TAMPEREEN KAUPUNKI

Rekisterinpidon ja käytönvalvonnan haasteet

TERVEYDENHUOLLON ATK-PÄIVÄT 2014

Jyväskylän Paviljonki 20. - 21.5.2014

tietohallinto.

Lähtökohta ja yleistä

- Tietosuojavastaavat ja rekisterinpitäjät tarvitsevat itsekin koulutusta
- Asiat ovat mutkikkaita ja lainsäädännön muutoksia pitää seurata aktiivisesti
  - Ohjaavia tahoja on monia. Organisaatioilta puuttuu ”yhden luukun periaate” saada ohjausta
- Kannattaa tehdä yhteistyötä esim. seudullisesti
- Työntekijöiden oikeusturva muistettava (YT-käsittelyt, perehdytys, koulutukset, ohjeet jne.)
- Tietojärjestelmien vaatimusmäärittelyt tehtävä huolella (rekisterinpito ja lokien hallinta huomioiden)
- Lokitietojen käsittelyyn pitää luoda pelisäännöt
- Käytönvalvontaan kannattaa luoda ”vuosikello” tai vähintään suunnitelma, jota noudatetaan systemaattisesti
- Valvonnasta raportoidaan johdolle ja epäkohtiin puututaan!

tietohallinto.

Kansalaiset ovat valveutuneita

- Ihmiset tuntevat oikeutensa ja pyytävät omien tietojensa tarkistamista, korjaamista, selvitystä tietojen käsittelystä jne.
- Alaikäisten lasten tietojen käsittelyistä pyydetään selvitystä (kenelle tietoja voidaan luovuttaa –kuka on laillinen edustaja? Onko alaikäinen itsemääräävä ja kieltänyt luovuttamasta tietoja jne.)
- Kuolleiden omaisten asiakirjoja pyydetään enenevästi (esim. testamenttiriidat)
- Käyttölokiselvitykset ovat lisääntyneet tasaisesti
- Potilasasiamiehelle ja sosiaaliasiamiehille sekä tietosuojavastaavalle tulee runsaasti tietosuojaan liittyviä kysymyksiä
- Selvityspyyntöjä, kanteluita ja kysymyksiä esitetään suoraan myös rekisterinpitäjille, tietosuojavaltuutetulle, poliisille sekä Valviraan ja aluehallintovirastoihin

tietohallinto.

Tunnistettuja haasteita

- Kuka tai mikä on rekisterinpitäjä eri henkilörekistereissä?
  - Tunnistetaanko vastuu?
  - Onko rekisterinpitäjä alusta lähtien mukana suunnittelemassa henkilötietojen käsittelyä?
  - Sopimuksien hallinta (esim. toimeksiantosopimukset)
- Onko rekisteri/tietosuojaselosteet ajan tasalla ja helposti löydettävissä?
- Isoissa rekistereissä ja isoissa organisaatioissa tietoja käsitellään valtavasti
  - Kymmeniä miljoonia kertoja vuositasolla
  - Kymmenillä/sadoilla tietojärjestelmillä
  - Käyttöoikeuksia on tuhansia (vastaavatko oikeudet työtehtäviä, onko haamukäyttäjiä tai vaarallisia työyhdistelmiä?)
  - Satunnainen ”pistokoevalvonta” ei ole riittävää
  - Kuka päättää sanktiot ja niiden toteuttamisen
- Miten käytönvalvonta automatisoidaan?
  - Miten järjestelmiä lisätään valvontaohjelman piirin
  - Miten hinnoittelu on rakennettu
  - Onko raportit hyviä ja palvelevatko valvojaa

Käyttövaltuuspolitiikka ja asiakastiedon käsittelyohjeet

- Ensin pitää määritellä kuka, miksi ja miten saa käyttöoikeuksia salassa pidettäviin tietoihin
- Käyttöä ei voi valvoa, jos ei ole tiedossa miten tietojen käsittely on ohjeistettu ja kuka tietojärjestelmiä/tietoja käyttää missäkin roolissa ja milloin
- Käytönvalvonnassa keskeinen apuväline on käyttölokitiedot. Asiakasaloitteinen prosessi on kuvattava –samoin sisäinen määrämuotoinen valvontasuunnitelma ja sen toteuttaminen
- Lokitietojen käsittely vie aikaa ja siihen pitää resursoida. Suuntana pitkällä tähtäimellä kannattaa pitää prosessin automatisointi
- Sanktiot syytä taulukoida, jottei tulisi ”huutoäänestys” tai ”paineta villasella”-tilanteita

tietohallinto.

Lokien eheys ja käytettävyys

- Koska lokit ovat todisteena jostakin tapahtumasta, on erittäin tärkeää huomioida, että lokeja ei saa oikeudettomasti käsitellä, tuhota tai muuttaa niiden sisältöä
- Pääperiaatteena voidaan todeta, että olemassa olevia tietojärjestelmien lokimerkintöjä ei pidä koskaan pystyä muuttamaan, vaan esimerkiksi virheellisen merkinnän korjaamisesta pitää syntyä uusi lokimerkintä. Lokit pitää kuitenkin voida hävittää niiden määritellyn säilytysajan päätyttyä (tämä huomioitava järjestelmien vaatimusmäärittelyissä/hankinnoissa/kehittämisessä)
- Lokeihin pääsy pitää rajoittaa vain niille henkilöille, joiden työtehtävien kannalta se on välttämätöntä. Tällaisia työrooleja on mm. tietoturvapäälliköllä ja tietosuojavastaavalla sekä osalla tietojärjestelmien ylläpitäjiä (SaaS-palvelut mietittävä tarkasti)
- Esimerkiksi Tampereen kaupungilla on erillinen pysyväismääräys tietojärjestelmien ylläpidosta sekä käyttölokien valvontasuunnitelma ja lokiohje

Lokitietojen luovuttaminen (mm. toisille viranomaisille)

- Erilaisissa poliisin rikostutkinnoissa sekä muiden valvontaviranomaisten selvityksiin liittyen voi olla perusteet luovuttaa lokeja myös ”ulkopuolelle”. Nämä luovutukset ovat tapauskohtaisesti harkittava ja niiden pitää **perustua kirjalliseen perusteltuun pyyntöön.** Pyynnössä oleva peruste pitää varmistaa ja luovutus tehdä vain siinä laajuudessa kuin tapauksen selvittäminen sitä vaatii. Lokitiedot ovat salassa pidettäviä ja merkintä salassa pidosta pitää tehdä luovutusasiakirjoihin
- KHOn tuore ratkaisu:2014:69 (julkisuuslain 11 § tulkintaa) http://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/139937233585 2.html

Kiitos!

tietohallinto.