Tietosuoja ja kirjaaminen

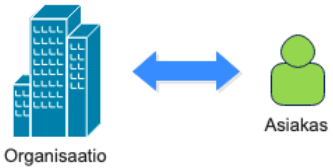
Kysymykset

- Esityksen aikana lähetetyt kysymykset löydät täältä

Sote-sääntely

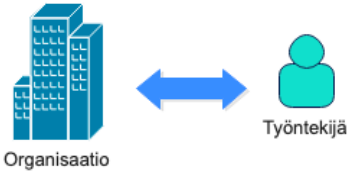
Toimialakohtainen

- Laki sosiaalihuollon asiakasasiakirjoista (254/2015)
- Sosiaalihuoltolaki (1301/2014)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (892/2000)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)
- Terveydenhuoltolaki (1326/2010)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki ikääntyneen väestön toimintakyvyn tukemisesta sekä iäkkäiden sosiaali- ja terveyspalveluista (980/2012)
- Päihdehuoltolaki (41/1986)
- Laki vammaisuuden perusteella järjestettävistä palveluista ja tukitoimista (380/1987)
- Laki kehitysvammaisten erityishuollosta (519/1977)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Työterveyshuoltolaki (1383/2001)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)



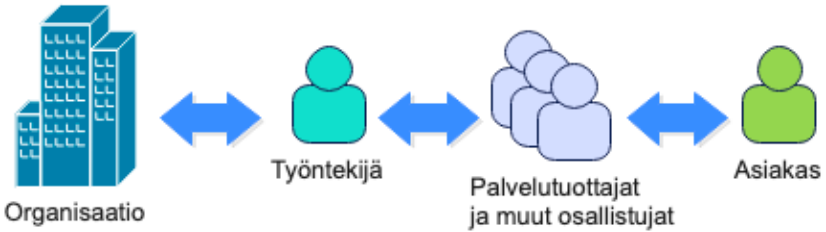
Työntekijän / Työnantajan vastuujako

- Osakeyhtiölaki (624/2006)
- Työsopimuslaki
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Tiedonhallintalaki
- Arkistolaki
- YT-lait 3 kpl
- Laki yhteistoiminnasta yrityksissä (334/2007)
- Laki työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnassa ja hyvinvointialueella (449/2007)
- Laki yhteistoiminnasta valtion virastoissa ja laitoksissa (1233/2013)
- Laki yksityisyyden suojasta työelämässä



Tietosuoja-asetus (679/2016) ja tietosuojalaki (1050/2018)

- Yleiset henkilötietojen käsittelyyn liittyvät reunaehdot kaikkialla
- Ensisijaisesti sovellettavaa lainsäädäntöä (SEUT)
  - Käsittelyn lainmukaisuusperusteet
  - Informointi käsittelystä
  - Rekisteröityjen oikeudet



Organisaatio

- Vastaa käsittelyn ohjeistamisesta ja kantaa vastuun käsittelystä. Palvelun järjestäjän vastuu käsittelyn lainmukaisuudesta.

Työntekijä

- Velvollisuus noudattaa työnantajan direktio-oikeutta ja toimia työnantajan intressejä edistävästi.

Palvelutuottajat
ja muut osallistujat

- Velvollisuus toimia palvelun järjestäjän / lain ja sopimusten määrittämissä raameissa ja rekisterinpitäjän ohjeistuksella (koskee myös heidän työntekijöitä).

Asiakas

- Oikeus saada riittävä tieto henkilötietojensa käsittelystä, mahdollisuus käyttää oikeuksiaan koko palveluverkostossa.

Lainmukaisuusperuste

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
  - henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja läpinäkyvästi ja vain, kun siihen löytyy jostain lainsäädännöstä johdettava syy, esimerkiksi
    - palvelujen tarjoamiseen liittyvä oikeus (palvelusopimus)
    - Lakisääteinen velvoite (laajuus vain se, mitä laki määrittää!)
    - Suostumus
- Käyttötarkoitussidonnaisuus
  - henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Muu käsittely on kiellettyä
- Tietojen minimointi
  - Vain niitä tietoja saa käsitellä, mitkä ovat tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.
- Täsmällisyysvaatimus
  - Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Tietojen tulee olla totta.
- Säilytyksen rajoittaminen
  - Saa säilyttää vain niin kauan, kuin tarve ja lainmukaisuusperuste on olemassa.
- Eheys ja luottamuksellisuus
  - Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus

Suostumus

- Jotta suostumus on pätevä, sen on oltava
  - yksilöity
  - tietoinen
  - aidosti vapaaehtoinen ja
  - yksiselitteinen tahdonilmaisu
- Kun pyydät suostumusta, on yksilöitävä käyttötarkoitus (tai tarkoitukset), johon tietoja kerätään. Eri käyttötarkoituksia varten on pyydettävä erilliset suostumukset.
- Suostumus ei ole aidosti vapaaehtoinen, jos rekisteröity on heikommassa asemassa suhteessa rekisterinpitäjään. Rekisteröity voi olla heikommassa asemassa esimerkiksi silloin, jos olet rekisteröidyn työnantaja tai viranomainen tai rekisteröity on lapsi, vanhus tai sairaudesta johtuvasta syystä kyvytön ymmärtämään suostumuksen sisältöä.
- Suostumuksen antamisesta on oltava mahdollisuus kieltäytyä, ja se on voitava peruuttaa ilman haitallisia seurauksia. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen.
- Sinun on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn, ja että annettu suostumus täyttää sille laissa säädetyt edellytykset.
- Suostumuksen saaminen on kyettävä erityisesti osoittamaan, kun käsitellään erityisiä tietoryhmiä

Suostumusta pyydettäessä on kerrottava...

- rekisterinpitäjä tai rekisterinpitäjät (yhteisrekisterinpitäjyys) ja muut mahdolliset tahot, joille tietoja luovutetaan
- kaikki erilliset käyttötarkoitukset, joita varten suostumus on pyydetty
- mitä tietoja rekisteröidyltä kerätään
- rekisteröidyn oikeus peruuttaa suostumus
- tietojen käyttäminen automatisoitujen yksittäispäätösten tekemiseen ja profilointiin
- riskit tietojen siirrosta EU:n ulkopuolisiin maihin, kun maan osalta ei ole tehty päätöstä tietosuojan tason riittävyyden osalta ja asianmukaisia suojatoimia ei ole toteutettu.

Oikeus saada tietoja

- Oikeus saada tietoa henkilötietojen käsittelystä
  - henkilötietojensa keräämisestä sekä käsittelystä
  - häneen kohdistuvasta tietoturvaloukkauksesta.
  - henkilötietojen oikaisuista tai poistoista, jos niistä on tehty ilmoitus tahoille, joille henkilötietoja on luovutettu.
- käsitelläänkö hänen henkilötietojaan vai ei, ja mitä henkilötietoja hänestä on tallennettu.
- Halutessaan kopio tiedoistaan
  - Terveydenhuollon tiedot arkistoituvat Kanta-palveluun, ja rekisteröidyt voivat katsoa omat potilastietonsa Omakanta –verkkopalvelusta, mutta hänellä on oikeus myös muihin kuin Kantaan siirrettyihin tietoihin!

Oikeudet vaikuttaa käsittelyyn

- Rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi, kuten profilointiin.
- Henkilöllä on oikeus vaatia, että häntä koskevat virheelliset, epätarkat tai puutteelliset henkilötiedot oikaistaan tai täydennetään.
- Henkilöllä on oikeus vaatia, että tarpeettomat henkilötiedot poistetaan.
- Henkilöllä on tietyissä poikkeustapauksissa oikeus saada henkilötietonsa kokonaan poistettua organisaation rekistereistä.
  - Poistamisoikeutta ei ole silloin, kun henkilötietojen käsittely perustuu lakisääteisen velvoitteeseen.
- Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista (esim. jos tietojen paikkansapitävyys on kiistetty).
- Oikeus siirtää tiedot järjestelmästä toiseen, jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen.
  - Tämä oikeus ei koske sellaista henkilötietojen käsittelyä, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Näin ollen oikeutta ei sovelleta kaikkiin sote-alan henkilörekistereihin, mutta on silti Kannan kautta usein mahdollista
- Henkilöllä on oikeus henkilökohtaiseen, erityiseen tilanteeseensa perustuen vastustaa henkilötietojensa käsittelyä.
  - Vastustamisoikeutta ei ole silloin, kun henkilötietojen käsittely perustuu lakisääteiseen velvoitteeseen.
- Henkilöllä on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta.

Erilaisen tiedon erottaminen

- Mikä on asiakastietoa
- Mikä on potilastietoa
- Mikä on henkilötietoa

- Tietojen kerääjä ja tallentaja vastaa lainmukaisuudesta
- Tietojen luovuttaja vastaa luovutuksen lainmukaisuudesta
  - Huomaa myös kenelle luovutat! WhatsAppia käytettäessä luovutat tietoja myös Meta:lle Yhdysvaltoihin.

Riskejä

- Käytetään sovelluksia tai laitteita, joita työnantaja ei ole määritellyt
  - ...eikä niiden tietoturva siten kunnossa
  - Tosiasiallinen käsittely ei vastaa organisaation käsittelytoimien selostetta
  - Henkilökohtaiset puhelimet ja niiden suojaus
- Tiedoilla on erilaisia välitallennuspaikkoja, jotka eivät ole hyväksyttyjä
  - Puhelin, paperilaput, ym.
- Ohjeet käsittelystä ei vastaa käytäntöjä
  - Ohjeiden vastainen ja ohjeistamaton käsittely voi kaatua työntekijän henkilökohtaiselle vastuulle (kuka on tehnyt päätöksen tietojen käsittelystä – ts. kuka on rekisterinpitäjä?)
- Laskuille tulostuu vääriä tietoja
  - Henkilötunnuksia, diagnoosin tai terveydentilan paljastavia tietoja
- Asiakkaan tunnistaminen puhelimessa
- Asiakastietoja lähtee väärälle henkilölle
  - Sähköpostin automaattitäydennys
- Tietojen siirto esim. Kantaan, vaikka tietojen luovutuskielto
  - Luovutuskieltojen, turvakieltojen ja suostumusten hallinta, miten varmistetaan käytännössä?
- Vaikka tietoihin pääsisi, se ei tarkoita, että niitä saa käsitellä (käyttötarkoitus ja tarve tulee täyttyä)
- ”Reissuvihot” eivät ole automaattisesti laittomia, mutta niiden laatija vastaa niiden suojaamisesta
- Turvakieltoasiakkaiden tietojen luovuttaminen edelleen viranomaiselta toiselle/muualle on kiellettyä
- Rekisteri ja tietojärjestelmä on eri asia!

Jari Ala-Varvi
Opsec Oy:n tietosuojavastaava
p. 020 198 6689, jari.ala-varvi@opsec.fi

OPSEC OY
Tiedekatu 2, 60320 Seinäjoki
Hämeenkatu 5 A, 33100 Tampere
p. 020 198 6690, info@opsec.fi
www.opsec.fi