# Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet

**Viittausohje:** ATT aineistonhallinnan ohje sensitiivisille aineistoille - työryhmä (2018) Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet, Tuuliprojekti

Sisällysluettelo

Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ..... 1

Keskeiset käsitteet ..... 11

## Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun

| **0. Esittely** | |
|---|---|
| | **TÄMÄ OHJE TÄYDENTÄÄ KANSALLISTA AINEISTONHALLINTASUUNNITELMAOHJETTA, LUE OHJEITA RINNAKKAIN!**<br><br>Tämä on ohje **tutkimussuunnitelmasta** erillisen **aineistonhallintasuunnitelman** laadintaan. Kuitenkin etenkin tutkimuksessa, joka perustuu aineiston keräämiseen ja analysointiin, tutkimussuunnitelma ja aineistonhallintasuunnitelma ovat läheisessä riippuvaisuussuhteessa ja usein osittain päällekkäisiä.<br><br>Tutkimussuunnitelman ja aineistohallintasuunnitelman eroa voidaan luonnehtia seuraavasti: tutkimussuunnitelmassa kerrotaan, millaisia aineistoja käytetään, miksi niitä käytetään ja miten niitä käytetään osana suunniteltavaa tutkimustyötä, kun aineistonhallintasuunnitelmassa puolestaan kerrotaan, miten näitä aineistoja hallinnoidaan ja miten niiden jatkokäyttö mahdollistetaan tutkimustyön kuluessa.<br><br>Tämä ohje täydentää yleistä aineistonhallintasuunnitelmaohjetta **arkaluonteisia henkilötietoja** sisältävien aineistojen osalta. Muiden kuin arkaluonteisten henkilötietojen käsittelyyn ei sovelleta kaikkia ohjeessa kuvattuja suojatoimia. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.<br><br>Arkaluonteisia henkilötietoja (tietosuoja-asetus 9,10 art) ovat:<br><br>1. Rotu tai etninen alkuperä<br>2. Poliittinen mielipide<br>3. Uskonnollinen tai filosofinen vakaumus<br>4. Ammattiliiton jäsenyys<br>5. Geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten<br>6. Terveyttä koskevat tiedot<br>7. Seksuaalinen käyttäytyminen tai suuntautuminen<br>8. Rikostuomiot ja rikkomukset<br><br>**Henkilötietojen käsittelystä säädetään lailla**. Henkilötietojen käsittelyä ohjaava lainsäädäntö muuttuu toukokuussa 2018, jolloin henkilötietojen käsittelyssä aletaan soveltaa **EU:n yleistä tietosuoja-asetusta** ja sitä täydentävää **tietosuojalakia**. Uudistuksen tarkoitus on parantaa henkilöiden mahdollisuuksia vaikuttaa itseään koskevien tietojen käsittelyyn, ja se tuo muutoksia myös henkilötietojen käsittelyyn tutkimuksessa. Uudistuksia ovat mm. osoitusvelvollisuus eli henkilötietojen käsittelijän tai rekisterinpitäjän on jatkossa osoitettava kirjallisesti noudattavansa tietosuojalainsäädäntöä ja henkilötietojen käsittelyä koskevia periaatteita sekä toteuttaa lainsäädännön edellyttämät rekisteröityjen oikeudet. Lisäksi suostumuksella kerättävien henkilötietojen käytössä on muutoksia aiempaan.<br><br>Monia henkilötietojen käsittelyn vaiheita varten on olemassa **myös organisaatiokohtaiset ohjeet**, joita sinun tulee noudattaa.<br><br>Henkilötietoja sisältävien aineistojen hallinnan suunnittelu on erityisen tärkeää, sillä sen kautta pystyt varmistamaan omat ja edustamasi organisaation sekä tutkittaviesi oikeudet. Tietosuojalainsäädännön rikkomisesta voi aiheutua **hallinnollisia sanktioita,** |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | **rikosoikeudellisia seuraamuksia ja vahingonkorvausvelvollisuus**. Henkilötietojen vuotaminen luvattomiin käsiin voi aiheuttaa **vakavaa haittaa tutkittaville**.<br><br>**Lisätietoa:** Tietosuojavaltuutetun toimisto laatii ohjeistusta tietosuojalainsäädännön soveltamisesta: http://www.tietosuoja.fi/fi/ |
| **1. Aineiston yleiskuvaus** | |
| **1.1 Millaiseen aineistoon tutkimuksesi perustuu? Millaista aineistoa kerätään, tuotetaan tai käytetään uudelleen? Missä tiedostomuodoissa aineisto on?** | Kuvaa **aineistonhallintasuunnitelmassa,** millaista henkilötietoja sisältävää dataa keräys- ja analyysimenetelmät tuottavat. Perustelut tutkimuksen oikeutukselle ja perusteet henkilötiedon keruulle ja käsittelylle kerrotaan sen sijaan **tutkimussuunnitelmassa**.<br><br>Kuvaa aineistonhallintasuunnitelmassa kaikki datalähteet. Listaa esimerkiksi tutkimukseen osallistuneet henkilöt/henkilöryhmät, viranomaiset tai rekisterit.<br><br>Jokaiselle datalähteelle:<br><br>• yksilöi *henkilötietoja* ja *arkaluonteisia henkilötietoja* sisältävät aineistot.<br>• jos datan lähde on rekisteri tai tilasto, kerro myös sen *rekisterinpitäjä*.<br>• kerro kuka, tai mikä taho, on itse keräämäsi tai tuottamasi aineiston *rekisterinpitäjä*.<br><br>Huomaa, että **henkilötietoja tai arkaluonteisia tietoja kerättäessä tai siirrettäessä pitää varmistua myös keräys- ja siirtovälineen tietoturvallisuudesta**, tämä kuvataan tarkemmin kohdassa 4.1. |
| **1.2 Miten aineiston yhtenäisyys ja laatu varmistetaan?** | Mieti datan laatua koko sen elinkaaren aikana, aina keräämisestä julkaisemiseen ja arkistointiin saakka. Mitkä ovat pahimmat riskit ja kuinka niitä hallitaan? Liittyykö henkilötietoja sisältävän datan keräämiseen elementtejä, jotka vaativat erityishuomiota datan laatuun liittyen? (Tietoturva asiat käsitellään vasta kohdassa 4.1)<br><br>**Vinkit**<br><br>• Mieti missä vaiheessa aineisto kannattaa suojata koodilla tai anonymisoida.<br>• Tunnista on anonymisoidun ja pseudonymisoidun datan ero.<br>• Mieti vaikuttaako *anonymisointi* tai *pseudonymisointi* datan laatuun. Onko data käyttökelpoista anonymisoinnin jälkeen?<br>• Muista varmistaa, ettei karkeistuksessa menetetä arvokasta informaatiota. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | • Metadatan kirjaaminen ja metadatastandardien käyttö ovat myös laatutoimenpiteitä, kirjaa nämä tarkemmin suunnitelman kohtaan "3. Dokumentointi ja metadata" |
| **2. Eettisten periaatteiden ja lainsäädännön noudattaminen** | |
| **2.1 Mitä eettisiä seikkoja aineistosi hallintaan liittyy (esim. arkaluonteisten tietojen käsittely, tutkittavien identiteetin suojaaminen ja tietojen jakamista koskevan suostumuksen hankkiminen)?** | Kerro suunnitelmassa kuka, tai mikä taho, on itse keräämäsi tai tuottamasi aineiston *rekisterinpitäjä*.<br><br>Kerro ketä ovat **käsittelijät**, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun. **Henkilötietojen käsittelyllä** tarkoitetaan kaikkia toimintoja, joita kohdistetaan henkilötietoihin, esimerkiksi henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.<br><br>Datan käsittelyksi luetaan myös organisaation/tutkimusprojektin ulkopuoliset tahot, jotka esimerkiksi analysoivat näytteitä. Ulkopuolisten tahojen kanssa laaditaan käsittelysopimukset.<br><br>Käsittelijän on toteutettava suojatoimia rekisteröidyn oikeuksien suojelemiseksi. Suojatoimia ovat esimerkiksi<br><br>○ Copy of Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet#pseudonymisointi<br>○ Copy of Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet#anonymisointi (pitäisikö selvittää tarkemmin mitä tarkoittaa)<br>○ riittävät Copy of Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet#suojatoimet: tekniset rajoitukset, käytön valvonta**, kuvataan suunnitelman kohdassa 4**<br>○ koulutus, ohjeet, määräykset, sitoumukset ja sopimukset<br>○ prosessit, käytännesäännöt ja sertifikaatit<br>○ tiedon salaaminen<br>○ auditoinnit<br><br>**Tietosuojaa koskeva vaikutusten arviointi**<br><br>Kerro suunnitelmassa miten vaikutusten arviointi tehdään. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarviointi on tehtävä, kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski. Vaikutustenarvioinnin tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen vaatimusten noudattamisessa ja noudattamisen osoittamisessa. Tietosuojaa koskeva vaikutustenarviointi olisi aloitettava mahdollisimman aikaisin henkilötietojen käsittelytoimien suunnitteluvaiheessa. Arviota on seurattava jatkuvasti ja päivitettävä aina tarpeen mukaan.<br><br>**Vinkkejä**<br><br>• Katso oman organisaation tietosuojaohjeet.<br>• Katso oman organisaation ohjeet käsittelysopimuksista.<br>• Katso oman organisaation ja Tietosuojavaluutetun toimiston ohjeet vaikutusten arviointiin.<br><br>**Linkkejä**<br><br>• Rekisteri- ja tietosuojaselosteet: http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html<br>• EU:n tietosuojauudistus: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html<br>• Tunnisteellisuus ja anonymisointi: http://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html<br>• Tietoarkiston aineistonhallinnan käsikirja, tutkittavien informointi: http://www.fsd.uta.fi/aineistonhallinta/fi/tutkittavien-informointi.html<br>• Tietosuojavaltuutetun toimiston ohjeet vaikutusten arviointiin: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/vaikutustenarviointi.html |
| **2.2 Miten aineiston omistajuuteen, tekijänoikeuksiin ja immateriaalioikeuksiin liittyviä asioita** | Aineiston omistajuuteen, tekijänoikeuksiin ja immateriaalioikeuksiin on aina kiinnitettävä huomiota. Arkaluoteisten aineistojen kohdalla tästä on oltava erityisen tarkka.<br><br>**Vinkkejä**<br><br>• Lue tarkasti kaikkien käyttämiesi tietojärjestelmäpalveluiden käyttöehdot. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| **hallintaan? Estävätkö tekijänoikeudet, käyttöoikeudet tai muut rajoitukset aineiston käyttämisen tai jakamisen?** | • Kirjalliset sopimukset datan omistajuudesta, käyttöoikeudesta ja julkaisujen tekijyydestä varmistavat osaltaan tietosuojan toteutumisen. |
| **3. Dokumentointi ja metatiedot** | |
| **3.1 Miten dokumentoit aineistosi, jotta se on löydettävissä, saavutettavissa, yhteentoimivaa ja uudelleen käytettävissä sekä itseäsi että muita varten? Mitä metatietostandardeja, README-tiedostoja ja muuta dokumentaatiota käytät, jotta muut voivat ymmärtää ja käyttää aineistoasi?** | **Vinkkejä**<br>• Lisää muuttujien kuvaukseen tieto siitä, sisältääkö muuttuja henkilötietoa tai arkaluonteista tietoa. Ks. esim. Aineistonhallinnan käsikirja.<br>• Vaikka tutkimusdatasi sisältäisi arkaluonteisia henkilötietoja, voi metadatan julkaista, jos metadata ei sisällä tunnisteellista tietoa, jonka avulla tutkittavan voi identifioida. |
| **4. Tallentaminen ja varmuuskopiointi tutkimushankkeen aikana** | |
| **4.1 Minne aineistosi tallennetaan ja miten se varmuuskopioidaan?** | Jos tutkimuksessa kerätään tai käytetään henkilötietoja tai arkaluonteisia henkilötietoja:<br>• huomioi mahdollisimman aikaisessa vaiheessa datan luovuttajan tai siirtäjän vaatimukset<br>• tee lain vaatima riskinarvio, josta selviää vaadittavat tietoturvatoimet<br><br>Tietoturvatoimia ovat<br>• Varmuuskopiointi: turvaa kyvyn palautua vikatilanteesta |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | • Pääsynhallinta: kenelle myönnetään pääsy ja millä perusteella, miten pääsyn rajaus tehdään, **tämä kuvataan tarkemmin kohdassa 4.2.**<br>• Salaus: tarpeen mukaan, erityisesti mobiililaitteet, kannettavat ja ulkoiset tallennuslaitteet on pyrittävä salaamaan.<br>• Valvonta (lokitus): sekä tekninen loki että aineistonkäsittelyn ja käytön valvonta, **tämä kuvataan tarkemmin kohdassa 4.2.**<br>• Teknisen ympäristön suojaus: miten käsittely-ympäristön suojataan ulkopuolisilta<br>• Henkilöstöturvallisuus: tutkimusryhmän jäsenten perehdytys, tietosuoja ja -turvakoulutus, ohjeet sekä yhteisesti sovitut käytännöt<br>• Tilaturvallisuus: työtilojen lukitukset, säilytyskalusteet, kameravalvonta sekä kulkuoikeuksien valvonta, **tämä kuvataan tarkemmin kohdassa 4.2.**<br><br>**Vinkkejä**<br><br>• Käytä aina kun mahdollista rekisterinpitäjien tarjoamia suojattuja käsittely-ympäristöjä.<br>• Muista, että henkilötietojen siirtoa EU:n/ETA-alueen ulkopuolelle on rajoitettu.<br>• Muista, että myös suostumuslomakkeet sisältävät henkilötietoa.<br><br>***Linkkejä***<br><br>• *Tietoarkiston Aineistonhallinnan käsikirja:* http://www.fsd.uta.fi/aineistonhallinta/fi/fyysinen-sailytys.html<br>• *Hyvinvointi- ja terveysdatan informaatioportaali:* http://hytedata.fi/<br>• *Viestintävirasto / Kyberturvallisuuskeskus: Terveyden huoltoalan kyberuhkia:* https://www.viestintavirasto.fi/attachments/tietoturva/TerveydenhuoltoalanKyberuhkia.pdf<br>• *Korkeakoulujen pilviohje:* https://wiki.eduuni.fi/display/pilviohje/Pilviohje |
| **4.2 Kuka valvoo pääsyä aineistoon ja miten suojattua pääsyä aineistoon valvotaan?** | **Pääsynhallinta**: kenelle myönnetään pääsy ja millä perusteella, miten pääsyn rajaus tehdään ja kuka siitä vastaa.<br><br>• Tarvitaan nimetty vastuuhenkilö<br>• Tarvitaan lista myönnetyistä oikeuksista ja käyttäjistä<br>• Oikeuksia myönnetään vain tarpeeseen ja mahdollisimman rajatusti<br>• Oikeuksia myönnettäessä tarve ja peruste tarkistetaan<br>• Käytössä pitää olla menetelmä käytäntöoikeuksien perumiseen ja poistamiseen<br><br>**Valvonta:** tämä tarkoittaa sekä teknistä lokia että sitä miten valvotaan aineiston käsittelyä ja käyttöä.<br><br>• Mieti miten aineiston käyttöä seurataan tutkimuksen aikana.<br>  ○ Missä ja millä tavoin aineistoa käsitellään?<br>  ○ Mihin ja kenelle sitä kopioidaan? |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | ○ Kuka ja millä perustein voi siirtää aineistoa tutkimusryhmästä? Muista, että tämän pitää olla linjassa suostumuksen kanssa, mikäli aineisto on saatu käyttöön suostumuksen perusteella.<br>• Selvitä ja kuvaa pystyvätkö käytetyt tekniset välineet pitämää kirjaa siitä kuka käytti, mitä aineistoa ja milloin. Kysy organisaatiosi IT-tuesta, onko tarjolla käyttö- ja muutoslokitusta.<br><br>**Tilaturvallisuus:** työtilojen lukitukset, säilytyskalusteet, kameravalvonta sekä kulkuoikeuksien valvonta.<br><br>• Tarvitaan nimetty vastuuhenkilö<br>• Tarvitaan lista kulkuoikeuksien haltijoista ja avaimista<br>• Mitkä ovet on lukittuja tai ne saa lukkoon työtilan ja ulkomaailman välillä?<br>• Onko käytettävissä murtosuojattuja säilytystiloja tai kalusteita työtiloissa papereille, muille analogisille aineistoille tai ulkoisille tallennuslaitteille?<br>• Onko kameravalvontaa?<br><br>**Vinkkejä**<br><br>Uuden tietosuoja-asetuksen myötä tarvitsette:<br><br>• Dokumentin, joka täyttää tietosuoja-asetuksen osoittamisvelvollisuuden<br>• Ilmoituksen tietosuojatoimista<br><br>***Linkkejä***<br><br>• *Viestintävirasto / Kyberturvallisuuskeskus: Ohje lokitietojen tallentamiseen ja hyödyntämiseen:* https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf |
| **5. Aineiston avaaminen, julkaiseminen ja arkistointi tutkimushankkeen päätyttyä** | |
| **5.1 Mikä osa aineistosta voidaan asettaa avoimesti saataville tai julkaista? Missä ja milloin aineisto tai siihen liittyvät metatiedot asetetaan saataville?** | Henkilötietoja sisältävät aineistot voidaan avata vain *anonymisoituina*. *Pseudonymisoituna* data on edelleen henkilötietoa ja sitä ei tästä syystä voi avata. Henkilötietoja sisältävä data voidaan kuitenkin jakaa siitä kiinnostuneiden kanssa luvanvaraisesti alkuperäisen käsittelyperusteen mukaiseen tarkoitukseen.<br><br>Henkilötietoja sisältävän aineiston käsittelyperuste, esimerkiksi lakiin perustuva tai suostumus, voi rajoittaa aineiston jatkokäyttöä. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | Henkilötietoja sisältävän aineiston avaamiseen tai julkaisemisen tapoja ovat:<br><br>1. Data anonymisoidaan ja avataan tietoturvatasoltaan sopivassa data-arkistossa.<br>2. Julkaistaan vain aineistoa koskeva metadata, sopivassa tutkimustietojärjestelmässä tai *datarepositoriossa*.<br><br>**Vinkkejä**<br><br>• Henkilötietoja sisältävän aineiston keskeiset metatiedot kannattaa avata, vaikka itse aineistoa ei voisi julkaista.<br>• Pseudonymisoitu aineisto on edelleen henkilötietoa ja sitä ei voi avata jatkokäyttöön. Aineiston jatkokäyttö voi kuitenkin olla mahdollista luvanvaraisesti.<br>• Aineiston jatkokäyttö voi vaatia uuden suostumuksen hankkimista tutkittavalta.<br><br>**Linkkejä**<br><br>• Tunnisteellisuus ja anonymisointi: http://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html |
| **5.2 Mihin pitkällä aikavälillä arvokkaat tiedot arkistoidaan ja kuinka pitkäksi ajaksi?** | Arkistointisuunnitelmaa tehtäessä on tärkeä miettiä, mikä osa aineistosta *arkistoidaan* ja kuinka pitkäksi aikaa. On tärkeä myös suunnitella mikä osa hävitetään ja miten se tehdään turvallisesti.<br><br>Perinteisesti arkaluontoinen aineisto kehotetaan tuhoamaan tutkimushankkeen jälkeen, koska sen säilyttäminen on riskialtista ja vaatii siksi erityisjärjestelyjä. Myös muut tarpeettomat tiedostot ja tietojärjestelmien käytön yhteydessä syntyvät väliaikaistiedostot on poistettava käyttötarpeen päätyttyä.<br><br>Pelkästään tiedoston poistaminen (deletointi) ja tietokoneen roskakorin tyhjentäminen ei tarkoita, että tiedosto olisi tuhoutunut lopullisesti. Poistettuja tietoja voi palauttaa jopa kiintolevyn uudelleen alustamisen jälkeen. Tiedon lopulliseen hävittämiseen on olemassa erilaisia ohjelmia, jotka perustuvat esimerkiksi tietojen ylikirjoittamiseen tai kiintolevyn magnetointiin. Tallennusväline voidaan myös murskata mekaanisesti lukukelvottomaksi. |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

| | |
|---|---|
| | Arkaluontoista henkilötietoja sisältävän aineiston arkistointi vaatii säilytysluvan Kansallisarkistolta, ja aineisto on minimoitava ennen säilytystä. Tällaisen aineiston jatkokäyttö on mahdollista tutkimusluvalla.<br><br>**Vinkkejä**<br><br>• Muistathan, että aineiston anonymisointi ja hävittäminen tai arkistointi tehdään viimeistään tutkimusluvan määräajan päättyessä.<br>• Aito anonymisointi edellyttää sekä suoran että välillisen tunnistamisen mahdollisuuden poistamista sekä tunnisteavaimen hävittämistä.<br>• Näytteisiin liittyvä data voidaan arkistoida biopankkiin.<br>• Useilla yliopistoilla ja virastoilla on oma sisäinen ohjeistuksensa tallennusvälineiden hävittämisestä.<br><br>**Linkkejä**<br><br>• FSD: Aineiston hävittäminen, URL: http://www.fsd.uta.fi/aineistonhallinta/fi/fyysinen-sailytys.html#havittaminen |
| **5.3 Arvioi, kuinka paljon aikaa ja työtä tarvitaan aineiston valmistelemiseen julkaisua tai arkistointia varten.** | Sensitiivisen datanhallinnan kustannuksia mietittäessä kannattaa ottaa huomioon mm:<br><br>• aineiston anonymisoinnin kustannukset (aika ja tarvittavat ohjelmistot)<br>• korkeamman turvatason vaatimukset tekniikalle |

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

## Keskeiset käsitteet

**anonymisointi** Tietoarkiston aineistonhallintakäsikirja, http://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html: Tieto on anonyymiä eli tunnisteetonta, jos tunnusomaiset piirteet (esimerkiksi epäsuorat tunnisteet yhdistettynä) koskevat samanlaisina useampaa henkilöä ja jos katsotaan, että henkilöä ei voida tunnistaa huomioiden kohtuullisesti toteutettavissa olevat toimenpiteet.

**arkaluonteinen henkilötieto** Henkilötietolain mukaan arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:

1) rotua tai etnistä alkuperää;

2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;

3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;

4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;

5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka

6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia. (Lähde: http://www.tietosuoja.fi/fi/index/sanasto.html)

**arkistointi** Arkistoinnilla varmistetaan asiakirjojen käytettävyys ja säilyminen sekä huolehditaan asiakirjoihin liittyvä tietopalvelu, https://www.finlex.fi/fi/laki/ajantasa/1994/19940831

**data-arkisto** Data-arkistoon tallennetaan tutkimusaineistoja projektin aikaista käsittelyä ja pitkäaikaissäilytystä varten.

**datarepositorio** sanaa käytetään ylätason käsitteenä eritasoisille tietokannoille, joihin datan voi tallentaa ja kuvailla. Data-arkisto sanasta tämä eroaa siten, että data-arkistot tulkitaan tietokannaksi, joissa data säilyy pitkään. Repositorio sen sijaan välttämättä takaa datan pitkäaikaisesta säilymisestä ja osaan repositorioista tallennetaan vain metadataa (ei varsinaista dataa). Datarepositorioita on listattu re3data-palveluun.

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

**eettinen ennakkoarviointi** – Tutkimuseettisen toimikunnan antama lausunto tutkimuksen eettisestä hyväksyttävyydestä.

**henkilörekisteri** Henkilörekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta (ns. looginen henkilörekisteri)
http://www.tietosuoja.fi/fi/index/sanasto.html

**henkilötieto** Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.
(Lähde: http://www.tietosuoja.fi/fi/index/sanasto.html)

**henkilötietojen käsittely** tarkoitetaan kaikkia toimintoja, joita kohdistetaan henkilötietoihin, esimerkiksi henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä (Lähde: http://www.tietosuoja.fi/fi/index/sanasto.html)

**henkilötietojen säilytysaika** eri tietoryhmien suunnitellut poistamisen määräajat tai ne kriteerit, joilla tietojen säilyttämisajat määritellään. Säilytysajat liittyvät tietojen minimoinnin sekä säilytyksen rajoittamisen periaatteisiin. Määritellyn säilytysajan perusteella on pystyttävä arvioimaan, kuinka kauan rekisteröityä koskevia tietoja käsitellään. Ei ole riittävää todeta, että henkilötietoja tullaan säilyttämään niin kauan kuin on tarpeellista tiettyjen laillisten tarkoitusten saavuttamiseksi.

**käsittelijä** Henkilötietojen käsittelijä käsittelee tietoja rekisterinpitäjän lukuun. Käsittelijän on toteutettava suojatoimia rekisteröidyn oikeuksien suojelemiseksi.

**käsittelyperuste** Henkilötietojen käsittely edellyttää aina laista löytyvää käsittelyperustetta. Peruste on määritettävä ennen käsittelyn aloittamista. Kun henkilötietojen käsittely sidotaan johonkin käsittelyperusteeseen, perustetta ei voi enää vaihtaa toiseen.

Tietosuoja-asetuksessa on kuusi eri perustetta, joilla henkilötietojen käsittely on mahdollista:

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

- rekisteröidyn suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleinen etu ja julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

http://tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/kasittelyperusteet.html

**käsittelytoimet** henkilötietojen kerääminen, tallettaminen, järjestämistäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistämistäminen, suojaaminen, poistamistaminen jatuhoaminen sekä muut mahdolliset käsittelytoimet

**käyttötarkoitus** yleisellä tasolla tieteellinen tutkimus, tarkennetaan esim. tutkimussuunnitelman ja suunnitelmassa kuvatun tarkoituksen avulla

**metadata/metatieto** on tietoa tiedosta eli kuvailevaa ja määrittävää tietoa jostakin tietovarannosta tai sisältöyksiköstä

**minimointi** henkilötietojen oltava tarpeellisia suhteessa käsittelytarkoituksiin

**pseudonymisointi** : henkilökohtaisesti tunnistettavan materiaalin korvaaminen keinotekoisilla tunnisteilla

- Henkilötietojen käsittelemistä niin, että tietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja (esim salausavainta). (Lähde: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html)

**rekisterinpitäjä** Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. (Lähde: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html)

*"Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn*

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083

*merkitys yksityisyyden suojan kannalta (Henkilötietolaki 32 §). Vastaavat velvoitteet sisältyvät EU:n yleiseen tietosuoja-asetukseen."*

Antti ketolan webinaari: Rekisterinpitäjä = määrittelee käsittelyn tarkoitukset ja keinot (tapauksen mukaan tutkimusorganisaatio tai tutkija/tutkijaryhmä)
•Funktionaalinen käsite, määrittelee vastuun

**seloste käsittelytoimista** Rekisterinpitäjän ja rekisterinpitäjän lukuun henkilötietoja käsittelevän on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista.

**suojatoimet** tietosuojalainsäädännön lisäksi sovellettavat lisätoimet, esimerkiksi kansallinen erityislainsäädäntö, tietosuojavastaavan nimittäminen, vaikutusten arviointi, auditoinnit, lokitietojen kerääminen jne.

**suostumus** (HetiL 3 §) (= Informoitu suostumus)
Suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.
(Lähde: http://www.tietosuoja.fi/fi/index/sanasto.html)

**Transparency** – avoimuus suhteessa tutkittaviin, kerrotaan mahdollisuuksien mukaan tutkimuksesta ja aineiston käytöstä

**tunnisteellinen aineisto** Tietoarkiston aineistonhallintakäsikirja, http://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html: Tieto on tunnisteellista, jos sen perusteella voidaan tunnistaa yksittäinen henkilö. Tunnistaminen voidaan tehdä yhden tai useamman henkilölle tunnusomaisen fyysisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella.

**vaikutusten arviointi** arviointi käsittelytoimien vaikutuksista henkilötietojen suojalle

Viittausohje: Tuuliprojekti. (2018, June 27). Ohje arkaluonteisia henkilötietoja sisältävän datan hallinnan suunnitteluun ja keskeiset käsitteet. Zenodo. http://doi.org/10.5281/zenodo.1299083