi jos

1. rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, tai
2. käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Kun tietoja käsitellään tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, rekisteröity voi vastustaa käsittelyä henkilökohtaiseen tilanteeseensa liittyvällä perusteella. Tällöin tietojen käsittely on lopetettava. Vastustamisoikeutta ei kuitenkaan ole, jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi. Kun tietoja käsitellään suoramarkkinointia varten, rekisteröity voi vastustaa käsittelyä ilman eri perusteluja. Vastustamisen jälkeen tietoja ei saa enää käsitellä suoramarkkinoinnin tarkoituksiin.

Rekisteröidylle on selkeästi kerrottava vastustamisoikeudesta. Tieto on esitettävä muusta tiedotuksesta erillään. Vastustamisoikeus on toteutettava viipymättä. Pyyntöön vastaamista ja sen maksullisuutta, pyynnöstä kieltäytymistä ja henkilöllisyyden todentamista koskee edellä esitetty.

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Kieltoon poikkeuksen muodostavat tilanteet, joissa päätös

1. on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten;
2. on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai
3. perustuu rekisteröidyn nimenomaiseen suostumukseen.