

Sosiaali- ja terveydenhuollon atk-päivät

23.5.2017

Finlandia-talo

Sessio 5: Sosiaali- ja terveydenhuollon tiedon integrointi

**Uusi EU:n tietosuoja-asetus,
mitä muuttuu
ja
mihin suuntaan**



Reijo Aarnio
tietosuojavaltuutettu



Tietosuojavaltuutetun toimisto

KILPAILUN EDISTÄMINEN LÄHTÖKOHTANA:

- 1) 28 MS → 28 erilaista lainsäädäntöä**
- 2) EU:n investointivaje erityisesti ITC:hen
→ tuottavuusvaje**
- 3) Digitaalinen kaupankäynti on kasvanut hitaammin EU:ssa**
- 4) EU:n uudistukset:**
 - pääomamarkkina-unioni turvaamaan START UP:n rahoitusta**
 - digitaalistrategia**
 - sisämarkkinastrategia**
 - tietosuojauudistus**
 - yhdistetty työllisyyden ja teollisuuden DG:t DG kasvuksi
(DG GROWTH)**

TIETOSUOJAN SUKUPOLVET

TIETOSUOJADIREKTIIVI 46/95/EY

Resitaali nro 2:

“Tietojenkäsittelyjärjestelmät on tehty palvelemaan ihmistä; järjestelmiä käytettäessä on **kunnioitettava yksilöiden perusoikeuksia ja –vapauksia** heidän kansalaisuudestaan tai asuinpaikastaan riippumatta, erityisesti oikeutta yksityisyyteen, ja osallistuttava **taloudelliseen ja sosiaaliseen kehitykseen, kaupan kehittämiseen sekä yksilöiden hyvinvoinnin lisäämiseen.**”

(Kts. Asetuksen resitaali 2)

1. SUKUPOLVI

- perusoikeudet
- EN-tietosuoja sopimus
- henkilörekisterilaki

2. SUKUPOLVI

- tietojärjestelmät
- tietosuojadirektiivi 46/95/EY
- henkilötietolaki

3. SUKUPOLVI

- digitaaliset sisämarkkinat
- tietosuoja-asetus
- TATTi-toimikunta?

EKOSYSTEMI

VERKKO (WEB) PALVELUT

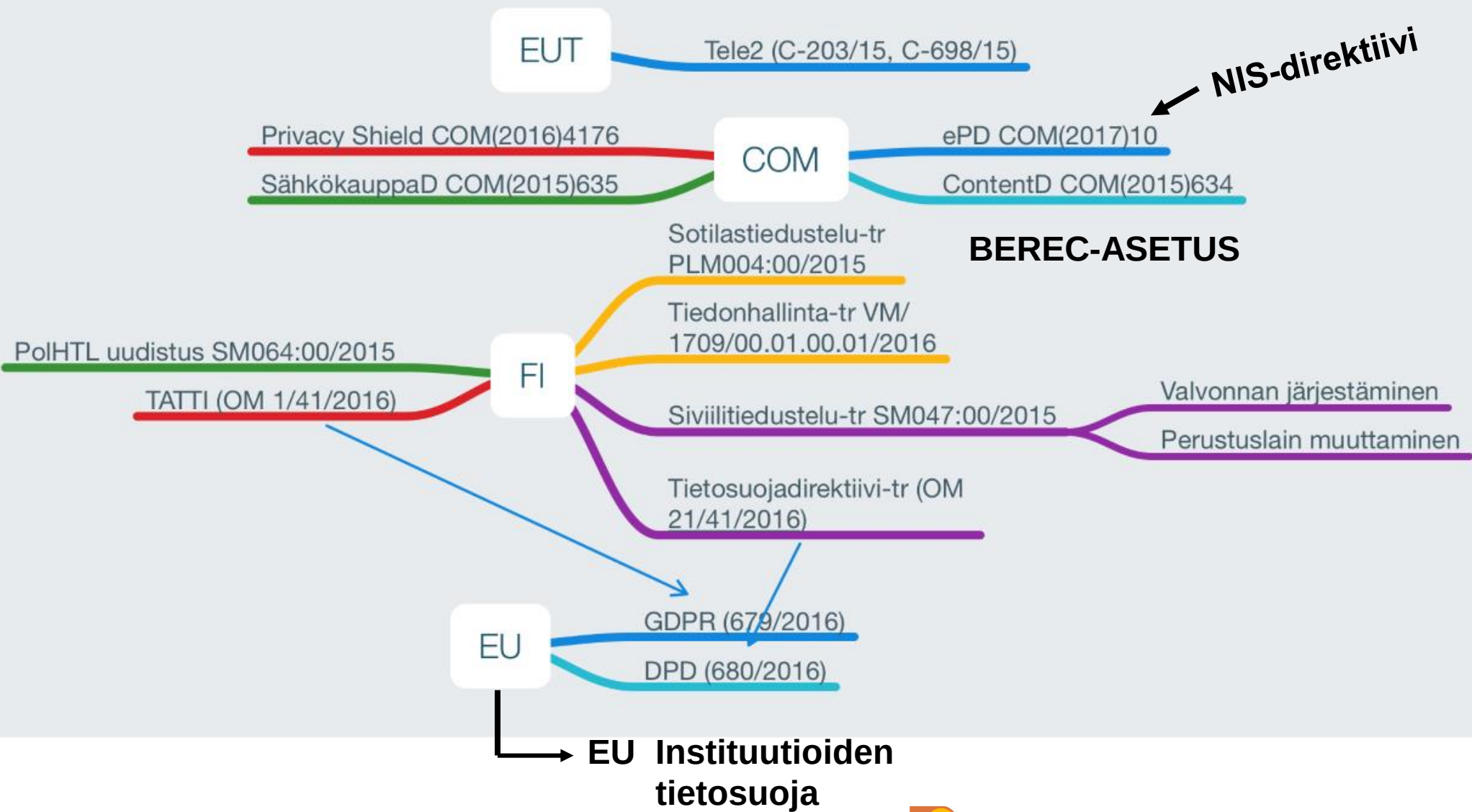
**Prop.
apps**

**3rd party
apps**

Operating apps

(Laite) hardware

Verkko infra



Tietosuoja-asetuksen vaikutukset kansalliseen lainsäädäntöön: OM:n työryhmä

Työryhmän tehtävänä on

- 1) selvittää Euroopan unionin yleisen tietosuoja-asetuksen edellyttämien kansallisten lainsäädäntötoimenpiteiden tarve sekä erityisesti se, onko voimassa olevan henkilötietolain kaltaiselle yleiselle kansalliselle tietosuojalainsäädännölle tarvetta ja valmistella ehdotus asiasta mahdollisesti tarvittavaksi yleiseksi lainsäädännöksi;
- 2) selvittää, onko kansallista tietosuojaviranomaista koskevaa kansallista lainsäädäntöä tarpeen tarkistaa ja valmistella ehdotus tarvittavaksi lainsäädännöksi kansallisesta tietosuojaviranomaisesta, sen organisaatiosta, tehtävistä ja toimivaltuuksista;
- 3) selvittää tietosuoja-asetuksen jäsenvaltion lainsäädännölle jättämän kansallisen liikkumavaran antamat mahdollisuudet sekä esittää periaatteet liikkumavaran tarkoituksenmukaisesta käytöstä;
- 4) koordinoida ja avustaa henkilötietojen käsittelystä annetun erityislainsäädännön tarkistamiseksi tehtävää lainvalmistelutyötä.  TIETOSUOJAVALTUUTETUN TOIMISTO

Henkilötietojen käsittelyn lainmukaisuus, 6 artikla

- **Yksiselitteinen suostumus**
- **Sopimus**
- **Rekisterinpitäjän lakisääteiset velvoitteet**
- **Rekisteröidyn elintärkeä etu**
- **Yleistä etua koskeva tehtävä / rekisterinpitäjälle kuuluva julkinen valta**
- **Rekisterinpitäjän oikeutettu etu**
- **Henkilötietojen käsittely historiallisia, tilastollisia ja tutkimustarkoituksia varten, arkistointitarkoitukset**
- **Henkilötietojen jatkokäsittely**

Mitä ?

- 1. Entiset tietosuojaperiaatteet säilyvät
 - 2. Asetuksessa joitakin ”uusia” asioita:
- } NÄITÄ YHDISTELLÄÄN

- COMPLIANCE; (”sääntöjen noudattaminen”)
 - Asetuksessa mennään pitemmälle
- ACCOUNTABILITY; ▶ TIETOTILINPÄÄTÖS
 - Tilintekokykyisyys eli osoita että noudatat lakeja
- PRIVACY BY DESIGN; (ennakkoon suunnitteleminen)
 - Henkilötietolain 6 §
- PRIVACY BY DEFAULT; (oletusarvoinen ja sisään-rakennettu)
 - Nyt kun kuluttaja asioi rekisterinpitäjän kanssa niin huolehtii esim. oman s-postin tietoturvasta.
 - Asetuksella rekisterinpitäjä velvoitetaan rakentamaan tietoturvallinen suojattu palvelu (nyt jo esim. pankit)



Mitä ?

- **DATA BREACH NOTIFICATION; (tietoturvaloukkauksista ilmoittaminen)**
 - Rekisterinpitäjän ilmoitusvelvollisuus valvontaviranomaiselle ja asiakkaalle
 - mm. tietomurto ja henkilörekisteririkos
- **VALVONTAVIRANOMAISTEN ROOLIN VAHVISTAMINEN; (viranomaisten toimivalta muuttuu)**
 - TSV:lle mahdollisesti sakottamisoikeus, josta valitustie ensin kansallisesti ja aina EY-tuomioistuimeen asti
- **RIGHT TO BE FORGOTTEN; (oikeus unohtaa)**
 - Esim. Facebook –tyyppiset palvelut; oikeus itse myötävaikuttaa, että tiedot poistetaan
 - Voi olla haasteellista toteuttaa
- **RIGHT TO DATA PORTABILITY (oikeus tietojen siirtoon)**
 - Rekisteröidyn oikeus viedä tiedot palveluntarjoajalta toiselle (esim. kanta-asiakasjärjestelmät)

DBN: DATA BREACH NOTIFICATION

**Henkilötietojen tietoturvaloukkauksesta ilmoittaminen
valvontaviranomaiselle ja rekisteröidyille
(tietoturvaloukkauksista ilmoittaminen)**

- **Rekisterinpitäjän ilmoitusvelvollisuus
valvontaviranomaiselle ja asiakkaalle**
- **mm. tietomurto ja henkilörekisteririkos**
- Jos tapahtuu henkilötietojen tietoturvaloukkaus
(esim. tietovuoto), rekisterinpitäjän on ilmoitettava siitä
mahdollisuuksien mukaan 72 tunnissa valvontaviranomaiselle.
Samoin ilmoitus pitää tehdä rekisteröidyille.

Hallinnolliset seuraamukset 83 artikla

Seuraamukset (muut) 84 artikla

Hallinnollisten sanktioiden on oltava tehokkaita, oikeasuhteisia ja varoittavia:

1. Porras

- 10.000.000 euroa tai jos kyseessä on yritys, 2 %
”...vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi määrä näistä on suurempi:”

2. Porras

- 20.000.000 tai jos4 % (tätä sovelletaan myös, jos ei noudata valvontaviranomaisten määräyksiä.)

Kriminalisointimääräys jäsenvaltioille

Huoneentaulu rekisteröityjen oikeuksista

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

PRIVACY BY DEFAULT



TIETOSUOJAVALTUUTETUN TOIMISTON NYKYISET PERUSPROSESSIT

- 1) Asiamies/valtuutettu**
- 2) Tarkastaja**
- 3) Konsultti**
- 4) Valistaja**
- 5) Poliittinen neuvonantaja**
- 6) Neuvottelija**
- 7) Täytäntöönpanija**
- 8) Kansainvälinen lähettäjä.**

UUDET PROSESSIT:

- 1) Yhdenmukaisuusmekanismi**
- 2) Hallinnolliset sanktiot**
- 3) Ennakkohyväksymistehtävät
(Auditointi)**
- 4) Ulkomaille siirrot**
- 5) Data Breach Notifications – ilmoitusprosessi**
- 6) Tarkastukset**
- 7) Sähköinen asiointialusta**
- 8) Kansallinen lainsäädäntö**
- 9) Tietosuojavastaavat**

TOIMENPITEET REKISTERINPITÄJILLE:

- 1) Määrää tietosuojan isäntä; Tietosuojavastaava
- 2) Analysoi henkilötietovarastosi ja –prosessit → eliminoi turhat
- 3) Tee riskiarvio; arvioi myös sopimuksesi (sopimustenhallinta)
- 4) Laadi toimintaohjeet ja –ohjelmat eri tilanteiden varalta; esim. tietoturva, -vuodot, rekisteröidyn oikeudet jne.
- 5) Huolehdi tietoturvasta, käytä salauksia
- 6) Huolehdi henkilöstön osaamisesta
- 7) Valvo henkilötietojen käyttöä
- 8) Käytä henkilötietolakia apunasi
- 9) Tunnista muu lainsäädäntö
- 10) Luo sisäinen ja ulkoinen raportointijärjestelmä;
LAADI "TIETOTILINPÄÄTÖS"



TIETOSUOJAVALTUUTETUN TOIMISTO

Miten valmistautua EU:n tietosuoja-asetukseen?

24.1.2017

www.tietosuoja.fi

Tietosuojavaltuutetun toimisto julkaisi 24. tammikuuta rekisterinpitäjille suunnatun oppaan EU:n tietosuoja-asetukseen valmistautumisesta. Oppaassa kerrotaan muun muassa henkilötietojen käsittelyn arvioinnista ja oikeusperusteista, tietosuojaperiaatteiden toteuttamisesta sekä tietoturvaloukkauksiin valmistautumisesta.

Oppaassa selvitetään myös esimerkiksi riskiperustaisen lähestymistavan merkitystä rekisterinpitäjille ja rekisteröidyn oikeuksiin tulevia muutoksia. Opas on kirjoitettu yhteistyössä oikeusministeriön kanssa ja se julkaistaan myöhemmin myös oikeusministeriön julkaisusarjassa.



TIETOSUOJAVALTUUTETUN TOIMISTO

Päiv. 11.3.2016

Rekisterinpitäjän (3 § 4 k) henkilötietojen käsittelyn kuvaus ja lainmukaisuuden arviointi



KYSYMYKSIÄ KUULIJOILLE

- 1) Miten vastaatte kilpailuun?
- 2) Miten otatte alihankintaketjunne haltuun & sopimukset?
- 3) Miten varmistatte osaamisenne?
- 4) Tietoturva?
- 5) Miten saavutatte tilintekokykyisyyden?
- 6) Toimintasuunnitelmanne DBN:n
(Data Breach Notification) varalle?
- 7) Miten arvioitte teknologiaa?
- 8) Hyödyt - Haitat -analyysi

KIITOS KUUNTELUSTA

Lisätietoja: www.tietosuoja.fi



Reijo Aarnio
tietosuojavaltuutettu



Tietosuojavaltuutetun toimisto