Henkilötietoja sisältävän datan säilytyksen ja käsittelyn tekniset ratkaisut

Ville Tenhunen

16. toukokuuta 2018

Agenda

1. Johdanto
2. Käsitteistä ja periaatteista
3. Keskeiset tietoturva-asiat
4. Käyttötapauksista ja valinnoista
5. Lopuksi

Johdanto

- Henkilötieto, arkaluontoinen henkilötieto, erityinen henkilötieto
- Yhdistelmätiedot
- Anonymisointi ja pseudonymisointi
- Tekniset ratkaisut sisällön mukaan eli yksi ratkaisu ei sovellu kaikkeen

Käsitteistä ja periaatteista

Tietoturva != tietosuoja

Tietoturva eli tietoturvallisuus tarkoittaa tiedon **saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä**. Turvattava tieto voi ilmetä useassa eri muodossa. Näitä ovat esimerkiksi digitaaliset tallenteen, fyysiset tallenteet sekä ihmisten, kuten työntekijöiden omaama tietämys. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana.[1]

Tietosuoja on osa perustuslain takaamaa **yksityisyyden suojaa**. Tietosuojalla viitataan viranomaisten ja yksityisten tahojen ylläpitämiin henkilörekistereihin sisältyviin tietoihin liittyvään salassapitovelvollisuuteen sekä muihin määräyksiin kuten ihmisten oikeuteen tutustua henkilötietoihinsa ja saada niihin aiheellisia poistoja ja korjauksia.[2]

[1] https://fi.wikipedia.org/wiki/Tietoturva
[2] https://fi.wikipedia.org/wiki/Tietosuoja

Hyvä tiedonhallintatapa (Julkisuuslaki 18 §)

Hyvällä tiedonhallintatavalla tarkoitetaan viranomaisen velvollisuutta huolehtia hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta **saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä**.

Hyvä tietojenkäsittelytapa

Hyvällä tietojenkäsittelytavalla tarkoitetaan rekisterinpitäjän velvollisuutta huolehtia hyvän tietojenkäsittelyn toteutumisesta henkilötietojen käsittelyssä.

Hyvän tietojenkäsittelytavan kannalta tärkeimmät yleiset periaatteet ovat tällöin **suunnittelu-, tarpeellisuus-, huolellisuus- ja suojaamisvelvoitteet sekä rekisteröityjen henkilöiden oikeuksien huomioon ottaminen**.

(kts. esim. poistuva henkilötietolaki 5 §)

Keskeisiä tietoturvakäsitteitä

- Saatavuus tai käytettävyys: Tieto on saatavilla, kun sitä tarvitaan
- Luottamuksellisuus: Tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus
- Eheys: Tieto ei saa muuttua tai muutos pitää ainakin havaita

Lisäksi:

- Kiistämättömyys: Henkilö ei voi kiistää tekoa, jonka hän on tehnyt
- Tunnistus: Käyttäjä voidaan tarvittaessa liittää käyttäjätunnukseen (joka voi olla anonyymi).
- Todennus: Käyttäjä voidaan luottavasti tunnistaa luonnolliseksi tai oikeushenkilöksi.

Käytännössä

- Saatavuus tai käytettävyys: Riittävä palvelinten ja tietoverkkojen kapasiteetti, käyttöliittymät, ylläpito
- Luottamuksellisuus: Salaus ja pääsynhallinta
- Eheys: Tarkistussummat, tarkistuskoodit ja digitaaliset allekirjoitukset
- Käyttäjän todentaminen ja kiistämättömyys: Digitaaliset allekirjoitukset ja muut todennustavat

Keskeiset tietoturva-asiat

Pääsynhallinta ja autentikointi

- Pääsynhallinta: Kenelle myönnetään pääsy ja millä perusteella, miten pääsyn rajaus tehdään
- Autentikointi ja pääsynhallinta
  - monivaiheinen tunnistus; esimerkiksi VDI- ja VPN-tekniikat tarjoavat
  - sisällön mukaan

(Monivaiheinen tunnistus: Käyttäjän identiteetti varmennetaan useaa tunnistusmenetelmää käyttäen, pyrkimyksenä estää järjestelmän luvaton käyttö)

Valvonta ja lokitus

- Tekninen loki, aineistonkäsittelyn loki
- Lokituksesta pitäisi saada selville:
  - Kenen tunnuksella käsiteltiin
  - mitä objektia,
  - milloin ja
  - mistä
- Käytön valvonta

Muita tietoturvatoimia

- Varmuuskopiointi: Turvaa kyvyn palautua vikatilanteesta
- Salaus: Tarpeen mukaan, erityisesti mobiililaitteet, kannettavat ja ulkoiset tallennuslaitteet
- Teknisen ympäristön suojaus: Miten käsittely-ympäristön suojataan ulkopuolisilta
- Henkilöstöturvallisuus: Tutkimusryhmän jäsenten perehdytys, koulutus, ohjeet sekä yhteisesti sovitut käytännöt
- Tilaturvallisuus: Työtilojen lukitukset, säilytyskalusteet, kameravalvonta sekä kulkuoikeuksien valvonta

Järjestelmävalinta ja tietoturva

- Henkilötietoja tai arkaluonteisia henkilötietoja kerättäessä tai siirrettäessä pitää varmistua koko käsittelyketjun tietoturvallisuudesta:
  - keräys- ja siirtovälineet
  - käsittely-ympäristöt
  - tallennusjärjestelmät ja ympäristöt

Tietoturva on yhtä vahvaa kuin ketjun heikoin lenkki.

Käyttötapauksista ja valinnoista

Käyttötapauksista

- Kerääminen / tuottaminen
- Tallentaminen
- Käsittely / laskenta
- Jakaminen
- Julkaiseminen
- Arkistointi

VPN ja VDI - huomioitavia tekniikoita

- VPN (Virtual Private Network), virtuaalinen verkko
  - tunnistetaan käyttäjä
  - turvaa tietoliikenteen
  - mahdollistaa yleensä laajempien resurssien käytön
- VDI (Virtual Desktop Infrastructure), etätyöpöytä
  - esimerkiksi silloin kun aineiston saa nähdä, mutta ei jakaa edelleen
  - mahdollistaa erilaiset käsittely-ympäristöt ja sovellukset

Järjestelmiä ja palveluita

- Yliopistojen omat tallennusjärjestelmät ja -palvelut
  - Verkko- ja ryhmälevyt (NAS, SAN, NFS jne.)
  - Verkkopalvelut (esim. ryhmätyöpalvelut)
- ePouta; käsittely-ympäristö
- eDuuni; ryhmätyöt
- Repositoryt

Salaamalla (esim. 7-zip, GnuPG, S/MIME jne.) voi dataa tallentaa ja käsitellä myös muualla

Pilveen?

- Lue aina ensin käyttöehdot ja tiedä mitä oikeuksia eri toimijoilla on
- Kun olet lukenut käyttöehdot, kysy itseltäsi a) ymmärsitkö ne ja b) voitko elää niiden kanssa?
- Tarkistuskysymys: Tiedätkö missä datasi on fyysisesti?
  - Henkilötietojen tallentamisen ja käsittelyn kannalta tällä on merkitystä
  - Nykyään pilvipalveluissa voi valita datan sijainnin
- Yleiset ja julkiset palvelut ovat sopimuksellisesti erilaisia kuin korkeakoulujen sopimuksilla hankitut palvelut
- Pilvipalveluissa usein hyvä tietoturva, mutta tietosuoja muodostuu haasteeksi

Tekeillä

- CSC:n sensitiivisen datan palvelu
- EUDAT Working Group on Sensitive Data Management
- Paikalliset sensitiivisen datan järjestelmäprojektit

Mihin voin tallentaa?

Lopuksi

Pohdintaa

- Jos sovellus on riittävän tietoturvallinen, sillä voi käsitellä henkilötietoja sisältävää dataa (mikäli tietosuojan muut edellytykset ovat voimassa)
- Tutkijalle palveluiden tietoturva ja tietosuoja ovat usein kuin musta laatikko, sen sisälle ei oikein näe
  - Käyttö perustuu tosiasiassa monessa tapauksessa luottamukseen
  - Käytä aina kun mahdollista uskottavien rekisterinpitäjien tarjoamia suojattuja käsittely-ympäristöjä
- Jos valittava ratkaisu tuntuu liian epävarmalta, älä käytä
- Kun kerran menettää kontrollin aineistoon, sen helposti menettää lopullisesti

Työpajasessiossa

Henkilötietoja sisältävän datan säilytyksen ja käsittelyn tekniset ratkaisut:

- Millainen olisi hyvä henkilötiedon tallennuspalvelu?
- Työstetään speksin piirteitä
  - Toiminnalliset vaatimukset
  - Laadulliset vaatimukset
  - Tekniset vaatimukset

Kiitos!

Sähköposti: ville.tenhunen@helsinki.fi

Twitter: @vtenhunen