Hallitus 15.5.2025
LIITE 2

Henkilötietojen käsittely REDUssa:

Tietosuojaperiaatteet ja tietosuojan yleisohjeet

4.4.2025
luonnos versioksi 4

luonnos versioksi 4

REDUn tietosuojaperiaatteet ja tietosuojan yleisohjeet

Sisällysluettelo

Päivitys- ja hyväksymismerkinnät

Versio	Päivä-määrä	Hyväksytty
3	1.3.2023	Hyväksytty yhtymähallituksen kokouksessa 23.2.2023 (§ 5). Voimaan 1.3.2023 alkaen, kumoaa 5.6.2019 hyväksytyn aiemman version.
3.1	19.3.2024	Korjattu teknisenä korjauksena *Tietosuoja- ja tiedonhallinnan työryhmän* nimi *Tietosuojaryhmäksi* kohdissa: 1.2, 2.9, 3.1.1, 3.1.5, 3.2.2, 3.3, 3.8.1 ja 3.8.2. Kuntayhtymän johtajan päätös tietosuojaryhmästä B6/2024.
luonnos versioksi 4	4.4.2025	Konsernijohtoryhmä 2025/04 (29.4.2025), yhtymähallitus 15.5.2025 Tarkennettu kohtaan 1.2 yhtymähallituksen toimivaltaa antaa myös tytäryhtiöitä koskevia periaatteita ja ohjeita sekä yhtiön toimitusjohtajan antamaan lisäohjeita. Muutettu kohtiin 3.1.1, 3.1.4 ja 3.1.5 uudistuneet tietoturva- ja tietosuojakoulutusvaatimukset, niistä päättäminen sekä koulutusten seurantajärjestelmä.

luonnos versioksi 4

1 Johdanto

1.1 Yleistä

Tämä asiakirja sisältää rekisterinpitäjän eli Rovaniemen koulutuskuntayhtymä REDU -konsernin henkilötietojen käsittelyssä ja rekisterinpitäjän tehtävien hoitamisessa noudatettavat tietosuojaperiaatteet ja tietosuojan yleisohjeet.

Asiakirjassa käytetään tietosuojalainsäädännön yleisiä käsitteitä sekä REDUssa vakiintuneita käsitteitä, nämä on tarkemmin avattu liitteessä 1.

1.2 Soveltamisala ja hyväksyntä

REDUn tietosuojaperiaatteita ja tietosuojan yleisohjeita sovelletaan Rovaniemen koulutuskuntayhtymässä (REDU) ja sen tulosalueilla ja kuntayhtymän määräysvallassa olevissa tytäryhteisöissä (tytäryhtiöt), joiden rekisterinpitäjänä REDU-konserni toimii REDUn konserniohjeen (15.6.2021) kohdan 16 mukaisesti. REDUn tulosalueita ovat Lapin koulutuskeskus REDU, Santasport Lapin Urheiluopisto ja REDUn sisäiset palvelut ja tytäryhtiöitä ovat REDU Edu Oy ja Santasport Finland Oy (1.1.2022 tilanne).

Tämän yleisohjeen valmistelusta vastaa REDUn tietosuojavastaava yhdessä REDUn tietosuojaryhmän kanssa.

REDUn tietosuojaperiaatteiden ja yleisohjeiden hyväksynnästä vastaa REDUn yhtymähallitus, joka voi samalla päättää tytäryhtiöitä koskevien periaatteiden ja ohjeiden antamisesta REDUn konserniohjeen kohdan 7 mukaisesti.

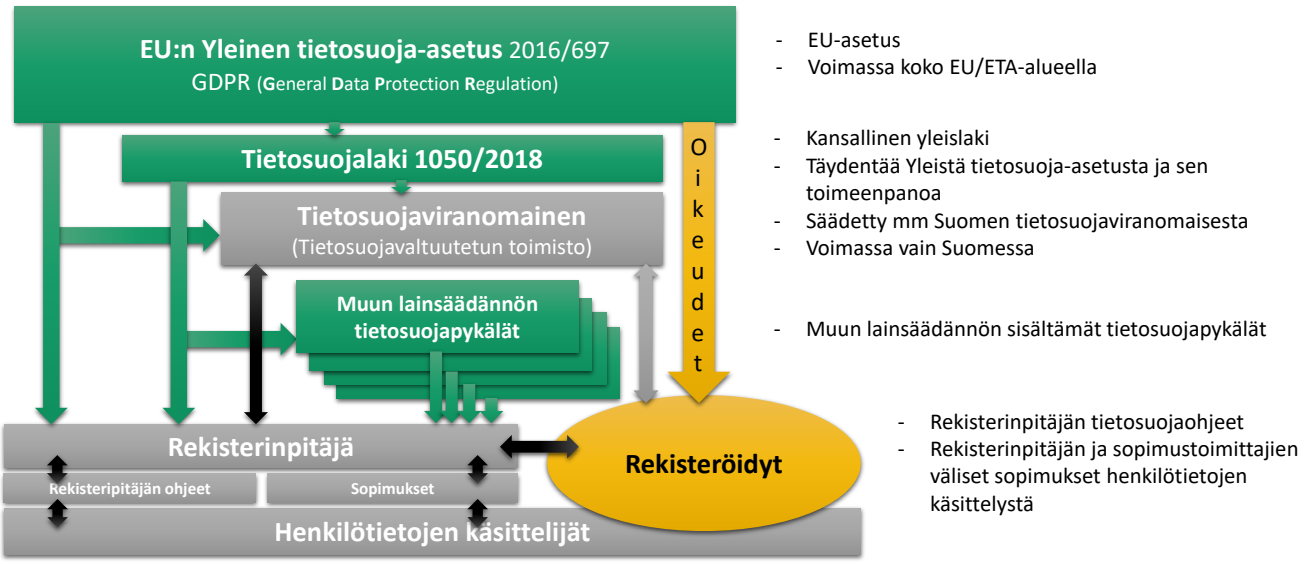
Kuntayhtymän johtaja, talouspäällikkö, henkilöstöpäällikkö, kiinteistöpäällikkö ja tulosalueen johtaja sekä tytäryhtiön toimitusjohtaja voivat antaa vastuualueensa henkilöstölle tätä tietosuojan yleisohjetta tarkentavia toiminta- ja menettelyohjeita. Lisäksi tulosaluejohtaja voi edelleen siirtää tätä toimivaltaa ja antaa toiminta- ja menettelyohjeita nimeämälleen henkilölle esim. toimialapäällikölle. (REDUn hallintosääntö 15.6.2021, 13 § kohta 18, 15 § kohta 10, 16 § kohta 15, 17 § kohta 16 ja 18 a § kohta 13).

1.3 Tietosuojalainsäädäntö

Lyhyesti:

- Henkilötietojen käsittelyä säätävä lainsäädäntö muodostuu Euroopan Unionin yleisestä tietosuoja-asetuksesta (GDPR) ja kansallisesta henkilötietojen käsittelyä koskevasta lainsäädännöstä.
- EU:n tietosuoja-asetus on voimassa suoraan kaikissa EU:n jäsenvaltioissa sekä ETA-alueella.
- Kansallisella lainsäädännöllä täydennetään EU:n tietosuoja-asetusta ja sen toimeenpanoa Suomessa.
- Tietosuojavaltuutetun toimisto on Suomen tietosuojaviranomainen.
- Tietosuojavaltuutetun toimisto valvoo henkilötietojen käsittelyä Suomessa.
- Lainsäädännön lähtökohtana rekisteröidyn oikeudet omiin henkilötietoihin ja niiden vapaa liikkuvuus EU/ETA-alueen sisällä.

Henkilötietojen käsittelyn tietosuojasta on säädetty EU-asetuksella ja sitä täydentävällä kansallisella lainsäädännöllä. Kansallista lainsäädäntöä ovat mm. Tietosuojalaki sekä muussa lainsäädännössä henkilötietojen käsittelystä ja tietosuojasta säädetyt pykälät. Tietosuojalainsäädäntö lähtee rekisteröityjen oikeuksista ja rekisterinpitäjien ja henkilötietojen käsittelijöiden velvollisuuksista. Tietosuojalainsäädännön toteuttamista ja toimeenpanoa kansallisesti valvoo kansallinen tietosuojaviranomainen eli Suomessa Tietosuojavaltuutetun toimisto.



KUVA 1. Tietosuojalainsäädäntö, ohjeistus ja sopimukset ja sekä niiden oikeudet ja velvoitteet

Rekisterinpitäjää ja kaikkia henkilötietojen käsittelijöitä velvoittaa EU:n yleinen tietosuoja-asetus, sen perusteella annettu kansallinen tietosuojalaki sekä muun lainsäädännön tietosuojasta säädetyt pykälät. Henkilötietojen käsittelijät toimivat aina rekisterinpitäjän lukuun oli sitten kyse henkilökunnan toimesta tapahtuvasta henkilötietojen käsittelystä tai ulkoistetuista henkilötietojen käsittelystä. Henkilötietojen käsittelijöitä velvoittaa näiden lisäksi rekisterinpitäjän antama ohjeistus ja rekisterinpitäjän ja sopimustoimittajan kanssa tehdyt sopimukset.

Rekisteröidyn oikeuksista on säädetty suoraan tietosuoja-asetuksessa ja niistä vastaa rekisteröidylle rekisterinpitäjä. Tarvittaessa rekisteröity voi olla yhteydessä tietosuojaviranomaiseen, mikäli rekisteröity on tyytymätön rekisterinpitäjältä saamansa vastaukseen tai jos rekisterinpitäjä ei ole vastannut rekisteröidyn yhteydenottoon esim. oikeuksien käyttöpyyntöön säädetyssä ajassa.

Tietosuojalainsäädäntö:

- **EU:n Yleinen tietosuoja-asetus** (**G**eneral **D**ata **P**rotection **R**egulation eli **GDPR**)
  Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta Euroopan Unionin (EU) sisällä on säädetty Euroopan parlamentin ja neuvoston asetuksella 2016/697. Tämä yleinen tietosuoja-asetus (jatkossa lyh. Tietosuoja-asetus) on EU-asetuksena sellaisenaan ollut voimassa kaikissa EU:n jäsenvaltioissa 25.5.2018 alkaen.

  EU Tietosuoja-asetus (suomenkielinen selattava versio), sis. muutokset:
  https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

- **Tietosuojalaki**
  Kansallinen Tietosuojalaki 1050/2018 täydentää em. EU:n tietosuoja-asetusta. Tietosuojalakia sovelletaan rinnan EU:n Tietosuoja-asetuksen kanssa. Tietosuojalaissa säädetään mm. kansallisesta Tietosuojaviranomaisesta (Tietosuojavaltuutetun toimisto) sekä eräistä henkilötietojen käsittelyyn liittyvistä erityistilanteista, kuten sananvapaudesta ja henkilötietojen suojan yhteensovittamisesta.

  Tietosuojalaki 1050/2018, sis. muutokset:
  https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

- **Muu lainsäädäntö**
  Varsinaisen tietosuojalainsäädännön lisäksi henkilötietojen käsittelyn tietosuojasta ja rekisterinpitäjän oikeudesta käsitellä henkilötietoja on säädetty muussa lainsäädännössä.

  REDUn toimintaa ohjaavaa lainsäädäntöä, jossa on myös säädetty tietosuojasta, ovat mm:
  - Laki ammatillisesta koulutuksesta 531/2017
  - Laki vapaasta sivistystyöstä 632/1998
  - Oppivelvollisuuslaki 1214/2020
  - Kuntalaki 410/2015
  - Osakeyhtiölaki 624/2006
  - Työsopimuslaki 55/2001
  - Laki kunnan ja hyvinvointialueen viranhaltijasta 304/2003
  - Laki yksityisyyden suojasta työelämässä
  - Rikoslaki 39/1889.

1.4 LUC yhteistyö

Rovaniemen koulutuskuntayhtymä on mukana Lapin korkeakoulukonsernissa (LUC), jossa REDU yhdessä Lapin yliopiston ja Lapin AMK:n kanssa tuottaa LUC-osapuolille mm. yhteisiä tietohallinnon palveluja ja ICT-palveluja. LUC-konsernin organisaatiot ovat jokainen oma rekisterinpitäjänsä ja vastaavat kukin osaltaan tietosuojastaan. LUC:n yhdessä tuottamissa palveluissa käsitellään henkilötietoja ristiin yli organisaatiorajojen. Lapin yliopisto ja Lapin AMK käsittelevät REDUn lukuun henkilötietoja ja REDU toimii Lapin yliopiston ja Lapin AMK:n henkilötietojen käsittelijänä. Lisäksi käytössä on yhteisiä tietojärjestelmiä ja henkilörekistereitä (yhteisrekisterejä). Näistä LUC:n yhdessä toteuttamien palvelujen ja yhteisrekisterien tietosuojasta ja osapuolten vastuista on sovittu osapuolten kesken LUC-tietosuojasopimuksella.

2 REDUn tietosuojaperiaatteet

2.1 Yleistä

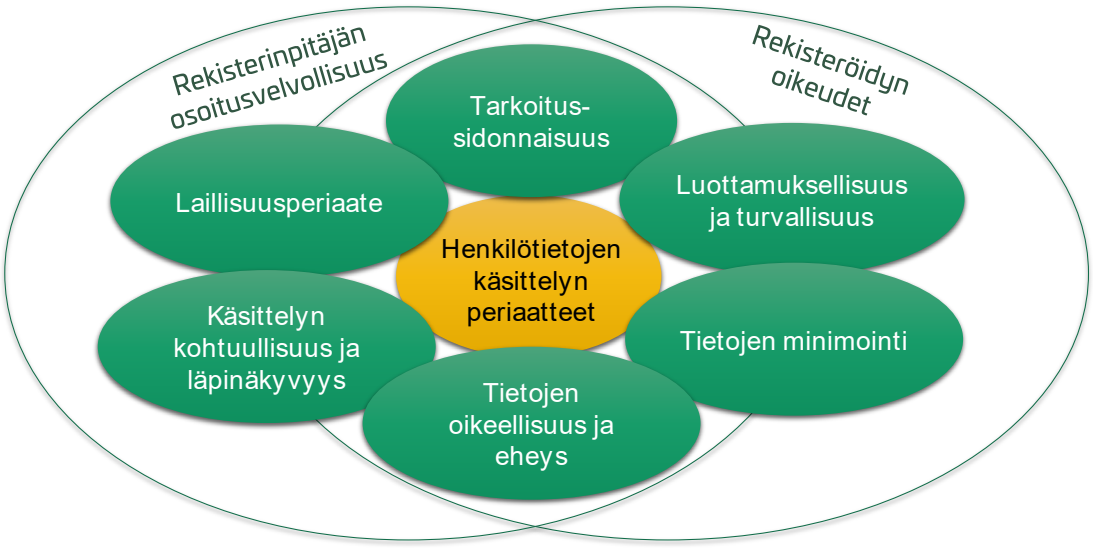
Henkilötietojen käsittely on Rovaniemen koulutuskuntayhtymän (REDU) perustehtävän mukaista toimintaa, jota ohjaavat REDUn arvot.

REDUlaisen arvolupaus:

- ***Olemme yhdessä tekeviä***
  REDUlaisina olemme yhteisöllisiä – yhdessä tekeviä ja vuorovaikutteisia. Näin edistämme luottamuksen ja kehittävän ilmapiirin syntymistä niin REDU:n sisällä, kuin asiakkaitten, kumppaneidemme ja muiden sidosryhmiemme kanssa. Kunnioitamme toistemme erilaisuutta ja kohtelemme toisiamme yhdenvertaisesti.
- ***Olemme vastuullisia***
  REDUlaisina meillä on vastuu toiminta-alueemme Lapin ammatillisen osaamisen kehittymisestä. Edistämme toiminnallamme Lapin elinvoimaa ja kestävää kehittymistä. Olemme toisillemme, asiakkaillemme, kumppaneille luotettavia ja vastuullisia.
- ***Olemme asiakaslähtöisiä***
  REDUna olemme asiakkaitamme eli työelämää ja opiskelijoita varten. Olemme kiinnostuneita heidän osaamisen kehittämisen tarpeista ja yhdessä heidän kanssaan löydämme heille parhaiten sopivat osaamisen kehittämisen ratkaisut. Kunnioitamme asiakkaidemme erilaisuutta ja kohtelemme heitä kunnioittavasti ja yhdenvertaisesti.

REDUn asiakkaat, henkilökunta ja osin vierailijat ovat rekisteröityjä, joiden henkilötietoja REDU rekisterinpitäjänä käsittelee.

Kaaviokuvassa (kuva 2) on esitetty henkilötietojen käsittelyn periaatteet REDUssa.



KUVA 2. Henkilötietojen käsittelyn periaatteet

REDUn henkilötietojen käsittelyn periaatteet perustuvat EU:n tietosuoja-asetuksen II luvun periaatteisiin (5–11 artiklat) sekä Tietosuojavaltuutetun toimiston verkkosivustolla esittämiin tietosuojaperiaatteisiin (Tietosuojavaltuutetun toimisto, Tietosuojaperiaatteet).

Henkilötietojen käsittelyn periaatteet REDUssa:
- käyttötarkoitussidonnaisuus.
- laillisuusperiaate.
- luottamuksellisuus ja turvallisuus.
- käsittelyn kohtuullisuus ja läpinäkyvyys.
- käsiteltävien tietojen minimointi ja
- tietojen oikeellisuus ja eheys.

Näiden lisäksi Tietosuoja-asetus velvoittaa rekisterinpitäjää (REDU) osoittamaan, että se noudattaa tietosuojavelvoitteitaan ja antaa rekisteröidylle oikeuksia koskien hänen omia henkilötietoja. Seuraavissa kappaleissa on kuvattu tarkemmin henkilötietojen käsittelyn periaatteet, rekisteripitäjän osoitusvelvollisuus ja rekisteröidyn oikeudet.

2.2 Käyttötarkoitussidonnaisuus

Lyhyesti:
- Käyttötarkoitussidonnaisuudesta on säädetty EU:n tietosuoja-asetuksen 5 artiklassa.
- Henkilötietojen käsittelylle on aina määritelty käyttötarkoitus.
- Käyttötarkoitus perustuu REDUssa perustehtävään ja sitä tukevaan toimintaan.
- Käyttötarkoitus on sitova. Siitä voidaan poiketa vain rekisteröidyn erikseen antamalla suostumuksella tai lainsäädännön erikseen säätämällä perusteella.
- Suoramarkkinointiin on saatava aina erillinen lupa (suostumus) rekisteröidyltä!

Henkilötietojen käsittelyn tarkoitus on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa myöhemmin käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla. (Tietosuojavaltuutetun toimisto, Käyttötarkoitussidonnaisuus.)

Kaikille REDUn henkilötietojen käsittelytoiminoilla on nimetty käyttötarkoitus (EU Tietosuoja-asetus, 5 artikla 1b). REDUssa tämän käyttötarkoituksen tulee perustua REDUn perustehtävään tai siihen liittyvään tai tukevaan toimintaan. Esim. käyttötarkoituksesta on koulutustoiminnan (perustehtävä) hakeutumisen, opiskelijatietojen sekä neuvonta- ja ohjauspalvelun henkilötietojen käsittely, henkilökunnan palvelussuhdetietojen käsittely (tukitoiminto/hallinto), yhtiön tuottaman palvelun tilaaminen/varaaminen ja tuottaminen (perustehtävä).

Käyttötarkoitussidonnaisuus tarkoittaa, että tämä määritelty käyttötarkoitus sitoo henkilötietojen käsittelyä ml. käsittelyssä käytettävien henkilörekisterien tietojen käyttämistä. Henkilötietojen käyttäminen muuhun käyttötarkoitukseen on lähtökohtaisesti kielletty, ellei lainsäädännössä ole säädetty poikkeusta. (EU Tietosuoja-asetus, 5 artikla 1b.) Alkuperäisestä käyttötarkoituksesta voidaan poiketa myös, kun siitä pyydetään rekisteröidyltä erillinen suostumus tai kun käsittely on tarpeen henkilön elintärkeiden etujen suojaamiseksi. Käyttötarkoitussidonnaisuus koskee myös ulkoistettua henkilötietojen käsittelyä. Palvelutuottaja saa käsitellä henkilötietoja kuin vain siten, kun palvelun sopimuksessa on sovittu.

Suoramarkkinointi
Suoramarkkinointi on aina oma erillinen käyttötarkoituksensa. Suoramarkkinoinnilla tarkoitetaan rekisteröidylle suoraan henkilön nimellä tai muulla tunnisteella esim. henkilökohtaiseen sähköpostiosoitteeseen, puhelinnumeroon puheluna tai tekstiviestinä, pikaviestinä tai postitse koti- tai työosoitteeseen lähetettyjä sähköisiä ja painettuja/tulostettuja markkinointiviestejä-, uutiskirjeitä, kirjeitä, esitteitä yms. Suoramarkkinoinnilla ei tarkoiteta koulutuksen/palvelun yhteydessä/palvelun tai tuottamisen aikana osana kyseistä palvelua (käyttötarkoitusta) tai palvelun jälkeen esim. kiitos- tai palautekyselyn yhteydessä kertaluonteisesti rekisteröidylle eli opiskelijalle tai asiakkaalle annettua tietoa muista REDUn tai tytäryhtiön tarjoamista palveluista, jotka liittyvät tarjottuun palveluun tai palveluryhmään.

Tietosuoja-asetuksen mukaisesti suoramarkkinointia voidaan toteuttaa lähtökohtaisesti vain rekisteröidyn antamalla suoramarkkinointisuostumuksella (oikeusperuste voi olla vain suostumus). Suoramarkkinointia ja siihen liittyvää suostumusta ei saa kytkeä toiseen käyttötarkoitukseen. Esim. tuote tai palvelu on oltava mahdollista hankkia ilman, että antaa suostumusta suoramarkkinointiin.

Suostumuksen suoramarkkinointiin on oltava aina vapaaehtoinen ja aktiivinen rekisteröidyn tahdonilmaisu. Sitä ei saa sisällyttää tai ”piilottaa” esim. myytävän palvelun sopimus- tai toimitusehtoihin. Suoramarkkinointiin suostumus on pyydettävä aina erikseen. Kiellettyä on sisällyttää suoramarkkinointia osaksi tuotteen tai palvelun tilausta tai myyntiä esim.: *”hyväksymällä toimitusehdot annat luvan suoramarkkinointiin”*. Suoramarkkinoinnin suostumus ei saa myöskään olla valmiiksi valittuna ruksina lomakkeella, jolla kysytään henkilötietoja.

2.3 Laillisuusperiaate

Lyhyesti:
- Henkilötietojen käsittelylle täytyy olla laillinen käsittelyperuste eli oikeusperuste.
- Laillisuusperusteet on säädetty Tietosuoja-asetuksen 6 artiklassa.

Henkilötietojen käsittelyn on oltava lainmukaista ja sille on oltava sopiva käsittelyperuste. Näistä laillisuusperiaatteen mukaisista käsittelyperusteista käytetään myös käsitettä oikeusperuste. (Tietosuojavaltuutetun toimisto, Lainmukaisuus, asianmukaisuus ja läpinäkyvyys). Käsittelyperusteista on säädetty EU:n tietosuoja-asetuksen 6 artiklassa. Näitä käsittelyperusteita ovat:

- **Rekisterinpitäjän lakisääteiseen velvoitteeseen** eli käsittelystä on säädetty lainsäädännössä (EU Tietosuoja-asetus, 6 artikla kohta 1c). Esim. ammatillisen koulutuksen opiskelijoiden henkilötietojen käsittelystä on säädetty ammatillisen koulutuksen lainsäädännössä ja henkilökuntaa koskevista mm. työlainsäädännössä.

- **Käsittely perustuu rekisterinpitäjän ja rekisteröidyn väliseen sopimukseen** (EU Tietosuoja-asetus, 6 artikla kohta 1b). Esim. asiakkaan ja REDUn välillä on kirjallinen tai suullinen sopimus, jossa asiakas hankkii (ostaa tai tilaa) REDUlta tietyn palvelun tai tuotteen ja henkilötietoja käsitellään vain tämän palvelun tuottamiseen tai tavaran toimittamiseen. Sopimus voidaan katsoa syntyneen myös ns. hiljaisena sopimuksena, kun rekisteröity aloittaa hankkimansa palvelun tai tuotteen käyttämisen tai vastaanottamisen esim. osallistuu järjestettyyn tilaisuuteen tai koulutukseen.

- **Yleistä etua koskeva tehtävä tai julkinen valta.**
  Henkilötietoja saa käsitellä, kun yleinen etu tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sitä edellyttää. Tämä voi toimia tilanteissa, joissa on kysymys Euroopan unionin tai Suomen valtion yleisestä edusta tai julkisesta vallasta. (EU Tietosuoja-asetus, 6 artikla kohta 1e.)

  Yleistä etua koskeva tehtävä tai julkinen valta on täytynyt antaa lailla tai muilla oikeudellisilla säännöksillä. Yleisen edun mukaista käsittelyä voi esimerkiksi olla henkilötietojen käsittely tieteellisen tai historiallisen tutkimuksen tai tilastoinnin tarkoituksia tai journalistista käyttötarkoitusta varten**.**

- **Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.**
  Henkilötietojen käsittely on sallittua silloin, kun se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi (EU Tietosuoja-asetus, 6 artikla kohta 1f). Se, milloin etu voidaan katsoa oikeutetuksi, saadaan selville niin kutsutulla tasapainotestillä. Siinä rekisterinpitäjän tai kolmannen osapuolen intressiä punnitaan rekisteröidyn intressejä ja perusoikeuksia vasten.

  Oikeutettu etu voi olla olemassa esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on jokin merkityksellinen suhde. Se tarkoittaa, että rekisteröity on esimerkiksi rekisterinpitäjän asiakas, opiskelija tai henkilökuntaa. Huom! Oikeutettu etu ei tule kyseeseen oikeusperusteena silloin, kun kyse on viranomaistehtävän hoitamisesta (EU Tietosuoja-asetus, 6 artikla 1. kohta).

- **Elintärkeiden etujen suojaaminen.**
  Henkilötietojen käsittely on sallittua, kun se on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi. Elintärkeiden etujen suojaaminen sopii käsittelyperusteeksi esimerkiksi tilanteisiin, joissa on kysymys elämästä ja kuolemasta tai uhkista, jotka voisivat johtaa rekisteröidyn tai jonkun toisen loukkaantumiseen tai olla muutoin terveydelle vahingollisia.

  Henkilötietojen käsittely voi palvella elintärkeää etua esimerkiksi humanitaarisissa hätätilanteissa, kuten luonnonkatastrofeissa tai epidemioissa. Henkilötietojen käsittelyä voidaan tarvita muun muassa silloin, kun halutaan seurata tai estää epidemian leviämistä.

- **Rekisteröidyn suostumus.** Rekisteröity voi antaa suostumuksensa sille, että hänen henkilötietojaan käsitellään yhtä tai useampaa käyttötarkoitusta varten. Suostumusta käytetään oikeusperusteena, kuin mikään muu edellä esitetyistä oikeusperusteita ei tule kyseeseen.

  - Suostumus on oltava aina peruutettavissa, joten suostumusta ei tule käyttää sellaisissa käsittelytarkoituksissa, joissa peruminen on käytännössä mahdotonta.
  - Suostumuksen on oltava aina vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Suostumusta ei saa sisällyttää/piilottaa muuten hyväksyttäviin sopimusehtoihin.
  - Suostumukselle tulee olla henkilötietoja keräävällä lomakkeella oma erillinen rastitettava kohtansa, jossa lukee yksiselitteisesti mihin kyseinen suostumus annettaan. Jos käytetään paperilla täytettävää lomaketta, lomakkeella tulee tarjota rastitettava kohta, jossa voi myös kieltää antamasta suostumuksen. Näin jälkikäteen ei voi lomakkeelle lisätä suostumusrastia.
  - Suostumus on voitava peruuttaa yhtä helposti kuin sen on voinut antaa. Rekisteröityä on informoitava suostumuksen antamisen yhteydessä, miten suostumuksen

voi myöhemmin perua. Tämä voidaan toteuttaa esim. linkittämällä suostumuskohtaan tietosuojaseloste, jossa on kerrottu, miten suostumus voidaan perua tai kertomalla asia suoraan lomakkeessa.

- Annettu suostumus on pystyttävä aina osoittamaan eli suostumuksen sisältävä asiakirja tai tieto suostumuksesta on tallennettava ja säilytettävä vähintään niin kauan, kuin kyseisiä henkilötietoja käsitellään.
- Mikäli rekisteröity peruu suostumuksen, henkilötietojen käsittely on lopetettava ja henkilön tiedot poistettava. Suostumuksen peruminen on myös välitettävä kaikkiin niihin käsittelytoimintoihin ja henkilötietojen käsittelijöille, joissa käsittely perustuu peruttuun suostumukseen. Tämä koskee myös ns. alihankintana tapahtuvaa henkilötietojen käsittelyä.

Suostumuksen edellytyksistä on säädetty EU Tietosuoja-asetuksen 7 artiklassa.

Lisätietoa käsittelyperusteista Tietosuojavaltuutetun toimiston verkkosivulla Henkilötietojen käsittelyperusteet: https://tietosuoja.fi/kasittelyperusteet ja rekisteröidyn suostumuksesta https://tietosuoja.fi/rekisteroidyn-suostumus.

2.4 Luottamuksellisuus ja turvallisuus

Lyhyesti:
- Rekisteröidyt luottavat REDUun henkilötietojen käsittelijänä.
- Henkilötietoja käsittelevää REDUn henkilökuntaa, luottamushenkilöitä sekä sopimustoimittajia, sitoo ehdoton vaitiolovelvollisuus.
- Tietoja voidaan luovuttaa kolmannelle osapuolelle vain lainsäädännössä säädetyllä perusteella.
- Henkilötietoja tulee käsitellä huolellisesti ja siten, että sivulliset eivät näe tai kuule niitä missään käsittelyn vaiheessa.

Henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista (Tietosuojavaltuutetun toimisto, Luottamuksellisuus ja turvallisuus).

Luottamuksellisuus
Rekisteröidyt eli opiskelijamme, asiakkaamme, vierailijat ja henkilökunnan jäsenenä luotamme siihen, että REDU käsittelee henkilötietojamme luottamuksellisesti ja tietoturvallisesti. Ja että henkilötietojamme käytetään vain siihen käyttötarkoitukseen, kuin olemme tietoja antaneet tai mitkä liittyvät hankkimanne koulutukseen tai palveluun tai palvelussuhteeseemme. Tätä luottamuksellista suhdetta ei tule missään vaiheessa rikkoa.

REDUn henkilökuntaa ml. johto ja luottamushenkilöt sitoo ehdoton vaitiolo työ-, virka- tai luottamustehtävissään saamiensa toisten henkilöiden (rekisteröityjen) henkilötietojen osalta, oli sitten kyse opiskelijoiden, asiakkaiden, vieraiden, henkilökunnan tai toisten luottamushenkilöiden henkilötiedoista. Ehdottomalla vaitiololla tarkoitetaan sitä, että rekisteröidyn tietoja ei saa millään tavalla ilmaista tai luovuttaa sivulliselle tai hyödyntää muulla käyttötarkoitukseen kuulumattomalla tavalla. Vaitiolo koskee myös niitä rekisteröityjen henkilötietoja, joita on mahdollisesti saanut tietoonsa ja jotka eivät suoraan liity oman työ-, virka- tai luottamustehtävän hoitamiseen. Silloin kun REDU käyttää rekisteröityjen henkilötietojen käsittelyyn sopimustoimittajia (alihankkijoita), heitä koskee myös em. tietojen luottamuksellisuus ja salassapito. Palvelun hankintasopimuksessa on sovittava henkilötietojen luottamuksellisuudesta ja salassapidosta.

Tietoja voimme luovuttaa kolmannelle osapuolelle vain silloin, kun luovuttamiselle on olemassa lakisääteinen peruste tai jos siihen saadaan rekisteröidyltä erikseen suostumus. Esim. alaikäisen opiskelijan tietoja voidaan lakisääteisellä perusteella luovuttaa huoltajalle. Myös toimivaltaiselle viranomaiselle, esim. poliisille, oikeuslaitokselle, tietosuojaviranomaiselle yms. luovutetaan rekisteröidyn tietoja lakisääteiseen tietopyyntöön perustuen. luovuttaessa on varmistettava, että tiedot siirtyvät tietoturvallisesti vastaanottajalle ja että tiedot ovat siirtyneet. Henkilötietojen vastaanottaja vastaa luovutuksessa saamiensa henkilötietojen käsittelystä ja käsittelyn tietosuojasta ja tietoturvasta henkilötietojen vastaanottamisen jälkeen.

Henkilötietojen käsittely tulee tehdä huolellisesti ja käsittelytilanteet ja tietojärjestelmien tietoturva tulee toteuttaa siten, että sivulliset eivät missään vaiheessa pääse näkemään, kuulemaan tai millään muulla tavalla pääse toisten rekisteröidyn henkilötietoihin. Esim. henkilön tiedoista ei saa keskustella siten, että sivulliset kuulevat keskustelun eikä henkilötietoja sisältäviä asiakirjoja säilytetä, siirretä, lähetetä tai hävitetä siten, että sivullisten on mahdollista nähdä ne.

Turvallisuus
Henkilötietojen käsittelyn turvallisuus muodostuu käsittelyn tietosuojasta ja tietoturvasta. Tietosuoja ja tietoturvat eivät ole sama asia. Sanoina ne ovat lähellä toisiaan ja siksi sekoitetaan usein. Tietoturvalla mahdollistetaan tietosuoja eli henkilötietojen suojelu.

Tietoturvalla tarkoitetaan niitä teknisiä tai manuaalisia hallinnollisia toimenpiteitä, joilla varmistetaan, että henkilötietojen käsittely ja säilyttäminen tapahtuvat siten, että niiden luottamuksellisuus säilyy ja että tiedot myös säilyvät muuttumattomina (eheinä) koko niiden säilytysajan eli mahdollistetaan henkilötietojen tietosuoja. Tietoturvaan sisältyy sekä tekninen (tieto- ja viestintätekniikkaa hyödyntävä) tietojen käsittely, tiedonsiirto ja säilyttäminen ml. manuaalinen tietojen käsittely, siirto ja säilyttäminen.

Manuaalisella henkilötietojen käsittelyllä tarkoitetaan käsin henkilötietojen käsittelijän toimesta tapahtuvaa toimintaa. Manuaalisessa käsittelyssä tieto voi siirtyä sähköisesti digitaalisessa muodossa, paperille kirjoitettuna tai tulostettuna näkyvänä tekstinä tai kuvina tai ääniviestinä esim. puheena.

Manuaalista käsittelyä ovat mm. henkilötietojen kirjaaminen, säilyttäminen ja niistä viestiminen. Manuaalisesti henkilötietoja tallennetaan mm. kynällä paperille tai sähköiseen tiedostoon tai viestiin kirjaamalla. Manuaalisesti henkilötietoja siirretään mm. keskustellen, puhelimitse, pikaviesteinä, kirjepostilla tai sähköpostilla ja säilytetään esim. paperilla mapeissa tai sähköisinä tallenteina (tiedostoina tai viesteinä).

Tietosuoja-asetuksen mukaisesti henkilötietoja on säilytettävä ja käsiteltävä tietoturvallisesti koko tiedon elinkaaren ajan, alkaen siitä, kun rekisteröidyn henkilötietoja käsitellään ja kirjataan ensimmäistä kertaa henkilörekisteriin ja loppuen siihen, kun henkilötietojen käsittely päättyy ja tiedot hävitetään pysyvästi.

REDUn on rekisterinpitäjänä arvioitava mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä henkilötietojen teknistä suojausta. Suojatoimien riittävyyttä on punnittava suhteessa olosuhteisiin ja riskeihin (Tietosuojavaltuutetun toimisto, Luottamuksellisuus ja turvallisuus.)

2.5 Käsittelyn kohtuullisuus ja läpinäkyvyys

Lyhyesti:
- Henkilötietojen käsittelyn tulee olla asianmukaista ja kohtuullista suhteessa käyttötarkoitukseen.
- Henkilötietoja käsitellään ja säilytetään vain käyttötarkoituksen vaatima aika, ellei lainsäädäntö muuta velvoita.
- Rekisteröidylle on kerrottava ymmärrettävästi ennen käsittelyä ja käsittely aikana mm. miksi ja miten tietoja käsitellään ja miten hän voi käyttää oikeuksiaan.
- Rekisteröidylle on ilmoitettava, mikäli henkilötietojen käsittelyssä tapahtuu tietoturvaloukkaus tai ilmenee muita ongelmia henkilötietojen käsittelyssä, missä rekisteröity voi omalla toiminnallaan vähentää tai estää niistä hänelle aiheutuvia riskejä, haittaa tai vahinkoa.
- Tietosuojaselosteella annamme rekisteröidylle tietoa henkilötietojen käsittelystä ja miten hän voi käyttää oikeuksiaan.
- Tietosuojaselosteen tulee olla rekisteröidyn saatavilla helposti ja siihen täytyy olla mahdollista tutustua ennen käsittelyn aloittamista.
- Tietosuoja on rekisteröidyn lakisääteinen oikeus. Tietosuojaseloste ei ole sopimus, eikä sitä siten hyväksytetä rekisteröidyllä.

Henkilötietojen käsittelyn on oltava asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen ja käsittelystä on kerrottava selkeästi ja ymmärrettävästi. (Tietosuojavaltuutetun toimisto, Lainmukaisuus, asianmukaisuus ja läpinäkyvyys).

Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen tietojen käyttötarkoitusta varten. (Tietosuojavaltuutetun toimisto, Säilytyksen rajoittaminen).

Kohtuullisuudella tarkoitetaan, että henkilötietojen käsittelyn on oltava asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen. Henkilötietoja tulee mm. käsitellä ja säilyttää vain se aika, mikä on tarpeen käsittelyssä, ellei lainsäädännöllä edellytetä pidempää säilytysaikaa tai rekisteröidyn kanssa ole muuta sovittu. Myös rekisteröidyn (henkilöiden) kanssa tehtävien sopimusten ehtojen tulee olla kohtuullisia suhteessa käyttötarkoitukseensa. Sopimuksilla ei saa myöskään sopia mistään sellaisesta, jolla vähennetään rekisteröidyn oikeuksia tai jotka muulla tavalla ovat ristiriidassa tietosuojalainsäädännön kanssa.

Henkilötietojen käsittelystä on informoitava rekisteröityä ymmärrettävällä tavalla eikä tietoja saa käsitellä tavalla, joka olisi rekisteröidyn kannalta ennalta arvaamatonta ja odottamatonta.

Informointivelvoite toteutetaan REDUssa laatimalla käsittelytoiminnosta tietosuojaseloste ennen kuin henkilötietoja aletaan käsitellä. Tietosuojaselosteen on oltava rekisteröidyn helposti saatavilla, esim. se on linkitettynä henkilötietoja keräävään sähköiseen lomakkeeseen, jolla henkilötietoja kysytään. Mikäli henkilötietojen käsittelyn aloittaminen, esim. tietojen kerääminen, tehdään suullisesti tai puhelimitse, käsittelystä on myös kerrottava suullisesti ennen tietojen kysymistä mihin käyttötarkoitukseen tietoja kysytään ja mistä voi saada lisätietoa tai löytää tietosuojaselosteen. Tällöin tiedot voi antaa suullisesti kertomalla tietosuojaselosteen sisältö ennen kuin tietoja kysytään, mikäli rekisteröity niin haluaa, tai muulla tavalla on tarjottava rekisteröidylle mahdollisuus tutustua selosteeseen ennen tietojen keräämistä.

Tietosuojaseloste ei ole koskaan sopimus. Rekisteröidyn oikeus saada tietoja käsittelystä on rekisteröidyn lakisääteinen subjektiivinen oikeus. Tämä tarkoittaa, että rekisteröidyltä ei saa pyytää tietosuojaselosteeseen minkäänlaista hyväksyntää eikä rekisteröityä saa muullakaan tavalla velvoittaa esim. lukemaan seloste. Esim. lomakkeella ei saa olla rastitettavaa kohtaa: *”Hyväksyn tietosuojaselosteen”* tai *”Olen lukenut tietosuojaselosteen ja hyväksyn sen”*. Myöskään tuotteen tai palvelun sopimusehtoihin ei saa sisällyttää em. hyväksymisiä.

Käsittelyssä tapahtuvista ongelmista kuten käsittelyn viivästyksistä, käyttökatkoista ja tietoturvaloukkauksista rekisteröityjen informointi on osa henkilötietojen käsittelyn läpinäkyvyyttä. Tietoturvaloukkauksista on informoitava rekisteröityjä aina kun rekisteröity voi omin toimin vähentää tai poistaa hänelle itselleen siitä aiheutuvaa haittaa, riskejä ja vahinkoja. Jos tietoturvaloukkaus koskee suurta joukkoa, tietoturvaloukkauksesta voidaan tiedottaa tiedotusvälineissä.

Tietoturvaloukkaustiedon saanut rekisteröity voi tiedon saatuaan käydä vaihtamassa salasanojansa eri palveluihin tai käydä sulkemassa tai rajaamassa käyttämiensä palvelujen asetuksia vähentääkseen sen vaikutuksia ja riskejä. Rekisteröity voi myös auttaa rekisterinpitäjää asian selvittämisessä ilmoittamalla tietoturvaloukkaukseen liittyvistä muista havainnoista.

2.6 Käsittelyn tietojen minimointi

Lyhyesti:
- Käsiteltävien henkilötietojen määrää tulee minimoida.
- Käsitellään vain käyttötarkoitukseen liittyviä asianmukaisia henkilötietoja.
- Jos käsittelyssä ei ole tarpeen henkilön tunnistettavuus, ei käsitellä tunnistetietoja.
- Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely on lähtökohtaisesti kielletty.
- Yksityisyyden suojan piiriin kuuluvien tietojen käsittelylle tulee olla erityinen peruste.
- Käsittelyn minimointi vähentää tietosuojariskejä.

Henkilötietoja ei saa kerätä tai käsitellä laajemmin kuin on välttämätöntä käyttötarkoituksen kannalta (Tietosuojavaltuutetun toimisto, Käsittelyn minimointi).

Käsiteltävien henkilötietojen määrän tulee olla minimoitu. Määrällä tarkoitetaan sekä rekisteröityjen että henkilötietoryhmien lukumäärää. Käsittelytoiminnossa tulee kerätä ja käsitellä vain sellaisia henkilötietoja, jotka ovat asianmukaisia ja oleellisia kyseiseen käsittelytarkoitukseen. Sellaista tietoa ei saa käsitellä ja kysyä, mitä ei tarvita käsittelyssä. Esim. tuotteen tai palvelun tilaaminen tai ostaminen ei saa edellyttää, että henkilöltä kysytään sellaisia tietoja, jotka eivät liity tilattuun tai ostettuun tuotteeseen tai palveluun. Rekisteröityä ei saa velvoittaa rekisteröitymään asiakasrekisteriin, ellei ko. tuotteen tai palvelun käyttäminen sitä edellytä (esim. pääsy/kirjautuminen palveluun). Jos asia on mahdollista hoitaa ilman, että henkilö on tunnistettavissa eli anonyymisti, niin silloin ei pidä kysyä tai kerätä henkilön tunnistetietoja. Esim. asiakaspalvelu- ja neuvontatilanteessa neuvoja ja opastusta voidaan antaa ilman, että kysytään henkilön nimi tms. tunnistetietoja.

Henkilön yksityisyyden piiriin kuluvien ml. kotiin ja vapaa-aikaan liittyvien tietojen käsittelylle pitää olla erityinen peruste. Esim. henkilön kotisosoitetietoa ei tule kysyä, ellei ole tarvetta toimittaa hänelle jotain suoraan kotiin joko tuomalla tai postitse.

Erityisiin henkilötietoryhmiin kuuluvia tietoja ei saa kysyä eikä käsitellä, ellei siihen ole lainsäädännössä säädettyä oikeutta tai siihen ei ole saatu henkilöltä erillistä suostumusta (EU Tietosuoja-asetus, 9 artikla). Tietosuoja-asetuksen 9 artiklassa on säädetty poikkeuksia, missä tapauksissa erityisiä henkilötietoryhmiä voi käsitellä ja millä edellytyksillä.

Käsittelyn minimointi vähentää tietosuojariskejä. Mitä vähemmän tietoja, sitä pienemmät vaikutukset ovat rekisteröidylle mahdollisessa tietoturvaloukkauksessa. Tietojen minimointi vähentää samalla tietojen oikeellisuuden tarkastamis- ja ylläpitotyötä (kts. kohta 2.7).

2.7 Tietojen oikeellisuus ja eheys

Lyhyesti:
- Käsiteltävien henkilötietojen on oltava täsmällisiä ja oikeita.
- Rekisteröidyllä on aina oikeus tarkastaa omat tietonsa.
- On suositeltavaa tarjota rekisteröidylle mahdollisuus itse suouraan tarkastaa omat tietonsa ja myös samalla tarjota mahdollisuutta ilmoittaa korjattavista tiedoista.
- Virheelliset ja puutteelliset tiedot on korjattava tai poistettava viivyttelemättä.
- Päätöksen perusteena olevien tietojen oikeellisuus on tarkistettava ennen kuin tehdään rekisteröidyn oikeuksiin ja velvollisuuksiin koskevia päätöksiä.

Käsiteltävien henkilötietojen on oltava täsmällisiä ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä. (Tietosuojavaltuutetun toimisto, Tietojen täsmällisyys).

Käsiteltävien henkilötietojen on oltava täsmällisiä ja oikeita. Erityisen tarkkana tulee olla henkilötietojen käsittelyssä tietojärjestelmissä, joista henkilötiedot siirtyvät automaattisesti muihin järjestelmiin, virhe tiedoissa voi levitä laajasti ja vaikuttaa yllättävästi. Virheellisten tai puutteellisten mm. vanhentuneiden tietojen käyttö voi johtaa rekisteröidyn kannalta virheellisiin päätöksiin ja tulkintoihin ja siten vaarantaa rekisteröidyn oikeuksia tai johtaa rekisteröidyn kannalta vääriin toimenpiteisiin. Esim. opiskelijan virheelliset opiskeluaikamerkinnät (päivämäärät) voivat johtaa siihen, että opiskelija ei saa hänelle kuuluvaa opintososiaalista etua esim. opintotukea, työttömyysetuutta tai tuen myöntäjä tekee virheellisen tuen takaisinperinnän.

Käsittelytoiminnossa tulee säännöllisesti tarkistaa tietojen oikeellisuus ja eheys. Virheelliset ja puutteelliset tiedot on tällöin samalla korjattava tai poistettava. Suositeltavaa on, että käytettävä tietojärjestelmä sisältää myös tiedon siitä, milloin kyseinen tieto on siihen tallennettu tai päivitetty. Tämän tiedon perusteella voidaan myös arvioida tiedon oikeellisuutta.

Rekisteröidylle on tarjottava mahdollisuus tarkastaa omat tietonsa sekä ilmoittaa tiedoissa olevista virheistä ja puutteista. Tietojen tarkastusoikeus on rekisteröidyn oikeus ja rekisterinpitäjän velvollisuus on viipymättä korjata virheelliset tiedot. Erityisen tärkeää on tarkistaa tietojen oikeellisuus aina ennen kuin tehdään rekisteröityjen oikeuksia ja velvollisuuksia koskevia päätöksiä. Siksi esim. päätökseen liittyvässä hakemus-, tilaus- yms. lomakkeella on perusteltua kysyä uudelleen mahdollisesti päätöksentekoon liittyviä muuttuneita tietoja, vaikka ne olisivatkin jo muuten rekisterissä.

Jos henkilötietoja siirretään käsittelytoiminnosta toiseen manuaalisesti, on muuttuneet tai korjatut tiedot myös siirrettävä eteenpäin kohdejärjestelmiin/käsittelytoimintoihin. Sama koskee mahdollisia suostumustietoja ja niissä tapahtuneita muutoksia sekä henkilötietojen luovutuksia silloin, kun kyse on säännönmukaisesta tai laissa säädetystä velvollisuudesta luovuttaa muuttunut tieto. Henkilötietojen siirrot tulee tästä syystä eritellä käsittelytoiminnon tietosuojaselosteessa, josta voidaan tarkistaa mihin korjattavat tiedot tulee siirtää, ellei siirto tapahdu automaattisesti.

2.8 Rekisteröidyn oikeudet

Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus:

- saada tietoa henkilötietojensa käsittelystä.
- saada tutustua tietoihin.
- oikaista tietoja.
- poistaa tiedot ja tulla unohdetuksi.
- rajoittaa tietojen käsittelyä.
- siirtää tiedot järjestelmästä toiseen.
- vastustaa tietojen käsittelyä.
- olla joutumatta automaattisen päätöksenteon kohteeksi.

Rekisteröityjen oikeuksista on säädetty EU:n tietosuoja-asetuksen III-luvussa (artiklat 37–39).

Rekisteröityjen oikeudet vaihtelevat sen mukaan, mitä mihin lailliseen käsittelyperusteeseen eli oikeusperusteeseen henkilötietojen käsittely missäkin käsittelytarkoituksessa perustuu. Seuraavalla sivulla olevassa taulukossa 1 on esitetty mitkä rekisteröidyn oikeudet (riveillä) käsittelyperusteittain (sarakkeet).

Rekisteröityjen oikeuksista lisää Tietosuojavaltuutetun toimiston verkkosivulla osoitteessa: https://tietosuoja.fi/rekisteroidyn-oikeudet.

REDU informoi rekisteröidyn oikeuksista tietosuojaselosteissa sekä verkkosivuilla osoitteessa: www.redu.fi/tietosuoja/rekisteroidyn-oikeudet.

TAULUKKO 1. Rekisteröidyn oikeudet käsittelyperiaatteet

Rekisteröidyn oikeus	Laki-sääteinen velvoite	Sopimus	Suostumus	Yleinen etu tai julkinen tehtävä	Rekisterin-pitäjän oikeutettu etu	Elin-tärkeiden etujen suojaami-nen
Oikeus saada tietoa henkilötietojen käsittelystä	**Kyllä,** ellei laissa ole säädetty poikkeusta	**Kyllä**	**Kyllä**	**Kyllä,** ellei laissa ole säädetty poikkeusta	**Kyllä**	**Kyllä**
Oikeus saada pääsy tietoihin	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**
Oikeus oikaista tietoja	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**
Oikeus poistaa tiedot	**Ei**	**Kyllä,** jos tietoja ei enää tarvita sopimuksen täyttämiseksi	**Kyllä,** perumalla suostumuksen	**Ei**	**Kyllä**	**Kyllä**
Oikeus rajoittaa tietojen käsittelyä	**Ei**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**	**Kyllä**
Oikeus vastustaa tietojen käsittelyä	**Ei**	**Ei**	**Ei**	**Kyllä**	**Kyllä**	**Ei**
Oikeus siirtää tiedot järjestelmästä toiseen	**Ei**	**Kyllä**	**Kyllä**	**Ei**	**Ei**	**Ei**
Oikeus olla joutumatta automaattisen päätöksenteon kohteeksi ilman laillista perustetta	**Kyllä**	**Kyllä,** paitsi jos automaattinen päätöksenteko on välttämätöntä sopimuksen täyttämiseksi	**Kyllä / Ei** Rekisteröidyltä pyydetään erikseen suostumus automaattiseen päätöksentekoon	**Kyllä**	Automaattinen päätöksenteko ei ole sallittu	Automaattinen päätöksenteko ei ole sallittu

2.9 Osoitusvelvollisuus

Lyhyesti:
- Rekisterinpitäjänä REDUn tulee osoittaa, että se noudattaa henkilötietojen käsittelyssä tietosuojalainsäädäntöä ja kunnioittaa rekisteröityjen tietosuojaa.
- Osoitusvelvollisuuden toteuttaminen on aktiivista toimintaa, jossa toimenpitein ja dokumentein todistetaan, että on noudatettu ja tullaan noudattamaan tietosuojalainsäädäntöä.

Rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä (Tietosuojavaltuutetun toimisto, Osoitusvelvollisuus)

Henkilötietojen käsittelyssä on noudatettava tietosuojalainsäädäntöä. Rekisterinpitäjän on pystyttävä osoittamaan aktiivisesti, että se noudattaa, kehittää ja parantaa tietosuojaa.

Tietosuojaan liittyvä dokumentaatio, eli suunnitelmat, sopimukset, linjaukset, päätökset, tietosuojavaikutusten arvioinnit, tietosuojaselosteet ja selosteet käyttelytoiminnoista, ovat osa osoitusvelvollisuutta. Mm. tämä REDUn tietosuojaperiaatteet ja tietosuojan yleisohjeet on osa rekisterinpitäjän osoitusvelvollisuutta.

Pelkkä tietosuoja-asioiden dokumentointi ei riitä. Osoitusvelvollisuutta toteutetaan myös toteuttamalla käytännössä tarvittavat tekniset, toiminnalliset ja organisatoriset tietosuojatoimet ja tietosuojan kehittämistoimet sekä dokumentoimalla mitä on tehty. Myös havaittuihin tietosuojapuutteiseen ja tietoturvaloukkauksiin tulee puuttua ja dokumentoida miten niissä on toimittu.

REDUssa osoitusvelvollisuutta on myös tietosuoja-asioiden säännöllinen ja dokumentoitu käsittely tietosuojaryhmässä sekä vuosittaiset johdon tietosuojakatselmukset, poikkeamien ja tietosuojaloukkausten ja rekisteröityjen oikeuksien käyttöpyyntöjen dokumentointi, henkilökunnan tietosuojakoulutukset ja niiden dokumentointi sekä tietosuojavaikutusten arvioinnit.

Tietosuojaviranomainen on luetellut toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi (taulukko 2):

TAULUKKO 2. Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi: (Tietosuojavaltuutetun toimisto, Osoitusvelvollisuus.)

Toimenpide tai dokumentti	**Tietosuoja-asetus**	**Lisätietoa**
Rekisterinpitäjän seloste käsittelytoimista eli henkilötietojen käsittelyn yleinen kuvaus. Koskee myös henkilötietojen käsittelijää	30 artikla	kohta 3.4.4
Tietosuojaperiaatteiden sisäänrakennettu toteutuminen omassa toiminnassa	5 ja 25 artiklat	Luku 2
Mahdolliset tietosuojaa koskevat laajemmat toimintaperiaatteet	24.2. artikla	
Informointikäytännöt.	12–14 artiklat	kohta 3.4
Käsittelyn oikeusperustetta koskevat arviot. - Jos käsitellään suostumuksen perusteella, suostumukseen liittyvä dokumentaatio. - Jos käsitellään rekisterinpitäjän tai sivullisen oikeutetun edun perusteella, tätä koskeva tasapainotesti.	6–10 artiklat 7 ja 8 artikla 6.1.f artikla	kohta 2.3
Muut sisäiset ja ulkoiset ohjeistukset. - Riskiarvioita koskeva dokumentaatio sekä toteutetut tekniset ja organisatoriset suojatoimenpiteet. - Sisäiset ja ulkoiset ohjeet rekisteröidyn oikeuksien toteuttamiseksi. - Ohjeet henkilötietoja käsitteleville työntekijöille ja henkilötietojen käsittelijöille. - Sisäiset tarkastukset ja auditoinnit.	12, 13, 14, 24, 25, 28, 29 ja 32 artiklat	kohta 3.6 kohta 3.8
Vaikutustenarviointeja ja ennakkokuulemista koskeva dokumentaatio.	35 ja 26 artiklat	kohta 3.6.4
Henkilötietojen tietoturvaloukkausten dokumentointi ja tätä koskeva prosessi.	33 ja 34 artilat	kohta 3.7.7 kohta 3.7.4
Tietosuojavastaavan asemaan ja tehtäviin liittyvä dokumentaatio. - On suositeltavaa aina dokumentoida perusteet sille, jos organisaatio päätyy henkilötietojen käsittelyä koskevassa asiassa eri ratkaisuun, kuin tietosuojavastaava on suositellut.	37–39 artiklat	kohta 3.2
Henkilötietojen käsittelyyn liittyvät sopimukset.	28 artikla	-
Yhteisrekisterinpitäjien vastuualueet.	26 artikla	-
Mahdollinen johtavan valvontaviranomaisen määrittämistä koskeva dokumentaatio	56 artikla	-
Henkilötietojen siirtoa kolmansiin maihin koskeva dokumentaatio.	5 luku	-

Lisätietoa osoitusvelvollisuudesta tietosuojavaltuutetun toimiston verkkosivuilla osoitteessa: https://tietosuoja.fi/osoitusvelvollisuus

3 Tietosuojan yleisohjeet

3.1 Tietosuojan vastuu ja tietosuojatyön organisointi REDUssa

3.1.1 Vastuu ja organisointi

Lyhyesti:

- REDUn johto vastaa siitä, että REDUssa toimitaan tietosuojalainsäädännön mukaisesti.
- Johto päättää henkilötietojen käsittelyn periaatteista, organisoi ja resursoi tietosuojatyön sekä antaa siihen liittyvät työnjohdolliset määräykset.
- Johto päättää, miltä osin henkilötietojen käsittelyä ulkoistetaan ja sopii käsittelystä sopimustoimittajien eli ulkopuolisten henkilötietojen käsittelijöiden kanssa.
- Johto vastaa tietosuojavaikutusten arvioinneista ja niiden perusteella tehtävistä päätöksistä.
- Esihenkilö vastaa alaistensa tietosuojaan perehdyttämisestä sekä varmistaa, että alaiset suorittavat ~~perustason tietosuojaosaamisen~~ heidän tehtävissään vaadittavat tietosuoja ja tietoturvakoulutukset.
- Henkilökuntaan kuuluva vastaa, että käsittelee henkilötietoja omissa virka- tai työtehtävissä esihenkilön, REDUn tietosuojaperiaatteiden ja REDUn tietosuojaohjeiden sekä tietosuojasäädösten mukaisesti.
- REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija ovat tietosuojan riippumattomia asiantuntijoita ja toimivat yhteyshenkilöinä tietosuojaviranomaisen ja rekisteröityjen kanssa.
- REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija neuvovat ja opastavat johtoa, henkilökuntaa ja rekisteröityjä tietosuoja-asioissa.
- REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija valvovat tietosuojalainsäädännön noudattamista REDUssa ml. Santasport ja raportoivat suoraan johdolle ja vastuuhenkilöille havainnoista.
- REDUn tietosuojaryhmä vastaa REDUn tietosuojatyön kehittämistyön valmistelusta ja tietosuojan valvonnasta.

Rovaniemen koulutuskuntayhtymä REDU ja sen tulosalueiden johtamisjärjestelmä perustuu Kuntalakiin ja Osakeyhtiölakiin, REDUn perustamissopimukseen ja hallintosääntöön sekä sen perusteella annettuihin organisointi- ja delegointipäätöksin. REDU-konsernin johtamisesta on lisäksi päätetty REDUn konserniohjeessa. Tietosuojan johtaminen, vastuu ja organisointi noudattavat tätä samaa johtamis- ja päätöksentekojärjestelmää.

3.1.2 Toimielimet

REDU-kuntayhtymän toimielimiä ovat mm. kuntayhtymän yhtymäkokous, yhtymähallitus, tarkastuslautakunta, yhteistyötoimikunta, työsuojelutoimikunta ja oikeusturvatoimielin. REDUn tytäryhtiöiden toimielimiä ovat mm. osakeyhtiön yhtiökokoukset ja hallitukset.

Toimielimien ja niiden jäsenten on noudatettava tietosuojalainsäädäntöä, REDUn tietosuojaperiaatteita ja tietosuojaohjeita käsitellessään henkilötietoja. Toimielimen jäsenet toimivat tällöin henkilötietojen käsittelijöinä ja heitä koskee mm ehdoton vaitiolo, kts. kohta 2.4. Myös varsinaisissa päätöksissä ja päätösasiakirjoissa on otettava huomioon tietosuojavaatimukset.

Toimielin osana REDUn johtamis- ja päätöksentekojärjestelmää vastaa tekemiensä päätösten laillisuudesta myös tietosuojan osalta. Toimielimen päätös voidaan palauttaa sille uudelleen käsittelyyn, mikäli REDUn laillisuusvalvonnassa ilmenee, että tehty päätös ei noudata tietosuojalainsäädäntöä.

Suositeltavaa on, että REDUn toimielimien jäsenet suorittavat vähintään tietosuojan perusosaamisen koulutuksen ja testin.

3.1.3 Johtajat ja päälliköt

REDUn johto (vastuullinen johto) eli johtavat viranhaltijat on määritelty REDUn hallintosäännössä. REDUn johtoon kuuluvat mm. kuntayhtymän johtaja, kehitysjohtaja, tulosaluejohtajat/rehtorit, talouspäällikkö, henkilöstöpäällikkö ja kiinteistöpäällikkö. Lisäksi johtoon kuuluviksi luetaan virkasuhteiset päälliköt (pedagoginen päällikkö ja toimialapäälliköt) sekä tytäryhtiöiden toimitusjohtajat.

Johto vastaa, että hänen vastuualueellansa käsitellään henkilötietoja tietosuojasäädösten mukaisesti, oli sitten kyse oman henkilökunnan toimesta tapahtuvasta henkilötietojen käsittelystä tai ulkoistetusta henkilötietojen käsittelystä.

Johto vastaa vastuualuettaan koskevista tietosuojariskien tunnistamisesta, tietosuojavaikutusten arvioinneista, päättää arviointien perusteella tehtävistä toimenpiteistä ja allekirjoittaa tehtyjen vaikutusarviontien raportit.

Johto nimeää vastuualueensa osalta myös henkilötietojen käsittelyn käsittelytoimintojen yhteyshenkilöt.

Johto päättää toimivaltansa mukaisesti vastuualueen henkilökunnalle annettavista työnjohdollisista määräyksistä koskien henkilötietojen käsittelyä ja tietosuojavaikutusten arviointeja. Johto myös sopii vastuualeensa osalta rekisterinpitäjän nimissä ulkopuolisten palveluntuottajien kanssa henkilötietojen käsittelystä ja tietosuojavaikutusten arvioinneista.

Johtajien rooli tietosuojan toteutumisessa on merkittävin. Johto, ml. toimielimet ja esihenkilöt, tekevät niitä päätöksiä, joilla johdetaan ja vaikutetaan siihen, miten tietosuoja REDUssa ja sen tytäryhtiöissä toteutuu. Johto toimii myös osaltaan esimerkkeinä henkilötietojen käsittelyssä.

Johto vastaa oman tietosuojaosaamisensa kehittämisestä ja käsitellessään omissa virka- tai työtehtävissä henkilötietoja, noudattaa tietosuojalainsäädäntöä, REDUn tietosuojaperiaatteita ja tietosuojaohjeita.

3.1.4 Esihenkilöt

Esihenkilö vastaa alaistensa virka- tai työtehtäväkohtaisesta tietosuojaan perehdyttämisestä. Henkilökunnan ~~tietosuojaosaaminen~~ tietosuoja- ja tietoturvaosaaminen rakentuu ~~tietosuojan~~ yleisestä perustason osaamisesta ja ~~tehtäväkohtaisesta~~ työtehtävä- tai alakohtaisesta syventävästä tietosuoja- ja tietoturvaosaamisesta. ~~henkilötietojen käsittelyn tietosuojaosaamisesta.~~

Esihenkilön tehtävä on valvoa ja varmistaa, että kaikilla heidän alaisillaan on REDUssa vaadittava ~~tietosuojan perusosaaminen~~ yleinen perustason sekä tehtävässä tarvittava työtehtävä- tai alakohtainen syventävä tietosuoja- ja tietoturvaosaaminen. ~~tietosuojaosaaminen.~~

Esihenkilöt toimivat osaltaan esimerkkeinä henkilötietojen käsittelyssä ja toimivat henkilötietojen käsittelijöinä mm. omien alaistensa henkilötietoja käsitellessään. Alaisten henkilötietoja tulee käsitellä huolellisesti. Esihenkilö ei saa millään tavalla ilmaista sivulliselle esim. alaisensa erityisiin henkilötietoryhmiin kuuluvia saamiansa tietoja esim. terveystietoja tai muita yksityisyyden suojaan kuuluvia tietoja.

3.1.5 Henkilökunta

Henkilön työ- tai virkatehtäviin kuuluu monenlaista henkilötietojen käsittelyä. Käytännössä kaikki REDUn henkilökuntaan kuuluvat, jotka ovat tekemissä REDUn asiakkaiden, opiskelijoiden, vierailijoiden tai muun henkilökunnan kanssa tai heihin liittyvien henkilötietojen tai niitä sisältävien asiakirjojen, dokumenttien ja tietojärjestelmien kanssa, käsittelevät työssään henkilötietoja.

Henkilökunnan velvollisuutena on noudattaa henkilötietoja käsitellessään tietosuojalainsäädäntöä, REDUn tietosuojaperiaatteita ja ohjeita sekä työantajana REDUn tai sen tytäryhtiön ja esihenkilön antamia tietosuoja- ja tietoturvaohjeita. Henkilökunnan on myös seurattava oman tehtäväalueensa osalta tietosuojalainsäädännössä tapahtuvia muutoksia ja tarvittaessa hankittava lisää tietosuojaosaamista osana omaa osaamisensa kehittämistä.

~~Jokaisella REDUn henkilökuntaan kuuluvalla täytyy olla vähintään tietosuojan perusosaaminen~~ REDUn henkilökunnalta ja johdolta edellytetään yleinen perustason tietosuoja- ja tietoturvaosaamisen hankkiminen ja osoittaminen. Lisäksi vaaditaan virka- tai työtehtävien mukaisen työtehtävä- tai alakohtaisen syventävän tietosuoja- ja tietoturvaosaaminen ja sen osoittaminen. Edellytetty osaaminen osoitetaan suorittamalla vaadittu koulutus ja siihen sisältyvät testi tai tentti hyväksytysti. ~~Suoritettavasta koulutuksesta ja suorittamistavasta päättää kuntayhtymän johtaja REDUn tietosuojaryhmän esityksestä.~~ Tämän lisäksi henkilön on osallistuttava esihenkilönsä määräämiin muihin tietosuojakoulutuksiin ja perehdytyksiin.

Ohjeistuksen henkilökunnalta vaadittavista osaamisista ja niiden osoittamistavasta valmistelee REDUn tietosuojaryhmä ja niistä päättää kuntayhtymän osalta kuntayhtymän johtaja ja tytäryhtiöiden osalta yhtiön toimitusjohtaja. Sitä ennen vaatimukset käsitellään REDUn konsernijohtoryhmässä.

~~Henkilön perustason tietosuojaosaamisesta pidetään kirjaa REDUn HR-järjestelmässä (Hemuli) henkilöstöpalvelujen ja tietosuojavastaavan antamien ohjeiden mukaisesti~~. Henkilöstö tietosuoja- ja tietoturvakoulutusten suorittamista seurataan REDUn tätä tarkoitusta varten hankkimassa tietosuoja- ja tietoturvakoulutusympäristössä. Aiemmin suoritettuja koulutustietoja on myös REDUn HR-järjestelmässä (Hemuli). Tietosuojan perusosaamisen suorittamisten toteutumista seurataan säännöllisesti REDUn tietosuojaryhmässä. Mahdollista koulutuspuutteista informoidaan esihenkilöitä. Tarvittaessa koulutuspuutteista tehdään tietosuojapoikkeamakirjaus.

~~REDUn johtoryhmässä Tietosuojaryhmän esityksestä päätetään tietosuojakoulutuksen toteuttamisesta. Henkilökunnan on osallistuttava johtoryhmässä päätetysti tietosuojakoulutuksiin.~~

Henkilökunnan velvollisuus on ilmoittaa viivyttelemättä havaitsemistaan tietosuojapoikkeamista ja tietoturvaloukkauksista esihenkilölle tai tietosuojavastaavalle.

3.1.6 Henkilötietojen käsittelijät, käsittelyn kilpailuttaminen, hankinnat ja sopiminen

Henkilötietojen käsittelijänä tarkoitetaan tietosuojalainsäädännössä rekisterinpitäjän ulkopuolista tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Eli henkilötietojen käsittelyä on ulkoistettu. Tämän ulkopuolinen taho voi olla toinen oikeushenkilö, luonnollinen henkilöt tai muu taho, joka ei ole rekisterinpitäjän johdon alaisuudessa (henkilökuntaa). Henkilötietojen käsittelijöitä ovat myös tietojärjestelmien ja -palvelujen toimittajat, kun ko. tietojärjestelmillä käsitellään REDUn rekisteröityjen esim. asiakkaiden tai henkilökunnan henkilötietoja. Kts. lisätietoa tietojärjestelmistä ja -palveluista kohdasta 3.5.

REDUn tai sen tytäryhtiön johto päättää miltä osin henkilötietojen käsittelyä on ulkoistettu.

REDUn tytäryhtiöt toimivat myös henkilötietojen käsittelijöinä REDU-konsernin/kuntayhtymän (rekisterinpitäjä) lukuun. Rekisterinpitäjänä toimiessaan REDU-konserni voi antaa tytäryhtiötä koskevia velvoittavia henkilötietojen käsittelyn tietosuojaohjeista. REDUn tytäryhtiö voi halutessaan päättää toimivansa itsenäisenä rekisterinpitäjänä. Yhtiön on ilmoitettava em. päätöksestä ennen sen voimaantuloa REDUlle (REDUn konserniohje, kohta 16).

Rekisterinpitäjänä REDU vastaa aina ensisijaisesti rekisteröityjen ml. ulkoistetusta sopimustoimittajien henkilötietojen käsittelystä. Sopimuksella REDU voi siirtää osin tätä vastuuta sopimustoimittajalle.

Lähtökohtaisesti henkilötietojen käsittelyä ei saa ulkoistaa EU/ETA-alueen ulkopuolelle. Tämä koskee myös sopimustoimittajan alihankkijoita. Sopimustoimittajan tulee sitoutua noudattamaan EU:n tietosuoja-asetusta ja muuta tietosuojalainsäädäntöä sekä vastaanottamaan rekisterinpitäjältä saatavaa ohjeistusta.

Henkilötietojen käsittelyn kilpailuttaminen ja hankinnat
Silloin kun ollaan suunnitelmassa hankintaa, jolla henkilötietojen käsittelyä ulkoistetaan sopimustoimittajalle, on ennen tarjouspyyntöjä ja kilpailuttamista tunnistettava, sisältyykö mahdolliseen ulkoistettavaan henkilötietojen käsittelyä ja sisältyykö siihen korkea riski. Jos todetaan, että kyseessä on korkean riskin henkilötietojen käsittely, on tehtävä tietosuojavaikutusten arviointi ennen hankinnan käynnistämistä tai viimeistään ennen kuin ko. palvelu tai tietojärjestelmä otetaan käyttöön, kts. kohta 3.6. Näin voidaan jo tarjouspyynnössä tarkentaa mitä tietosuojavaatimuksia hankittavalta palvelulta tai järjestelmältä edellytetään, ja vältytään mahdollisilta jälkikäteen tehtäviltä kalliilta tai aikaa vieviltä muutoksilta palveluun tai järjestelmään.

Henkilötietojen käsittelystä sopiminen
Henkilötietojen käsittelyä sovitaan sopimustoimittajan kanssa aina kirjallisesti ennen kuin henkilötietoja aletaan käsitellä. Sopimus voi olla osa toimittajan kanssa tehtyä hankinta- tai palvelusopimusta tai siihen liitettävä erillinen tietosuojasopimusliite.

Sopimuksessa tulee olla vähintään seuraavat sisältökohdat:
- sopimusosapuolten tiedot,
- sopimusosapuolten roolit (rekisterinpitäjä ja henkilötietojen käsittelijä/käsittelijät),
- mahdolliset muut sopimustoimittajat (alihankkijat),
- käsiteltävät henkilötiedot/henkilötietoryhmät,
- käsittelyn maantieteellinen rajaus (vain EU/ETA-alueen sisällä),
- sopimusosapuolten yleiset velvollisuudet,
- rekisteröityjen oikeuksien toteuttaminen,
- toiminta tietoturvaloukkaustilanteessa,

- toimittajan osallistuminen mahdollisiin tietosuojavaikutusten arviointeihin.

Sopijatoimittajan tulee allekirjoituksin vahvistaa sopimus. Jos kyse on erillisestä sopimusliitteestä, tulee siitä mainita ja viitata sopimuksessa tai liite on erikseen allekirjoitettava.

3.2 REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija

3.2.1 Tietosuojavastaavan tehtävät ja asema

Tietosuojavastaava on organisaation sisäinen tietosuoja-asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa (Tietosuojavaltuutetun toimisto, Tietosuojavastaavat). Tietosuojavastaava ei ole vastuussa REDUn tietosuojasta. Tietosuojasta vastaa REDUn toiminnasta vastaava johto ja esihenkilöt sekä henkilötietojen käsittelijät siten, kun edellä on esitetty. Tietosuojavastaavan tehtävistä ja asemasta on säädetty tietosuoja-asetuksen 37–39 artikloissa.

Tietosuojavastaava (tehtävät):
- seuraa tietosuojasääntöjen noudattamista ja tuo esiin havaitsemiaan puutteita johdolle ja käsittelytoiminnoista vastaaville,
- antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietojen käsittelyssä henkilökunnalle ja muille sidosryhmille,
- 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 (Tietosuojavaltuutetun toimisto, Tietosuojavastaavat).

REDUssa lisäksi tietosuojavastaava em. lisäksi:
- vastaanottaa ilmoitukset tietosuojapoikkeamista ja -loukkauksista sekä rekisteröityjen oikeuksien käyttöpyynnöt ja ylläpitää niihin liittyvää dokumentaatiota,
- seuraa henkilöstön ja johdon tietosuojakoulutusten suorittamista ja raportoi niistä tarvittaessa johdolle ja esihenkilöille.

Rekisteröidyt voivat ottaa suoraan yhteyttä tietosuojavastaavaan heidän henkilötietojen käsittelyyn ja tietosuoja-asetukseen perustuviin oikeuksiin liittyvissä asioissa.

Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietoja koskevien kysymysten käsittelyyn.

Tietosuojavastaavaa sitoo tehtäviensä suorittamista koskeva salassapitovelvollisuus.

Tietosuojavastaavan asema organisaatiossa
Tietosuojavaltuutetun toimisto on antanut seuraavia ohjeita tietosuojavastaavan nimittäneille organisaatoille:

1. Tietosuojavastaavalla on oltava riittävästi työaikaa, -välineitä ja osaamista tehtävän suorittamiseen. Tietosuojavastaavalla pitäisi olla myös mahdollisuus kouluttautua.
2. Tietosuojavastaava tai hänen tiiminsä otetaan mahdollisimman aikaisessa vaiheessa mukaan kaikkien tietosuojakysymysten käsittelyyn.

3. Tietosuojavastaavan suositellaan olevan paikalla aina silloin, kun tehdään tietosuojaan vaikuttavia päätöksiä. Kaikki olennaiset tiedot toimitetaan tietosuojavastaavalle viipymättä, jotta hän voi antaa asianmukaisia neuvoja.
4. Tietosuojavastaavalla on oltava mahdollisuus raportoida suoraan johdolle. Tietosuojavastaava kutsutaan säännöllisesti ylemmän tai keskitason johdon kokouksiin.
5. Tietosuojavastaavan näkemykselle annetaan aina asianmukainen painoarvo. Mahdollisissa erimielisyystilanteissa on hyvä dokumentoida perusteet, joiden vuoksi tietosuojavastaavan neuvoa ei noudateta.
6. Jos tietoturvaloukkaus tai muu tietosuojaan liittyvä ongelma ilmenee, tietosuojavastaavaa kuullaan mahdollisimman nopeasti.
7. Tietosuojasäännösten noudattaminen on rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla. Tietosuojavastaavat eivät ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen rikkomisesta. (Tietosuojavaltuutetun toimisto, Tietosuojavastaavat.)

3.2.2 Tietosuojavastaavan tehtävien organisointi REDUssa

REDUssa tietosuojavastaavan tehtävät on jaettu kahdelle henkilölle, varsinaiselle REDUn tietosuojavastaavalle sekä Santasportin tietosuoja-asiantuntijalle. He molemmat vastaanottavat tietosuoja@redu.fi ja tietosuojavastaava@redu.fi -sähköpostiosoitteeseen tulevat viestit. Tarvittaessa he toimivat myös toistensa sijaisina tietosuojavastaavan tehtävien osalta. Milloin he molemmat ovat yhtä aikaa vuosilomilla tai muuten estyneitä hoitamasta tietosuojavastaavan tehtäviä, tietosuojaryhmässä sovitaan, miten sijaisuus hoidetaan tai REDUn kehitysjohtaja määrää tehtävään sijaisen.

3.2.3 REDUn tietosuojavastaava

REDUn tietosuojavastaavan vastuualuetta on:
- Lapin koulutuskeskus REDU,
- REDU Edu Oy,
- REDUn sisäisten palvelut,
- Rovaniemen koulutuskuntayhtymä REDUn ja REDU-konsernin hallinto.

REDUn tietosuojavastaava
- vastaa kaikista kohdassa 3.2.1 esitetyistä tietosuojavastaavan tehtävistä em. vastuualueella,
- toimii rekisterinpitäjän eli REDU-konsernin yhteyshenkilönä valvontaviranomaisen eli Tietosuojavaltuutetun toimiston kanssa,
- toimii myös REDUn tietosuojaryhmän puheenjohtajana sekä työryhmässä tietosuoja-asioiden valmistelijana siten kuin ko. työryhmän toimeksiantopäätöksessä on tarkennettu,
- ylläpitää yhdessä Santasportin tietosuoja-asiantuntijan kanssa luetteloa käsittelytoiminnoista ja tarkastaa kaikki tietosuojaselosteet ennen niiden julkaisemista,
- ylläpitää yhdessä Santasportin tietosuoja-asiantuntijan kanssa luetteloa tietosuojapoikkeamista ja tietoturvaloukkauksista sekä rekisteröityjen oikeuksien käytöstä,
- toimii tarvittaessa tietosuojavastaavana myös Santasportin tietosuoja-asiantuntijan vastuualueella silloin, kun Santasportin tietosuoja-asiantuntija on estynyt hoitamasta tehtäviään.

3.2.4 Santasport tietosuoja-asiantuntija

Santasport -kokonaisuuden tietosuojavastaavan tehtäviä hoitaa Santasportin tietosuoja-asiantuntija. Santasport-kokonaisuuteen kuuluvat:
- Santasport Lapin Urheiluopisto,
- Santasport Finland Oy ja
- Lapin kesäyliopisto.

Santasportin tietosuoja-asiantuntija:
- vastaa kaikista kohdassa 3.2.1 esitetyistä tietosuojavastaavan tehtävistä em. Santasport -kokonaisuuden vastuualueella lukuun ottamatta REDUn yhteyshenkilön tehtäviä valvontaviranomaisen kanssa,
- tekee Santasportia koskevissa tietosuoja-asioissa, kuten tietosuojaloukkausten käsittelyssä, yhteistyötä REDUn tietosuojavastaavan ja tietosuojaviranomaisten kanssa,
- vastaa Santasportin tietosuojaselosteiden ja selosteen käsittelytoiminnon ylläpidosta,
- ylläpitää yhdessä REDUn tietosuojavastaavan kanssa luetteloa tietosuojapoikkeamista ja tietoturvaloukkauksista sekä rekisteröityjen oikeuksien käytöstä,
- toimii tarvittaessa REDUn vara-tietosuojavastaavana REDUn tietosuojavastavan ollessa estynyt hoitamasta tehtäviään.

3.3 Tietosuojaryhmä

REDUssa toimii tietosuojaryhmä, joka kehittää yhdessä REDU konsernijohdon, johtoryhmän sekä tytäryhteisöjen toimitusjohtajien kanssa henkilötietojen käsittelyn tietosuojaa ja tiedonhallintaa.

Tietosuojaryhmä:
- valmistelee henkilötietojen käsittelyä koskevat suunnitelmat ja yleiset ohjeet,
- ylläpitää luetteloa ja selostetta henkilötietojen käsittelytoiminnoista osana REDUn tiedonhallintamallia,
- ylläpitää luetteloa ja tietoja henkilötietojen käsittelyyn liittyvistä poikkeamista, tietoturvaloukkauksista ja muista havainnoista,
- ylläpitää luetteloa rekisteröityjen oikeuksien käyttöpyynnöistä siltä osin, kun niitä ei ole suoraan osoitettu käsittelytoiminnoista vastaaville,
- seuraa ja valvoo säännöllisesti henkilötietojen käsittelyä ja niiden suojausmenetelmiä,
- valmistelee tietosuojan johdon katselmukset.
- hoitaa tietosuojavastaavan sijaistehtävät mm. vuosilomien aikana työryhmässä päätetysti, ellei asiasta ole muuta päätetty.

Työryhmän puheenjohtajana ja tietosuoja-asioiden vetäjänä toimii REDUn tietosuojavastaava.

Työryhmän muista tehtävistä, toimikaudesta, toimivallasta, jäsenistä ja heidän tehtävistään työryhmässä päättää kuntayhtymän johtaja REDUn hallintosäännön mukaisesti (13 § kohta 13).

3.4 Käsittelytoiminnot ja rekisteröityjen informointi

3.4.1 Mikä on käsittelytoiminto?

Henkilötietojen käsittelytoiminnolla tarkoitetaan tiettyyn käyttötarkoitukseen (kts. käyttötarkoitussidonnaisuus kohta 2.2) tarkoitettua henkilötietojen käsittelyn kokonaisuutta (prosessia). Käsittelytoiminnossa voi olla käytössä yksi tai useita henkilörekistereitä ja niiden tietojärjestelmiä. Eri käsittelytoiminnot voivat myös siirtää henkilötietoja toistensa välillä siten kuin niiden kuvauksissa eli tietosuojaselosteissa on tarkemmin kuvattu.

Tietosuoja-asetus velvoittaa rekisterinpitäjää informoimaan henkilötietojen käsittelystä.

REDUssa henkilötietojen käsittelytoiminnot kuvataan käsittelytoimintokohtaisissa määrämuotoisissa tietosuojaselosteissa. Niiden avulla REDU dokumentoi käsittelytoimintojaan sekä informoi rekisteröityä henkilötietojen käsittelystä. Käsittelytoimintojen tietosuojaselosteiden tietojen perusteella muodostuu lakisääteinen REDUn seloste käsittelytoiminnoista.

3.4.2 Rekisteröityjen informointi

Tietojen kerääminen rekisteröidyltä
Rekisterinpitäjänä REDUn on informoitava rekisteröityä henkilötietojen käsittelystä. Informointi on tehtävä ennen, kuin henkilötietoja aletaan käsitellä, esim. kun tietoja kerätään suoraan rekisteröidyltä lomakkeella.

Henkilötietojen kerääminen muualta
Jos henkilötiedot kerätään muualta kuin rekisteröidyltä itseltään suoraan, tulee henkilötietojen käsittelyä koskevat tiedot toimittaa rekisteröidylle kohtuullisen ajan, mutta viimeistään yhden kuukauden kuluessa. Tiedot on toimitettava ennen yhden kuukauden määräaikaa näissä tilanteissa:

- Jos henkilötietoja käytetään viestintään rekisteröidyn kanssa ennen määräajan umpeutumista, henkilötietojen käsittelyä koskevat tiedot tulee tällöin toimittaa.
- Jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle ennen määräajan umpeutumista, käsittelyä koskevat tiedot on toimitettava rekisteröidylle viimeistään silloin, kun tietoja luovutetaan ensimmäisen kerran.

Rekisteröidylle toimitettava tietosisältö on osittain riippuvainen siitä, kerätäänkö henkilötiedot rekisteröidyltä itseltään tai muualta. Informoinnin tietosisältö on osittain riippuvainen käsittelyn oikeusperusteesta. Jos henkilötietoja esimerkiksi käsitellään rekisteröidyn suostumuksen perusteella, on rekisteröityä informoitava myös mahdollisuudesta peruuttaa annettu suostumus. REDUssa rekisteröityjen informointiin käytetään käsittelytoimintokohtaista tietosuojaselostetta.

3.4.3 Tietosuojaseloste ja sen laatiminen

REDUssa tietosuojaselosteella informoidaan rekisteröityä käsittelytoiminnosta sekä kerätään selosteeseen käsittelytoiminnoista (kts. kohta 3.4.4) tarvittavat tiedot käsittelytoiminnosta.

Tietosuojaselosteen laatii ko. käsittelytoiminnosta vastaava johto tai hänen nimeämänsä käsittelytoiminnon asiantuntija/yhteyshenkilö. REDUn tietosuojavastaava ja Santasportin

tietosuoja-asiantuntija neuvovat selosteen laadinnassa. REDUn tietosuojavastaava tarkistaa ja julkaisee selosteen.

Tietosuojaselosteen tulee olla valmis ja julkaistu ennen kuin henkilötietoja aletaan käsitellä silloin, kun tiedot kysytään suoraan rekisteröidyltä ja muissa tapauksissa kuukauden sisällä käsittelyn aloittamisesta.

Tietosuojaselosteen sisältö (REDUn lomake A):

1. Rekisterinpitäjä ja tietosuojavastaava.
2. Käsittelytoiminnosta vastaavat tulosalue, yksikkö tai yhtiö:
   - tulosalueen tai yhtiön nimi ja tarvittaessa toimialan tai yksikön nimi
   - käsittelytoiminnosta vastaava johtaja (prosessin omistaja)
   - käsittelytoiminnon tai rekisterin yhteyshenkilö (asiantuntija/pääkäyttäjä).
3. Käsittelytoiminnon tiedot:
   - käsittelytoiminnon nimi.
   - käsittelyssä käytettävän rekisterin tai tietovarannon nimi.
   - käsittelyn tarkoitus.
   - käsittelyn oikeusperuste (*.
4. Rekisteröidyt.
5. Käsiteltävät henkilötiedot, niiden lähteet ja siirto (henkilötiedot ja niiden tietovirta):
   - henkilötieto tai henkilötietoryhmä,
   - henkilötiedon lähde
   - henkilötiedon siirron kohde (jos tietoja siirretään toiseen käsittelytoimintoon).
6. Henkilötietojen luovutus ja julkaiseminen.
7. Tietojärjestelmät, tietoturva ja manuaalinen henkilötietojen käsittely.
8. Rekisteröidyn oikeudet ja niiden käyttäminen.
9. Selosteen jakelu.

*) Mikäli oikeusperuste on suostumus, kuvataan lisäksi, miten suostumus annetaan, miten suostumustietoja säilytetään ja miten suostumus voidaan perua sekä miten annetut tiedot hävitetään, kun suostumus perutaan.

REDUn tietosuojaselosteet tallennetaan ja julkaistaan ROKKI-intrassa. Tietosuojaselosteet ovat osa Tiedonhallintalain 5 §:n REDUn tiedonhallintamallia.

Silloin kun käsitellään REDUn ulkopuolisten henkilötietoja, tietosuojaseloste julkaistaan myös REDUn verkkosivujen tietosuojasivuilla www.redu.fi/tietosuoja > Tietosuojaselosteet.

3.4.4 Seloste käsittelytoiminnoista

REDU rekisterinpitäjänä pitää yllä luetteloa henkilötietojen käsittelytoiminnoista. Käsittelytoimintojen luettelo on tarkoitettu REDUn sisäiseen käyttöön ja sen ylläpidosta vastaavat REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija yhdessä. Tietosuojavaltuutetun toimiston niin pyytäessä, luettelosta annetaan ko. viranomaiselle tietoja. Käsittelytoimintojen selosteen sisällöstä on säädetty tietosuoja-asetuksen 30 artiklassa ja tietosuojavaltuutettu on antanut tarkempia ohjeita sen sisällöstä.

REDUn seloste käsittelytoiminnoista muodostuu kohdassa 3.4.3 kuvattujen tietosuojaselosteiden tietojen perusteella. Seloste käsittelytoiminnoista on käytännössä taulukkomuotoinen

luettelo, joka sisältää seuraavat tiedot jokaisesta käsittelytoiminnosta:

- käsittelytoiminnon nimi,
- käsittelyn tarkoitus,
- mahdollisen yhteisrekisterin tiedot,
- tietojen siirto EU/ETA-alueen ulkopuolelle,
- tietojen säilytysaika tai sen määräytymisperuste,
- tietoturva,
- vastuullinen johtajan nimi,
- yhteyshenkilön nimi.

Lisäksi seloste sisältää rekisterinpitäjän ja tietosuojavastaavan tiedot yhteystietoineen.

Seloste käsittelytoiminoista löytyy REDUn ROKKI-intrasta. Seloste käsittelytoiminnoista on myös osa Tiedonhallintalain 5 §:n REDUn tiedonhallintamallia.

3.5 Henkilötietojen käsittelyssä käytettävät tietojärjestelmät ja -palvelut

Lyhyesti:
- Henkilötietojen käsittelyn tulee olla kaikissa vaiheissa tietoturvallista.
- EU/ETA-alueen ulkopuolisten tietojärjestelmien ja -palvelujen käyttö henkilötietojen käsittelyssä REDUssa on lähtökohtaisesti kielletty.
- Tietojärjestelmän tai -palvelun tuottajan kanssa on sovittava kirjallisesti niiden käytöstä ja käytön tietosuojasta ja tietoturvasta.
- Ennen uuden tietojärjestelmän tai -palvelun hankintaa tai käyttöönottoa on tehtävä tietosuojavaikutusten arviointi, mikäli käsittelyyn sisältyy korkea riski.
- Henkilötietojen käsittelyyn ei saa käyttää tietojärjestelmiä, sovelluksia tai palveluja, joita REDU ei ole hankkinut käyttöönsä.

Turvallisuus ja luottamuksellisuus
REDUn tietosuojaperiaatteiden mukaisesti Henkilötietojen käsittelyn tulee olla luottamuksellista ja turvallista, kts. kohta 2.6. Rekisterinpitäjän REDU myös vastaa, että sen henkilötietojen käsittelyssä käyttämät tietojärjestelmät ja palvelut ovat tietoturvallisia ja että REDUn asiakkaat, opiskelija, henkilökunta ym. rekisteröidyt voivat luottaa REDUun ja sen käyttämien tietojärjestelmien ja -palvelujen tietoturvaan.

EU/ETA-alueen ulkopuolisten tietojärjestelmien ja -palvelujen käyttö REDUn henkilötietojen käsittelyssä on lähtökohtaisesti kielletty.
EU:n tietosuoja-asetus on sellaisenaan suoraan ja velvoittavana voimassa EU ja ETA-alueella. Tietosuoja-asetus rajaa, että EU:n jäsenvaltioissa toimivan rekisterinpitäjän eli myös REDUn henkilötietojen käsittelyn on lähtökohtaisesti tapahduttava Euroopan unionin talousalueen (EU/ETA-alue) sisälle (Tietosuoja-asetus, 3. artikla). Erityistapauksessa voidaan käyttää EU/ETA-alueen ulkopuolisia palvelutuottajia, mutta ne täytyy sopimuksellisesti sitovasti velvoittaa noudattamaan EUn tietosuoja-asetuksen velvoitteita koskien henkilötietojen käsittelyä.

Tietojärjestelmän tai palvelun tuottajan kanssa on aina sovittava kirjallisesti.
Tietojärjestelmän tai -palvelun tuottajan kanssa sovitaan aina kirjallisesti niiden käytöstä ja käytön tietosuojasta ja tietoturvasta. Sopimustoimittajan tulee sitoutua noudattamaan EU:n tietosuoja-asetusta ja muuta tietosuojalainsäädäntöä sekä vastaanottamaan rekisterinpitäjältä saatavaa ohjeistusta, kts. kohta 3.1.6.

Arvioi riskit ennen käyttöä
Ennen kuin uutta tietojärjestelmä tai -palvelu otetaan käyttöön REDUn rekisteröityjen henkilötietojen käsittelyyn, on arvioitava, sisältyykö käsittelyyn korkea ja tarvittaessa tehtävä tietosuojavaikutusten arviointi. Riskit on arvioitava myös silloin, kun järjestelmää tai palvelua muutetaan tai päivitetään oleellisesti. Lisätietoa kts. kohta 3.6.

Henkilötietojen käsittelyssä ei saa käyttää tietojärjestelmiä tai palveluja, joita REDU rekisterinpitäjänä ei ole hankkinut käyttönsä. REDUn henkilökuntaan kuuluva tai ulkopuolinen palvelutuottaja, joka käsittelee REDUn rekisteröityjen (asiakkaat, opiskelijat, henkilökunta, yms) henkilötietoja, ei saa käyttää henkilötietojen käsittelyssä tietojärjestelmää tai palvelua, jota REDU ei ole hankkinut käyttöönsä tai jonka käytöstä REDU rekisterinpitäjänä ei ole sopinut henkilötietojen käsittelijän kanssa. Esim. ns. kuluttajille tai yksityiskäyttöön tarkoitettujen ilmaisohjelmien-, sovellusten- ja palvelujen sekä demo-versioiden käyttö REDUn henkilötietojen käsittelyssä on kielletty.

Lisätietoja REDUn käytössä olevista tietojärjestelmistä ja -palveluista antaa REDUn ICT-palvelut.

3.6 Tietosuojan riskien tunnistaminen ja tietosuojavaikutusten arviointi

3.6.1 Yleistä tietosuojan riskeistä

Lyhyesti:
- Rekisterinpitäjänä REDUn on tunnistettava, sisältyykö henkilötietojen käsittelyyn riskejä rekisteröidylle.
- Tietosuojariskejä tarkastellaan esisijaisesti rekisteröidyn näkökulmasta, mutta ne voivat olla samalla riskejä REDUlle, esim. maineen menetys, taloudellinen menetys.
- Tietosuojariskien tunnistaminen (kartoittaminen) on tehtävä aina, kun aletaan käsittelemään henkilötietoja uudella tavalla ja/tai kun hankintaan uutta tietojärjestelmää tai nykyiseen tietojärjestelmään tehdään merkittävä päivitys tai uudistus.
- Mikäli tietosuojariskien kartoituksessa todetaan, että ns. korkean riskin kriteerit täyttyvät, on tehtävä **tietosuojavaikutusten arviointi** ja tämä arviointi on myös dokumentoitava.
- Tietosuojariskien tunnistaminen ja tietosuojavaikutusten arvioinnit ovat osa rekisterinpitäjän osoitusvelvollisuutta.
- Rekisterinpitäjänä REDUn on pyydettävä tietosuojaviranomaiselta ennakkokuuleminen, jos ns. korkeita tietosuojariskejä ei voida poistaa tai niiden vaikutusta vähentää merkittävästi.

Rekisterinpitäjänä REDUn on arvioitava henkilötietojen käsittelyyn rekisteröidylle liittyviä tietosuojariskejä aina, ennen kuin se ryhtyy käsittelemään henkilötietoja.

Tietosuojariskien arviointi tehdään aina rekisteröidyn näkökulmasta eli on arvioitava mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja millaista vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Rekisteröidylle aiheutuvat vahingot voivat olla aineellisia tai aineettomia esim.

- rekisteröity voi joutua petoksen kohteeksi
- rekisteröityydelle aiheutuu taloudellisia menetyksiä
- rekisteröidyn maineen menetys tai muu sosiaalinen vahinko
- pseudonymisoidussa käsittelyssä paljastuu henkilöllisyys.

Riskien arvioinnin avulla REDU tunnistaa jo suunnitteluvaiheessa ne toimenpiteet, joihin sen on ryhdyttävä riskien hallitsemiseksi ja henkilötietojen asianmukaisen käsittelyn turvaamiseksi. REDUn on myös varmistettava myös tietosuojaperiaatteiden tehokas toteutuminen suhteessa käsittelyyn liittyvään riskiin. Lisätietoa: https://tietosuoja.fi/arvioi-riskit

3.6.2 Korkeiden riskien tunnistaminen (alkukartoitus)

Lyhyesti:

- Kartoita, sisältyykö henkilötietojen käsittelyyn korkea riski, voit käyttää apuna REDUn alkukartoitustestiä (pika-arviointi).
- Jos vähintään kaksi korkean riskin kriteeriä täyttyy, tee tietosuojavaikutusten arviointi.
- Kysy tarvitessa tietosuojavastaavalta tai tietosuoja-asiantuntijalta neuvoja ja opastusta.

Tietosuojavaltuutetun toimisto on määritellyt kriteerit korkean tietosuojariskin arvioimiseksi. Kriteerit on esitetty taulukossa 3.

TAULUKKO 3. Kriteerit korkean riskin arvioimiseksi (Tietosuojavaltuutetun toimisto, Vaikutustenarviointi)

Korkean tietosuojariskin kriteeri	Määritelmä
Henkilötietojen arviointi tai pisteytys	Rekisteröidyn työsuorituksen, taloudellisen tilanteen, terveyden, henkilökohtaisten mieltymysten, kiinnostuksen kohteiden, luotettavuuden, käyttäytymisen, sijainnin tai liikkumisen arviointi tai pisteytys (mukaan lukien profilointi ja ennakointi).
Automaattinen päätöksenteko, jolla on oikeusvaikutuksia	Kun henkilötietojen perusteella tehdään rekisteröityyn kohdistuvia päätöksiä automaattisesti ja päätöksillä on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia.
Rekisteröidyn järjestelmällinen valvonta	Henkilötietoja kerätään olosuhteissa, joissa rekisteröidyt eivät välttämättä ole tietoisia siitä, kuka kerää heidän tietojaan ja miten niitä tullaan käyttämään. Lisäksi yksittäisten henkilöiden voi olla mahdotonta välttyä joutumasta tällaisen tietojenkäsittelyn kohteeksi julkisissa tai yleisölle avoimissa tiloissa. Valvonnalla voidaan tarkoittaa esimerkiksi kulunvalvontaa, kameravalvontaa tai vastaavia toimenpiteitä.
Erityisiin henkilötietoryhmiin tai muuten hyvin henkilökohtaisten tietojen käsittely	Tähän ryhmään kuuluvat tietosuoja-asetuksen erityiset henkilötietoryhmät sekä rikoksia ja rikkomuksia koskevat henkilötiedot. Tämän kriteerin alle voi kuulua myös henkilökohtaisia asiakirjoja, kuten sähköposteja, päiväkirjoja, muistiinpanotoiminnolla varustetun e-kirjan lukulaitteen muistiinpanoja ja henkilökohtaisen elämän tallentamiseen tarkoitettujen lifelogging-sovellusten hyvin henkilökohtaisia tietoja.
Tietojen laajamittainen käsittely	Laajamittaisuutta arvioitaessa suositellaan ottamaan huomioon muun muassa seuraavat asiat: - rekisteröityjen lukumäärä, joko täsmällisenä lukuna tai osuutena tietystä ryhmästä, kuten kaupungin tai valtion väestöstä - käsiteltävien tietojen määrä ja/tai käsiteltävien erillisten tietoyksikköjen määrä - tietojenkäsittelytoimen kesto tai pysyvyys - käsittelytoimen maantieteellinen ulottuvuus.
Tietokokonaisuuksien yhdistäminen	Tietokokonaisuuksien yhteen sovittaminen tai yhdistäminen rekisteröidyn kannalta ennakoimattomalla ja odottamattomalla tavalla. Esim. yhdistämällä kahteen täysin eri käyttötarkoitukseen tarkoitettuja tietoja tai yhdistetään eri toimijoiden asiakasrekistereitä.
Heikommassa asemassa olevan henkilötietojen käsittely	Rekisteröidyn voi olla vaikeaa esimerkiksi vastustaa tietojensa käsittelyä tai käyttää muita oikeuksiaan, jos hän on heikossa asemassa rekisterinpitäjään nähden. Heikossa asemassa olevilla tarkoitetaan esimerkiksi lapsia, työntekijöitä, ikääntyneitä ja turvapaikanhakijoita.
Uuden teknologian tai organisatorisen ratkaisun soveltaminen tai innovatiivinen käyttö	Uuden teknologian käyttöön voi liittyä uudenlaisia tietojen keräämisen ja käytön muotoja, joihin mahdollisesti liittyy henkilöiden oikeuksiin ja vapauksiin kohdistuva korkea riski. Esimerkiksi tietyillä esineiden internet (IoT) -sovelluksilla voi olla huomattava vaikutus ihmisten arkielämään ja yksityisyyteen.

Mikäli taulukossa 3 esitetyistä kriteereistä vähintään kaksi kriteeriä täytyy, tietosuojavaikutusten arviointi on tehtävä ennen käsittelyn aloittamista. Tietosuojavaltuutetun toimisto saattaa antaa lisää tai tarkentavia ohjeita em. korkean riskin kriteereihin, joten uusimmat kriteerit on syytä tarkistaa Tietosuojavaltuutetun toimiston sivulta osoitteesta: https://tietosuoja.fi/vaikutustenarviointi

REDUn tietosuojan alkukartoitus ja tietosuojariskien pikaitsearviointi -testi
REDUssa on käytössä tietosuojariskien alkukartoitus -testilomake, jonka avulla henkilötietojen käsittelyä tai siihen liittyvää hankintaa suunnitteleva voi arvioida, sisältyykö suunniteltuun käsittelytoimintoon tai hankittavaan tietojärjestelmään korkea riski. Kyseinen itsearviointi-testi perustuu taulukossa 3 esitettyihin kriteereihin.

Lomakkeen linkki ja ohje sen käyttämiseen löytyvät REDUn ROKKI-intrasta sivulta:
Tietosuojan riskien ja tietosuojavaikutusten arviointi (TVA)

Testitulos on suuntaa antava ja täytetty lomake toimii samalla dokumentaationa siitä, että tietosuojan riskejä on kartoitettu.

REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija auttavat ja neuvovat riskien tunnistamisessa ja korkean riskin kriteereiden arvioinnissa.

3.6.3 Tietosuojavaikutusten arviointi

Lyhyesti:
- Tietosuojavaikutusten arviointi on tehtävät, mikäli käsittely sisältää korkean riskin.
- Arviointi on tehtävä ennen kuin rekisteröityjen henkilötietojen käsittely aloitetaan uudella tavalla tai uudella tietojärjestelmällä.
- Jos korkeita riskejä ei saa poistettua, käsittelyä ei saa aloittaa ennen kuin tietosuojaviranomaista on kuultu
- Suositeltavaa on tehdä arviointi jo suunnitteluvaiheessa ennen tietojärjestelmän tai ulkoistetun henkilötietojen käsittelyn palvelun hankintaprosessin käynnistämistä, jotta saadaan hankittua sellainen tuote tai palvelu, joka täyttää arvioinnissa määritellyt tietosuojariskien poistamisen tai vähentämisen laatukriteerit.

Ennen kuin henkilötietojen käsittelyssä otetaan käyttöön uutta teknologiaa tai käsittelyprosessi, jossa käsittelyn luonne, laajuus ja tarkoitus huomioon ottaen voi aiheuttaa rekisteröitävän henkilön oikeuksien ja vapauksien kannalta korkean riskin, on ennen käsittelyn aloittamista tehtävä tietosuojavaikutusten arviointi.

Mikäli korkean riskin kriteerit täyttyvät, tietosuojavaikutusten arviointi on tehtävä ennen käsittelyn aloittamista! Korkea riski täytyy, kun kaksi tai useampia kohdan 3.6.3 taulukossa 3 esitettyjä kriteereitä täytyy.

Tietosuojavaikutusten arviointi on suositeltavaa tehdä jo suunnitteluvaiheessa ennen kuin käynnistetään siihen liittyvä henkilötietojen käsittelyn tai tietojärjestelmän hankintaprosessin tarjouspyyntömenettely. Näin voidaan jo tarjouspyynnössä tarkentaa hankinnan laatuvaatimuksia esim. tietoturvan ja toiminnallisuuksien suhteen siten, että niissä poistetaan tai vähennetään arvioinnissa arvioituja korkean riskin tietosuojariskejä.

Tietosuojavaikutusten arvioinnin tekemisestä vastaa käsittelytoiminnosta vastaava (vastuullinen johto) tai hänen nimeämänsä käsittelytoiminnon yhteyshenkilö esim. hankintaa valmisteleva henkilö. REDUn tietosuojavastaava tai Santasportin tietosuoja-asiantuntija neuvovat ja opastavat arvioinnin toteuttamisessa ja voivat olla siinä mukana, mutta heitä ei voi nimetä arvioinnin tekijöiksi.

Tietosuojavaikutusten arvioinnissa kuvataan henkilötietojen käsittelyprosessi, arvioidaan sen oikeasuhteisuutta ja tarpeellisuutta, käydään läpi rekisteröidyn oikeudet ja niitä edistävä toimet sekä kuinka hallitaan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä. Näiden osalta tarkennetaan mitä ne ovat, mikä on niiden todennäköisyys ja vakavuus ja mitä riskin poistamiseksi tai vähentämiseksi tehdään ja milloin. Arvioinnissa kuvataan myös suunnitellut toimenpiteet riskeihin puuttumiseksi (poistamiseksi tai vähentämiseksi).

Tietosuojavaikutusten arviointiin on REDUssa käytössä lomakepohjat ja mallit. Näiden lisäksi voidaan käyttää tietosuojaviranomaisen tietosuojavaikutusten työkalua. Nämä löytyvät ROKKI-intrasta Tietosuojan riskien ja tietosuojavaikutusten arviointi (TVA) -sivulta.

Tietosuojavaikutusten arviointiraportti on REDUn sisäinen asiakirja. Mikäli arviointiraportti sisältää Julkisuuslain 24 § 1, mom. lueteltuja salassa pidettäviä tietoja, raportti luokitellaan salaiseksi. Tietosuojaviranomainen voi pyytää arviointiraportin nähtäväkseen, myös salaiseksi luokitellun, esim. kun tutkitaan tietoturvaloukkausta tai rekisteröidyn tekemää kantelua viranomaiselle. Arviointiraportti on myös toimitettava tietosuojaviranomaiselle, mikäli siltä haetaan ennakkokuulemista ennen korkean riskin käsittelyn aloittamista kts. kohta 3.6.4.

Valmiin arviointiraportin, joka sisältää myös suunnitelman toimenpiteistä riskeihin puuttumiseksi vahvistavat allekirjoituksillaan valmistelija ja vastuullinen johtaja. Vastuullinen johtaja myös vastaa, että arviointiraportissa suunnitellut toimenpiteet riskeihin puuttumiseksi ja poistamiseksi toteutetaan.

Tietosuojavaikutusten arviointi on tarvittaessa päivitettävä, mikäli käsittelytoiminto muuttuu oleellisesti tai tulee ilmi uusia tai aiemmin tunnistamattomia uhkia tai aiemmin valitut riskejä vähentävät tai poistavat suojaustoimet eivät enää suoraa riittävästi siten, että käsittely muuttuu tai on muuttunut korkean riskin käsittelyksi.

Raportit arkistoidaan REDUn tiedonohjaussuunnitelman (TOS) mukaisesti. Allekirjoitetun raportin kopio toimitetaan REDUn tietosuojavastaavalle, joka ylläpitää luetteloa tehdyistä tietosuojavaikutusten arvioinneista.

Mikäli edellä tietosuojavaikutusten arvioinnin perusteella todetaan, että käsittely aiheuttaisi edelleen korkean riskin, ja jota ei voida REDUn omin toimenpitein pienentää, on REDUn ennakkokuultava asiassa tietosuojavaltuutettua (viranomaista) tietosuoja-asetuksen 36 artiklan mukaisesti, ennen kuin henkilötietojen käsittely uudella tai muutetulla tavalla aloitetaan.

3.6.4 Ennakkokuuleminen, kun korkeaa riskiä ei voida poistaa

Henkilötietojen käsittelyä ei saa aloittaa tietosuojavaikutusten arvioinnin jälkeen, mikäli käsittelyyn edelleen sisältyy korkea riski. Käsittelyn aloittaminen on kuitenkin korkean riskin tapauksissa mahdollista, mikäli tietosuojaviranomaista eli Tietosuojavalutettua on ennakkokuultu asiasta.

Ennakkokuuleminen voidaan toteuttaa vasta REDUn oman tietosuojavaikutusten arvioinnin jälkeen. REDUn arviointiraportti toimitetaan osana ennakkokuulemista viranomaiselle.

Tietosuojaviranomainen antaa ennakkokuulemisessa REDUlle kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi. Tarvittaessa viranomainen voi ennakkokuulemisen yhteydessä käyttää myös sille tietosuoja-asetuksessa annettuja toimivaltuuksia, kuten

varoitusta. REDUn tai sen lukuun henkilötietoja käsittelevän on toteuttava ohjeen mukaiset lisätoiminpiteet ennen henkilötietojen käsittelyn aloittamista. Käsittely on vasta tämän jälkeen lainmukaista.

Lisätietoa: https://tietosuoja.fi/ennakkokuuleminen.

3.7 Tietosuojapoikkeamat ja tietoturvaloukkaukset

3.7.1 Milloin on kyse tietosuojapoikkeamasta ja milloin tieturvaloukkauksesta

Lyhyesti:
- **Tietosuojapoikkeamassa** on kyse tapauksesta tai toiminnasta, jossa ei ole noudatettu tietosuojalainsäädäntöä, REDUn antamia tietoturva- ja tietosuojaohjeita tai henkilötietojen käsittelijää tai rekisterinpitäjää velvoittavia tietosuojasopimuksia.
- Tietosuojapoikkeamassa ei ole tapahtunut tietoturvaloukkausta, mutta se voi johtaa sellaiseen tai se voi johtaa REDUlle määrättävään hallinnolliseen maksuun tai henkilötietojen käsittelykieltoon.
- **Tietoturvaloukkauksessa** henkilöntietoja tuhoutuu, häviää, muuttuu tai sivullinen pääsee niihin tavalla tai toisella ja se aiheuttaa rekisteröidylle korkean tietosuojariskin.

Tietosuojapoikkeama
Tietosuojalainsäädäntö velvoittavana koskee kaikkia EU/ETA-alueella toimivia rekisterinpitäjiä ja henkilötietojen käsittelijöitä. REDU rekisterinpitäjänä vastaa opiskelijoiden, asiakkaiden, kumppaneiden ja henkilökunnan eli rekisteröityjen henkilötietojen käsittelystä ja että siinä toimitaan tietosuojalainsäädännön mukaisesti. Lainsäädäntö velvoittaa myös REDUn henkilökuntaa, johtoa, luottamushenkilöitä ja sopimustoimittajia, kun he käsittelevät REDUn rekisteröityjen henkilötietoja.

REDUlla on rekisterinpitäjänä velvoite ohjeistaa ja/tai sopia henkilötietojen käsittelystä ja nämä ohjeet ja sopimukset velvoittavat henkilötietojen käsittelijöitä. Ohjeistamisen tulee olla selkeää ja mieluiten kirjallista, jotta jälkikäteen on mahdollista osoittaa, että ohjeistusta on annettu. Tietosuojaohjeista REDUssa päättää tai sopii ulkopuolisten toimittajien kanssa vastuullinen johto johtamisjärjestelmän ja hallintosäännön mukaisesti. Myös esihenkilöiden antamat tietosuojaohjeet ovat henkilöstöä velvoittavia. Mm. tämä REDUn Tietosuojaperiaatteet ja tietosuojan yleisohje on yksi näistä rekisterinpitäjän velvoittavista ohjeista. Tietosuojavastaava ja Santasportin tietosuoja-asiantuntija antavat ohjeistukseen liittyvää neuvontaa.

Tietosuojapoikkeamalla REDUssa tarkoitetaan tapahtumaa tai toimintaa, jossa ei ole menetelty em. tietosuojalainsäädännön, REDUn tietoturva- ja tietosuojaohjeiden ja tietosuojasopimusten mukaisesti eli on tapahtunut poikkeama. Tietosuojapoikkeama eroaa tietoturvaloukkauksesta siinä, että siinä ei ole vielä tapahtunut varsinaista henkilötietojen tietoturvaloukkausta. Poikkeaman korjaamisella on tarkoitus ennaltaehkäistä, ettei mahdollista tietoturvaloukkausta syntyisi jatkossa ja että rekisterinpitäjän velvoitteet tulevat hoidetuksi ja näin ennalta ehkäistään myös mahdollisia rekisterinpitäjälle tulevia hallinnollista maksuja tai korvausvaatimuksia.

Tietoturvaloukkaus
Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. (Tietosuojavaltuutetun toimisto, Tietoturvaloukkaukset ja Tietosuoja-asetus, 4 artikla, kohta 12.)

Tietoturvaloukkaus saattaa tapahtua esim.:
- Henkilötietojen käsittelijän toimesta vahingossa, huolimattomuuttaan, osaamattomuuttaan tai tuottamuksellisesti (tietosuojarikos).
- Tietovuodosta, esim. tietojärjestelmän virhetoiminto tai puutteellinen tietoturva.
- Tietomurrosta, hakkeroinnista, haittaohjelmasta, kyperhyökkäyksestä.
- Palvelunestohyökkäys.
- Laaja tai pitkäaikainen käyttökatkos, sähkökatko, jos se vaikuttaa suoraan rekisteröidyn oikeuksiin ja vapauksiin.
- Murtautuminen tiloihin ja pääsy manuaalisesti säilytettäviin henkilötietoihin.
- Tulipalo, palvelimen rikkoutuminen (tietojen häviäminen).

Tietoturvaloukkauksessa on siis jo tapahtunut tai mahdollisesti tapahtunut henkilötietojen tietoturvan loukkaus. Silloin kun on epäselvää, onko kyseessä mahdollisesti tietoturvaloukkaus vai ei, käsitellään se aina lähtökohtaisesti tietoturvaloukkauksena.

Tietoturvaloukkauksesta silloin, kun kyse on henkilötiedoista, voidaan käyttää myös käsitettä tietosuojaloukkaus, vaikka tietosuojalainsäädäntö käyttää käsitettä tietoturvaloukkaus. Tietoturvaloukkaus voi koskea myös muita kuin henkilötietoja, jolloin kyse ei varsinaisesti ole tietosuojalainsäädännössä tarkoitetusta henkilötietojen tietoturvaloukkauksesta.

Lisätietoa: https://tietosuoja.fi/tietoturvaloukkaukset.

3.7.2 Tietosuojapoikkeamasta ja turvaloukkauksesta ilmoittaminen ja tiedon saaminen

Jos havaitset tietosuojapoikkeaman tai tietoturvaloukkauksen, ilmoita siitä välittömästi
REDUn tietosuojavastaavalle tai Santasportin tietosuoja-asiantuntijalle (tietosuojavastaava@redu.fi) tai ICT-palveluihin (servicedesk@redu.fi).

Käytä ilmoittamisessa edellä mainittuja organisaatio -sähköpostiosoitteita henkilökohtaisten osoitteiden sijaan, sillä niihin lähetyt viestit ohjautuvat mm. henkilöiden vuosilomien aikaan tehtävää hoitavalle sijaiselle.

Havaitusta tietosuojapoikkeamasta tai tietoturvaloukkauksesta on ilmoitettava viivyttelemättä. Ilmoitusvelvollisuus koskee kaikkia REDUn palveluksessa olevia. Ilmoituksen voi tehdä REDUn tietosuojavastaavalle, Santasportin tietosuoja-asiantuntijalle tai ICT-palveluihin.

Mitä nopeammin tieto on saatu, sitä nopeammin sen vaatimiin toimenpiteisiin voidaan ryhtyä. Jos kyse on tietoturvaloukkauksesta, nopea ilmoittaminen auttaa myös vähentämään tai poistamaan siitä mahdollisesti rekisteröidylle aiheutunutta haittaa tai vahinkoa.

Havaitsijan ei pidä ryhtyä pohtimaan, onko ilmoitettava tietosuojapoikkeama tai tietoturvaloukkaus kyseessä tai onko sillä merkitystä. REDUn tietosuojavastaava, Santasportin tietosuoja-asiantuntija tai ICT-palvelut auttavat asian selvittämisessä.

Ilmoitusvelvollisuus koskee myös niitä tapauksia, joissa henkilökuntaan kuuluva on itse omalla toiminnallaan aiheuttanut tai mahdollisesti aiheuttanut tietosuojapoikkeaman tai tietoturvaloukkauksen.

Tietosuojapoikkeamasta ja tietoturvaloukkauksesta voi tulla tieto myös tietosuojaviranomaiselta (Tietosuojavaltuutetun toimisto) tai muulta toimivaltaiselta viranomaiselta. Tieto voi tulla myös henkilötietojen käsittelijältä, esim. tietojärjestelmän ylläpitäjältä tai toiselta organisaatiolta, joka on asian havainnut. Myös rekisteröity voi tehdä ilmoituksen havaitsemastaan tietosuojapoikkeamasta tai tietoturvaloukkauksesta.

Tietosuojapoikkeaman ilmoittamisessa voidaan käyttää myös REDUn sisäistä väärinkäytösten ilmoituskanavaa (tulossa käyttöön 2023), mutta sitä ei suositella käytettävän tietoturvaloukkausten sekä kiireellistä käsittelyä vaativien tietoturvapoikkeamien ilmoittamiseen, sillä ilmoituskanavan kautta tieto ei tule suoraan ja käsittelyyn tulee siten tarpeetonta viivettä.

Tietosuojapoikkeamasta tai tietoturvaloukkauksesta ilmoittaneelle vastataan, että ilmoitus on vastaanotettu. Tapauksesta riippuen ilmoittajaa informoidaan myös, miten käsittely etenee ja kuka tai ketkä vastaavat asian käsittelystä.

3.7.3 Tietosuojapoikkeaman dokumentointi ja käsittely

Lyhyesti:
- Tietosuojapoikkeamista pidetään kirjaa (luetteloa).
- Tietosuojapoikkeamista ilmoitetaan aina käsittelytoiminnosta vastuulliselle johdolle ja yhteyshenkilölle.
- Tietosuojavastaava ja tietosuoja-asiantuntija voivat antaa neuvoja poikkeaman korjaamiseksi. Johto päättää toimenpiteistä poikkeaman korjaamiseksi.
- Vastuullisen johto vastaa siitä, että tehdään tarvittavat korjaavat toimenpiteet.
- Johto voi myös päättää, että mitään ei tehdä poikkeaman korjaamiseksi. Tämä päätös on perusteltava.
- Tietosuojavastaavalle tai tietosuoja-asiantuntijalla on ilmoitettava, kun korjaavat toimenpiteet on tehty tai jos on päätetty, että mitään ei tehdä, jotta poikkeamatapaus voidaan kirjata käsitellyksi.
- Mikäli poikkeamailmoitus on tullut REDUn sisäisen ilmoiskanavan tai oikeuskanslerin viraston keskitetyn ilmoituskanavan kautta, asian käsittelyn toimenpiteet dokumentoidaan ko. ohjeistuksen mukaisesti.

Havaituista ja tiedoksi saaduista tietosuojapoikkeamista REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija pitävät kirjaa ja ne diarioidaan. Poikkeamat kirjataan REDUn tietosuojapoikkeamat ja tietoturvaloukkaukset -luetteloon. Luettelon ylläpito on osa rekisterinpitäjän osoitusvelvollisuutta (kts. kohta 2.9).

REDUn tietosuojavastaava tai Santasportin tietosuoja-asiantuntija ilmoittaa poikkeamasta ko. käsittelytoiminnosta vastaavalle johdolle ja yhteyshenkilölle aina kirjallisesti sähköpostilla ja kiiretilanteessa tarvittaessa lisäksi esim. puhelimitse. Jos kyse on tietojärjestelmästä, asiasta ilmoitetaan heti myös ICT-palveluihin. Poikkeamailmoituksen viestin otsikkoon lisätään poikkeaman diaarinumero. Mikäli asia koskee tiettyä REDUn henkilökuntaan kuuluvaa tai kuuluvia, poikkeamasta ilmoitetaan henkilön esihenkilölle. Poikkeamailmoituksessa tietosuojavastaava tai tietosuoja-asiantuntija voi antaa poikkeaman korjaamiseksi neuvontaa.

Poikkeaman käsittelystä vastaa aina ko. käsittelytoiminnon vastaava johtaja tai hänen nimeämänsä, esim. käsittelytoiminnon yhteyshenkilö tai esihenkilö, ja jos kyseessä on tietojärjestelmä, ICT-palvelut ja/tai palveluntoimittaja sopimuksen mukaisesti.

Poikkeaman käsittelyn tarkoituksena on korjata tai muuttaa REDUn tai REDUn käyttämän sopimustuottajan toimintaa siten, että henkilötietojen käsittelyn tietosuoja ja tietoturva paranevat ja ko. toimenpitein estetään mahdollinen tietoturvaloukkaus tulevaisuudessa. Näin vähennetään rekisteröidyn tietosuojariskiä tai REDUlle rekisterinpitäjänä ja henkilötietojen käsittelijälle mahdollisesti tulevia hallinnollisia maksuja, vahingonkorvausvaatimuksia tms. Rekisterinpitäjälle ja henkilötietojen käsittelijälle voidaan antaa hallinnollinen seuraamusmaksu (EU:n Yleinen tietosuoja-asetus, artiklat 58 ja 83) tai tuomita tietosuojarikoksesta tai muusta siihen liittyvästä tieto- tai viestintärikoksesta sakkoa tai vankeutta (Rikoslaki, 38. luku).

Tarvittaessa esihenkilön on annettava alaisilleen esim. työnjohdollinen määräys, mikäli poikkeaman korjaaminen sitä edellyttää sekä valvoa, että määräys tulee toteutetuksi. Suositeltavaa on antaa ja toimittaa tämä työnjohdollinen määräys kirjallisena, jolloin se voidaan myös jälkikäteen todentaa. Jos kyse on sopimuksella ulkoistetusta henkilötietojen käsittelystä, käsittelytoiminnosta vastaavan johdon tai yhteyshenkilön on otettava yhteyttä sopimustoimittajaan asian korjaamiseksi tai asiasta on tehtävä reklamaatio.

Tietosuojavastaavan tai tietosuoja-asiantuntijan ilmoittama tietosuojapoikkeus ja siihen mahdollisesti esittämä korjausvaihtoehto (neuvonta) ei ole johtoa tai esihenkilöä velvoittava. Vastuullinen johto tai esihenkilö päättää aina korjaavista toimenpiteistä. Johto tai esihenkilö voi myös päättää, että poikkeama-asialle ei tehdä mitään. Tällöin vastuullisen johdon tai esihenkilön on tällöin perusteltava, miksi poikkeamaa ei korjata.

Poikkeaman käsittelijän on vastattava tietosuojapoikkeamasta ilmoittaneelle REDUn tietosuojavastaavalle tai Santasportin tietosuoja-asiantuntijalle mihin toimenpiteisin on ryhdytty tai mitä toimenpiteitä on tehty tai jos korjaaviin toimenpiteisiin ei ryhdytä sekä millä perusteella poikkeamaa ei korjata. Poikkeaman käsittely jää ns. auki eli ”käsittelyssä” tilaan siihen saakka, kunnes asiasta on ilmoitettu tietosuojavastaavalle tai tietosuoja-asiantuntijalle.

Tietosuojavastaava tai tietosuoja-asiantuntija voi tämän tiedon saatuaan kirjata tapahtuman tilaksi ”päätetty”, mikäli asia on käsitelty loppuun. Luetteloon kirjataan myös toimenpiteet, mitkä on tehty poikkeaman korjaamiseksi tai millä perusteella poikkeamaa ei korjata.

Tietosuojavastaava tai tietosuoja-asiantuntija voi myös todeta ja kirjata poikkeaman päätetyksi siinä tilanteessa, että poikkeama on todistettavasti poistunut tai korjautunut.

Mikäli poikkeamailmoitus on tullut REDUn väärinkäytösten sisäisen ilmoituskanavan kautta, (tulee käyttöön 2023) asian käsittely dokumentoidaan myös ko. järjestelmään. Ilmoituskanavan kautta tulleiden ilmoitusten käsittelystä annetaan omat ohjeet 2023.

3.7.4 Tietoturvaloukkauksen käsittelyn vaiheet ja käsittelyn organisointi

Lyhyesti:
- Tietoturvaloukkauksiin on reagoitava ja ne on käsiteltävä viivyttelemättä.
- Loukkausten käsittelystä vastaa käsittelytoiminnosta vastaava johto.
- Laajoissa ja merkittävissä tietoturvaloukkauksissa ja kyberiskuissa tietoturvaloukkauksen käsittelystä vastaa REDUn kriisijohto yhteistyössä tietosuojavastaavan ja/tai tietosuoja-asiantuntijan kanssa.

Tietoturvaloukkauksen käsittely sisältää seuraavat työvaiheet:
- Tietoturvaloukkauksen riskin arviointi.
- Tietoturvaloukkauksesta ilmoittaminen viranomaisille ja rekisteröidylle.
- Tietoturvaloukkauksen dokumentointi.

Tietoturvaloukkauksessa on jo tapahtunut henkilöntietojen tuhoutuminen, häviäminen, muuttuminen tai niihin on päässyt sivullinen tavalla tai toisella ja se aiheuttaa rekisteröidylle korkean tietosuojariskin. Kts. tietoturvaloukkauksen määritelmä kohdasta 3.7.1. Tietoturvaloukkaus voi olla myös osa tahallista kyberiskua.

Tietoturvaloukkauksiin on reagoitava ja ne on käsiteltävä viivyttelemättä. Tarvittaessa ns. normaali toiminta on keskeytettävä asian käsittelemiseksi.

Suppeissa eli vain muutamia rekisteröityjä koskevissa tietoturvaloukkauksissa sekä vähäisen tai kohtalaisen riskin tapauksissa tietoturvaloukkauksen käsittelystä vastaa käsittelytoiminnosta vastaava johto ja yhteyshenkilö yhteistyössä REDUn tietosuojavastaavan tai Santasportin tietosuoja-asiantuntijan kanssa. Tarvittaessa käsittelyyn kutsutaan mukaan henkilötietojen käsittelyyn osallistuneita henkilöitä ja/tai heidän esihenkilöitä sekä sopimustoimittajia.

Laajasti ja suurta määrää rekisteröityjä koskevissa tietoturvaloukkauksissa, kun niihin sisältyy korkea riski, tai jos kyseessä on ns. kyberisku, tietoturvaloukkauskäsittelyä varten kutsutaan koolle REDUn kriisijohtoryhmä.

Kriisijohtoryhmän koolle kutsumista esittää REDUn tietosuojavastaava, Santasportin tietosuoja-asiantuntija, tietohallinnosta tai ICT-palveluista vastaava, kuntayhtymän johtaja tai varajohtaja. Kriisijohtoryhmän koolle kutsumisesta ja kriisiviestinnästä on REDUssa erilliset ohjeet ja suunnitelmat.

Kun kyse on henkilötietojen käsittelyn tietoturvaloukkauksesta, kriisijohtoryhmään osallistuu myös REDUn tietosuojavastaava ja/tai Santasportin tietosuoja-asiantuntija. Tämä on tärkeää, sillä tietosuojavastaava, tai hänen poissa ollessaan vara-tietosuojavastaavana toimiva Santasportin tietosuoja-asiantuntija, vastaa yhteydenpidosta tietosuojaviranomaisen kanssa.

Tietoturvaloukkauksen käsittelyn vaiheet ja dokumentointi on esitetty tarkemmin kohdissa 3.7.5–3.7.7.

3.7.5 Tietoturvaloukkauksen riskin arviointi

Lyhyesti:
- Tietoturvaloukkauksesta aiheutunut riski rekisteröidylle arvioidaan.
- Tietoturvaloukkauksesta aiheutuneen riskin arvioi REDUn tietosuojavastaava.
- Riskin perusteella päätetään, mihin toimenpiteisiin ryhdytään.
- Korkean riskin tapaukset ilmoitetaan aina tietosuojaviranomaiselle ja rekisteröidyille.
- Viranomaiselle ilmoittamisesta päättää riippumattomasti REDUn tietosuojavastaava.

Kun on epäselvää, onko tapahtunut tietoturvaloukkaus vai onko kyse mahdollisesta tietoturvaloukkauksesta, asia käsitellään tietoturvaloukkauksena.

Kun tieto tietoturvaloukkauksesta on saatu tai havaittu, REDUn tietosuojavastaava tai Santasportin tietosuoja-asiantuntija arvioi ensiksi minkä tasoinen riski siitä on tai mahdollisesti tulee kohteena oleville rekisteröidyille. REDUssa on käytössä riskiasteikko:

- ei riskiä,
- vähäinen,
- kohtalainen ja
- korkea riski.

Arvioinnissa tarkastellaan tapahtunutta tietoturvaloukkausta rekisteröidyn vapauksien ja oikeuksien näkökulmasta. Ei riskiä -tapauksia ovat mm. sellaiset tapaukset, joissa on kyse muusta, kuin henkilötietojen käsittelyn tietoturvaloukkauksesta.

Arvioinnin tekemiseksi tietosuojavastaava tai tietosuoja-asiantuntija pyytää tarvittaessa lisätietoja ilmoittajalta, käsittelytoiminnosta vastaavalta johdolta, yhteyshenkilöltä, ICT-palveluista, henkilötietojen käsittelijältä ja/tai rekisteröidyltä. Riskin taso voi käsittelyn aikana muuttua (nousta tai laskea) sen mukaan, mitä tietoa tietoturvaloukkauksesta on saatu.

Riskin taso määrittää ne toimenpiteet, joihin REDUssa on ryhdyttävä. Kaikki tietoturvaloukkaukset, lukuun ottamatta ”ei riskiä” -tapaukset, kirjataan REDUn tietosuojapoikkeamat ja tietoturvaloukkaukset tiedostokirjastoon ”tietoturvaloukkauksina”. Kaikki korkean riskin tapaukset ilmoitetaan Tietosuojavaltuutetun toimistoon ja rekisteröidyille ja jos kyse on kyberiskusta, tehdään myös ilmoitus Kyberturvallisuuskeskukselle ja rikostapauksessa myös Poliisille.

Kohtalaisen riskin tapauksissa käytetään tapauskohtaista arviointia, täyttyykö ns. ilmoituskynnys. Tietosuojaviranomainen on antanut esimerkkejä, milloin tulee ilmoitus tehdä ja milloin sitä ei tarvitse tehdä.

Lisätietoa: https://tietosuoja.fi/tietoturvaloukkaukset

Esimerkkiluettelo (Viitattu 31.10.2022)
https://tietosuoja.fi/documents/6927448/8214536/Esimerkkej%C3%A4+tietoturvaloukkauksista/754c16aa-152e-4f15-a458-d1579c5ea4b2/Esimerkkej%C3%A4+tietoturvaloukkauksista.pdf?t=1536128589000v

3.7.6 Tietoturvaloukkauksesta ilmoittaminen viranomaisille ja rekisteröidylle

Lyhyesti:

Ilmoittaminen viranomaisille:

- Tietoturvaloukkauksen ilmoituksen tietosuojaviranomaiselle tekee aina REDUn tietosuojavastaava tai hänen ollessa estyneenä varatietosuojavastaava. Hän myös päättää riippumattomasti tehdäänkö ilmoitus vai ei.
- Tietoturvaloukkauksesta ilmoitetaan myös Kyberturvallisuuskeskukselle silloin kun siihen liittyy tietojen kalastelua, palvelunestohyökkäys tai niiden yritys.
- Tietoturvaloukkauksesta voidaan myös tehdä rikosilmoitus Poliisille, jos selviää, että se johtuu rikollisesta toiminnasta.
- Kyberturvallisuustapauksissa Ilmoittamisesta vastaa Kyberturvallisuuskeskuksella ja Poliisille vastaa ensisijaisesti ICT-palvelut.

Ilmoittaminen rekisteröidyille:

- Tietoturvaloukkauksesta ilmoittamisesta rekisteröidylle vastaa aina käsittelytoiminnosta vastaava johto ja/tai yhteyshenkilö.
- Tietoturvaloukkauksesta laajemmin esim. julkisissa viestintäkanavissa tiedottaessa toimitaan REDUn viestintäohjeiden mukaisesti.

Tietoturvaloukkauksesta ilmoittaminen tietosuojaviranomaiselle
Tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivästystä tietosuojavaltuutetulle (tietosuojaviranomainen), jos tietoturvaloukkauksesta aiheutuu rekisteröidylle luonnolliselle henkilölle/henkilöille oikeuksiin tai vapauksiin liittyviä riskejä.

REDUssa tietosuojaviranomaiselle ilmoittamisesta päättää riippumattomasti REDUn tietosuojavastaava tietoturvaloukkauksesta saamiensa tietojen, kun hän on arvioinut riskien perusteella ilmoituskynnyksen täyttyneen. Myös käsittelytoiminnosta vastaava johto voi erikseen pyytää ilmoituksen tekemistä. Ilmoittaminen tietosuojaviranomaiselle on tärkeää, koska sitä kautta voi mm. selvitä, että kyse on esim. laajemmasta tietoturvaongelmasta esim. tietyn sopimustoimittajan tietojärjestelmässä. Tietoturvaloukkauksesta ilmoittamisesta vastaa REDUn tietosuojavastaava tai hänen ollessa estyneenä varatietosuojavastaava (Santasportin tietosuoja-asiantuntija).

Ilmoitus tietosuojaviranomaiselle on tehtävä 72 tunnin kuluessa siitä, kun tieto tietoturvaloukkauksesta on saatu. REDUssa katsotaan tieto saaduksi, kun tieto on saapunut arkipäivinä klo 9–15 välisenä aikana. Jos tieto tulee muina aikoina, tieto katsotaan saapuneeksi seuraavana arkipäivänä viimeistään klo 9 alkaen. Ilmoitus voidaan antaa myös alustavana 72 tunnin sisällä ja myöhemmin täydentää.

Ilmoituksen tekemisestä on ohjeet https://tietosuoja.fi/tietoturvaloukkaukset -sivulla.

Tietoturvaloukkauksesta ilmoittaminen Kyberturvallisuuskeskukselle.
Tietoturvaloukkauksesta ilmoitetaan myös Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle, kun tietoturvaloukkaukseen liittyy tietojen kalastelua, palvelunestohyökkäys tai niiden yritys. Näitä tapauksia ovat mm:

- tietojen kalastelu tai sen yritys,
- palvelunestohyökkäys tai sen yritys,
- haittaohjelma,
- tietomurto,
- tietovuoto,

- roska- tai huijauspostin leivitystä,
- huijauspuheluja.

Näissä tapauksissa on yleensä myös kyse rikollisesta toiminnasta, joten asiassa tehdään rikosilmoitus Poliisille. Kyberturvallisuuskeskukselle ilmoittamisesta REDUssa organisaationa vastaa ICT-palvelut. Ilmoituksen voi myös tehdä kuka tahansa yksityishenkilönä.

Lisätietoa: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Kyberturvallisuusilmoituksen antamiselle ei ole säädettyä määräaikaa, mutta suositeltavaa on antaa ilmoitus samassa yhteydessä, kun tietoturvaloukkauksesta ilmoitetaan tietosuojaviranomaiselle. Näin eri viranomaiset saavat tiedon asiasta ja voivat myös yhdessä selvittää asiaa ja auttaa rekisterinpitäjää.

Tieturva- ja tietosuojarikosilmoituksen tekeminen Poliisille
Mikäli tietoturvaloukkaukseen liittyy selkeä tuottamuksellisuus ja rikos, asiasta tehdään myös rikosilmoitus. Lähtökohtaisesti tällöin on kyse edellä esitetystä kyberrikollisuudesta tai tuottamuksellisesta henkilötietojen käsittelyssä tapahtuneesta tietosuojarikoksesta, esim. tahallisesta henkilötietojen levittämisestä, tietojen urkkimisesta jne. Rikosilmoituksen tekeminen mahdollistaa, että Poliisi voi aloittaa rikoksen tutkinnan.

REDUssa organisaation puolesta rikosilmoituksen tietoturvaloukkaustapauksessa tekee ICT-palvelut yhdessä käsittelytoiminnasta vastaavan johdon kanssa. Myös tietosuojavastaava tai tietosuoja-asiantuntija voi esittää tai antaa neuvoa käsittelytoiminnasta vastaavalle tai hänen esihenkilölleen rikosilmoituksen tekemiseksi.

Lisätietoa: https://poliisi.fi/tee-rikosilmoitus

Ilmoitus rekisteröidyille
Mikäli rekisteröidyn eli REDUn opiskelijan, asiakkaan, yhteistyökumppanin tai henkilökunnan oikeuksiin ja vapauksiin liittyy korkeaa riskiä, tietoturvaloukkauksesta on ilmoitettava jokaiselle rekisteröidylle, jota tietoturvaloukkaus koskee.

Ilmoitus rekisteröidylle on tehtävä mahdollisimman pian, mikäli rekisteröity voi omin toimin estää tai vähentää hänelle siitä aiheutuvaa haittaa ja vahinkoa. Esim. henkilö voi vaihtaa palveluissa käyttämiänsä salasanoja, sulkea luottokortin tms. Rekisteröidylle ilmoittaminen voi myös auttaa asian selvittämisessä.

Ilmoitus tietoturvaloukkauksesta rekisteröidylle tehdään aina kohdennetusti ko. henkilöille, mikäli se on mahdollista. Ilmoittamisessa käytetään REDUn rekisterissä olevia henkilökohtaisia sähköpostiosoitteita tai puhelinnumeroja (tekstiviestillä). Mikäli kohdennettu henkilökohtainen viestintä ei ole mahdollista, käytetään yleisiä viestikanavia, esim. intraa, verkkosivuja, somekanavia tai tiedotusvälineitä. Viestinnässä voidaan myös yhdistää kohdennettua ja yleistä viestintää esim. siten, että yleisellä viestikanavalla kerrotaan yleisesti mitä on tapahtunut ja ilmoitetaan, että tietoturvaloukkauksen kohteena oleville ilmoitetaan erikseen, että juuri he ovat kohteena.

Ilmoituksen rekisteröidylle tekee REDUssa lähtökohtaisesti aina käsittelytoiminnosta vastaava johto tai hänen nimeämänsä käsittelytoiminnon yhteyshenkilö. Ilmoittamisessa noudatetaan REDUn viestintäohjeistusta ja viestintävaltuuksia.

Kiireellisessä tilanteessa, milloin se on välttämätöntä tietosuojariskin ja sen vaikutusten vähentämiseksi, ilmoituksen voi antaa myös esim. ICT-palvelut suoraan.

REDUn tietohallinto ja ICT-palvelut voi ryhtyä myös tarvittavaan tietoturvatoimenpiteisiin välittömästi, kun tieto loukkauksesta on tapahtunut, esim. sulkea ja rajata käyttöoikeuksia tai tietoliikennettä, vaihtaa salasanoja tai palauttaa varmuuskopioista mahdollisia muuttuneita tai muutettuja tietoja takaisin. Päätöksen näihin turvaamistoimiin tekee tietohallinnosta tai ICT-palveluista vastaava.

Mikäli tietoturvaloukkauksessa on kyse LUC-konserniyhteistyössä yhdessä tuotettavasta palvelusta, ilmoittamisessa otetaan huomioon, mitä LUC-tietoturvasopimuksessa on osapuolten kesken sovittu.

3.7.7 Tietoturvaloukkauksen dokumentointi

REDUn tietosuojavastaava ja Santasportin tietosuoja-asiantuntija pitävät kirjaa tietoturvaloukkauksista ja ne diarioidaan. Loukkaukset kirjataan REDUn tietosuojapoikkeamat ja tietoturvaloukkaukset -luetteloon. Luetteloon kirjataan myös tapauskohtaiset viranomaisten diaarinumerot.

Tämän lisäksi kaikista kohtalaisen ja korkean riskin tietoturvaloukkaukset ja mitä niissä on tehty, dokumentoidaan vaiheittain (käsittelypäiväkirja). Dokumentoinnista vastaa REDUn tietosuojavastaava tai Santasportin tietosuoja-asiantuntija. Dokumentteihin liitetään kaikki käsittelyn viranomaisviestit ja tiedotteet rekisteröidyille.

Luettelon ja tietoturvaloukkauksen dokumentaatio ovat osa rekisterinpitäjän osoitusvelvollisuutta (kts. kohta 2.9).

3.8 Tietosuojan toteutumisen seuranta ja valvonta REDUssa

3.8.1 Tietosuojan jatkuva valvonta

REDUn tietosuojavastaava, Santasportin tietosuoja-asiantuntija ja REDUn tietosuojaryhmä seuraavat tietosuojasääntöjen ja REDUn antamien ohjeiden ja sopimusten noudattamista ja tuovat esiin havaitsemiaan tai tietoonsa saamiaan puutteita ja tietosuojapoikkeamia käsittelytoiminnasta vastaavalle johdolle ja yhteyshenkilöille.

Tietosuoja-asioita käsitellään myös säännöllisesti ja dokumentoidusti (kuukausittain) REDUn tietosuojaryhmässä. Työryhmän tehtävistä tarkemmin kohdassa 3.3 sekä työryhmän toimeksianto/nimittämispäätöksessä.

Työryhmän kokouksista laaditaan muistiot, jotka myös osaltaan ovat osa rekisterinpitäjän osoitusvelvollisuutta.

3.8.2 Tietosuojan johdon katselmukset

REDUn johto katselmoi tietosuojan tilanteen vähintään kerran vuodessa. Katselmuksen valmistelee tietosuojavastaava yhdessä tietosuojaryhmän kanssa.

Katselmukseen osallistuu REDUn johtoryhmä ja tytäryhtiöiden toimitusjohtajat sekä REDUn tietosuojaryhmän jäsenet. Katselmukseen voidaan kutsua myös muita henkilöitä. Katselmuksen ajankohdasta sekä siihen muista kutsuttavista henkilöstä päättää REDUn johtoryhmä.

Katselmuksessa REDUn tietosuojavastaava raportoi johdolle tietosuojan tilanteen edelliseltä tarkastelujaksolta. Raportoinnissa esitetään määrällisesti mm. tietosuojapoikkeamien ja tietoturvaloukkausten määrä ja laatu sekä käsittelytilanne.

Katselmuksesta laaditaan raportin lisäksi muistio, johon kirjataan katselmukseen osallistuneiden ja katselmoitujen asioiden lisäksi katselmuksessa mahdollisesti esille nousseet tietosuojan kehittämiskohteet ja -tarpeet. Muistion pohjalta päivitetään REDUn tietosuojan kehittämissuunnitelma. REDUn johto (johtoryhmä) päättää erikseen kehittämissuunnitelmasta.

Lähteet

EU:n Yleinen tietosuoja-asetus, Euroopan parlamentin asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä niiden vapaasta liikkuvuudesta.
Viitattu 29.4.2025: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Julkisuuslaki, Laki viranomaisten toiminnan julkisuudesta 621/1999
Viitattu 29.4.2025: https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

REDUn Hallintosääntö 1.1.2024, Rovaniemen koulutuskuntayhtymä REDU.
Viitattu 29.4.2025: https://redu.fi/media/tietoa-redusta/paatoksenteko/saannot-ja-ohjeet/redu-hallinto-saanto-2024-versio-3-s.pdf

REDU Konserniohje 15.6.2021, Rovaniemen koulutuskuntayhtymä REDU
Viitattu 29.4.2025: https://redu.fi/media/tietoa-redusta/paatoksenteko/saannot-ja-ohjeet/REDU%20konserniohje%2015.62021%20(versio-2).pdf

Rikoslaki 39/1889.
Viitattu 29.4.2025: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Tiedonhallintalaki, Laki julkisen hallinnon tiedonhallinnasta 906/2019
Viitattu 29.4.2025: https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

Tietosuoja-asetus, kts. EU:n Yleinen tietosuoja-asetus.

Tietosuojalaki 1050/2018.
Viitattu 29.4.2025: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojavaltuutetun toimisto, Käyttötarkoitussidonnaisuus
Viitattu 29.4.2025: https://tietosuoja.fi/kayttotarkoitussidonnaisuus

Tietosuojavaltuutetun toimisto, Lainmukaisuus, asianmukaisuus ja läpinäkyvyys
Viitattu 29.4.2025: https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys

Tietosuojavaltuutetun toimisto, Luottamuksellisuus ja turvallisuus
Viitattu 29.4.2025: https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus

Tietosuojavaltuutetun toimisto, Osoitusvelvollisuus
Viitattu 29.4.2025: https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto, Säilytyksen rajoittaminen
Viitattu 29.4.2025: https://tietosuoja.fi/sailytyksen-rajoittaminen

Tietosuojavaltuutetun toimisto, Tietosuojaperiaatteet
Viitattu 29.4.2025: https://tietosuoja.fi/tietosuojaperiaatteet

Tietosuojavaltuutetun toimisto, Tietosuojavastaavat
Viitattu 29.4.2025: https://tietosuoja.fi/tietosuojavastaavat

Tietosuojavaltuutetun toimisto, Tietojen minimointi
Viitattu 29.4.2025: https://tietosuoja.fi/tietojen-minimointi

Tietosuojavaltuutetun toimisto, Tietojen täsmällisyys
Viitattu 29.4.2025: https://tietosuoja.fi/tietojen-tasmallisyys

Tietosuojavaltuutetun toimisto, Tietoturvaloukkaukset
Viitattu 29.4.2025: https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto, Vaikutustenarviointi
Viitattu 29.4.2025: https://tietosuoja.fi/vaikutustenarviointi

LIITE 1: Käsitteiden määritelmiä

Rekisteröity
Rekisteröity on luonnollinen tunnistettu tai tunnistettavissa oleva henkilö (ihminen), jonka henkilötietoja käsitellään.

Rekisterinpitäjä
Rekisterinpitäjä on ihminen tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu.

Henkilötieto
Henkilötiedoilla tarkoitetaan luonnolliseen **tunnistettuun** tai **tunnistettavissa olevaan henkilöön** eli rekisteröityyn **liittyviä mitä tahansa tietoja**.

Henkilöä pidetään tunnistettavana, jos hänet voidaan suoraan tai epäsuorasti tunnistaa esim. nimen, henkilötunnuksen, ID-numeron, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen tai fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Tällaisia henkilön tunnistettavuus tietoja ovat esimerkiksi:

- nimi,
- henkilötunnus (HETU),
- henkilönumero, ID-numero,
- opiskelijanumero,
- sähköpostiosoite,
- puhelinnumero,
- sijaintitieto (esim. kotiosoite tai paikannustieto),
- verkkotunnistetiedot (esim. ip-osoite),
- yksi tai useampi henkilöä koskeva tunnusomainen fyysinen, geneettinen, psyykkinen, taloudellinen, kulttuurinen tai sosiaalinen tekijä (esim. valokuva, sormenjälki, hiusten-, silmien-, ihonväri, video- tai äänitallenne).

Myös silloin, kun esim. julkisia tai kaikkien nähtävillä olevia tietoja yhdistelemällä on jälkikäteen mahdollista tunnistaa yksilöidä henkilö, kyse on henkilötietojen käsittelystä. Esim. tietyn koulutuksen ryhmän ainoa toista sukupuolta oleva, maahanmuuttaja, eri-ikäinen tms.

Mikäli käsiteltävistä henkilötiedoista poistetaan pysyvästi kaikki sellaiset tiedot, joilla henkilö voidaan yksilöidysti tunnistaa (tietojen muuttaminen anonyymeiksi), voidaan henkilötietojen käsittelyssä poiketa siten, kun tietosuoja-asetuksessa ja tietosuojalaissa on tarkemmin säädetty. Mikäli kuitenkin säilytetään jossain, esim. rinnakkaisessa luettelossa tieto henkilön tunnistamiseksi, kyse on edelleen henkilötietojen käsittelystä eli pseudonymisoidusta henkilötietojen käsittelystä.

Erityiset henkilötietoryhmät ja arkaluonteiset tiedot
Tietosuoja-asetukseen 9 artiklassa sekä Tietosuojalain (1050/2018) 6 §:ssä on säädetty ns. erityisistä henkilötietoryhmistä (arkaluonteiset henkilötiedot). Näiden tietojen käsittely on lähtökohtaisesti kiellettyä.

Erityisiä henkilötietoryhmiä, joiden käsittely on kielletty:
- rotu tai entinen alkuperä,
- poliittiset mielipiteet,
- uskonnollinen tai filosofinen vakaumus,
- ammattiliiton jäsenyys,
- terveyttä koskevat tiedot,
- seksuaalista suuntautuminen ja käyttäytyminen,
- geneettisiä ja biometrisia tietoja henkilön tunnistamista varten.

Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Näitä tietoja voidaan kuitenkin käsitellä niissä tapauksissa, joista on säädetty Tietosuoja-asetuksen 9 artiklan 2 kohdassa sekä Tietosuojalain 1050/2018 6 §:ssä. Näitä ovat mm:

- Kun rekisteröity on antanut nimenomaisen suostumuksen kyseisten henkilötietojen käsittelyyn.
- Kun käsittely on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi tilanteessa, jossa rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan.
- Kun 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.
- Kun käsittely koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi esimerkiksi julkaisemalla ne verkkosivuillaan.
- Kun käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Lisäksi käsittely on mahdollista aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään.

Seuraavissa tapauksissa erityisten henkilötietoryhmien tietojen käsittely ei ole mahdollista suoraan asetuksen perusteella, vaan se edellyttää lisäksi tarkentavaa sääntelyä tai muuta menettelyä:

- Kun käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla siltä osin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä tai työehtosopimuksessa. Tässä yhteydessä on myös säädettävä toimenpiteistä, joilla suojataan rekisteröidyn perusoikeudet ja edut.

- Kun käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla. Käsittelyn mahdollistavan sääntelyn tulee olla oikeassa suhteessa käsittelyn tavoitteeseen nähden, ja siinä tulee noudattaa keskeisiltä osin oikeutta henkilötietojen suojaan. Tässä yhteydessä on myös säädettävä toimenpiteistä, joilla suojataan rekisteröidyn perusoikeudet ja edut.

- Kun käsittely on tarpeen ennaltaehkäisevää terveydenhuoltoa, työterveydenhuoltoa, työkyvyn arviointia, lääketieteellisiä diagnooseja, terveys- tai sosiaalihuollollista hoitoa tai terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten unionin oikeuden, jäsenvaltion lainsäädännön tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti. Edellytyksenä on, että tietoja käsittelee vain ammattilainen tai henkilö, jolla on lakisääteinen salassapitovelvollisuus.

- Kun käsittely on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön perusteella, jossa säädetään myös rekisteröidyn oikeuksia ja vapauksia suojaavista toimenpiteistä, erityisesti salassapitovelvollisuudesta.

- Kun käsittely on tarpeen yleisen edun mukaista arkistointia, tieteellistä ja historiallista tutkimusta tai tilastointia varten tietosuoja-asetuksen mukaisesti unionin oikeuden tai jäsenvaltion lainsäädännön nojalla. Käsittelyn mahdollistavan sääntelyn tulee olla oikeassa suhteessa käsittelyn tavoitteeseen nähden, ja siinä tulee noudattaa keskeisiltä osin oikeutta henkilötietojen suojaan. Tässä yhteydessä on myös säädettävä toimenpiteistä, joilla suojataan rekisteröidyn perusoikeudet ja edut.

Henkilötunnus (HETU) ja henkilön tunnistaminen
Henkilötunnuksen käsittelyssä on oltava erityisen huolellinen. Henkilötunnusta voidaan käyttää silloin, kun se on tarpeen henkilön yksilöimiseksi ja muita yksilöimiseen käytettävissä olevia tunnuksia ei ole. Esim. jos käytettävissä on muu henkilön yksilöivä ID-, opiskelija- tai asiakasnumero, henkilötunnusta ei tarvita.

Henkilötunnuksen käytöstä on erikseen säädetty Tietosuojalain 1050/2018 29 §:ssä. Laissa on tarkennettu mm. missä tilanteissa henkilötunnusta voidaan käsitellä. Esim. jos yksityishenkilölle myydään luotolla (laskutuksella), voidaan tieto velvoittaa antamaan. Mikäli henkilötunnusta käytetään henkilörekisterissä, sitä ei saa tulostaa tai merkitä rekisteristä otettuihin tulosteisiin ja otteisiin, ellei sille ole ko. tulosteessa tarvetta henkilön yksilöimiseksi. Esim. henkilölle toimitettavassa laskussa ei henkilötunnusta tarvita, koska laskun maksamisessa sitä ei tarvita.

Palvelussuhteen sopimuksissa, koulutussopimuksissa ja oppisopimuksissa henkilötunnuksen kirjaaminen on tarpeen henkilön yksilöimiseksi, sillä sitä tarvitaan henkilön yksilöimiseksi mm. palkkojen ja verojen maksamiseen, mahdollisten työpaikan turvallisuusselvitysten yms. tekemisessä.

Henkilötunnusta tai sen loppuosaa ei esim. saa kysyä suullisesti tai kirjallisesti henkilöltä siten, että sivullisten on mahdollista saada se tietoonsa esim. asiakaspalvelutilanteessa.

Niissä tilanteissa, missä henkilötunnuksen käyttö on perusteltua tietosuojalain perusteella, suositeltavin tapa on, että henkilö esittää henkilötunnuksen sisältävän henkilökortin, ajokortin tai kuvallisen Kela-kortin, josta käsittelijä voi sen kirjata ja samalla varmistaa henkilöllisyyden.

Henkilötietojen käsittely
Henkilötietojen käsittely tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista. Henkilötietojen käsittelyä on myös muista kuin omista henkilötiedoista keskustelu tai niiden kysyminen suullisesti tai kirjallisesti Henkilötietojen käsittelyä on myös suullisten tai kirjallisten henkilötietojen kääntäminen tai tulkkaaminen. Kaikki henkilötietoihin kohdistuvat toimenpiteet henkilötietojen käsittelyn suunnittelusta henkilötietojen poistamiseen ovat henkilötietojen käsittelyä.

Henkilötietojen käsittelyyn sisältyy tietojen käsittelyn koko tiedon elinkaari keräämisestä hävittämiseen. Henkilötietojen käsittelymuotoja ovat: tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, muuttaminen. Käsittelyyn kuuluvat myös henkilötietojen haut, kyselyt, tietojen luovuttamiset, siirtämiset, levittämisen ja saataville asettaminen (julkaisu), tietojen yhteensovittaminen ja yhdistäminen, rajoittaminen, poistaminen sekä tuhoaminen.

Henkilötietojen käsittelijä
Tietosuojalainsäädännössä henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee rekisterinpitäjän rekisteröityjen henkilötietoja rekisterinpitäjän lukuun, mutta joka ei ole suoraan rekisterinpitäjän johdon alaisuudessa toimiva. Henkilötietojen käsittelijä on siis rekisterinpitäjään nähden ulkopuolinen taho esim. sopimustoimittaja.

Henkilötietojen käsittelijänä toimivat käytännössä myös rekisterinpitäjän henkilökuntaan kuuluvat, mutta koska he ovat rekisterinpitäjän johdon alaisuudessa, heidät ovat tietosuojalainsäädännön näkökulmasta ”rekisterinpitäjää”.

Henkilörekisteri
Henkilörekisteri muodostuu henkilötietojen tietojoukosta eli useammasta kuin yhden henkilön henkilötiedoista. Tietosuoja-asetuksessa henkilörekistereistä käytetään käsitettä henkilötietojen tietojoukko, mutta selvyyden vuoksi tässä ohjeessa käytetään vakiintunutta käsitettä henkilörekisteri.

Henkilötiedoista muodostuu henkilörekisteri aina silloin, kun samassa tietojärjestelmässä, tiedostossa, luettelossa, kortistossa, mapissa tms. kootaan ja säilytetään samaa käyttötarkoitusta tai käyttötarkoituksia varten useiden eri henkilöiden henkilötietoja.

LIITE 2: Tietosuojan huoneentaulu

Henkilötietojen käsittely on kyseessä, kun käsitellään yhden tai useamman suoraan tai välillisesti tunnistettavissa olevan henkilön henkilötietoja manuaalisesti tai sähköisesti.

Henkilötietojen käsittelijä vastaa, että hän noudattaa tietosuojasta annettua lainsäädäntöä sekä REDUn tietosuoja ja tietoturvaohjeistusta. Henkilö saa käsitellä vain niitä henkilötietoja, jotka kuuluvat hänen työtehtäviinsä ja vain niihin käyttötarkoituksiin, joihin tieto on kerätty ja henkilörekisteri koottu.

Seuraavassa yleisiä henkilötietojen käsittelyä koskevia ohjeita:

- Henkilötietojen käsittelijöitä koskee vaitiolovelvollisuus. Henkilötietoja ei saa luovuttaa eikä millään tavalla ilmaista, suoraan tai epäsuorasti niiden sisältöä ulkopuolisille.
- Henkilötietojen käsittelyssä on otettava huomioon tietoturva eli ettei missään käsittelyn vaiheessa tiedot eivät ole sivullisten nähtävillä, kuultavilla tai millään tavalla saatavilla. Henkilötietoja sisältävät tulosteet ja tiedostot on säilytettävä ja hävitettävä asianmukaisesti tietoturvallisesti.
- Henkilötiedoista ei saa käsitellä keskustellen sellaisessa paikassa, jossa sivullisten on mahdollista kuulla keskustelu, ei myöskään ilman nimeä. Sivullinen kuulija voi yhdistää kuulemansa henkilötiedot tietojen sekä niistä keskustelevien henkilöiden perusteella tiettyyn tunnistettavaan henkilöön (rekisteröityyn).
- Henkilötietoja sisältäviä tulosteita, tiedostoja yms. on säilytettävä lukitussa huoneessa tai kaapissa tai ne on teknisesti suojattava tai salattava siten, ettei sivullinen näe niitä tai pääse niihin käsiksi silloin, kun ne eivät ole käsittelijän valvonnassa. Jos tietoja käsitellään sähköisesti työasemalla, on varmistettava, ettei sivullinen pääse näkemään näyttöä ja työasema lukitaan, kun se ei ole enää valvonnassa.
- Erityisen varovainen pitää olla, kun kuljettaa tai lähettää henkilötietoja sisältäviä asiakirjoja. Henkilötietoja sisältäviä tietoja ja tiedostoja ei saa lähettää salaamattomina sähköpostilla, mikäli sähköposti lähetetään REDUn sähköpostijärjestelmän ulkopuolelle.
- Henkilötietoja sisältäviä tiedostoja ei saa tallentaa tai ottaa niistä kopioita suojaamattomalle ulkopuoliselle tallennusmedialle (USB-tikku, CD-ROM tms.).
- Kirjepostissa on käytettä suljettua kirjekuorta, jonka läpi henkilötiedot, vastaanottajan osoitetietoja lukuun ottamatta, eivät ole näkyvissä.

ICT-palvelut antaa lisätietoa tietoturvallisista henkilötietojen lähettämis- ja tallentamisratkaisuista.

REDUn henkilökuntaan kuuluvalla henkilötietojen käsittelijällä on oikeus ja velvollisuus kieltäytyä käsittelemästä henkilötietoja johdon, esihenkilön tai muun henkilökunnan pyynnöstä tai määräyksestä silloin, kun ko. käsittelyssä rikottaisiin voimassa olevaa tietosuojalainsäädäntöä tai REDUn ohjeistusta. Tällaisesta säädösten ja ohjeiden vastaisesta henkilötietojen käsittelyn ohjeistamisesta tai sen pyynnöstä tai määräämisestä on ilmoitettava tietosuojavastaavalle.

Henkilötiedon käsittelijää ei saa erottaa, siirtää työtehtävästä toiseen tai antaa kurinpitorangaistusta, sillä perusteella että hän on kieltäytynyt toimimasta tietosuojasäädösten ja -ohjeiden vastaisesti ja että hän on ilmoittanut asiasta tietosuojavastaavalle tai tietosuojaviranomaiselle.