Tietosuoja-asetus ja tieteellinen tutkimus – mikä muuttuu?

Ylitarkastaja Raisa Leivonen

Tietosuoja tutkijan arjessa-seminaari

16.5.2018

Alkusanat

Peruslähtökohdat – pysyvät samana

Keskeisiä muutoksia

Lopuksi

Alkusanat

Peruslähtökohdat – pysyvät samana

Keskeisiä muutoksia

Lopuksi

Tietosuoja-asetus

- Ryhdytään soveltamaan 25.5.2018
- Kaikissa jäsenvaltioissa suoraan sovellettavaa oikeutta, sisältää kuitenkin kansallista liikkumavaraa
    - Tietosuojalaki (HE 9/2018)
    - Kansallinen erityislainsäädäntö

- Sovelletaan niin yksityisellä kuin julkisella sektorilla – kattaa siis koko tutkimuskentän!

- This is evolution, not revolution!

Tutkimustoiminnan lainsäädäntökehikko..

On kokonaisuudessaan murroksessa..

- Tietosuoja-asetus
- Kansallinen tietosuojalaki
- Tiedonhallintalaki
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä
- Laki kliinisestä lääketutkimuksesta
- Laki lääketieteellisestä tutkimuksesta
- Biopankkilaki
- Genomikeskus jne…

Alkusanat

Peruslähtökohdat – pysyvät samana

Keskeisiä muutoksia

Lopuksi

Tietosuoja-asetus ja tieteellinen tutkimus

- Tieteellinen ja historiallinen tutkimus tunnistetaan yhä erityisen tärkeänä toimintana tietosuoja-asetuksessa
    - Poikkeuksia mm. tietosuojaperiaatteista ja rekisteröidyn oikeuksista

- Tieteellisen ja historiallisen tutkimuksen tarkoituksia varten voi yhä käsitellä henkilötietoja
    - tietosuoja-asetuksen perusteella (6 art. ja 9 art.) tai
    - kansallisen tietosuojalain perusteella (4 §, 6 §)

- Käsittelyn tulee kuitenkin tapahtua tietosuojasäännöksiä noudattaen

Henkilötiedon käsite

- Henkilötietoja ovat kaikki tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen
- Myös pseudonymisoidut tiedot ovat henkilötietoja!

Esimerkkejä henkilötiedoista

- Nimi
- Kotiosoite
- Sähköpostiosoite, kuten etunimi.sukunimi@yritys.com
- Puhelinnumero
- IP-osoite
- Potilastiedot
- Valokuva

Tietojen anonymisointi

- Anonymisointi tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei enää voida tunnistaa niistä.
- Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi.
  - Arvioissa huomioitava mm. saatavilla oleva tiedot ja muiden rekisterinpitäjien rekisterit
- Anonymisoinnissa on otettava huomioon kaikki kohtuudella toteutettavissa olevat keinot, joiden avulla tiedot voitaisiin muuttaa takaisin tunnisteellisiksi
  - tunnistamisesta aiheutuvat kulut,
  - tunnistamiseen tarvittava aika sekä
  - käytettävissä oleva teknologia

Rekisterinpitäjä

- Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot;

- Toiminnallinen käsite: jaetaan vastuuta sinne, missä todellinen vaikutus on!
- Käsittelyn laillisuuden kannalta olennaiset kysymykset kuuluvat rekisterinpitäjälle

Rekisterinpitäjä määrittää

- Tarkoitukset=miksi tietoja käsitellään?
  - Ennakoitu tulos, johon pyritään
- Keinot=miten henkilötietoja käsitellään?
  - Toimintatavat tuloksen saavuttamiseksi
    - Tekniset ja organisatoriset toimenpiteet
    - Mitä tietoja käsitellään?
    - Kenellä pääsy tietoihin?
    - Kuinka kauan tietoja käsitellään? Jne.

Vastuut asetuksen mukaan

- Rekisterinpitäjän vastuu säilyy
  - Ei voi ulkoistaa vastuuta tietosuojavastaavalle
  - Osoitusvelvollisuus
    - Käytännesäännöt
    - Sertifioinnit
    - Tietotilinpäätös
- Yhteisrekisterinpitäjät (art. 26)
  - Määriteltävä läpinäkyvällä tavalla vastuualueet
- Muutos: henkilötietojen käsittelijä (28 art.)

Alkusanat

Peruslähtökohdat – pysyvät samana

Keskeisiä muutoksia

Lopuksi

Eräitä keskeisiä muutoksia..

- Osoitusvelvollisuus
  - Periaatteiden kautta asetukseen
  - Käsittelyperusteet
  - Rekisteröidyn oikeudet
- Riskiperusteinen lähestymistapa
- Velvollisuus ilmoittaa tietoturvaloukkauksesta
  - Tietosuojaviranomaisille
  - Rekisteröidyille

Tietosuojaperiaatteet

Muutos?

Vaatimustenmukaisuudesta
”Compliance” - lainsäädännön noudattaminen

Osoitusvelvollisuuteen
”Accountability” – lainsäädännön noudattamisen osoittaminen

Tieteellisen tutkimuksen käsittelyperusteita

- Suostumus (6 1 a)
- Kansallisen lainsäädännön nojalla, kun käsittely on tarpeen yleistä etua koskevan tehtävän vuoksi (6 1 e)
  - Kansallinen tietosuojalaki 4 §:n 3 kohta (HE 9/2018)

  ”käsittely on tarpeen tieteellistä tai historiallista tutkimusta taikka tilastointia varten ja se on oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen nähden”
- Rekisterinpitäjän oikeutettu etu (6 1 f)

Erityiset henkilötiedot (TSA 9 art. 1 kohta)

- rotu tai etninen alkuperä
- poliittiset mielipiteet
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettinen tieto tai
- biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

Erityisten henkilötietojen käsittelyperusteita

- Nimenomainen suostumus (9 2 a)
- Käsittely koskee tietoja, jotka rekisteröity saattanut nimenomaisesti julkisiksi (9 2 e)
- Kansallinen lainsäädäntö
  - kun käsittely tarpeen tärkeää yleistä etua koskevasta syystä (9 2 g)
  - Käsittely tarpeen yleisen edun mukaisia tieteellisiä ja historiallisia tutkimustarkoituksia varten (9 2 j)
    - Tietosuojalaki 6 § 7 kohta: tieteellinen ja historiallinen tutkimus ja tilastointi

Onko tutkimus jo käynnissä ja käsittelyperusteena suostumus?

- Tarkista, että suostumus on tietosuoja-asetuksen mukainen!! (TSA res. 171)

- Suostumus on oltava
    - YKSILÖITY (käyttötarkoituksen on oltava ennalta määritelty, nimenomainen ja laillinen)
    - TIETOINEN (informaation oltavaa erillään, helposti ymmärrettävissä ja saatavilla olevassa muodossa ja yksinkertaisella kielellä + 13 art. informointivelvoite)
    - aidosti VAPAAEHTOINEN (heikommassa asemassa olevat) ja
    - YKSISELITTEINEN tahdonilmaisu (edellyttää aktiivista toimea)
    - NIMENOMAINEN erityisten henkilötietoryhmien osalta
    - DOKUMENTOITU osoitusvelvollisuuden osoittamiseksi
    - PERUUTETTAVISSA yhtä helposti, kuin annettukin (tästä informoitava jo suostumusta pyydettäessä)
    - Hallinnointia koskevien käytänteiden oltava TIETOSUOJA-ASETUKSEN MUKAISIA..

Onko tutkimus jo käynnissä ja käsittelyperusteena suostumus?

- Jos suostumus ei ole tietosuoja-asetuksen mukainen
  - Pyydä uusi, tietosuoja-asetuksen mukainen suostumus
  - Arvioi, voiko käsittely perustua johonkin muuhun käsittelyperusteeseen
    - Varmista, että lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä koskevat periaatteet toteutuvat
      - Jos käsittely peruste muuttuu, informoitava rekisteröityjä
    - Käsittelyperusteen vaihtaminen toiseen ei mahdollista, kun tietosuoja-asetusta ryhdytään soveltamaan
  - Jos et voi perustaa käsittelyä toiseen oikeusperusteeseen tai pyytää uutta tietosuoja-asetuksen vaatimukset täyttävää suostumusta, henkilötietojen käsittely on lopetettava.

Rekisteröidyn oikeudet

- Lähtökohta: rekisteröidyllä on myös tutkimustoiminnassa käytössään tietosuoja-asetuksen mukaiset oikeudet (riippuvaisia käsittelyperusteesta)
  - Jos käsitellään samanaikaisesti myös muihin tarkoituksiin, poikkeuksia sovelletaan ainoastaan historiallisessa ja tieteellisessä tutkimuksessa

- Tieteellisessä tutkimuksessa oikeuksia voidaan rajoittaa tapauskohtaisen harkinnan perusteella, joka on kaksiportainen
  - Tietosuoja-asetuksen 89 art. 2 kohta mahdollistaa kansallisten poikkeuksien säätämisen, vain SILTÄ OSIN,
    1) kun tällaiset oikeudet estävät erityisten tarkoitusten saavuttamisen tai vaikeuttavat sitä suuresti JA
    2) tällaiset poikkeukset ovat tarpeen näiden tarkoitusten täyttämiseksi

Tietosuojalaki 31 § rajoitusten edellytykset

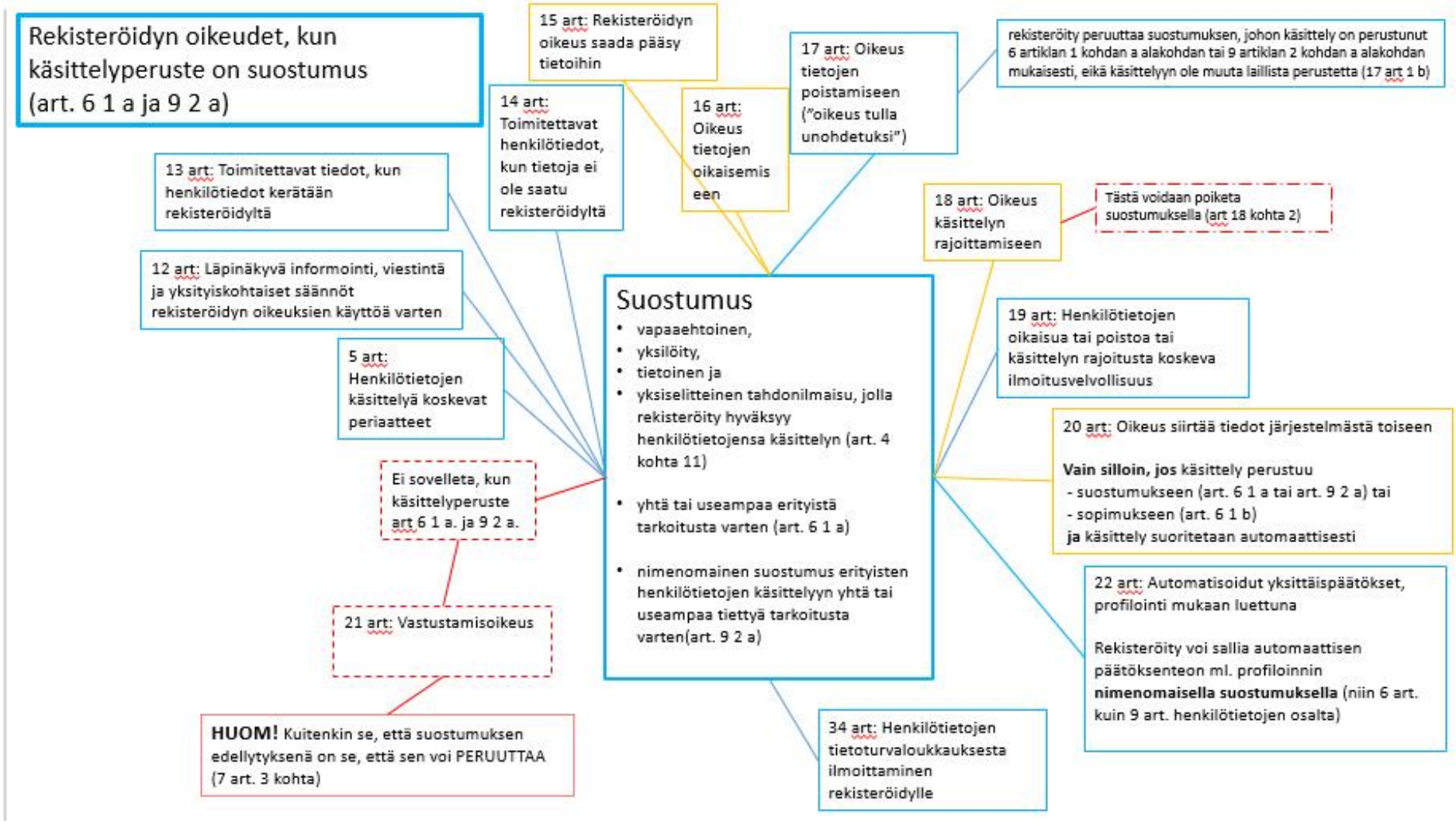
Käsiteltäessä henkilötietoja tieteellistä tai historiallista tutkimustarkoitusta varten voidaan tietosuoja-asetuksen 15, 16, 18 ja 21 artiklassa säädetyistä rekisteröidyn oikeuksista tarvittaessa poiketa edellyttäen, että:

1) käsittely perustuu asianmukaiseen tutkimussuunnitelmaan;

2) tutkimuksella on vastuuhenkilö tai siitä vastaava ryhmä; ja

3) henkilötietoja käytetään ja luovutetaan vain historiallista tai tieteellistä tutkimusta taikka muuta yhteensopivaa tarkoitusta varten sekä muutoinkin toimitaan niin, että tiettyä henkilöä koskevat tiedot eivät paljastu ulkopuolisille

- Vaikutustenarviointi tulee toimittaa kirjallisesti tiedoksi tietosuojavaltuutetulle 30 päivää ennen käsittelyyn ryhtymistä


Rekisteröidyn oikeudet, kun käsittelyperuste on suostumus (art. 6 1 a ja 9 2 a)
15 art: Rekisteröidyn oikeus saada pääsy tietoihin
14 art: Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä
16 art: Oikeus tietojen oikaisemiseen
17 art: Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")
rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut 6 artiklan 1 kohdan a alakohdan tai 9 artiklan 2 kohdan a alakohdan mukaisesti, eikä käsittelyyn ole muuta laillista perustetta (17 art 1 b)
13 art: Toimitettavat tiedot, kun henkilötiedot kerätään rekisteröidyltä
18 art: Oikeus käsittelyn rajoittamiseen
Tästä voidaan poiketa suostumuksella (art 18 kohta 2)
12 art: Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten
Suostumus
vapaaehtoinen,
yksilöity,
tietoinen ja
yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn (art. 4 kohta 11)
yhtä tai useampaa erityistä tarkoitusta varten (art. 6 1 a)
nimenomainen suostumus erityisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten(art. 9 2 a)
19 art: Henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus
5 art: Henkilötietojen käsittelyä koskevat periaatteet
20 art: Oikeus siirtää tiedot järjestelmästä toiseen
Vain silloin, jos käsittely perustuu
- suostumukseen (art. 6 1 a tai art. 9 2 a) tai
- sopimukseen (art. 6 1 b)
ja käsittely suoritetaan automaattisesti
Ei sovelleta, kun käsittelyperuste art 6 1 a. ja 9 2 a.
22 art: Automatisoidut yksittäispäätökset, profilointi mukaan luettuna
Rekisteröity voi sallia automaattisen päätöksenteon ml. profiloinnin nimenomaisella suostumuksella (niin 6 art. kuin 9 art. henkilötietojen osalta)
21 art: Vastustamisoikeus
HUOM! Kuitenkin se, että suostumuksen edellytyksenä on se, että sen voi PERUUTTAA (7 art. 3 kohta)
34 art: Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Riskiperusteinen lähestymistapa

- Henkilötietojen käsittelyyn liittyvä riski on arvioitava AINA, ennen kuin henkilötietoja ryhdytään käsittelemään
  - Osoitusvelvollisuus
  - Riskien todennäköisyys ja vakavuus vaihtelee
  - Objektiivinen arvio

- Rekisterinpitäjä ja henkilötietojen käsittelijä velvoitetaan ryhtymään toimiin, jotka vastaavat henkilötietojen käsittelyyn kulloinkin liittyvää riskiä
  - Tekniset ja organisatoriset toimenpiteet

- Riskiarviointi on jatkuvaa toimintaa: toimenpiteiden riittävyyttä on arvioita jatkuvasti ja päivitettävä tarvittaessa

Riskit

- fyysisiä, aineellisia tai aineettomia vahinkoja,
  - käsittely saattaa johtaa syrjintään,
  - identiteettivarkauteen tai
  - petokseen,
  - taloudellisiin menetyksiin,
  - maineen vahingoittumiseen,
  - salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetykseen tai
  - aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa

Riskiarvio tehdään tutkittavan (rekisteröidyn) näkökulmasta

89 artikla ”yleisen edun mukainen arkistoin taikka tieteellinen tai historiallinen tutkimus tai tilastointi”

- Sovellettava tämän asetuksen mukaisia rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia.
- Suojatoimilla on varmistettava, että on toteutettu tekniset ja organisatoriset toimenpiteet
  - Erityisesti varmistettava tietojen minimoinnin periaatteen toteutuminen
    - voidaanko anonymisoida?
    - voidaanko pseudonymisoida?

Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun käsittelyyn kohdistuu korkea riski (35 art.)

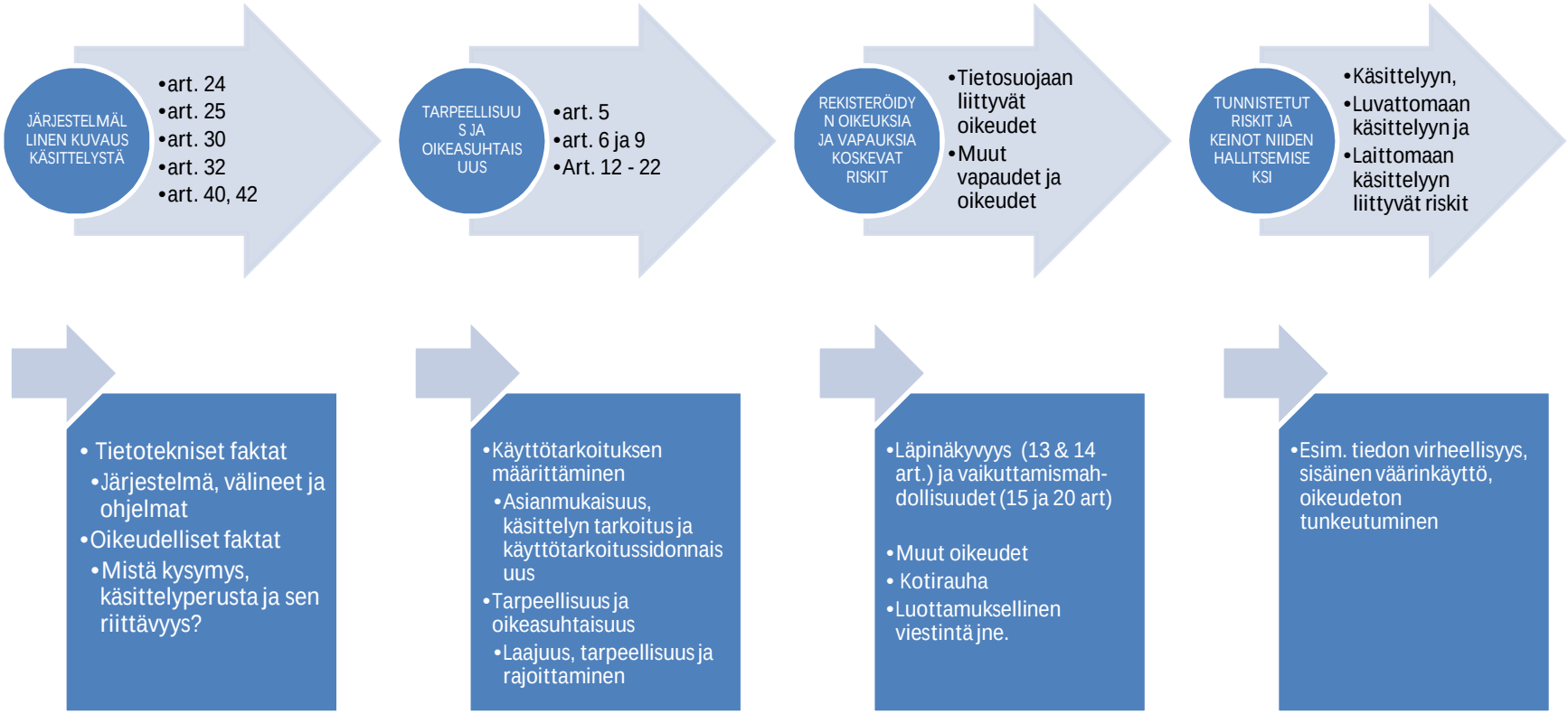
1. Tietosuoja-asetus 35 art. Kohta 3
- Systemaattinen ja kattava profilointi
- Laajamittainen erityisten henkilötietoryhmien käsittely
- Laajamittainen ja järjestelmällinen yleisölle avoimen paikan valvonta

2. WP 29 Ohje 248 liite 2.

3. Valvontaviranomaisen lista korkean riskin käsittelytoimista

4. Kansallinen lainsäädäntö edellyttää vaikutustenarviointia suojatoimena

Vaikutustenarviointi



Käsittelytoimien systemaattinen kuvaus

- Luodaan käsittelystä kokonaiskuva
  - Huomioidaan luonne, laajuus, asiayhteys, tarkoitukset ja näistä seuraavat
  - Tunnistetaan vastaanottajat, tietovirrat ja säilytysaika
  - Toiminnallinen kuvaus käsittelytoimenpiteistä
  - Käsittelytoiminpiteet ja niihin liittyvät päätöksenteko dokumentoidaan
  - Luodaan tarkistus ja päivityskäytännöt

Tarpeellisuus ja oikeasuhtaisuus

- Käsittelyperuste
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen
- Eheys ja luottamuksellisuus
- Rekisteröidyn oikeudet
- Yksilön vapaudet

Riskin arviointi ja suunnitellut toimenpiteet

- Riskiarvio
- Arvioi mahdolliset seuraukset
- Arvioi riskin vakavuus
- Tunnista uhat
- Arvioi riskin todennäköisyys
- Valitse toimenpiteet riskien hallitsemiseksi

Esimerkkejä toimenpiteistä:

- päätös olla käsittelemättä tietyn tyyppisiä tietoja
- käsittelyn kohteen täsmentäminen tai rajaaminen
- säilytysaikojen lyhentäminen
- lisäsuojaustoimenpiteiden käyttöönotto
- henkilötietojen anonymisointi tai pseudonymisointi
- kirjallisten käsittelyohjeiden käyttöönotto
- järjestely tai menettelytapa, joka tukee rekisteröityjen oikeuksien käyttöä

Vaikutustenarvioinnin validointi

- Jos käsittely voi johtaa suureen riskiin yksilön oikeuksien ja vapauksien näkökulmasta, vaikutustenarviointi on pakollinen
- Ymmärrä vaikutustenarvioinnin tarkoitus;
  1. Tunnista riskit,
  2. Arvioi tarpeelliset toimenpiteet ja
  3. Pienennä käsittelyyn liittyvä riski!
- Kun vaikutustenarviointia edellytetään, sen laiminlyönti on tietosuoja-asetuksen mukainen rikkomus
- Laadi asianmukainen dokumentaatio tehdystä arvioista, ja hanki tarvittaessa johdon katselmus, päätös ja hyväksyntä

Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on

- siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen
- vahingossa tapahtuva tai lainvastainen
- tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin

Tietoturvaloukkauksista ilmoittaminen

- Tietosuojarikkomuksesta seuraa todennäköinen riski yksilön oikeuksille ja vapauksille

  → ILMOITUS TIETOSUOJAVIRANOMAISELLE

  - Ilmoitus on tehtävä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta (tietoiseksi tulemisesta)

- Tietosuojarikkomuksesta seuraa todennäköisesti korkea riski yksilön oikeuksille ja vapauksille

  → ILMOITUS REKISTERÖIDYLLE

RISKIARVIOINNISSA HUOMIOITAVA SEIKAT

1) Tietoturvarikkomuksen tyyppi
2) Henkilötietojen luonne, arkaluonteisuus ja määrä
3) Tunnistamisen helppous
4) Tietovuodon seurauksien vakavuus
5) Rekisteröidyn erityiset ominaisuudet
6) Rekisterinpitäjän erityiset ominaisuudet
7) Yleiset huomiot

Alkusanat

Peruslähtökohdat – pysyvät samana

Keskeisiä muutoksia

Lopuksi

Tietosuojatyökaluja tutkijalle (1/2)

1. Määritä tutkimussuunnitelmassa tutkimustehtävä ja henkilötietojen käyttötarkoitus mahdollisimman täsmällisesti.
2. Analysoi, mitkä henkilötiedot ovat tarpeellisia tutkimuksesi toteuttamiseksi (tietojen määrä ja luonne). Arvioi henkilötietojen tarpeellisuutta myös tutkimuksen aikana ja pyri minimoimaan käsiteltävien henkilötietojen määrä mahdollisimman nopeasti.
3. Tee riskiarvio käsittelytoimistasi ja suhteuta suojaustoimenpiteet sen mukaisesti koko käsittelyn elinkaaren ajaksi.
4. Suunnittele etukäteen menettelytavat eri tilanteiden, kuten tietoturvaloukkausten varalle.
5. Tunnista käsittelyperuste ja päivitä se tarvittaessa tietosuoja-asetuksen mukaiseksi (esim. suostumus).

Tietosuojatyökaluja tutkijalle (2/2)

6. Kartoita käsittelyperusteeseen liittyvät rekisteröidyn oikeudet ja varmista niiden toteutuminen.

7. Varaudu osoittamaan, että tietosuojasäännökset on huomioitu tutkimuksessasi: dokumentoi tietosuojaperiaatteiden toteutuminen ja muut tietosuoja-asetuksen mukaiset menettelytavat.

8. Tunnista roolisi ja vastuusi! Rekisterinpitäjänä vastaat henkilötietojen käsittelyn lainmukaisuudesta koko käsittelyn elinkaaren ajan – tee käsittelijöiden kanssa kirjallinen sopimus ja laadi selkeät ohjeet käsittelylle.

9. Vaali luottamusta ja varmista tulevaisuuden tutkimuksen edellytykset noudattamalla tietosuojasäännöksiä sekä huolehtimalla läpinäkyvyydestä ja avoimuudesta.

10. Tietosuojatyökalut ovat välttämätön osa tutkijan työkalupakkia! Päivitä osaamistasi ja seuraa verkkosivuja: www.tietosuoja.fi

Lisätietoja

Tietosuojavaltuutetun verkkosivut:

www.tietosuoja.fi

Tietosuoja-asetus teksti:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT