EU:n tietosuoja-asetuksen voimaantulo ja vaikutukset

Terveydenhuollon ATK-päivät, Lahden Messukeskus
24.5.2016

Ylitarkastaja Arto Ylipartanen,
Tietosuojavaltuutetun toimisto

Luennon aiheet

A. EU:n tietosuoja-asetuksen voimaantulo

B. EU:n tietosuoja-asetuksen vaikutukset:

1. Virittäytyminen
2. Tietosuojan merkityksen kasvu
3. Tietosuojaviranomaisen rooli ja asema
4. Tietosuojariskien lisääntyminen 2000-luvulla
5. EU:n tietosuoja-asetus
6. Tietosuoja: esteestä – menestystekijäksi!

A. Euroopan parlamentin ja neuvoston asetus (2016/679, yleinen tietosuoja-asetus) voimaan tulo - pitkä taival

Komission ehdotus
Tammikuu 2012

Neuvoston versio
Kesäkuu 2015

Lopullinen Hyväksyminen
huhtikuu 2016

Soveltaminen
25.5. 2018

2012 2013 2014 2015 2016 2017 2018

Parlamentin versio
maaliskuu 2014

HaV:n Lausunto
joulukuu 2015

Trilogi-neuvottelujen ratkaisu
joulukuu 2015

B. EU:n tietosuoja-asetuksen vaikutukset

1. Virittäytyminen

Puhummeko yhteistä kieltä?

- Valitettavan usein tietosuoja ymmärretään suppeasti, ja virheellisesti jonkinlaisena ”tiedon panttaamisena”
  - **Tietosuojalla tarkoitetaan** henkilötietolain mukaan asiakastietojen asiallisesti perusteltua käsittelyä; ***keräämistä, tallentamista, käyttöä, yhdistämistä, siirtoa, luovuttamista, arkistointia, hävittämistä sekä muita asiakastietoihin kohdistettavia toimenpiteitä***
  - Kun on puutteita tietosuojaosaamisessa (tietojen käsittely): Seurauksena on tehottomuutta, ei saavuteta kustannussääs-töjä, potilasturvallisuus vaarantuu, työntekijän oikeusturva vaarantuu, yksityisyyden suoja on liian heikko tai liian tiukka.

B. EU:n tietosuoja-asetuksen vaikutukset
2. Tietosuojan merkityksen kasvu

Uusi digitalisoituva toimintaympäristö

- Informaatioteknologian vallankumous
  - Tietoliikenneyhteyksien kehitys
  - Tallennuskapasiteetin kehitys
- Verkottuneet tietojärjestelmät
  - Pilvipalvelut (Cloud Computing)
  - Offshoring-ulkoistukset
- Teknologian käytön ja työn tekemisen uudet tavat
  - Mobiiliratkaisut ja etätyö

Yksityisyyden suojaan kohdistuvat uhat

- Yksilön ”digitaalinen jalanjälki” kasvaa
  - Yli 90% kaikesta koskaan syntyneestä tiedosta on tallennettu 2010-luvulla
  - Mooren laki: tietokoneiden suorituskyvyn kasvu tuo kaiken tiedon käsiteltäväksi
- Kiinnostus tietosuojaan kasvaa
  - Tiedon käyttö- ja väärinkäyttömahdollisuudet ennalta arvaamattomia
  - Yksilöt tietoisempia uhista ja oikeuksistaan
  - Median kiinnostus voimakasta
- Kyberturvallisuusriskeistä tullut todellisia

Uusi asennoituminen tietosuojaan

- Tietosuojan rooli muuttunut
  - Yrityksille osa vastuullista liiketoimintaa ja riskienhallintaa
- Tietosuoja ei ole uhka vaan mahdollistaja
  - Haettaessa uudesta teknologiasta hyötyjä ja tehokkuutta, ymmärretään tietosuojan olevan välttämätön osatekijä
- EUn tietosuoja-asetus tarjoaa porkkanaa mm.
  - Organisaatioille lisää tuottavuutta+tehokkuutta
  - Oikeusturvaa työntekijälle+tietosuojaa asiakkaalle

3. Tietosuojaviranomaisen rooli ja asema

nyt

- tietosuojavaltuutetun tehtävät

  (* mitä toimivaltaan ei kuulu)

tulevaisuudessa

- Mitä EU:n tietosuoja-asetus tuo tullessaan?
- Miltä viranomaisen tuleva rooli näyttää?

Tietosuojaviranomaiset tällä hetkellä

Tietosuojavaltuutettu

Tietosuojalautakunta

WP29-työryhmä

- koostuu jäsenmaiden kansallisista tietosuojaviranomaisista
- riippumaton, neuvoa antava elin
- www.ec.europa.eu/justice/data-protection/article-29/index_en.htm

Tietosuojavaltuutettu on

- valtuutettu
- tarkastaja
- konsultti
- valistaja
- poliittinen neuvonantaja
- neuvottelija
- täytäntöönpanija
- kansainvälinen lähettiläs

Rekisterinpitäjän näkökulmasta valtuutettu on

- ennakollisen yleisohjauksen antaja
  (ei kuitenkaan hyväksyjä)
- ennakkovalvonnan suorittaja (ei ennakkolupia)
- jälkikäteisen laillisuusvalvonnan suorittaja
- määräysten antaja (tarkastusoikeus ja tiedonkorjaaminen)
- erilaisten tarkastusten tekijä
- toimialakohtaisten käytännesääntöjen tarkastaja
- sidosryhmäyhteistyökumppani
- tiedottaja
- jne.

4. Tietosuojariskien lisääntyminen 2000-luvulla

Kohti sähköisiä valtakunnallisia keskitettyjä rekistereitä/ arkistoja:

- Laki sähköisestä lääkemääräyksestä (61/2007, voimaan 1.4.2007);
  - Kelan Reseptikeskus/eResepti
- Terveydenhuoltolaki 9 § (1326/2010, voimaan 1.5.2011);
  - SHPn alueen yhteiskäytössä oleva potilastietorekisteri
  - Kunkin SHP:n alueen sisällä sijaitsevat julkisen terveydenhuollon toimintayksiköt
- Asiakastietolaki (159/2007, voimaan 1.7.2007);
  - Valtakunnallinen Kelan ylläpitämä potilastiedon sähköinen eArkisto otetaan käyttöön (2014-2016)
- Asiakas-/potilastietojen käsittelyn keskittymisen seurauksena tietosuojariskit kasvavat:
  - paljon asiakkaita/potilaita ja paljon tietoja, joilla paljon käyttäjiä.

”Tietosuojavastaavan nimittäminen on jäävuoren huippu”

Tietosuojavastaavan nimittäminen organisaation riskien hallintaan.

1. Johtajan päätöksellä tietosuojatyön organisointi sekä
2. Tietosuojavastaavan/-ryhmän tietosuojatyön tekeminen.

TAVOITE: Joustava asiakastietojen käsittely+tietoturva+tuottavuus +tehokkuus+potilasturvallisuus +työntekijän oikeusturva+tietosuoja = **Työssä viihdytään - EI SÄHLÄTÄ!**

Asiakastietojen käsittelyn tasapaino ja luottamus

SOTE: AsiakastietoL 20 § ja 19h §, ja eReseptiL (61/2007) 24 §;

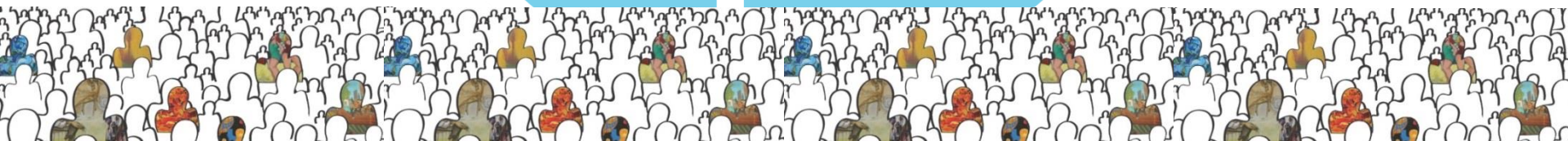
1) Tietosuojavastaava nimettävä organisaatioon
   - tehtävät ja toimenkuva määriteltävä
2) Vastaavan johtajan velvollisuus
   - annettava kirjalliset ohjeet työntekijöille asiakastietojen käsittelystä + varmistuttava henkilöstön tietosuojaosaamisesta
3) Rekisterinpitäjän velvollisuus käytönvalvontaan
   - lokitietojen kerääminen ja pitkäaikaissäilytys
     + asiakastietojen käsittelyn seuranta ja valvonta
   - (Kansalaisen omien asiakastietojen lokimerkintöjen OmaKanta –katselu)
4) Tietojärjestelmien auditoinnit sekä organisaation tietosuojan ja –turvan omavalvontasuunnitelma (THL/OPERin määräys 2/2015 ja mallipohjat)

Tietosuojakysely 2016 tietosuojavastaaville

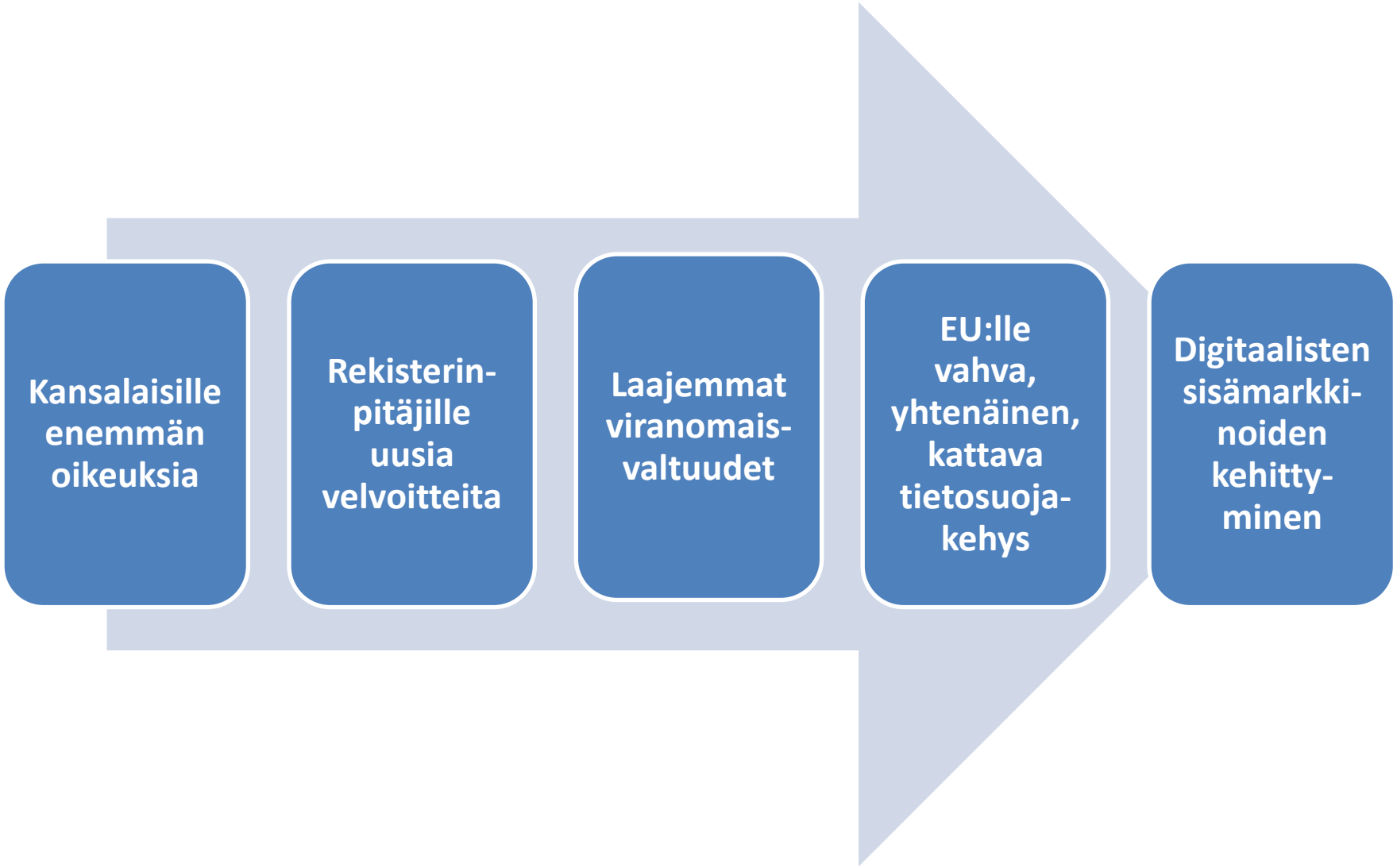
- **Tietosuojakysely 2016 tietosuojavastaaville (tiedote+tulokset julkaistu 17.5.2016):** http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2016/05/terveydenhuollontietosuojakyselyn2016tulokset.html

- **EU:n tietosuoja-asetus:** Accountability –periaate (tilintekovelvollisuus ja tilintekokykyisyys)
  - Ei riitä enää pelkkä “do it”, vaan organisaatioilta vaaditaan enemmän
  - **“prove it”;** osoita, että tietosuoja-asiat on otettu huomioon asiakastietojen etukäteissuunnittelussa ja toteutuksessa - ankaran hallinnollisen sakon uhalla.

5. EU:n tietosuoja-asetus



Asetuksen sisältö ja tavoite pähkinänkuoressa



EU:n tietosuoja-asetus julkaistiin 4.5.2016 Euroopan unionin virallisessa lehdessä L 119.

– Asetus tulee voimaan 20. päivänä julkaisemisen jälkeen, ja sitä sovelletaan 25.5.2018 alkaen eli kahden vuoden siirtymäaika
  - rekisterinpitäjällä korkea vastuu
  - tilintekokykyisyys korostuu (Accountability)
  - ilmoitusvelvollisuuksia tietosuojapoikkeamista tietosuoja-viranomaisille ja asiakkaille
  - mahdollisia suuria rahallisia sakkoja tietosuojapuutteista (huom. Accountability)
  - henkilötietojen käsittelyyn liittyen on tehtävä PIA (Privacy Impact Assessment) eli vaikutusten etukäteinen arviointi

EUn tietosuoja-asetuksesta (2016/679) löytyy suomennos:

http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&qid=1463503990319&from=EN

Tietosuoja-asetus (EU)
poimintoja

DATA PROTECTION BY DESIGN =suunnitteluvelvollisuus

DATA PROTECTION BY DEFAULT =oletusarvoinen ja sisäänrakennettu tietosuoja

COMPLIANCE =sääntöjen noudattaminen, ”do it”

ACCOUNTABILITY =rekisterinpitäjän tilintekokykyisyys; tietotilinpäätös, ”prove it”

PIA =tietosuojaa koskevien vaikutusten arviointi

Tietosuojaviranomaiset tulevaisuudessa

Jäsenvaltioon perustetaan yksi tai useampi riippumaton valvontaviranomainen

Oikeusministeriön asettama työryhmä

- selvittää, onko kansallista tietosuojaviranomaista koskevaa lainsäädäntöä tarpeen tarkistaa
- valmistelee ehdotuksen lainsäädännöksi kansallisesta viranomaisesta, sen organisaatiosta, tehtävistä ja toimivaltuuksista
- määräaika lainsäädännön muutosehdotuksille 31.5.2017

Euroopan tietosuojaneuvosto

WP29 -> EDPB

Unionin toimielin, oikeushenkilö

Varmistaa, että asetusta sovelletaan yhdenmukaisesti

- Toimii oma-aloitteisesti tai komission pyynnöstä
- Seuraa. Antaa lausuntoja, suosituksia ja suuntaviivoja

Monissa suhteissa kansallisia viranomaisia ylempi taho

- Esim. kiistanratkaisumenettely: antaa oikeudellisesti sitovia päätöksiä asioihin, joista kansallisilla viranomaisilla on eriävät näkemykset

”Asetus vahvistaa tietosuojaviranomaisten roolia monella tapaa.”

Mitä kansallinen viranomainen tulee tekemään rekisterinpitäjän näkökulmasta katsottuna?

- Lisää tietämystä rekisterinpitäjien velvollisuuksista, tiedottaa ja kouluttaa
- Käsittelee rekisteröityjen valituksia
- Tekee tarkastuksia
- Vastaanottaa ilmoituksia tietosuojavastaavista, joistain tietojen siirroista ulkomaille sekä tietoturvaloukkauksista

- Vastaanottaa ennakkoselvityksiä tietyissä suuririskisissä käsittelytilanteissa (ennakkokuulemisvelvoite).

- Voi viedä asian yhdenmukaisuusmekanismiin tai EDPB:n arvioitavaksi

- Edistää käytännesääntöjen laatimista, lausuu luonnoksista ja hyväksyy niitä.

- Kannustaa ottamaan käyttöön sertifiointimekanismeja sekä tietosuojasinettejä ja –merkkejä, joilla rekisterinpitäjät voivat osoittaa asetuksen noudattamista. Myöntää sertifikaatteja ja voi peruuttaa ne.

- Voi määrätä hallinnollisia seuraamuksia kuten hallinnollisen sakon, joka suuruudeltaan
  - max. 20 milj. € tai
  - 4 % yrityksen maailmanlaajuisesta kokonais-liikevaihdosta, jos se on suurempi.

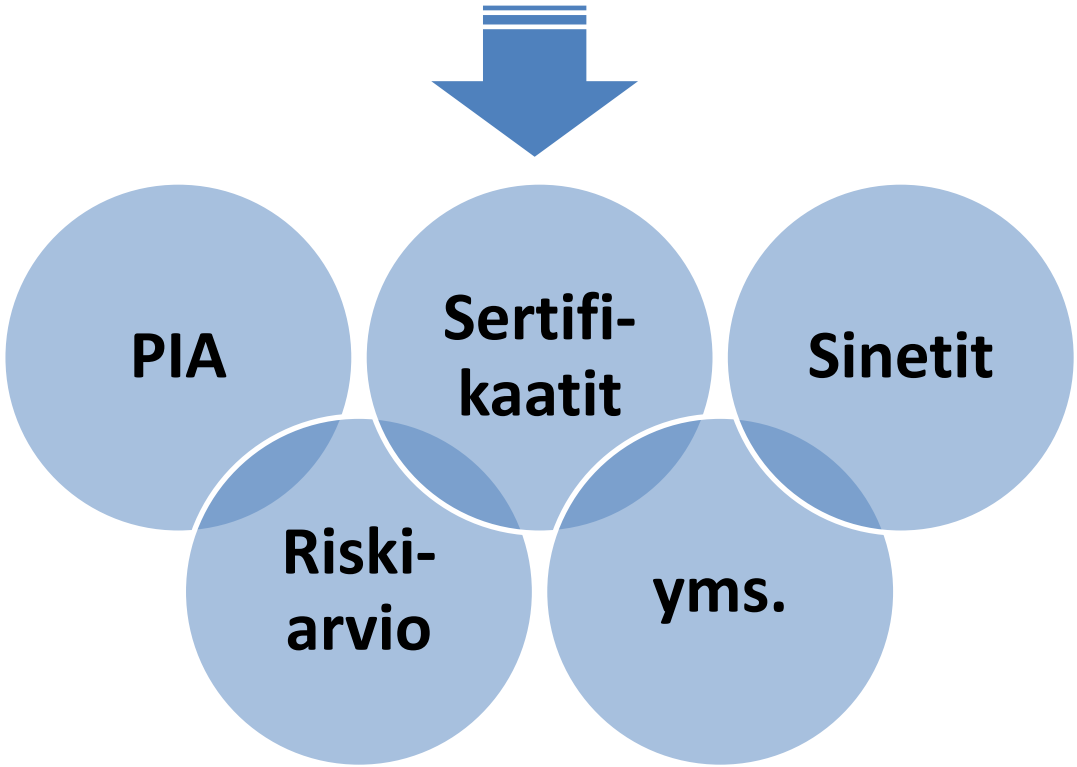
- Pitää sisäistä rekisteriä asetuksen rikkomisista ja niiden vuoksi toteutetuista toimenpiteistä (kuten varoituksista ja seuraamuksista)

- Jne.

Jos rekisterinpitäjä rikkoo asetusta, viranomainen voi hallinnollisen sakon asemesta tai rinnalla esim.:

- varoittaa siitä, että aiotut käsittelytoimet ovat todennäköisesti asetuksen vastaisia
- antaa huomautuksen, jos käsittelytoimet ovat olleet asetuksen vastaisia
- määrätä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat rekisteröidyn oikeuksien käyttöä
- määrätä saattamaan käsittelytoimet asetuksen mukaisiksi, tarvittaessa tietyllä tavalla ja määräajassa
- asettaa väliaikaisen tai pysyvän rajoituksen käsittelylle, myös käsittelykiellon

Nykymuotoinen ilmoitusvelvollisuus poistuu pääosin.

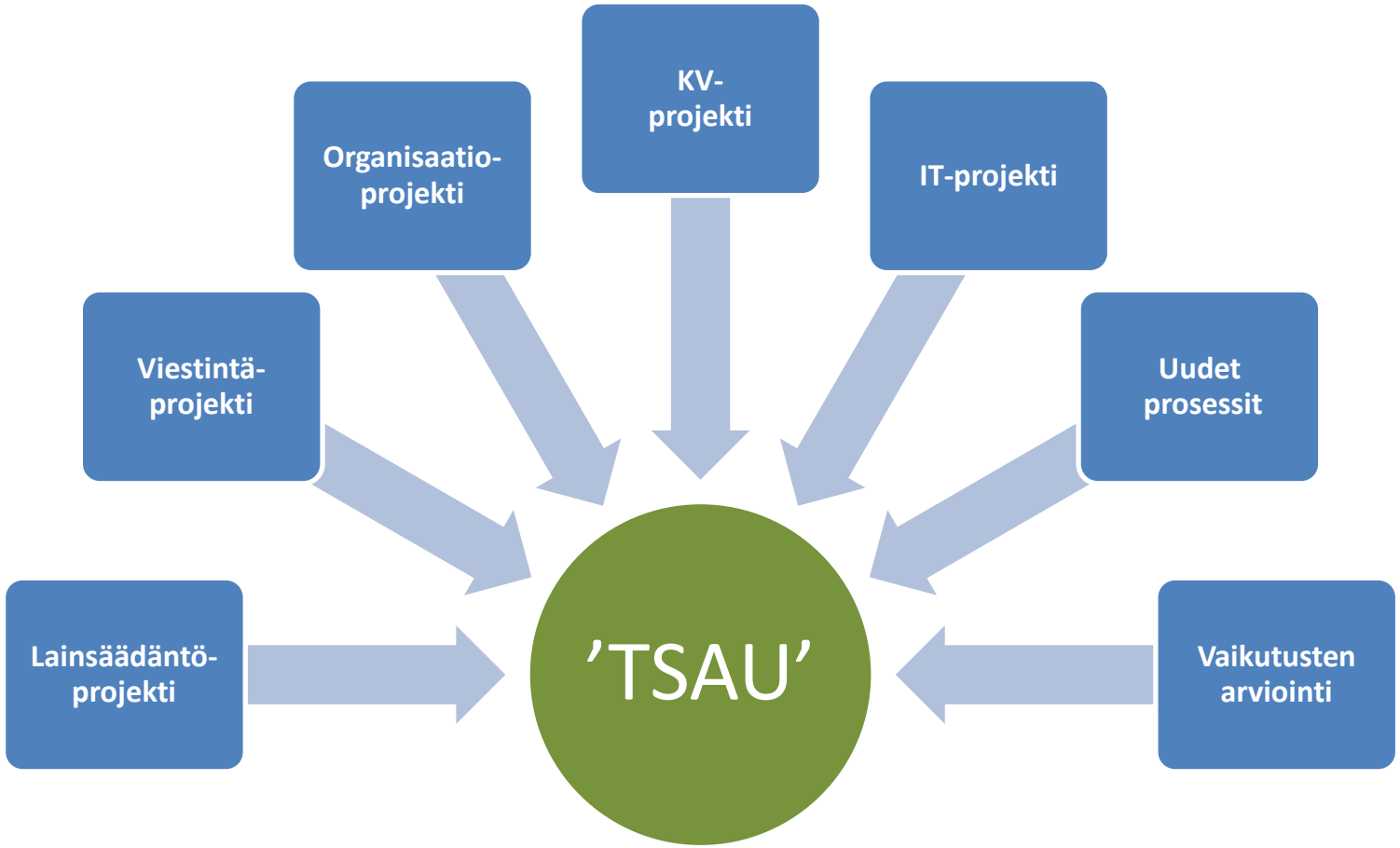


Valvontaviranomaisen on seurattava asetuksen soveltamista ja edistettävä sen yhdenmukaista soveltamista koko unionissa yksilöiden suojaamiseksi henkilötietojen käsittelyssä ja henkilötietojen vapaan liikkuvuuden varmistamiseksi sisämarkkinoilla.

Siirtymäajan valmistelutyötä WP29:n johdolla

- WP29:llä työohjelma ja tiekartta valmistautumiseen
- Ohjeiden ja lomakkeiden laatimista
- Viranomaisprosessien suunnittelua ja luomista
- Yhteisen kriteeristön määrittelyä
  - Mitä on suuririskinen tietojen käsittely (~PIA)?
  - Mitä Data portability tarkoittaa käytännössä?
  - Milloin hallinnollinen sakko määrätään?
- Jne.

TSV:n toimiston siirtymäajan projekti 2016-2017



6. Tietosuoja: Esteestä – menestystekijäksi!

Mahdollisuutena, kun **organisaation johto**

1. **organisoi** tuottavalla ja tehokkaalla tavalla **tietosuojatyön**
2. hyödyntää tietosuojavastaavan **tietosuojatyön tekemisen**
3. laatii kirjalliset ohjeet ja kouluttaa henkilöstön sekä **varmistuu työntekijöiden tietosuojaosaamisesta**:

   a) **henkilöstön** osaaminen ja oikeusturva paranevat sekä työviihtyvyys ja työteho lisääntyy, josta seuraa että
   b) **organisaation** tuottavuus ja tehokkuus kasvaa sekä saavutetaan kustannussäästöjä (EI ENÄÄ SÄHLÄTÄ!), huom! osaavan henkilöstön ansiosta potilasturvallisuus paranee, organisaatio näyttää ulospäin luotettavalta palvelujen antajalta, ja halutulta yhteistyökumppanilta
   c) samalla **asiakkaan (potilaan)** tietosuoja on oikein toteutettu, ei liian tiukka eikä liian heikko.

KIITOS,
mielenkiinnostasi !

Ylitarkastaja Arto Ylipartanen
Tietosuojavaltuutetun toimisto