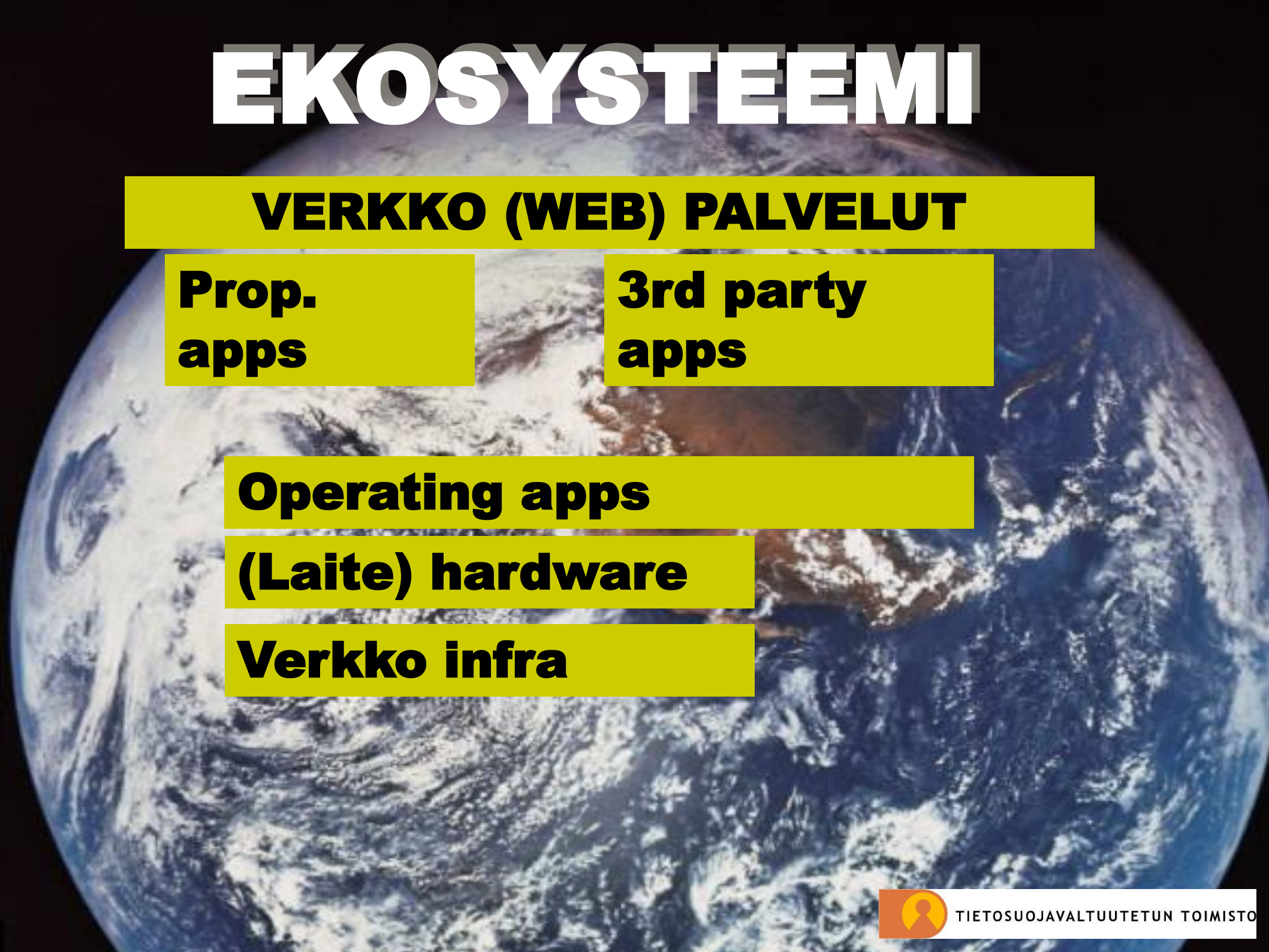
Sosiaali- ja terveydenhuollon atk-päivät
Avaussessio
Jyväskylän Paviljonki
22.5.2018

EU-TIETOSUOJA-ASETUS

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto

MIKSI UUDISTUS?


EKOSYSTEEMI
VERKKO (WEB) PALVELUT
Prop. apps
3rd party apps
Operating apps
(Laite) hardware
Verkko infra
TIETOSUOJAVALTUUTETUN TOIMISTO

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-tietosuojasopimus
- henkilörekisterilaki

2. SUKUPOLVI
- tietojärjestelmät
- tietosuojadirektiivi 46/95/EY
- henkilötietolaki

3. SUKUPOLVI
- digitaaliset sisämarkkinat
- tietosuoja-asetus
- TATTi-toimikunta?

TIETOSUOJA-ASETUS:

II LUKU
Periaatteet
5 artikla
Henkilötietojen käsittelyä koskevat periaatteet

2. Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (”osoitusvelvollisuus”).

TIETOSUOJA-ASETUS:

IV LUKU
Rekisterinpitäjä ja henkilötietojen käsittelijä
1 Jakso
Yleiset velvollisuudet

24 artikla

Rekisterinpitäjän vastuu

1. Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.
2. Kun se on oikeasuhteista käsittelytoimiin nähden, 1 kohdassa tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.
3. Jäljempänä 40 artiklassa tarkoitettujen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että rekisterinpitäjälle asetettuja velvollisuuksia noudatetaan.

TIETOSUOJA-ASETUS:

25 artikla

Sisäänrakennettu ja oletusarvoinen tietosuoja ”PRIVACY BY DEFAULT”

1. Ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten tietojen pseudonymisointi ja tarvittavat suojatoimet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tämän asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin.
2. Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.
3. Hyväksyttyä 42 artiklan mukaista sertifiointimekanismia voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 ja 2 kohdassa asetettuja vaatimuksia noudatetaan.

TIETOSUOJA-ASETUS:

42 artikla
Sertifiointi

1. Jäsenvaltiot, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja sekä tietosuojasinettejä ja -merkkejä erityisesti unionin tasolla, minkä tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat käsittelytoimia suorittaessaan tätä asetusta. Mikroyritysten sekä pienten ja keskisuurten yritysten erityistarpeet on otettava huomioon.

5. Tämän artiklan mukaisen sertifioinnin myöntävät 43 artiklassa tarkoitetut sertifiointielimet tai toimivaltainen valvontaviranomainen kyseisen toimivaltaisen valvontaviranomaisen 58 artiklan 3 kohdan nojalla tai tietosuojaneuvoston 63 artiklan nojalla hyväksymien kriteerien perusteella. Jos tietosuojaneuvosto on hyväksynyt kriteerit, voidaan tehdä yhteinen sertifiointi, eurooppalainen tietosuojasinetti.

TIETOSUOJA-ASETUS:

43 artikla
Sertifiointielimet

1. Sertifioinnin myöntää ja uusii sertifiointielin, jolla on tietosuojaan liittyvä asianmukaisen tason asiantuntemus, sen jälkeen kun se on tiedottanut valvontaviranomaiselle valvontaviranomaisen 58 artiklan 2 kohdan h alakohdan mukaisten valtuuksien käyttämisen mahdollistamiseksi, sanotun kuitenkaan rajoittamatta toimivaltaisen valvontaviranomaisen 57 ja 58 artiklan mukaisia tehtäviä ja valtuuksia. Jäsenvaltioiden on säädettävä siitä, akkreditoiko nämä sertifiointielimet yksi tai molemmat seuraavista:

a) 55 tai 56 artiklan nojalla toimivaltainen valvontaviranomainen;

b) Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 (20) mukaisesti nimitetty kansallinen akkreditointielin noudattaen EN-ISO/IEC 17065/2012 - standardia ja 55 tai 56 artiklan nojalla toimivaltaisen valvontaviranomaisen vahvistamia lisävaatimuksia.

TIETOSUOJA-ASETUS:

43 artikla
Sertifiointielimet

2. Tämän artiklan 1 kohdassa tarkoitettu sertifiointielin voidaan akkreditoida kyseisen kohdan mukaisesti ainoastaan, jos

a) se on osoittanut riippumattomuutensa ja asiantuntemuksensa sertifioinnin kohteesta toimivaltaista valvontaviranomaista tyydyttävällä tavalla;

b) se on luvannut noudattaa 42 artiklan 5 kohdassa tarkoitettuja ja 55 tai 56 artiklan nojalla toimivaltaisen valvontaviranomaisen tai 63 artiklan nojalla tietosuojaneuvoston hyväksymiä kriteerejä;

c) se on vahvistanut menettelyt tietosuojasertifioinnin, -sinettien ja -merkkien myöntämistä, määräaikaistarkastelua ja peruuttamista varten;

d) se on vahvistanut menettelyt ja rakenteet, joilla käsitellään valituksia, jotka koskevat sertifiointimenettelyjen rikkomisia tai tapaa, jolla rekisterinpitäjä tai henkilötietojen käsittelijä on pannut tai panee sertifioinnin täytäntöön, ja saattaa nämä menettelyt ja rakenteet rekisteröityjen ja yleisön kannalta läpinäkyviksi; ja

e) se osoittaa toimivaltaista valvontaviranomaista tyydyttävällä tavalla, että sen tehtävät ja velvollisuudet eivät aiheuta eturistiriitoja.

TIETOSUOJA-ASETUS:

43 artikla
Sertifiointielimet

3. Tämän artiklan 1 ja 2 kohdassa tarkoitetut sertifiointielimet akkreditoidaan 55 tai 56 artiklan nojalla toimivaltaisen valvontaviranomaisen tai 63 artiklan nojalla tietosuojaneuvoston hyväksymien kriteerien perusteella. Jos akkreditointi tapahtuu tämän artiklan 1 kohdan b alakohdan nojalla, nämä vaatimukset täydentävät asetuksen (EY) N:o 765/2008 vaatimuksia ja sertifiointielinten menetelmiä ja menettelyjä kuvaavia teknisiä sääntöjä.

ASETUS JA DIREKTIIVI

* Tarkistuspisteissä:
- Tilanne
- Päivitystarve
- Toteutumat
- Riskianalyysi
- kirjanpito, arvioidut kulut
- sisäinen tiedotus / hlöstö
- Miten asetuksen vaikutukset on huomioitu kansallisesti ja EU-tasolla

ALOI-TUS 18.11. 2015

Projektille annettiin nimi ”TSAU”

Projekti-suunni-telman hyväk-syntä

- Esittely
- Nimitykset
- Tehtäväjako

Riskianalyysi ****

Sisäinen tiedotus

A. Osaamisen hallinta
- A.1.a Sisäinen
- A.1.b - Henkilöstösuunnitelma 2016-2019 - Koulutussuunnitelma 2016-2019 - Help desk -toiminta
- A.1.c Asianhallinta-järjestelmän laatu
- A.1.d Toteutus ja raportointi
- A.1.e Tarkistus-piste
- A.2.a Ulkoinen
- A.2.b Yhteistyö-kumppanin valinta
- A.2.c - Kotisivut - SOME - Koulutus
- A.2.d Tietosuoja-vastaavat
- A.2.e Tarkistus-piste

B. Organisaatio
- B.1.a Resurssit
- B.1.b Tarkistus-piste
- B.1.c Organisaatio-suunnitelma
- B.1.d - Toimen-kuvat - Palkat
- B.1.e - Nimitykset
- B.1.f Tarkistus-piste

C. Vaikuttavuus
- C.1.a Projekti-suunnitelma
- C.1.b Tarkistus-piste

Pohjoismainen kokous,Islanti

* Maalis 2016 Tarkistus-piste 1
* Touko 2016 Tarkistus-piste 2 (kans. väl.)
* Syys 2016 Tarkistus-piste 3
* Joulu 2016 Tarkistus-piste 4
* Kesä 2017 Tarkistus-piste 5

SEURANTA

PÄÄT TYY 2018

D. Uudet prosessit
- D.1.a Lain-säädäntö-kehikko
- D.1.a.a Nykyprosessien päivitystarve **
- D.1.a.b Työmetodit (8 uutta prosessia ***)
- D.1.b.1 Testaus
- D.1.b.2 Käyttöön-otto
- D.1.b.3 Tarkistus-piste

E. Muut projektit
- E.1.a Oikeusministeriö - toimikunta
- E.1.b Alatyöryhmät
- E.1.c Tarkistus-piste

F. Kansain-välinen yhteistyö
- F.1.a. Euroopan tietosuojaneuvosto
- F.1.b Tarkistuspiste
- F.2.a. Substanssiasiat
- F.2.b. WP 29 ohjeistus
- F.2.c Tarkistuspiste
- F.3.a. Hallinnolliset asiat
- F.3.b WP 29 ohjeistus
- F.3.c Tarkistuspiste

G. IT-alusta
- G.1.a. Kansainväliset valitusasiat
- G.1.b. Yhteiset operaatiot
- G.1.c. Yhdenmukaisuusmekanismi
- G.1.d Tarkistus-piste
- G.2.a. Kansalliset konvertiot
- G.2.b. - Vaikuttavuus - Osaamisen hallinta - Laadun tarkkailu
- G.2.c Tarkistus-piste

H. Yleis-tarkistus piste

I. SAUNA-ILTA

J. KÄYTTÖÖN-OTTO

** NYKYISET PERUSPROSESSIT:
1) Asiamies/valtuutettu
2) Tarkastaja
3) Konsultti
4) Valistaja
5) Poliittinen neuvonantaja
6) Neuvottelija
7) Täytäntöön panija
8) Kansainvälinen lähettiläs.

*** 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

PeVL lausunto 14/2018 vp

KIITOS KUUNTELUSTA

Lisätietoja: www.tietosuoja.fi

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto