Liite 1B Tietosuojakriteerit

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.

Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen vaatimuksia, kun käsittely on kokonaan tai osittain automaattista tai tiedot muodostavat rekisterin osan. Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi tietojärjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa.

HenkilötietojenHenkilötietojen suojaamisessa voidaan hyödyntää edellä kuvattujen osa-alueiden tietoturvakriteereitäJokainen osa-alueilla oleva kriteeri on luokiteltu sen mukaan, sovelletaanko sitä myös henkilötietojen käsittelyssä ja jos sovelletaan, koskeeko kriteeri kaikkia henkilötietoja vai ainoastaan erityisiä henkilötietoryhmiä.

Tunniste	**TSU-01, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsiteltävien henkilötietojen tunnistaminen**
Vaatimus	Organisaatio tunnistaa kaikki käsittelemänsä henkilötiedot.
Yleiskuvaus	Käsiteltävien henkilötietojen tunnistaminen on välttämätön edellytys henkilötietojen suojaamiselle ja liittyy läheisesti organisaation tiedonhallintamallin laatimiseen sekä sen yhteydessä tehtävään organisaation tietovarantojen tunnistamiseen.
Toteutusesimerkki	Käsiteltävien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.
Lainsäädäntö	906/2019 5 §
Viitteet	HAL-04,
Tunniste	**TSU-01.1, L:, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	**Käsiteltävien henkilötietojen tunnistaminen - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot**
Vaatimus	Organisaatio tunnistaa käsittelmänsä erityisiin henkilötietoryhmiin kuuluvat tai rikostuomioihin ja rikoksiin liittyvät tiedot.
Yleiskuvaus	Erityisiin henkilötietoryhmiin kuuluvat tiedot, joista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, sekä geneettiset tai biometriset tiedot (henkilön yksiselitteistä tunnistamista varten), terveyttä koskevat tiedot tai henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot. Edellä mainitut erityiset henkilötietoryhmät ovat julkisuuslain perusteella salassa pidettäviä tietoja, joihin kohdistuvat korkeammat turvallisuusvaatimukset. Tämän vuoksi organisaation tulee tunnistaa, mikäli käsittely koskee erityisiä henkilötietoryhmiä sekä luokitella tiedot erityisiin henkilötietoryhmiin kuuluviksi. Rikostuomioihin ja rikoksiin liittyvät henkilötiedot ovat myös salassa pidettäviä ja niihin sovelletaan tavanomaisia henkilötietoja korkeampia turvallisuusvaatimuksia sekä erillisiä käsittelyn lainmukaisuuteen liittyviä vaatimuksia, minkä johdosta ne tulee tunnistaa ja luokitella erikseen.
Toteutusesimerkki	Näihin henkilötietoryhmiin kuuluvien henkilötietojen tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia.
Lainsäädäntö	679/2016 Art 9 ja 10
Viitteet	HAL-04.2,
Tunniste	**TSU-02, L:, E:, S:, TS:Henkilötieto**
Nimi	**Organisaation roolit**
Vaatimus	Organisaatio määrittelee käsittelemiensä henkilötietojen osalta, toimiiko organisaatio rekisterinpitäjänä, yhteisrekisterinpitäjänä vai henkilötietojen käsittelijänä.

Yleiskuvaus	Rekisterinpitäjäksi kutsutaan henkilöä, yritystä, viranomaista tai yhteisöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Henkilötietojen käsittelijäksi kutsutaan rekisterinpitäjästä ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun rekisterinpitäjän ohjeiden mukaisesti. HUOM. Organisaation rooli voi olla eri kussakin henkilötietojen käsittelytapauksessa, sillä se on riippuvainen siitä, kuka määrittää käsittelyn tarkoitukset ja keinot. Organisaatio voi käsitellä henkilötietoja toisen lukuun käsittelijänä. Se on kuitenkin rekisterinpitäjä sellaisten henkilötietojen käsittelyssä, joita se käsittelee omasta puolestaan, eikä asiakkaina olevien rekisterinpitäjien puolesta. Organisaatio on rekisterinpitäjä esimerkiksi silloin, kun se käsittelee organisaation oman henkilökunnan henkilötietoja. Henkilötietojen käsittelijä voi käsitellä henkilötietoja vain rekisterinpitäjän määrittelemiin tarkoituksiin. Henkilötietojen käsittelijä ei voi ryhtyä käsittelemään rekisterinpitäjän lukuun käsiteltäviä tietoja omiin tarkoituksiinsa määrittelemällä henkilötietojen käsittelyn tarkoituksia ja keinoja.
Toteutusesimerkki	Organisaation rooli voidaan dokumentoida yhdeksi lähtötiedoksi henkilötietojen käsittelyä kuvaavaan dokumentaatioon, esimerkiksi selosteisiin käsittelytoimista ja tiedonhallintamalliin.
Lainsäädäntö	679/2016 Art 4(7-8), 26 ja 28
Tunniste	**TSU-03, L:, E:, S:, TS:Henkilötieto**
Nimi	**Yhteisrekisterinpitäjät**
Vaatimus	Toimiessaan yhteisrekisterinpitäjänä organisaatio määritelee läpinäkyvällä järjestelyllä muiden yhteisrekisterinpitäjien kanssa rekisterinpitäjien velvoitteiden noudattamisesta sekä rekisteröityjen informoinnista.
Yleiskuvaus	Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Ne määrittelevät keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueen tietosuoja-asetuksessa vahvistettujen velvoitteiden noudattamiseksi, erityisesti rekisteröityjen oikeuksien käytön ja rekisteröityjen informoinnin osalta. Järjestelyn yhteydessä voidaan nimetä rekisteröidyille yhteyspiste. Järjestelystä on käytävä asianmukaisesti ilmi yhteisten rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla. Riippumatta järjestelyn ehdoista rekisteröity voi käyttää tietosuoja-asetuksen mukaisia oikeuksiaan suhteessa kuhunkin rekisterinpitäjään ja kutakin rekisterinpitäjää vastaan.
Toteutusesimerkki	Organisaatio voi esimerkiksi dokumentoida kirjallisesti yhteisrekisterinpitäjyyteen liittyvät menettelyt sekä julkaista ne verkossa ja asettaa saataville toimipisteissä.
Lainsäädäntö	679/2016 Art 26
Tunniste	**TSU-04, L:, E:, S:, TS:Henkilötieto**

Nimi	Henkilötietojen käsittelijä
Vaatimus	Organisaatio käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet.
Yleiskuvaus	Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Henkilötietojen käsittelijöiden toimet voivat olla hyvin tarkkaan rajattuja, kuten postin toimituksen ulkoistaminen. Tehtävät voivat olla myös laajoja ja yleisiä, ja niihin voi liittyä tietyn palvelun hallinta toisen organisaation puolesta, esimerkiksi yrityksen työntekijöiden palkanmaksuun liittyvät tehtävät. Henkilötietojen käsittelijää koskeva sääntely koskee esimerkiksi seuraavia palveluntarjoajia: - IT-palveluntarjoajat, ohjelmistojen integroijat, kyberturvallisuusyritykset ja IT-konsulttiyritykset, joilla on pääsy rekisterinpitäjän henkilötietoihin. - Terveydenhuollon laboratorio, joka käsittelee näytteitä rekisterinpitäjän lukuun. - Markkinointi- ja viestintätoimistot, jotka käsittelevät henkilötietoja asiakkaidensa puolesta. - Yleisemmin kaikki organisaatiot, joiden tarjoamiin palveluihin sisältyy henkilötietojen käsittelyä toisen organisaation puolesta. - Myös julkista viranomaista tai järjestöä voidaan pitää henkilötietojen käsittelijänä. Ohjelmistojulkaisijoita ja laitevalmistajia, esimerkiksi työajan seurantalaitteiden, biometristen laitteiden tai lääkinnällisten laitteiden valmistajia, ei pidetä henkilötietojen käsittelijöinä, jos niillä ei ole pääsyä henkilötietoihin, eivätkä ne käsittele henkilötietoja.
Toteutusesimerkki	Organisaatio voi arvioida käsittelijän kyvykkyyttä esimerkiksi käsittelijän toimittaman dokumentaation, hyväksyttyjen käytännesääntöjen tai sertifiointien avulla.
Lainsäädäntö	679/2016 Art 28
Viitteet	HAL-16,
Tunniste	**TSU-04.1, L:, E:, S:, TS:Henkilötieto**
Nimi	**Henkilötietojen käsittelijä - Sopimukset**
Vaatimus	Organisaatio laatii henkilötietojen käsittelijöiden kanssa tietosuoja-asetuksen vaatimukset täyttävät sopimukset.
Yleiskuvaus	Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Sopimuksen yksityiskohtaisemmat sisältövaatimukset on määritelty tietosuoja-asetuksen 28 artiklassa.

Toteutusesimerkki	Organisaatio voi laatia henkilötietojen käsittelyä koskevan sopimuksen esimerkiksi hyödyntämällä dokumenttia: JHS 166 Julkisen hallinnon IT-hankintojen yleiset sopimusehdot, Liite 9. Erityisehtoja henkilötietojen käsittelystä (JIT 2015 – Henkilötiedot) osana sopimusta. Sopimusehtojen lisäksi rekisterinpitäjän tulee toimittaa käsittelijälle tai muutoin sopia käsittelijän kanssa henkilötietojen käsittelyssä noudatettavat ohjeet.
Lainsäädäntö	679/2016 Art 28
Viitteet	HAL-16.1,
Tunniste	**TSU-05, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tehtävät ja vastuut**
Vaatimus	Organisaatio määrittelee henkilötietojen käsittelyyn liittyvät tehtävät ja vastuut.
Yleiskuvaus	Organisaation johdon tehtävänä on määritellä henkilötietojen käsittelyyn liittyvät vastuut. Tietosuojavastuut liittyvät tietoturvavastuiden määrittelyyn mm. käsittelyn turvallisuuteen liittyvien toimenpiteiden osalta, jotka ovat monissa tilanteissa yhteisiä henkilötiedoille ja muille organisaation käsittelemille tiedoille.
Toteutusesimerkki	Tehtävät ja vastuut kirjata työjärjestyksiin, tehtävänkuvauksiin, toimintaohjeisiin tai vastuumatriiseihin. Tehtävät voi kirjata myös roolipohjaisesti, mutta tällöin on varmistettava, että rooleihin liittyvät henkilöt on löydettävissä helposti dokumentaation perusteella. Tietosuojaan liittyvien tehtävien laajuus vaihtelee organisaatiokohtaisesti. Henkilötietointensiivisissä organisaatioissa voidaan toimia esimerkiksi siten, että organisaatio nimeää yhden tai useamman henkilön vastuuseen koko organisaation laajuisen hallinnointi- ja tietosuojaohjelman kehittämisestä, toteuttamisesta, ylläpitämisestä ja seurannasta, jotta voidaan varmistaa vaatimustenmukaisuus suhteessa kaikkiin soveltuviin henkilötietojen käsittelyä koskeviin lakeihin ja viranomaisvaatimuksiin. Joissakin organisaatioissa voi olla myös tarve nimetä erikseen henkilöt toteuttamaan rekisteröidyn oikeuksia koskevia pyyntöjä.
Lainsäädäntö	679/2016 Art 12, 24
Viitteet	HAL-02,
Tunniste	**TSU-05.1, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tehtävät ja vastuut - Tietosuojavastaava**
Vaatimus	Organisaatio nimeää tehtävään soveltuvan tietosuojavastaavan ja julkistaa hänen yhteystiedot.

Yleiskuvaus	Viranomaisen on nimettävä tietosuojavastaava paitsi jos kyseessä on lainkäyttötehtäviään hoitava tuomioistuin. Usemmalla viranomaisella voi olla yhteinen tietosuojavastaava. Tietosuojavastaavaksi nimetyllä henkilöllä tulee olla asiantuntemusta tietosuojalainsäädännöstä sekä kyky hoitaa tietosuojavastaavalle asetuksessa määritellyt tehtävät. Tietosuojavastaava voi kuulua henkilöstöön tai hoitaa tehtäviä palvelusopimuksen perusteella. Organisaation tulee julkistaa tietosuojavastaavan yhteystiedot sekä ilmoittaa ne valvontaviranomaiselle.
Lainsäädäntö	679/2016 Art 37-39
Tunniste	**TSU-05.2, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tehtävät ja vastuut - Tietosuojavastaavan asema ja tehtävät**
Vaatimus	Organisaatio määrittelee tietosuojavastaavan aseman, resurssit ja valtuudet siten, että hänellä on edellytykset hoitaa tietosuojavastaavalle kuuluvat tehtävät.
Yleiskuvaus	Tietosuojavastaavalle kuuluvat seuraavat tehtävät: - seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita - antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille - antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta - on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa - on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa Tietosuojavastaavan aseman ja toimintaedellystysten varmistamiseksi organisaation tulee - varmistaa että tietosuojavastaava otetaan mukaan tietosuojaa koskevien asioiden käsittelyyn - varmistaa tietosuojavastaavan resurssit ja pääsy tarvittaviin tietoihin - varmistaa tietosuojavastaavan riippumattomuus tehtävien suorittamisessa Tietosuojavastavaa koskee tehtäviin liittyen salassapitovelvollisuus.
Toteutusesimerkki	Tietosuojavastaavan tehtävien toteutus voi vaihdella paljonkin riippuen henkilötietojen käsittelyn laajuudesta ja luonteesta organisaatiossa. Tietosuojavastaava voi suorittaa muita tehtäviä edellyttäen, että ne eivät aiheuta eturistiriitoja tietosuojavastaavan tehtävien kanssa. Laajoissa organisaatioissa tietosuojavastaavan tehtäviä voidaan hajauttaa usealle henkilölle.
Lainsäädäntö	679/2016 Art 37-39
Tunniste	**TSU-06, L:, E:, S:, TS:Henkilötieto**
Nimi	**Henkilötietojen käsittelyn ohjeet**
Vaatimus	Organisaatio laatii henkilötietojen käsittelyä koskevat ohjeet ja varmistaa, että henkilötietoja käsitellään näiden ohjeiden mukaisesti.

Yleiskuvaus	Henkilötietojen käsittelijä tai kukaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, ei saa käsitellä niitä muuten kuin rekisterinpitäjän ohjeiden mukaisesti. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.
Toteutusesimerkki	Organisaatio voi muodostaa yleiset henkilötietojen käsittelyä koskevat ohjeet sekä täydentää niitä tarpeen mukaan prosessikohtaisilla lisäohjeilla. Organisaation tulee myös varmistaa ohjeiden jakelun, perehdytystan, koulutusten ja viestinnän avulla, että ajantasaiset henkilötietojen käsittelyä koskevat ohjeet ovat kaikkien niitä tarvitsevien saatavilla ja tiedossa.
Lainsäädäntö	679/2016 Art 29, 32(4)
Viitteet	HAL-12,
Tunniste	**TSU-07, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn lainmukaisuus**
Vaatimus	Organisaatio tunnistaa käsittelemiensä henkilötietojen lainmukaiset käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy: 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 suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi. (f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.) Mikäli käsittely koskee henkilötunnusta, erityisiä henkilötietoryhmiä, rikostuomioita ja rikoksia ja niihin liittyviä turvaamistoimia tai perustuu suostumukseen, organisaatio ottaa huomioon niihin liittyvät lisävaatimukset.
Toteutusesimerkki	Organisaatio määrittää kaikki henkilötietojen käsittelyiden perusteet on ennen käsittelyiden aloittamista. Kun henkilötietojen käsittely sidotaan johonkin käsittelyperusteeseen, perustetta ei voi enää vaihtaa toiseen. Organisaatio dokumentoi käsittelyperusteet.

Lainsäädäntö	1050/2018 4 §, 5 §, 7 §, 29 §; 679/2016 Art art 5(1)(a), 6, 7, 8, 10
Tunniste	**TSU-07.1, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn lainmukaisuus - Suostumus**
Vaatimus	Jos henkilötietojen käsittely perustuu suostumukseen, organisaatio varmistaa, että suostumuksen tietosuoja-asetuksessa säädetyt edellytykset täyttyvät.
Yleiskuvaus	Suostumuksen pyytämiselle on tietosuoja-asetuksessa säädetty seuraavat edellytykset: 1. Jos tietojenkäsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. 2. Jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Mikään tätä asetusta rikkova osa sellaisesta ilmoituksesta ei ole sitova. 3. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Ennen suostumuksen antamista rekisteröidylle on ilmoitettava tästä. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen. 4. Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten.
Toteutusesimerkki	Organisaatio voi ensin selvittää perustuuko mikään henkilötietojen käsittely suostumukseen. Mikäli perustuu, organisaatio voi määritellä prosessit sekä suostumuksen pyytämiseen että peruuttamiseen, joissa varmistetaan että kaikki pyytämisen edellytykset täyttyvät. Prosesseissa tulee huomioida dokumentointi, jotta suostumuksen edellytysten täyttyminen on osoitettavissa jälkikäteen.
Lainsäädäntö	679/2016 Art 7
Tunniste	**TSU-07.2, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn lainmukaisuus - Lapsen suostumus**
Vaatimus	Jos henkilötietojen käsittely perustuu alle 13-vuotiaan lapsen suostumukseen, organisaatio pyytää suostumuksen tämän huoltajalta tai muulta vanhempainvastuun kantajalta. Lapsi voi kuitenkin käyttää neuvonta- ja tukipalveluja sekä ennalta ehkäiseviä palveluja ilman huoltajan suostumusta.

Yleiskuvaus	Kun kyseessä on tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle ja käsittely perustuu suostumukseen, lapsen henkilötietojen käsittely on lainmukaista, jos lapsi on vähintään 13-vuotias. Jos lapsi on alle 13 vuotta, tällainen käsittely on lainmukaista vain siinä tapauksessa ja siltä osin kuin lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen tai valtuutuksen.
Toteutusesi-merkki	Organisaatio voi määritellä suostumuksen antamisen prosessin siten, että tarkastetaan suostumuksen antajan ikä, ja mikäli kyseessä on alle 13 vuotias lapsi, pyydetään suostumus huoltajalta tai muulta vanhempainvastuun kantajalta.
Lainsäädäntö	1050/2018 5 §; 679/2016 Art 8
Tunniste	**TSU-07.3, L:, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	**Käsittelyn lainmukaisuus - Erityiset henkilötietoryhmät**
Vaatimus	Organisaatio tunnistaa käsittelemiensä erityisten henkilötietoryhmien käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Erityisten henkilötietoryhmien, kuten etnistä alkuperää tai terveyttä koskevien tietojen käsittely on lähtökohtaisesti kiellettyä. Käsittely on kuitenkin mahdollista silloin, kun käsittelykieltoon on säädetty poikkeus tietosuoja-asetuksessa tai kansallisessa lainsäädännössä.
Toteutusesi-merkki	Ennen erityisiin henkilötietoryhmiin liittyvän henkilötietojen käsittelyn aloittamista organisaatio voi toimia esimerkiksi seuraavalla tavalla: - Organisaatio selvittää ja dokumentoi käsittelyn perusteet ja varmistaa, että ne perustuvat johonkin tietosuoja-asetuksessa tai kansallisessa lainsäädännössä määriteltyyn poikkeukseen.
Lainsäädäntö	1050/2018 6 § 1 mom; 679/2016 Art 9
Tunniste	**TSU-07.4, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn lainmukaisuus - Henkilötunnus**
Vaatimus	Organisaatio tunnistaa henkilötunnuksen käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää: 1) laissa säädetyn tehtävän suorittamiseksi; 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai 3) historiallista tai tieteellistä tutkimusta taikka tilastointia varten. Henkilötunnusta saa käsitellä luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Sen lisäksi, henkilötunnuksen saa luovuttaa osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi suoritettavaa tietojenkäsittelyä varten, jos henkilötunnus jo on luovutuksensaajan käytettävissä.

Toteutusesimerkki	Organisaatio voi esimerkiksi erikseen määritellä kaikki ne käsittelytoimet, joissa henkilötunnusta käytetään ja varmistaa kunkin toimenpiteen kohdalla, että henkilötunnuksen käytölle on laissa hyväksytty peruste.
Lainsäädäntö	1050/2018 29 §
Tunniste	**TSU-07.5, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn lainmukaisuus - Rikostuomioihin ja rikoksiin liittyvät henkilötiedot**
Vaatimus	Organisaatio tunnistaa käsittelemiensä rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittelyperusteet ja dokumentoi ne.
Yleiskuvaus	Rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely lainmukaisella käsittelyperusteella on mahdollista vain viranomaisen valvonnassa tai jos a. käsittely on tarpeen oikeusvaateen selvittämiseksi, laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi; b. tietojen käsittelystä säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä; tai c. tietoja käsitellään tieteellistä tai historiallista tutkimusta taikka tilastointia varten. Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.
Toteutusesimerkki	Ennen rikostuomioihin ja rikkomuksiin liittyvän henkilötietojen käsittelyn aloittamista organisaatio voi toimia esimerkiksi seuraavalla tavalla: - Organisaatio selvittää ja dokumentoi käsittelyn perusteet ja varmistaa niiden asianmukaisuuden.
Lainsäädäntö	1050/2018 7 §; 679/2016 Art 10
Tunniste	**TSU-08, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tarpeellisuus ja oikeasuhtaisuus**
Vaatimus	Organisaatio varmistaa, että henkilötietojen käsittely on tarpeellista ja oikeasuhtaista käsittelyn laillisten tarkoitusten saavuttamiseksi.
Yleiskuvaus	Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoilla.
Toteutusesimerkki	Ennen henkilötietojen käsittelyn aloittamista organisaatio selvittää ja dokumentoi voidaanko käsittelyn tarkoitusta kohtuudella toteuttaa ilman henkilötietojen käsittelyä. Jos käsittelyn tarkoitus, esimerkiksi palvelun toteuttaminen, on mahdollista tehdä siten, että tiettyjä tietoja ei käsitellä, ei henkilötietojen käsittely niiltä osin ole tarpeellista eikä henkilötietoja tule silloin käsitellä.
Lainsäädäntö	679/2016 Art 5
Tunniste	**TSU-09, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käyttötarkoitussidonnaisuus**
Vaatimus	Organisaatio kerää henkilötietoja vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa, eikä käsittele henkilötietoja alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.

Yleiskuvaus	Henkilötietojen käsittelyn tarkoitus tai tarkoitukset on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin. Henkilötietojen käsittely voi olla mahdollista määritetyn käyttötarkoituksen ohella myös sellaiseen käyttötarkoitukseen, joka katsotaan yhteensopivaksi alkuperäisen käyttötarkoituksen kanssa. Käsittelyn on oltava lainmukaista myös muiden tietosuojasäännösten näkökulmasta; yhteensopiva käyttötarkoitus ei oikeuta rekisterinpitäjää poikkeamaan muista tietosuojasäännöksistä. Henkilötietojen käsittely seuraaviin tarkoituksiin on yhteensopivaa, jos tietosuoja-asetuksen suojatoimia noudatetaan asianmukaisesti. - yleisen edun mukainen arkistointi - tieteellinen tai historiallinen tutkimus - tilastolliset tarkoitukset
Toteutusesimerkki	Organisaatio voi varmistaa käyttötarkoitussidonnaisuuden noudattamista esimerkiksi: - dokumentoimalla huolellisesti kaikki henkilötietojen käyttötarkoitukset ja käsittelyprosessit, - tarkastamalla säännöllisesti, että henkilötietoja ei käytetä muihin käyttötarkoituksiin sekä - tiedottamalla käyttötarkoitussidonnaisuuden periaatteesta ohjeissa ja koulutuksissa.
Lainsäädäntö	679/2016 Art 5(1)(b), 6(4)
Tunniste	**TSU-10, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tietojen minimointi**
Vaatimus	Organisaatio käsittelee henkilötietoja vain siinä määrin, kun se on tarpeellista käsittelyn tarkoituksen kannalta.
Yleiskuvaus	Tiedon minimoinnilla tarkoitetaan rekisteröidyistä kerättävien ja käsiteltävien tietojen määrän minimointia. Käsiteltävien henkilötietojen on oltava - asianmukaisia eli kerättyjen tietojen on oltava sellaisia tietoja, joilla kyetään täyttämään määritelty käyttötarkoitus - olennaisia eli kerätyillä henkilötiedoilla on oltava selkeä yhteys määriteltyyn käyttötarkoitukseen ja - rajoitettuja eli tarpeellisia määritellyn henkilötietojen käyttötarkoituksen kannalta. Henkilötietojen oikean määrän arvioimiseksi on selkeästi tunnistettava se syy, miksi kyseisiä henkilötietoja tarvitaan. Käyttötarkoituksen kautta pystytään määrittelemään, mitkä henkilötiedot ovat välttämättömiä käsittelyn tarkoituksen toteuttamiseksi Organisaatio varmistaa, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Toteutusesimerkki	Henkilötietojen tarpeellisuuden arviointi voidaan määritellä osaksi henkilötietojen käsittelyn aloittamiseen ja muutostilanteisiin liittyviä prosesseja. Arvioinnissa on tulee käydä läpi kaikki yksittäiset henkilötietoryhmät ja arvioida niiden tarpeellisuus suhteessa käsittelyn tarkoituksiin.. Organisaatio voi ennen henkilötietojen käsittelyn aloittamista toimia esimerkiksi seuraavalla tavalla: - Pseudonymisoida tai anonymisoida tiedot silloin kun se on mahdollista. - Varmistaa, että järjestelmien näytöissä, sekä tulostettavissa ja laadittavissa asiakirjoissa ei näy tarpeettomia henkilötietoja (erityisesti henkilötunnusta ja erityisiä henkilötietoryhmiä) esimerkiksi järjestelmien näkymien suunnittelulla, ohjeistamalla asian, nostamalla asian esiin perehdytyksissä ja koulutuksissa tai tekemällä tarkastuksia henkilötietoja sisältäviin asiakirjoihin. - Varmistaa, että henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.
Lainsäädäntö	1050/2018 29.4 §; 679/2016 Art 51)(c), 25(2)
Tunniste	**TSU-11, L:, E:, S:, TS:Henkilötieto**
Nimi	**Säilytyksen rajoittaminen**
Vaatimus	Organisaatio säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa, ainoastaan niin kauan, kun on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten.
Yleiskuvaus	Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan henkilötietojen säilytysaika. Henkilötietojen säilytysajat on myös dokumentoitava. Rekisterinpitäjän on arvioitava henkilötietojen säilytysaikaa ja tarpeellisuutta kysymyksessä olevaa käyttötarkoitusta vasten. Henkilötietoja saa säilyttää vain niin kauan, kun ne ovat tarpeen henkilötietojen käyttötarkoituksen kannalta. Henkilötietojen säilytysaikaan voi vaikuttaa myös kansallinen lainsäädäntö, jossa säädetään säilytysajoista, esimerkiksi kirjanpitolaki. Rekisterinpitäjän on itse huomioitava laista tulevat säilytysajat. Kun henkilötietoja ei enää tarvita, ne tulee anonymisoida tai poistaa. Rekisterinpitäjän on varmistettava, että sen käytössä olevat tietojärjestelmä (ml. pilvipalvelut) ja muut käsittelyprosessit tukevat säilytysaikojen noudattamista ja säännöllistä arvioimista. Myös rekisteröity voi pyytää rekisterinpitäjää poistamaan henkilötiedot silloin, kun niitä ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä käsiteltiin. Henkilötietoja voi säilyttää alkuperäistä käyttötarkoitusta kauemmin ainoastaan silloin, kun henkilötietoja käsitellään ainoastaan yleisen edun mukaista arkistointia, tieteellistä tai historiallista tutkimusta tai tilastollisia tarkoituksia varten, jos tietosuoja-asetuksen suojatoimia noudatetaan asianmukaisesti. Suojatoimien on katettava niin tekniset kuin organisatoriset toimenpiteet, joilla taataan erityisesti tietojen minimoinnin periaatteen noudattaminen. Minimoinnin periaate edellyttää myös mahdollisimman lyhyttä säilytysaikaa. Henkilötietoja ei saa käsitellä, jos tarkoitukset on mahdollista toteuttaa anonyymeillä tiedoilla.

Toteutusesimerkki	Organisaatio voi määritellä osaksi henkilötietojen käsittelyn aloittamisen prosessia henkilötietojen säilytysajan tai sen määräytymisen perusteen määrittelyn sekä prosessin, jonka mukaan henkilötiedot poistetaan säilytysajan päättyessä Organisaatio varmistaa, että myös varmuuskopiot poistuvat henkilötietoja poistettaessa.
Lainsäädäntö	679/2016 Art 5(1) (e), 25(2)
Tunniste	**TSU-12, L:, E:, S:, TS:Henkilötieto**
Nimi	**Täsmällisyys**
Vaatimus	Organisaatio varmistaa, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä sekä toteuttaa kaikki mahdolliset kohtuulliset toimenpiteet käsittelyn tarkoituksiin nähden epätarkkojen ja virheellisten henkilötietojen poistamiseksi tai oikaisemiseksi viipymättä.
Yleiskuvaus	Organisaation tulee varmistua hallussaan olevien tietojen täsmällisyydestä. Tietojen oikeellisuuden varmistaminen on erityisen tärkeää silloin, kun henkilötietojen perusteella tehdään yksilön kannalta olennaisia päätöksiä. Epätäsmälliset ja virheelliset tiedot voivat vakavalla tavalla vaarantaa rekisteröidyn oikeuksia. Esimerkiksi virheelliset terveydentilaa koskevat tiedot potilasrekisterissä voivat johtaa vääriin hoitotoimenpiteisiin. Organisaation tulee toteuttaa kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Mitä tärkeämpää tiedon täsmällisyys on, sitä enemmän rekisterinpitäjän on tehtävä toimenpiteitä tietojen oikeellisuuden varmistamiseksi. Rekisterinpitäjällä on oltava käytössään menetelmiä tiedon täsmällisyyden ja oikeellisuuden säännölliseen arviointiin sekä tarpeellisten päivitysten tekemiseen. Myös rekisteröidyllä on yleensä oikeus arvioida rekisterinpitäjän käyttämiä henkilötietoja ja tarvittaessa esittää oikaisupyyntöjä epätarkkojen tai virheellisten tietojen osalta sekä poistopyyntöjä tarpeettomien tietojen osalta. Jos rekisterinpitäjä luovuttaa hallussaan olevia henkilötietoja eteenpäin, on vastaanottajista syytä pitää kirjaa. Rekisterinpitäjällä on velvollisuus ilmoittaa kaikenlaisista henkilötietojen oikaisuista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Ilmoitusvelvollisuudesta on mahdollista poiketa vain silloin, kun se osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Rekisteröidyllä on myös oikeus pyytää tietoa henkilötietojen vastaanottajista. Tieto henkilötiedon virheellisyydestä tulee tarvittaessa voida välittää myös alkuperäiselle tietolähteelle, minkä vuoksi henkilötiedon oheen tulee merkitä tietolähde kun tietoja saadaan toiselta rekisterinpitäjältä.
Toteutusesimerkki	Rekisterinpitäjä voi esimerkiksi määritellä prosessit tiedon täsmällisyyden ja oikeellisuuden säännölliseen arviointiin, tarpeellisten päivitysten tekemiseen sekä henkilötietojen oikaisuista ilmoittamiseen jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu ja tietolähteelle jolta alkuperäinen korjattu tieto on saatu.
Lainsäädäntö	679/2016 Art 5(1)(d)
Tunniste	**TSU-13, L:, E:, S:, TS:Henkilötieto**
Nimi	**Käsittelyn turvallisuus**

Vaatimus	Organisaatio varmistaa henkilötietojen turvallisuuden käyttäen asianmukaisia teknisiä tai organisatorisia toimia.
Yleiskuvaus	Ottaen huomioon toteuttamiskustannukset, käsittelyn luonne, laajuus, sekä todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten a) henkilötietojen pseudonymisointi ja salaus; b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa; d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi. Hyväksyttyjen käytännesääntöjen tai hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että asetettuja vaatimuksia noudatetaan.
Toteutusesimerkki	Henkilötietojen käsittelyn turvallisuuden varmistaminen voidaan toteuttaa osana organisaation muiden tietoturvakontrollien määrittelyä ja toteutusta ottamalla henkilötietoihin kohdistuvat riskit yhdeksi osaksi riskien arviointia päätettäessä minkä tasoisia teknisiä ja organisatorisia suojatoimia organisaation vastuulla oleviin tietoihin kohdistetaan. Organisaatio voi varmistaa käsittelyn turvallisuutta esimerkiksi toteuttamalla tämän kriteeristön mukaisia kriteereitä ja kiinnittämällä erityisesti huomiota vähimmäiskriteereitä täydentävien kriteerien valintaan riskiperusteisesti.
Lainsäädäntö	679/2016 Art 5, 32
Tunniste	**TSU-13.1, L:, E:, S:, TS:Erityinen henkilötietoryhmä**
Nimi	**Käsittelyn turvallisuus - Erityiset henkilötietoryhmät tai rikostuomioihin ja rikoksiin liittyvät tiedot**
Vaatimus	Käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tai rikostuomioihin ja rikoksiin liittyviä henkilötietoja organisaatio toteuttaa asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi.

Yleiskuvaus	Näitä erityisiä toimenpiteitä ovat: 1) toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty; 2) toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista; 3) tietosuojavastaavan nimittäminen; 4) rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin; 5) henkilötietojen pseudonymisointi; 6) henkilötietojen salaaminen; 7) toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa; 8) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi; 9) erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen; 10) tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskevan vaikutustenarvioinnin laatiminen; 11) muut tekniset, menettelylliset ja organisatoriset toimenpiteet.
Toteutusesimerkki	Käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja organisaatio: - varmistaa henkilötietojen käsittelyn turvallisuuden ottaen huomioon, että kyseessä ovat salassa pidettävät henkilötiedot, joiden luottamuksellisuuteen ja eheyteen kohdistuu korkeampia vaatimuksia ja suurempia riskejä - arvioi tarpeen erityisille toimenpiteille rekisteröidyn oikeuksien suojaamiseksi ja toteuttaa riskiarvion perusteella niistä tarpeelliset.
Lainsäädäntö	1050/2018 6§ 2 mom ja 7§ 2 mom; 679/2016 Art 5, 32
Tunniste	**TSU-14, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tietoturvaloukkaukset**
Vaatimus	Organisaatio dokumentoi kaikki henkilötietojen tietoturvaloukkaukset, sekä määrittelee toimintatavat niistä ilmoittamiseen valvontaviranomaiselle ja rekisteröidyille.
Yleiskuvaus	Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksen yhteydessä on dokumentoitava siihen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on havaittu, jos tietoturvaloukkaus todennäköisesti aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Jos loukkaus voi aiheuttaa henkilöille korkean riskin, heille on ilmoitettava tapahtuneesta tietoturvaloukkauksesta henkilökohtaisesti ilman aiheetonta viivytystä. Mikäli organisaatio toimii henkilötietojen käsittelijänä, sen on on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

Toteutusesimerkki	Organisaatio voi esimerkiksi määritellä osaksi yleistä häiriönhallintaprosessia henkilötietoihin kohdistuvien tietoturvaloukkausten arvioinnin ja käsittelyn, johon sisältyvät ohjeet ja vastuut tietoturvaloukkausten arvioinnista, käsittelystä, tietoturvaloukkauksiin liittyvien tietojen keruusta sekä tietoturvaloukkauksista ilmoittamisesta tietosuojavaltuutetulle ja rekisteröidyille. Organisaatio kerää ja tallentaa tapahtuneesta henkilötietojen tietoturvaloukkauksesta mm. tietoturvaloukkauksen kuvauksen (kuten sen luonne ja kohteena olevat tiedot), tapahtuma-ajan lokitiedot, ilmoitusvelvoitteiden täyttämiseksi tarvittavat tiedot, tiedot loukkauksen vaikutuksista ja seurauksista, riskiarvioinnin sekä tehdyt toimenpiteet ja tietoturvaloukkaukseen liittyvät päätökset.
Lainsäädäntö	679/2016 Art 33
Viitteet	HAL-08, HAL-09,
Tunniste	**TSU-15, L:, E:, S:, TS:Henkilötieto**
Nimi	**Osoitusvelvollisuus**
Vaatimus	Organisaatio pystyy osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia.
Yleiskuvaus	Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen säännöksiä. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on myös pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet täyttääkseen osoitusvelvollisuuden vaatimukset. Osoitusvelvollisuus tarkoittaa myös dokumentointivelvollisuutta, käytännössä tiettyjen toimenpiteiden tekemistä ja kirjaamista. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Tietosuoja-asetuksessa on osoitusvelvollisuutta koskevia vaatimuksia, joiden velvoittavuus on arvioitava tapauskohtaisesti. Osoitusvelvollisuuden laajuus riippuu muun muassa organisaation koosta, henkilötietojen määrästä ja siitä, millaisia henkilötietoja rekisterinpitäjä käsittelee. Rekisterinpitäjän on huomioitava osoitusvelvollisuus jo henkilötietojen käsittelyn suunnitteluvaiheessa.
Toteutusesimerkki	Osoitusvelvollisuuden toteuttamiseksi organisaatio voi esimerkiksi määritellä ja dokumentoida kirjallisesti kaikki tietosuojan toteuttamiseen liittyvät prosessit sekä varmistaa, että näiden prosessien lopputuloksena syntyy dokumentaatio, jolla voidaan osoittaa että prosesseja on noudatettu.
Lainsäädäntö	679/2016 Art 5(2), 24
Viitteet	HAL-09,
Tunniste	**TSU-16, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tietosuojariskien hallinta**
Vaatimus	Organisaatio arvioi henkilötietojen käsittelyyn kohdistuvat olennaiset riskit sekä toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet riskiarvioinnin mukaisesti.

Yleiskuvaus	Tietosuojariskien hallinta tarkoittaa järjestelmällistä, koordinoitua ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä. Tietosuojariskien arvio on tehtävä rekisteröidyn näkökulmasta eli organisaation on arvioitava - mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja - mitä vahinkoja (fyysisiä, aineellisia tai aineettomia) rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Tietosuojariskien arvioinnissa on otettava huomioon seuraavat tekijät: a) käsittelyn luonne (esim. erityiset henkilötietoryhmät, rekisteröidyn vaikeus käyttää oikeuksiaan johtuen esim. käsittelyn ennakoimattomuudesta tai läpinäkymättömyydestä, uusi teknologia ja innovaatiot, rekisteröidyn heikko asema), b) käsittelyn laajuus (rekisteröityjen lukumäärä, tiedon määrä, säilytysaika, maantieteellinen kattavuus), c) käsittelyn asiayhteys (esim. luottamuksellisuus, kotirauha, eri yhteyksissä kerättyjen henkilötietojen yhdistely), d) käsittelyn tarkoitukset (esim. rekisteröityjen tarkkailu, seuranta ja valvonta, henkilöiden arviointi tai pisteytys, automaattinen päätöksenteko, jolla on vaikutuksia rekisteröityyn , sekä e) luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Riskin tunnistamisen merkitys korostuu erityisesti silloin, kun rekisterinpitäjä määrittää teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuojan toteutuminen henkilötietojen käsittelyssä. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi, omavalvonnan kautta tapahtuvaa käytönvalvontaa, tietojärjestelmien tietoturvaa, henkilötietojen tietoturvaloukkauksesta ilmoittamista, henkilötietojen salausta, henkilötietojen pseudonymisointia ja muita suojatoimenpiteitä. Riskien hallinta on jatkuvaa toimintaa: toimenpiteiden riittävyyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Rekisterinpitäjällä on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta.
Toteutusesimerkki	Tietosuojariskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Organisaatio toteuttaa tämän kriteeristön mukaisia hallintakeinoja ja kiinnittämää erityisesti huomiota vähimmäiskriteereitä täydentävien kriteerien valintaan riskiperusteisesti. Tietosuojariskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. Tietosuojan vaikutusten arviointi (TSU-17) sekä siihen sisältyvä erityinen tietosuojariskien arviointi on pakollinen silloin, kun suunniteltu käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.
Lainsäädäntö	679/2016 Art 24, 25, 32-34, 35
Viitteet	HAL-06,
Tunniste	**TSU-17, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tietosuojan vaikutustenarviointi**

Vaatimus	Organisaatio toteuttaa ennen henkilötietojen käsittelyä arvioinnin suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle silloin, kun henkilötietojen käsittelyyn liittyy korkeita riskejä rekisteröidylle.
Yleiskuvaus	Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Vaikutustenarvioinnissa kuvataan henkilötietojen käsittelyä, arvioidaan käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Tavoitteena on sen arviointi, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä käsillä olevissa olosuhteissa. Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa. Organisaation on tehtävä vaikutustenarviointi silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista ja sitä on päivitettävä tarvittaessa. Vaikutustenarviointi on tehtävä erityisesti silloin, kun - henkilötietojen käsittelyssä käytetään uutta teknologiaa - käsitellään laajamittaisesti rikostuomioihin ja rikoksiin liittyviä henkilötietoja tai erityisiä henkilötietoryhmiä, kuten terveystietoja, etnistä alkuperää, poliittisia mielipiteitä, uskonnollista vakaumusta tai seksuaalista suuntautumista - henkilön henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn avulla, järjestelmällisesti ja kattavasti, ja arvio johtaa päätöksiin, joilla on oikeusvaikutuksia tai jotka muuten vaikuttavat henkilöön merkittävästi - yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajamittaisesti. Tietosuojavaltuutetun toimisto on julkaissut verkkosivuillaan luettelon käsittelytoimien tyypeistä, joiden yhteydessä rekisterinpitäjän tulee tehdä tietosuojaa koskeva vaikutustenarviointi. Lisäksi kansallinen erityislainsäädäntö voi edellyttää tietosuojan vaikutusten arvioinnin tekemistä. Vaikutustenarvioinnin tekemistä koskevia vaatimuksia sovelletaan myös ennen 25.5.2018 alkaneisiin, jo käynnissä oleviin käsittelytoimiin.

Toteutusesimerkki	Organisaatiolla voi määritellä prosessin, jonka mukaisesti arvioidaan vaikutustenarvioinnin tarpeellisuus organisaation suorittamille erilaisille henkilötietojen käsittelytoimille. Vaikutustenarviointien toteuttamista varten organisaatio voi laatia ohjeet ja dokumentointimenettelyt, joilla varmistetaan vaikutustenarviointien oikeanlainen ja yhdenmukainen toteutus. Organisaation on pyydettävä tietosuojavastaavan neuvoja vaikutustenarvioinnin tekemisessä, jos rekisterinpitäjä on nimennyt tietosuojavastaavan. Jos henkilötietoja käsittelee osittain tai kokonaan henkilötietojen käsittelijä, hänen on autettava vaikutustenarvioinnin tekemisessä. Vaikutustenarviointien ohjeiden ja pohjien laatimisessa organisaatio voi hyödyntää tietosuojavaltuutetun sivuilla olevia ohjeita. Huom! Pääosa vaikutustenarvioinnissa koottavista tiedoista ja suoritettavista toimenpiteistä on sellaisia, jotka tulee tehdä kaikille henkilötietojen käsittelytoimille riippumatta siitä, tarvitaanko vaikutustenarviointia vai ei. Organisaation kannattaa varmistaa että tällaiset lähtötiedot ovat saatavilla ja hyödyntää niitä vaikutustenarvioinnissa.
Lainsäädäntö	679/2016 Art 35
Tunniste	**TSU-17.1, L:, E:, S:, TS:Henkilötieto**
Nimi	**Tietosuojan vaikutustenarviointi - Ennakkokuuleminen**
Vaatimus	Organisaatio kuulee tarvittaessa tietosuojavaltuutetun toimistoa ennen henkilötietojen käsittelyn aloittamista.
Yleiskuvaus	Organisaation on kuultava tietosuojavaltuutettua ennen henkilötietojen käsittelyn aloittamista, kun vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin rekisteröidylle, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi. Tietosuojaviranomaista on kuultava esimerkiksi silloin, kun rekisteröidyt voisivat joutua kärsimään huomattavista tai peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan. Ennakkokuulemisen johdosta tietosuojavaltuutettu antaa rekisterinpitäjälle tai käsittelijälle kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi. Tarvittaessa tietosuojavaltuutettu voi ennakkokuulemisen yhteydessä käyttää myös sille tietosuoja-asetuksessa annettuja toimivaltuuksia, kuten varoitusta. Rekisteripitäjän ja käsittelijän on toteuttava ohjeen mukaiset lisätoiminpiteet ennen henkilötietojen käsittelyn aloittamista, jotta käsittely voidaan katsoa lainmukaiseksi.
Toteutusesimerkki	Organisaatio voi määritellä ennakkokuulemisen tarpeen tarkastuksen ja ennakkokuulemisen suorittamisen esimerkiksi yhdeksi osaksi vaikutustenarvioinnin ja henkilötietojen käsittelyn aloittamisen prosesseja.
Lainsäädäntö	679/2016 Art 36
Tunniste	**TSU-18, L:, E:, S:, TS:Henkilötieto**
Nimi	**Henkilötietojen siirto ETA:n ulkopuolelle**

Vaatimus	Organisaatio on tunnistanut toimintaansa liittyvät kansainväliset henkilötietojen siirrot ETA-alueen ulkopuolelle ja niihin käytettävät siirtoperusteet, sekä varmistanut tapauskohtaisesti, että siirrettäville henkilötiedoille taataan kolmannen maan lainsäädännössä ja käytännöissä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa.
Yleiskuvaus	Organisaatio voi siirtää henkilötietoja kolmansien maiden julkisille elimille tai kansainvälisille järjestöille Euroopan komission hyväksymän tietosuojan riittävyyttä koskevan päätöksen perusteella (45 art). Jos siirtoon soveltuvaa päätöstä tietosuojan riittävyydestä ei ole tehty, tietoja voidaan siirtää joko - julkisten elinten välisten kansainvälisten sopimusten (46(2)(a) art), - julkisten elinten välisten hallinnollisten järjestelyjen avulla (46(3)(b) art), - muita asianmukaisia suojatoimia soveltaen (46 art), tai - viimesijaisesti erityistilanteita koskevia poikkeuksia soveltaen ja suppeasti tulkiten, jos asianmukaisten suojatoimien käyttö ei ole mahdollista (49 art); poikkeuksien käytön on liityttävä pääasiassa satunnaisiin käsittelytoimiin, jotka eivät ole toistuvia. Organisaatio on tapauskohtaisesti arvioinut riittääkö käytetty siirtomekanismi takaamaan olennaisilta osin saman tietosuojan tason kuin ETA-alueella ja ottanut tarvittaessa käyttöön täydentäviä suojatoimia. HUOM. Organisaatio on huomioinut myös henkilötietojen käsittelijöiden (esimerkiksi pilvipalveluiden tarjoajien) osalta, missä henkilötiedot fyysisesti sijaitsevat. Esimerkiksi palveluntarjoajana toimivan henkilötietojen käsittelijän pääsy etäyhteydellä henkilötietoihin ETA:n ulkopuolelta katsotaan henkilötietojen siirroksi ETA- alueen ulkopuolelle. HUOM. Lähtökohtaisesti pilvipalveluntarjoajalla on aina pääsy palvelussa käsiteltävään tietoon, mikäli tieto on elinkaarensa aikana palvelussa selväkielisessä muodossaan (esimerkiksi asiakkaalle näytettävä kuvana) tai palveluntarjoajalla on pääsy tiedon salaamiseen käytettyihin salausavaimiin. HUOM. Jos minkään siirtoperusteen edellytykset eivät täyty, henkilötietoja ei voida siirtää ETA:n ulkopuolelle.

Toteutusesimerkki	Kolmansiin maihin siirrettävien henkilötietojen, käytettyjen siirtoperusteiden, siirron vastaanottajien ja siirron suorittajien tunnistaminen ja dokumentointi voidaan tehdä osana organisaation suojattavien kohteiden tunnistamista, tehtäessä selostetta käsittelytoimista tai muodostettaessa tiedonhallintamallia. Organisaatio voi varmistaa, että siirrettävät henkilötiedot ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään, noudattaen esimerksi tiedon täsmällisyyden (TSU-13) arviointiin määriteltyjä prosesseja ja käytäntöjä. Organisaatio voi hyödyntää varhaisessa vaiheessa tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston sivuilta löytyviä ohjeita (erityisesti tietosuojaneuvoston ohje 2/2020 henkilötietojen siirtämisessä ETA-alueen ja sen ulkopuolisten viranomaisten ja julkisten elinten välillä) varmistaessaan, että julkisten elinten välisissä oikeudellisesti sitovissa välineissä tai hallinnollisissa järjestelyissä (kansainväliset sopimukset), noudatetaan yleistä tietosuoja-asetusta. Organisaatio voi tapauskohtaisesti arvioidessaan taataanko siirrettäville henkilötiedoille kolmannen maan lainsäädännössä ja/tai käytännöissä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin ETA-alueen tasoa, sekä valitessaan mahdollisesti tarvittavia täydentäviä suojatoimenpiteitä hyödyntää Euroopan tietosuojaneuvoston suosituksia 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, sekä suosituksia 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista. Organisaatio selvittää soveltuvat menettelylliset vaatimukset, mikäli se siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle soveltaen jotain seuraavista suojatoimista: vakiosopimuslausekeet (Art. 46(2)(c) ja (d) GDPR), julkisten elinten väliset hallinnollisiset järjestelyt (Art. 46(3)(b) GDPR), hyväksytyt käytännesäännöt (Art. 46(2)(e), hyväksytty sertifiointimekanismi (Art. 46(2)(f)GDPR) tai ad hoc sopimuslausekkeet (Art. 46.3(a) GDPR). Voit hyödyntää soveltuvien menettelyllisten vaatimusten arvioinnissa Euroopan tietosuojaneuvoston suosituksia 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi Organisaaatio arvioi säännöllisin väliajoin yhdessä siirron vastaanottajien kanssa tapahtuuko kolmannen maan henkilötietojen suojan tasossa tai eurooppalaisten tietosuojaviranomaisten ohjeistuksissa muutoksia ja päivitä käytäntöjä tarvittaessa.
Lainsäädäntö	679/2016 V luku
Tunniste	**TSU-19, L:, E:, S:, TS:Henkilötieto**
Nimi	**Rekisteröidyn oikeudet**
Vaatimus	Organisaatio toteuttaa rekisteröidyn oikeudet.

Yleiskuvaus	Kun rekisterinpitäjä käsittelee henkilötietoja, sen on toteutettava asianmukaiset toimenpiteet rekisteröityjen oikeuksien toteuttamiseksi sekä helpotettava näiden oikeuksien käyttämistä. Organisaation on varmistettava pyyntöjä esittävän rekisteröidyn henkilöllisyys ja noudatettava tietosuoja-asetuksessa asetettuja pyyntöön vastaamisen määräaikoja. Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus - saada tietoa henkilötietojensa käsittelystä - saada pääsy tietoihin - oikaista tietoja - poistaa tiedot ja tulla unohdetuksi - rajoittaa tietojen käsittelyä - siirtää tiedot järjestelmästä toiseen - vastustaa tietojen käsittelyä - olla joutumatta automaattisen päätöksenteon kohteeksi.
Toteutusesimerkki	Rekisteröityjen oikeuksien toteuttamista varten organisaatio voi toteuttaa ja dokumentoida prosessit, joiden avulla varmistetaan ja voidaan osoittaa rekisteröityjen oikeuksien totautuminen. Rekisteröityjen oikeuksiin liittyvien prosessien suunnittelu on tärkeää erityisesti niissä tapauksissa, joissa rekisteröityjen tiedetään käyttävän oikeuksiaan paljon.
Lainsäädäntö	679/2016 Art 12-21
Tunniste	**TSU-19.1, L:, E:, S:, TS:Henkilötieto**
Nimi	**Rekisteröidyn oikeudet - Rekisteröidyn käytettävissä olevien oikeuksien tunnistaminen**
Vaatimus	Organisaatio on määritellyt tunnistamansa henkilötietojen lainmukaisen käsittelyperusteen mukaisesti, mitkä rekisteröidyn oikeudet liittyvät kyseessä olevaan käsittelyyn.
Yleiskuvaus	Rekisteröity ei voi käyttää kaikkia oikeuksiaan kaikissa tilanteissa. Se, mitä oikeuksia rekisteröity voi kulloinkin käyttää, riippuu siitä, millä perusteella kyseessä olevia henkilötietoja käsitellään. Organisatio voi hyödyntää tietosuojavaltuutetun toimiston verkkosivuilla olevaa aineistoa siitä, millä tavalla käsittelyperuste vaikuttaa käytettävissä oleviin oikeuksiin. Kunkin oikeuden toteuttamisesta voi yksittäistapauksessa kieltäytyä. Kieltäytyminen on mahdollista, jos käsillä on jokin oikeuden kohdalla relevantti kieltäytymisperuste tai oikeuden toteuttamisen edellytykset eivät muutoin täyty. Oikeuksiin voi lisäksi olla säädetty poikkeuksia kysymyksessä olevaa organisaatiota koskevassa erityislainsäädännössä.
Toteutusesimerkki	Organisaatio määrittele käsittelyperusteen mukaisesti, mitkä tietosuojaoikeudet liittyvät kyseessä olevaan käsittelyyn. Organisaatio kuvaa, millä tavalla oikeudet otetaan huomioon henkilötietojen käsittelyssä sekä miten oikeuksia koskevat pyynnöt käsitellään ja toteutetaan.
Lainsäädäntö	1050/2018 31-34 §; 679/2016 Art 14(5)(b-d), 17(3), 20(1) ja (3), 21(1) ja (6), 22(2), 23, 85, 89
Tunniste	**TSU-19.2, L:, E:, S:, TS:Henkilötieto**

Nimi	**Rekisteröidyn oikeudet - Läpinäkyvä informointi**
Vaatimus	Organisaatio informoi rekisteröityjä henkilötietojen käsittelystä säädetyllä tavalla.
Yleiskuvaus	Henkilötietoja on käsiteltävä rekisteröidyn kannalta läpinäkyvästi. Tästä yleisestä informoinnista on joitakin poikkeuksia. Informoinnin tarkoituksena on, että rekisteröity saa kattavan ja selkeän kuvan henkilötietojen käsittelyn kokonaisuudesta. Rekisterinpitäjän tulee arvoida, onko annettu informaatio kielen ja johdonmukaisuuden kannalta ymmärrettävää kohderyhmän näkökulmasta. Informoinnin tarkemmat vaatimukset riippuvat osittain siitä, kerätäänkö tietoja henkilöltä itseltään vai muualta. Informoinnin tarkempia vaatimuksia ovat: - tietosisältö - esittämistapaa koskevat vaatimukset - jakelua ja toimittamistapaa koskevat vaatimukset - ajankohtaa koskevat vaatimukset Informointi on toteutettava tietojen keruun yhteydessä tai kohtuullisen ajan (viimeistään kuukauden) kuluessa henkilötietojen saamisesta, jos tietoja ei ole saatu rekisteröidyltä. Informointi on toteutettava viimeistään, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran tai kun tietoja luovutetaan ensimmäisen kerran tilanteissa, joissa tietoja saadaan muualta kuin rekisteröidyltä itseltään ja niitä käytetään viestintään rekisteröidyn kanssa tai niitä on tarkoitus luovuttaa toiselle vastaanottajalle.
Toteutusesimerkki	Sähköisesti tehtävän tiedonkeruun yhteydessä informointi voidaan hoitaa esimerkiksi tietosuojaselosteella, johon on suora linkki lomakkeelta, jolla tietoja kerätään. Tietosuojaselosteesta kerrotaan näkyvillä ilmoituksilla. Mikäli tietojen keruu tapahtuu rekisteröidyn ollessa fyysisesti läsnä, voidaan informointi tehdä kirjallisesti tai pyydettäessä myös suullisesti. Olennaista on, että rekisteröity saa helposti henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja selkeässä muodossa.
Lainsäädäntö	679/2016 Art 5, 13-14
Tunniste	**TSU-19.3, L:, E:, S:, TS:Henkilötieto**
Nimi	**Rekisteröidyn oikeudet - Oikeus saada pääsy tietoihin**
Vaatimus	Organisaatio toimittaa pyynnöstä rekisteröidylle jäljennöksen käsiteltävistä henkilötiedoista sekä informaatiota henkilötietojen käsittelystä.

Yleiskuvaus	Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin sekä henkilötietojen käsittelyä koskevat tiedot kuten esimerkiksi käsittelyn tarkoitukset, henkilötietoryhmät, vastaanottajat ja säilytysajat. Jos henkilötietoja siirretään kolmanteen maahan tai kansainväliselle järjestölle, rekisteröidyllä on oikeus saada ilmoitus siirtoa koskevista asianmukaisista suojatoimista. Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.
Toteutusesimerkki	Organisaatio voi määritellä prosessin rekisteröityjen pyyntöjen täyttämiseen sekä sisällyttää rekisteröityjen informointiin tiedot siitä, miten pyynnöt toimitetaan rekisterinpitäjälle. Mikäli pyyntöjä on paljon, organisaation kannattaa myös suunnitella ja ohjeistaa menettelyt, joilla pyynnöt voidaan täyttää tehokkaasti.
Lainsäädäntö	679/2016 Art 15
Tunniste	**TSU-19.4, L:, E:, S:, TS:Henkilötieto**
Nimi	**Rekisteröidyn oikeudet - Tietojen oikaiseminen, poistaminen, siirtäminen, käsittelyn rajoittaminen ja vastustaminen**
Vaatimus	Organisaatio toteuttaa tietojen oikaisemiseen, poistamiseen, siirtämiseen, käsittelyn rajoittamisen ja vastustamiseen liittyvät pyynnöt.

Yleiskuvaus	Rekisteröidyllä on joukko henkilötietoihin liittyviä oikeuksia, jotka organisaation tulee toteutaa pyydettäessä kuten: Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys. Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, edellyttäen että jokin asetuksessa mainituista perusteista täyttyy. Näitä perusteita ovat esimerkiksi tietojen käyttötarpeen päättyminen tai suostumuksen peruuttaminen. Rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä tietyissä tilanteissa kuten esimerkiksi, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden. Rekisterinpitäjä on myös velvollinen ilmoittamaan edellä mainituista toimenpiteistä jokaiselle henkilötietojen vastaanottajalle. Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle jos käsittely perustuu suostumukseen tai sopimukseen. Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu yleiseen etuun, julkisen vallan käyttämiseen tai oikeutettuun etuun. Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten, mukaan lukien profilointia silloin kun se liittyy tällaiseen suoramarkkinointiin.
Toteutusesimerkki	Oikeuksien käyttämiseen liittyvät yksityiskohtaiset prosessit voi suunnitella ottaen huomioon pyyntöjen määrän sekä tietosuoja-asetuksessa määritellyt eri oikeuksiin liittyvät yksityiskohdat. Jos pyyntöja on paljon, prosessit kannattaa suunnitella ja ohjeistaa huolella. Muussa tapauksessa riittää, että organisaatio varmistaa kyvykkyyden tarvittaessa toteuttaa rekisteröityjen pyynnöt ja että sillä on riittävä tuntemus tietosuoja-asetuksessa esitetyistä yksityiskohtaisista pyyntöjen toteuttamiseen liittyvistä vaatimuksista.
Lainsäädäntö	679/2016 Art 16-21
Tunniste	**TSU-20, L:, E:, S:, TS:Henkilötieto**
Nimi	**Automatisoidut yksittäispäätökset**
Vaatimus	Organisaatio tunnistaa tilanteet, joissa henkilötietojen käsittelyyn sisältyy automaattista päätöksentekoa sekä varmistaa että automaattista päätöksentekoa ei tehdä muutoin kuin tietosuoja-asetuksessa erikseen sallituissa tapauksissa.

Yleiskuvaus	Organisaatio ei saa tehdä rekisteröityjä koskevia päätöksiä, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Automaattinen päätöksenteko (ml. profilointi) on sallittua, jos päätös - on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten - on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä - perustuu rekisteröidyn nimenomaiseen suostumukseen. Profilointi tarkoittaa henkilötietojen automaattista käsittelyä, jossa arvioidaan ihmisen henkilökohtaisia ominaisuuksia. Profiloinnilla tarkoitetaan erityisesti työsuoritukseen, taloudellisen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin liittyvien piirteiden analysointia tai ennakointia. Profilointi - on automaattista tai osittain automaattista - kohdistuu henkilötietoihin ja - arvioi henkilökohtaisia ominaisuuksia. Päätöksenteko on automaattista, kun - on kyse pelkästään automaattiseen henkilötietojen käsittelyyn perustuvasta päätöksenteosta ja - tehtävillä päätöksillä on oikeusvaikutuksia tai tällaiset päätökset muuten vaikuttavat rekisteröityyn merkittävästi.
Toteutusesimerkki	Mikäli organisaatio tekee automaattista päätöksentekoa tai profilointia, organisaatio voi käsittelyn aloittamisen yhteydessä sekä määräajoin varmistaa suhteessa tietosuoja-asetuksessa esitettyihin yksityiskohtaisiin vaatimuksiin, että automaattiseen päätöksentekoon ja profilointiin liittyvät vaatimukset täyttyvät. Organisaatio on huolehdittava automaattiseen päätöksenteon yhteydessä (ml. profilinti) vähintään seuraavista suojatoimenpiteistä: - rekisteröidyille kerrotaan tietojen käsittelystä - rekisteröidyille tarjotaan yksinkertaisia tapoja vaatia ihmisen osallistumista tietojen käsittelemiseen, esittää oma kantansa ja riitauttaa päätös - käsiteltävät tiedot ja algoritmit tarkistetaan säännöllisesti, jotta voidaan varmistaa, että päätöksentekoprosessi toimii kuten tarkoitettu, eikä johda esimerkiksi yksilöitä syrjivään tietojen käsittelyyn. - henkilötietojen käsittelystä on tehty vaikutusten arviointi
Lainsäädäntö	679/2016 Art 22
Tunniste	**TSU-21, L:, E:, S:, TS:Henkilötieto**
Nimi	**Seloste käsittelytoimista**
Vaatimus	Organisaatio laatii kirjallisen kuvauksen organisaation suorittamista henkilötietojen käsittelytoimista.

Yleiskuvaus	Seloste käsittelytoimista on tehtävä, jos organisaatiossa on yli 250 työntekijää ja sen on katettava kaikki käsittelytoimet. Seloste käsittelytoimista on tehtävä työntekijöiden määrästä riippumatta, kun - henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille tai - henkilötietojen käsittely ei ole satunnaista tai - käsiteltävät henkilötiedot sisältävät erityisiä tietoryhmiä tai rikostuomioihin ja rikoksiin liittyviä henkilötietoja. Tällöin selosteeseen on sisällytettävä vain niihin liittyvät käsittelytoimet.
Toteutusesimerkki	Rekisterinpitäjä ja henkilötietojen käsittelijä voivat laatia selosteet käsittelytoimista esimerkiksi hyödyntämällä tietosuojavaltuutetun sivuilta löytyviä ohjeita ja mallipohjia.
Lainsäädäntö	679/2016 Art 30