



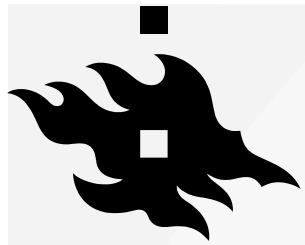
KUINKA VALMISTAUTUA YLEISEEN TIETOSUOJA- ASETUKSEEN?

Jarkko Reittu
Tietosuojavastaava, Lakimies
Helsingin yliopisto, Yleishallinto
jarkko.reittu@helsinki.fi



ESITYKSEN SISÄLTÖ

1. Yleisen tietosuoja-asetuksen asettamat vaatimukset
2. Kuinka valmistautua asetukseen käytännössä?



EU:N YLEISESTÄ TIETOSUOJA-ASETUKSESTA

- Asetus nojautuu periaatteisiin
- Hylättävä vanha ajattelutapa henkilörekistereistä ja rekisterinpitäjistä
- Asetusta lähestyttävä henkilötietojen käsittelyn kautta
- Asetuksen suomennos on keho ja saattaa johtaa harhaan
- Asetukseen on jätetty tarkoituksella paljon tulkinnanvaraa: rekisterinpitäjän tulee päättää itse tarvittavat toimenpiteet
- Kuka täytyy vastuuttaa? yksikön johtaja, tietojärjestelmän omistaja tai vastuullinen tutkija
 - TIKE, tietosuojavastaava tai juristit eivät voi vastata käsittelyn lainmukaisuudesta: toimivat ainoastaan rajallisena tukena
- Kaikkia velvoitteita ei pystytä hoitamaan kerralla: kyseessä on jatkuva prosessi ja asiat on hoidettava paloissa keskittyen ensiksi suurimpiin riskeihin

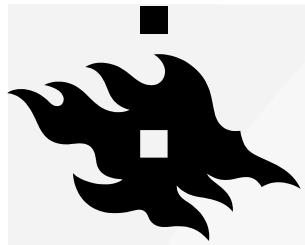


ARTIKLA 5 - HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET

Henkilötietojen käsittelylle asetetut vaatimukset:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen
- Tietojen eheys ja luottamuksellisuus

➤ **Osoitusvelvollisuus**



REKISTERINPITÄJÄN VELVOLLISUUDET

- **Osoitusvelvollisuus:** Rekisterinpitäjän on pystyttävä osoittamaan **kirjallisesti**, että rekisterinpitäjä noudattaa tietosuojalainsäädäntöä, henkilötietojen käsittelyä koskevia periaatteita sekä toteuttaa lainsäädännön edellyttämät rekisteröityjen oikeudet
- Vastuuta ei voida ulkoistaa; rekisterinpitäjä on 24 artiklan mukaisesti vastuussa siitä, että se toteuttaa tietosuoja-asetuksen edellyttämät **tekniset** ja **organisatoriset** toimenpiteet
 - Toimenpiteet tulee mitoittaa riskiperustaisen arvioinnin perusteella
 - Organisatoriset toimenpiteet: organisaation hallinnollinen tietosuoja, kuten tietosuojapolitiikat ja käytännöt, tietosuojaohjeet ja toimintamallit, sertifikaatit
 - Tekniset toimenpiteet: tietoturva, tekniset suojaustoimenpiteet uusien teknologia ja kustannukset huomioiden
- Artikla 25: Sisäänrakennettu ja oletusarvoinen tietosuoja
- Artikla 30: Kirjanpitovelvollisuus kaikista henkilötietojen käsittelyprosesseista
- Artikla 35: Tietosuojan vaikutustenarviointi (DPIA) pakollinen tietyissä tilanteissa



SISÄÄNRAKENNETTU JA OLETUSARVOINEN TIETOSUOJA

- Tietosuoja ja tietoturva on otettava huomioon jo suunnitteluvaiheessa ennen käsittelyn aloittamista
- Huolehdittava, että henkilötietoja käsitellään tietoturvallisessa ja tietosuojavaatimukset täyttävässä ympäristössä
- Toteuttamisessa voidaan käyttää esimerkiksi seuraavia toimenpiteitä:
 - Henkilötietojen pseudonymisointi
 - Riittävät suojatoimet
 - Koulutus, ohjeet, määräykset, sitoumukset ja sopimukset
 - Prosessit, käytännesäännöt, sertifikaatit
 - Tiedon salaaminen
 - Auditoinnit
 - Tekniset rajoitukset ja valvonta



ILMOITUSVELVOLLISUUS TIETOTURVALOUKKAUKSISTA 72H SISÄLLÄ

- Ilmoitus tehdään tietosuojaviranomaisella ja rekisteröidylle
- 33 artiklan mahdollistama poikkeus: jos tiedot on salattu, ilmoitusta ei tarvitse tehdä rekisteröidylle
- Sisältää myös velvollisuuden pitää kirjaa tapahtuneista loukkauksista



HUONEENTAULU REKISTERÖITYJEN OIKEUKSISTA

- **Oikeus saada läpinäkyvää informaatiota (Artikla 12-14, Artikla 19)**
 - Silloin, kun henkilötiedot kerätään suoraan rekisteröidyltä
 - Silloin, kun henkilötiedot kerätään muualta kuin rekisteröidyltä
- **Oikeus saada pääsy tietoihin (*tarkastusoikeus, Artikla 15*)**
- **Oikeus tietojen oikaisemiseen (*virheen oikaisu, Artikla 16*)**
- **Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi", Artikla 17)**
- **Oikeus käsittelyn rajoittamiseen (Artikla 18)**
- **Oikeus siirtää tiedot järjestelmästä toiseen (Artikla 20)**
- **Vastustamisoikeus (Artikla 21)**
- **Automatisoidut yksittäispäätökset; profilointi mukaan luettuna**
- **Oikeus tulla informoiduksi henkilötietojen tietoturvaloukkauksista**
- **Lasten erityisasema**
- **Oikeus saada valvontaviranomaiselta apua**
- **Oikeus luottaa tietoturvaan**



MAHDOLLISET SANKTIOT YKSILÖLLE?

- Asetuksen mukainen vahingonkorvausvastuu ja sakot kohdistuvat rekisterinpitäjään ja henkilötietojen käsittelemään (data processor, ei yksilöön joka käsittelee tietoja), ei yksilöön
- Virkavastuu rikoslain 40 luvun mukaan, jos käsittely katsotaan julkisen vallan käytöksi
 - virkasalaisuuden rikkominen (salassa pidettävän henkilötiedon paljastaminen tai hyödyntäminen)
 - virka-aseman väärinkäyttäminen (henkilötietojen käsittelyä koskevien sääntöjen ja määräysten rikkominen luovutustilanteessa omaksi tai toisen hyödyksi)
 - virkavelvollisuuden rikkominen (henkilötietojen käsittelyä koskevien sääntöjen ja määräysten rikkominen henkilötietojen käsittelyssä)
- Työntekijän vahingonkorvausvastuu työnantajaa kohtaan, kun vahinko on seurausta työntekijän törkeästä huolimattomuudesta tai tahallisuudesta



RIKOSLAKIIN TULEVA UUSI SÄÄDÖS HENKILÖREKISTERIRIKOKSEN TILALLE

9 § . Tietosuoja rikos

Joka muutoin kuin Euroopan parlamentin ja neuvoston luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa asetuksessa (EU) 2016/679 tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin

- 1) yleisen tietosuoja-asetuksen,
- 2) tietosuojalain (xxx/xxxx),
- 3) [henkilötietojen käsittelystä rikosasioissa annetun lain (xxx/xxxx)] tai
- 4) henkilötietojen käsittelyä koskevan muun lain

henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava tietosuoja rikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietosuoja rikoksesta tuomitaan myös 1 momentissa tarkoitettu henkilö, joka toimii vastoin sitä, mitä momentin 1—4 kohdassa tarkoitettussa säännöksessä säädetään henkilötietojen käsittelyn turvallisuudesta.



RIKOSLAKIIN TULEVA UUSI SÄÄDÖS

- Esimerkki 1 rangaistavasta toiminnasta olisi uteliaisuudesta tapahtuva henkilötietojen käsittely ilman käsittelyn oikeuttavaa perustetta.
- Esimerkki 2: Rekisterinpitäjän palveluksessa oleva hävittää henkilötietoja vastoin tietoturvallisuudesta säädettyä. Rangaistavaa voisi olla muun muassa menettely, jossa henkilö lainvastaisesti heittää pois henkilörekisteristä tulostetut asiakirjat huolehtimatta niiden tietoturvallisesta hävittämisestä.
- Tietämättömyys lain sisällöstä koituu tekijän vahingoksi (ignorantia juris nocet)



KUINKA VALMISTAUTUA ASETUKSEEN KÄYTÄNNÖSSÄ?



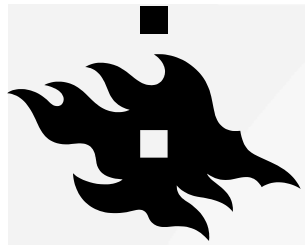
KUINKA VALMISTAUTUA TIETOSUOJA- ASETUKSEEN KÄYTÄNNÖSSÄ?

1. Kartoita ja analysoi henkilötietoja käsittelevät prosessit
2. Päivitä henkilörekisteriselosteet?
3. Toteutuuko informointivelvollisuus?
4. Tarkasta sopimukset
5. Milloin täytyy tehdä tietosuojan vaikutusten arviointi?
6. Selvitä vaatimukset tietojärjestelmille



1. KARTOITA HENKILÖTIETOJA KÄSITTELEVÄT PROSESSIT

- Mitä henkilötietoja kerätään? Miten henkilötietoja kerätään? Laadi tietovuokaavio?
- **Mihin tarkoitukseen henkilötiedot kerätään? Ovatko kaikki kerätyt tiedot tarpeellisia?**
- **Mikä on oikeusperuste henkilötietojen käsittelylle?**
- Kuinka henkilötietoja käsitellään ja säilytetään?
- Kuinka huolehditaan tietoturvasta ja tietosuojasta?
- Kuinka henkilötietojen käsittelyä valvotaan?
- Kuinka on hoidettu henkilötietojen luovutukset ja siirrot?
- **Mitä henkilötiedoille tapahtuu käyttötarkoituksen päättymisen jälkeen?**
- Kuinka hyvin rekisteröidyn oikeudet toteutuvat?



1. HENKILÖTIETOJEN KÄYTTÖTARKOITUS

- Vain käyttötarkoituksen kannalta tarpeellisia ja virheettömiä henkilötietoja voidaan käsitellä (minimisointiperiaate)
 - Tuhoa käyttötarkoituksen kannalta tarpeettomat henkilötiedot. Esim. Onko tieto työntekijän omaisesta työnantajan toiminnan kannalta tarpeellista?
 - Henkilötietoja voidaan käyttää vain siihen tarkoitukseen mihin ne kerätty. Esim. Henkilötietoja ei voida käyttää ohjelmiston kehitystyössä, jos niitä ei ole kerätty tähän tarkoitukseen
 - Poikkeus: tutkimus- ja tilastointi on yhteensopiva alkuperäisen käyttötarkoituksen kanssa
 - Huom. Edes suostumuksellakaan ei ole mahdollista ohittaa käyttötarkoitussidonnaisuutta ja tietojen minimisointiperiaatetta. Esim. henkilötietojen tallentuminen muun toiminnan ohessa sivutuotteena



1. HENKILÖTIETOJEN KÄSITTELYN OIKEUSPERUSTA

- Yleisimmät vaihtoehdot käsittelyn oikeusperustaksi:
 1. Suostumus
 - Laajenee asetuksen myötä tutkimuksen osalta
 - Mahdollista antaa laaja suostumus koskien tiettyjä tutkimusaloja
 2. Laillinen intressi (esim. sopimuksen täyttäminen)
 3. Lakiin perustuvan tehtävän suorittaminen (Yliopistot: tutkimus, opetus sekä tutkimuksen ja taiteellisen toiminnan yhteiskunnallisen vaikuttavuuden edistämien)
 4. Yleinen etu (uusi mahdollisuus asetuksen myötä)
 - Säädetty kansallisessa laissa, jotta peruste olisi käytettävissä
 - Mahdollisesti tulossa tutkimuksen osalta



1. HENKILÖTIEDOT KÄSITTELYN LOPUTTUA

- Vaihtoehdot:
 1. Tuhoaminen
 2. Anonymisointi pysyvästi
 - Anonymisoinnin tasoa on arvioitava ajan kuluessa
 3. Arkistointi kansallisarkiston luvalla
- Tarkasta arkistonmuodostussuunnitelmasta (AMS) asiakirjan ja muun aineiston säilytysajat!
- Koskee myös henkilötietoja sisältäviä tutkimusaineistoja



2. PÄIVITÄ REKISTERISELOSTEET?

- Voimassa olevan lainsäädännön mukaan ”Rekisterinpitäjän on pidettävä rekisteriseloste jokaisen saatavilla.”
- Henkilörekisteriselosteet/tietosuojaselosteet ovat kerätty tällä hetkellä Helsingin yliopiston Kirjaamon WWW-sivuille:
<https://www.helsinki.fi/fi/yliopisto/tietosuojaselosteet-0>
- Tietosuoja-asetus **EI** kuitenkaan sisällä nykyisen henkilötietolain mukaista velvollisuutta koskien rekisteriselosteita, koska asetuksessa ei edes ole henkilörekisterin käsitettä
 - Sen sijaan asetuksen mukaan rekisterinpitäjällä on
 - a) 30 artiklan mukainen velvollisuus pitää kirjaa käsittelytoimista
 - b) 12-14 artiklan mukainen rekisteröidyn informointivelvollisuus



2. KIRJANPITOVELVOLLISUUS KÄSITTELYTOIMISTA

- Asetuksen mukainen velvoite tarkoittaa käytännössä kirjapitovelvollisuutta kaikista henkilötietojen käsittelytoimista
- Sisältö määräytyy artikla 30 mukaan
- Kirjanpito on esitettävä viranomaisille pyydetessä
- Julkinen julkisuuslain puitteissa ja saattaa sisältää salassa pidettävää materiaalia, kuten yksityiskohdat tietoturvasta
- HY:ssä kerätään aluksi e-lomakkeella, myöhemmin itsepalveluna sopivalla työkalulla



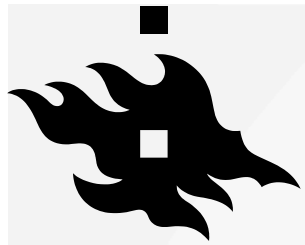
2. TIETOJÄRJESTELMÄSELOSTEET

- Julkisuuslaki 18 § - Hyvä tiedonhallintatapa
- Julkisuuslain mukaan tietojärjestelmistä tulee laatia ja pitää saatavilla seloste, josta tulee myös ilmetä saatavilla olevat julkiset tiedot
 - Koskee kaikkia tietoja
 - Koskee myös tutkimusta, jonka osalta salassapito on mahdollista vain jos voidaan osoittaa mahdollinen vahinko tietojen luovuttamisen seurauksena (vahinkoedellytys)
- Nykyisen julkisuuslain mukainen velvoite, jota ei ole aina muistettu täyttää



3. TOTEUTUUKO INFORMOINTIVELVOLLISUUS?

- Artikloissa 12-14 säädetään rekisteröidyn informointivelvollisuudesta
 - 12 Artikla: yleiset periaatteet
 - 13 Artikla: annettavat tiedot, kun kerätään tiedot rekisteröidyltä
 - 14 Artikla: annettavat tiedot, kun tietoja ei ole saatu rekisteröidyltä
- Vanha tietosuojaseloste täyttää vaatimuksen osittain
- Yhtenäinen prosessi tekeillä HY:ssa



4. TARKASTA SOPIMUKSET

- Kiinnitä huomiota erityisesti henkilötietojen siirtoon* EU/ETA:n ulkopuolelle
 - Toteutuu erityisesti pilvipalveluita käytettäessä
 - Huomioi myös mahdolliset tukipalvelutilanteet, jossa annetaan etätukea EU/ETA-alueen ulkopuolelta
 - Käytännön vaihtoehdot tällä hetkellä:
 1. Rekisteröidyn yksiselitteinen suostumus
 2. **Vain USA:** Privacy Shield, epävarmalla pohjalla USA:n tiedustelulainsäädännön vuoksi
 3. Komission määrittelemät riittävän tietosuojan maat tällä hetkellä: **Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay**
 4. **Komission mallisopimuslausekkeet**, tällä hetkellä paras vaihtoehto. Mallisopimuslausekkeet ovat myös vaarassa (*Irish Data Protection Commissioner v. Facebook and Max Schrems*)
- Uusi velvollisuus: Data Processing Agreement (DPA)

* Huom.! Henkilötietojen siirto ei ole sama asia kuin henkilötietojen luovuttaminen



4. DATA PROCESSING AGREEMENT

- Laadittava henkilötietojen käsittelijän ja rekisterinpitäjän välille, kun tietoja käsitellään rekisterinpitäjän puolesta ja lukuun
 - Tietojärjestelmäsopimukset, **Huom.! Henkilötietojen tallennus on henkilötietojen käsittelyä**
 - Materiaalinsiirtosopimukset (MTA), esim. analyysit rekisterinpitäjän puolesta
 - Tutkimussopimukset
 - Mahdollisesti myös tutkijan ja yliopiston välille, kun tutkija on rekisterinpitäjä ja yliopisto henkilötietojen käsittelijä. Kenellä on pääasiallinen vastuu sopimisesta?
- Myös vanhat sopimukset käytävä läpi, jos tietojen käsittely jatkuu myös 25.5.2018 jälkeen
- Rekisterinpitäjän tulee varmistaa, että suunniteltu henkilötietojen käsittelijä täyttää tietosuoja-asetuksen asettamat vaatimukset henkilötietojen käsittelylle.
- Tietosuoja-asetuksen mukaisesti rekisterinpitäjän ja henkilötietojen käsittelijän välille on laadittava osapuolia sitova **kirjallinen sopimus**, jossa **vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet.**
- Kirjallisen sopimuksen tekemättä jättämisestä uhkana sakko, max. 10 000 000 euroa tai 2 % edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta



4. DATA PROCESSING AGREEMENT - JATKUU

- Sovittava kirjallisesti edellä kuvatun lisäksi:
 1. Käsiteltävä tietoja rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti
 2. Salassapitoehto
 3. Tietoturvasta huolehtiminen 32 artiklan mukaisesti
 4. DPA:n sopimusehtojen ulottaminen myös alihankkijoihin
 5. Rekisterinpitäjää tukevat toimenpiteet, joilla turvataan rekisteröidyn oikeuksien toteutuminen
 6. Avustaminen 32-36 artiklassa säädettyjen velvollisuuksien toteuttamiseksi
 7. Henkilötietojen palauttaminen tai hävittäminen rekisterinpitäjän pyynnöstä
 8. Tarvittavien tietojen toimittaminen rekisterinpitäjälle osoitusvelvollisuuden toteuttamiseksi



4. DATA PROCESSING AGREEMENT - JATKUU

- Helsingin yliopistolla on oma DPA-sopimusmalli suomeksi ja englanniksi
- Katso myös ohje ” Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja”, ohjeen lopusta löytyy suomenkielinen DPA-sopimusmalli:
https://www.hansel.fi/media/filer_public/1d/2c/1d2c32ab-bb9a-49c0-b75c-da64871d1df9/tietosuojaohje.pdf
- Voidaan ottaa tarvittaessa pääsopimuksen liitteeksi
- Ehdot eivät ole lähtökohtaisesti neuvoteltavissa, koska sisältö määräytyy tietosuoja-asetuksen mukaan
- Haasteita DPA:n käyttöönotossa:
 - Ei välttämättä mene läpi isojen toimijoiden kanssa
 - Kuinka saadaan pienet toimijat ymmärtämään tietosuoja-asetuksen asettamat velvollisuudet



5. MILLOIN TEHDÄ TIETOSUOJAN VAIKUTUSTEN ARVIOINTI (DPIA)?

- Arviointi on artiklan 35 mukaan tehtävä kun käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen käsittely aiheuttaa korkean riskin
 - Rekisterinpitäjä tekee riskiarvion ja päätöksen arvioinnin tekemisestä itse
 - Tehtävä erityisesti, jos käsittely koskee arkaluonteisia tietoja ja käsittely on laajamuotoista
- Pyydettävä neuvoja arvion tekemiseksi tietosuojavastaavalta
- Kansallinen lainsäädäntö lisäämässä tiukennuksia asetukseen nähden
 - Lakiehdotuksen mukaan tehtävä aina, kun käsitellään arkaluonteisia tietoja
 - Arviointi toimitettava viranomaisille 30 päivää ennen suunnitellun käsittelyn aloittamista
 - Haaste erityisesti potilastietoja ja näytteitä koskevan tutkimuksen osalta
- HY:ssa tehty yksi asetuksen mukainen DPIA, kysymykset ja työkalut ovat olemassa



5. TIETOSUOJAN VAIKUTUSTEN ARVIOINTI - SISÄLTÖ

- Sisältö määrätty 35 artiklassa:
 - a) Järjestelmällinen kuvaus suunnitelluista käsittelytoimista, ja käsittelyn tarkoituksista, mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut
 - b) Arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden
 - c) Arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä
 - d) Suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.
- Tapauksen mukaan pyydettävä rekisteröityjen tai näiden edustajien näkemyksiä suunnitelluista käsittelytoimista
- Tehtävä uudelleen arviointi suunnitellun käsittelyn toteutumisesta ja ainakin riskin muuttuessa



5. SELVITÄ VAATIMUKSET TIETOJÄRJESTELMILLE

- Onko rekisteröidyn oikeuksien toteutumiseen varauduttu, esim. tietopyynnöt ja tietojen siirrot?
 - Esim. vastaus tietopyyntöön annettava GDPR:n mukaan ilman aiheetonta viivytystä, mutta max. 1 kk sisällä. Huom. julkisuuslain mukaisiin tietopyyntöihin vastattava 14 pv. sisällä.
- Ilmoitus tietoturvaloukkauksista 72 tunnin sisällä loukkauksen tunnistamisesta
 - Huom.! Tietojen salaaminen tärkeää -> ei ilmoitusvelvollisuutta rekisteröidylle
 - HY: Prosessi suunnittelussa TIKE:ssä
- Tarkasta järjestelmän tietoturva-vaatimukset (perustuttava riskiperustaiseen arvioon)
 - Riskiarvioon vaikuttavat
 - Käsiteltävien tietojen määrä
 - Käsiteltävien tietojen laatu (henkilötieto, arkaluonteinen henkilötieto, henkilötunnus)
 - Tietosuojaloukkausten vaikutukset
- Henkilötietojen käsittelyn valvominen



HENKILÖTIETOJEN KÄSITTELYN VALVONTA

- Lokitusvelvollisuus:
 - Seuraa 25 artiklasta (Sisäänrakennettu ja oletusarvoinen tietosuoja)
 - Asetuksessa todetaan, että myös rekisteröidyn tulee pystyä valvomaan henkilötietojensa käsittelyä
 - Lisäksi julkisuuslain 18 § :n (Hyvä tiedonhallintatapa) voidaan katsoa edellyttävän lokitusta
 - Tietoturvaloukkauksista raportointi edellyttää lokitusta
- Lokituksen taso on jätetty rekisterinpitäjän omaan harkintaan riskiarvioon perustuen
- Esim.: tietojen kerääminen, muuttaminen, kysely, luovuttaminen ja siirrot, yhdistäminen ja poistaminen. Tapauskohtaisesti lisäksi myös tehtyjen toimien perusteet, toteutuspäivä ja -aika sekä henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys
- Käytännön esim.: Oodi-järjestelmä: lokitetaan laajasti tietojen lisääminen, katseleminen, muuttaminen ja poistaminen
- Koskee myös manuaalista käsittelyä, lokitus voidaan tehdä myös käsin



KYSYMYKSIÄ?

<https://www.helsinki.fi/>