EU:n tietosuoja-asetus:

Mitä uusi yleinen tietosuoja-asetus edellyttää organisaatiolta?

Teknologiateollisuus ry 13.2.2017

Ylitarkastaja Anna Hänninen

Esityksen sisältö

I. **Tietosuoja-asetus**

   I. Tietosuoja-asetuksen tausta ja sen tuomat muutokset

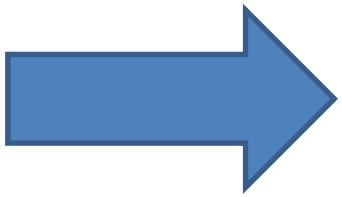
   II. Riskiperusteinen lähestymistapa, tietosuojaperiaatteet ja osoitusvelvollisuus

   III. Tietosuojavastaavat

I. Tietosuoja-asetuksen tausta ja sen tuomat muutokset

Tausta ja tavoitteet

- Tietosuojadirektiivi 1995 95/46/EY
- 28 jäsenvaltion hajanaiset tietosuojasäännökset
- Sosiaalinen ja taloudellinen yhdentyminen
- Teknologian nopea kehitys ja globalisaatio
- Luottamus on toiminnan elinehto sekä digitaalimarkkinoiden kehityksen ehto



”Vahva ja johdonmukaisempi tietosuojakehys, jota tuetaan tehokkaalla täytäntöönpanolla.”

Tausta ja tavoitteet

- Luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus
- Henkilötietojen suojan yhteensovittaminen muiden oikeuksien ja vapauksien kanssa
- Asetuksen punaisena lankana on havaittavissa riskiperusteinen tietojen käsittely ja rekisteröityjen itsemääräämisoikeuden vahvistaminen
- Teknologianeutraliteetti

Tausta ja tavoitteet

- Rekisteröityjen itsemääräämisoikeuden vahvistaminen
  - Rekisteröidyn oikeuksien ja rekisterinpitäjän velvollisuuksien kautta

- Tehokas valvontaviranomainen
  - Hallinnolliset sanktiot

Tietosuoja-asetus

- Kaikissa jäsenvaltioissa suoraan sovellettavaa oikeutta
  - Kansallista liikkumavaraa
    - Arvioidaan OM asettamassa TATTI-työryhmässä

- Sovelletaan 25.5.2018 alkaen niin yksityisellä kuin julkisella sektorilla

Vanhaa ja uutta

- Vanhojen käsitteiden rinnalle uusia
  - Esim. pseudonymisointi, geneettiset tiedot, biometriset tiedot, profilointi
- Käsittelyn oikeusperusteiden, periaatteiden, rekisterinpitäjän velvoitteiden ja rekisteröityjen oikeuksien osalta uutta ja täsmennyksiä
- Aineellinen soveltamisala lähtökohtaisesti sama kuin direktiivissä
- Alueellinen soveltamisala laajenee

Henkilötietojen käsittelyn oikeusperusteet

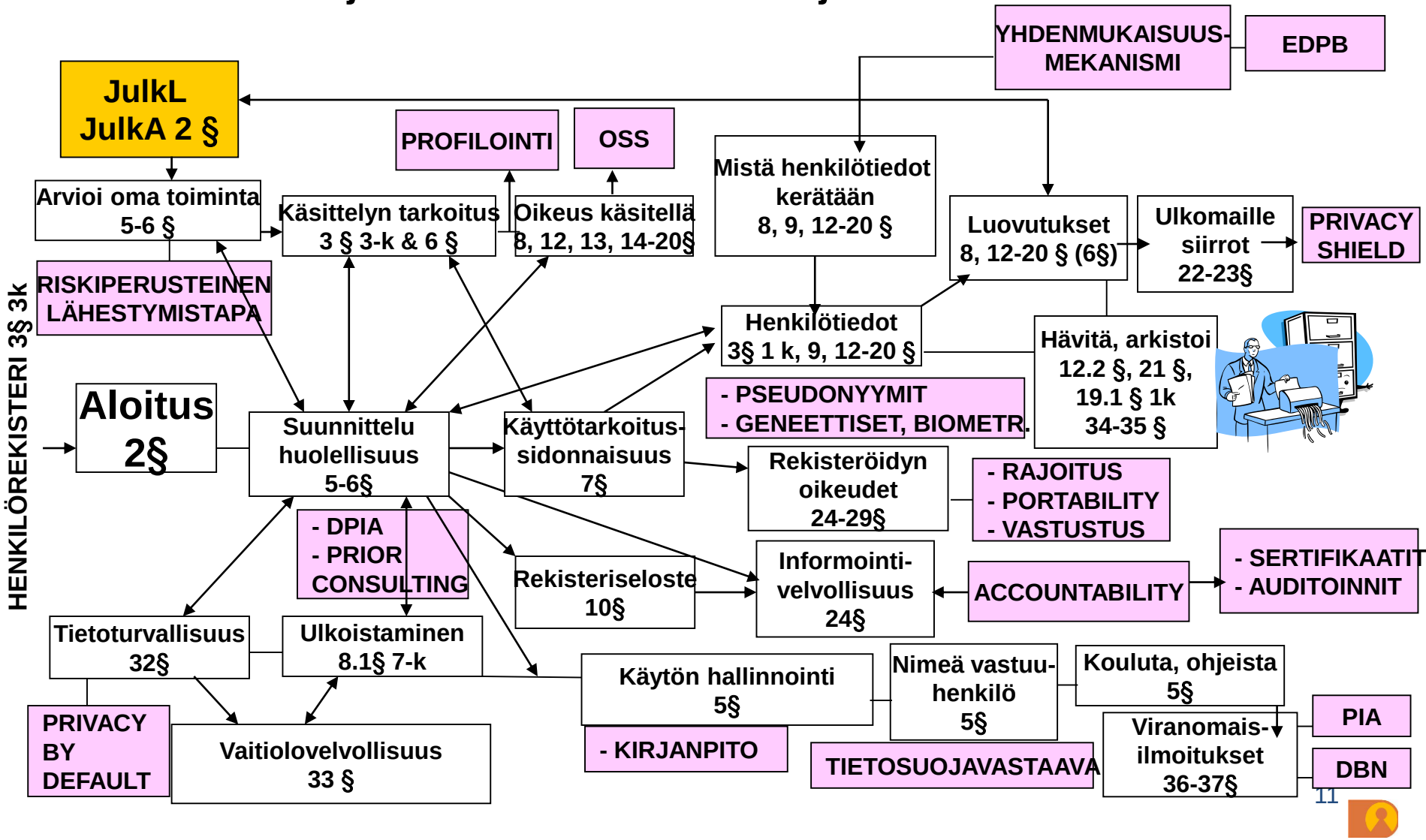
- Tietosuoja-asetuksen 6 artikla
  - Oikeutettu etu
- Tietosuoja-asetuksen 9 artikla (erityisiä henkilötietoryhmiä koskeva käsittely)
- Tietosuoja-asetuksen 10 artikla rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot
- Tietosuoja-asetuksen 5 luku henkilötietojen siirto kolmansiin maihin
- Käsittelyn oikeusperusteen lisäksi on täyttyvä muut tietosuoja-asetuksen velvoitteet ja periaatteet **!**

Muutoksia

- Tietosuojaa koskeva vaikutusten arviointi
- Tietosuojavastaavat
- Osoitusvelvollisuus
- Velvollisuus ilmoittaa tietoturvaloukkauksesta
  - Tietosuojaviranomaisille
  - Rekisteröidyille
- Sanktiot
- Rajat ylittävä valvonta

Henkilötietolaki ja TIETOSUOJA-ASETUS

Sisäänrakennettu ja oletusarvoinen tietosuoja 25 art.



II Riskiperusteinen lähestymistapa, tietosuojaperiaatteet ja osoitusvelvollisuus

Riskiperusteinen lähestymistapa

- Tarkoituksena on ottaa sääntelyssä huomioon henkilötietojen käsittelyyn kulloinkin liittyvät riskit ja **yhtäältä välttää vähäriskisten toimien ylisääntelyä ja toisaalta varmistaa rekisteröidyn suoja korkean riskin toiminnassa**
- Rekisterinpitäjä ja henkilötietojen käsittelijä velvoitetaan ryhtymään toimiin, jotka **vastaavat henkilötietojen käsittelyyn kulloinkin liittyvää riskiä**.

Tietosuojaperiaatteet

- Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Tietojen täsmällisyys
- Tietojen säilytyksen rajoittaminen
- Tietojen eheys ja luottamuksellisuus
-  Osoitusvelvollisuus

Osoitusvelvollisuus

- Uudenlainen suhtautuminen tietosuojaa koskeviin kysymyksiin
- Edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia
- Eri tasoilla:
  - Miten periaatteet toteutuvat? Asetuksen noudattamisen osoittaminen?
- Sertifikaatit ja käytännesäännöt

Sisäänrakennettu ja oletusarvoinen tietosuoja

- Tietosuojaperiaatteet otetaan tehokkaasti osaksi henkilötietojen käsittelyä sisältäviä toimintoja niiden kaikissa vaiheissa
  - toteutettava tietosuojaperiaatteiden täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet
- Rekisterinpitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja
- Tietosuojaa koskevat kysymykset tunnistetaan ja otetaan huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja tai kehitetään tietojärjestelmiä

Roolit

- Rekisteröity
- Rekisterinpitäjä tai yhteisrekisterinpitäjät
- Henkilötietojen käsittelijä
- Valvontaviranomainen
- Euroopan tietosuojaneuvosto

Vastuut asetuksen mukaan

- Rekisterinpitäjän vastuu säilyy
  - Ei voi ulkoistaa vastuuta tietosuojavastaavalle
- Yhteisrekisterinpitäjät (art. 26)
  - Määriteltävä läpinäkyvällä tavalla vastuualueet
- Henkilötietojen käsittelijä (28 art.)
  - Asetuksen vaatimusten täyttäminen
  - Ketjutukseen valtuutus
  - Sopimus tai muu oikeudellinen asiakirja
  - Komission vakiosopimuslausekkeet
  - Valvontaviranomaisen hyväksymismenettely vak.sop. lausekkeille
  - Kirjallinen

III Tietosuojavastaavat

- Tietosuojatyöryhmä WP 29 ohje ”tietosuojavastaavista” http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/WC2W0GhSR/Guidelines_on_Data_Protection_Officers.pdf.

Milloin on nimitettävä

- **Viranomainen tai julkishallinnon elin**
- Rekisterinpitäjän tai henkilötietojen käsittelijän **ydintehtävät** muodostuvat käsittely toimista, jotka luonteensa, laajuutensa ja/tai tarkoitusten vuoksi edellyttävät **laajamittaista** rekisteröityjen **säännöllistä ja järjestelmällistä seurantaa**
- Rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu 9 art. tai 10 art. mukaisiin tietoihin.

- Myös vapaaehtoisesti tietosuojavastaava tai **muu henkilö**?

Tietosuojavastaavan asema

- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn
- Osoitetaan tarpeelliset resurssit tehtävien hoitamiselle
- Itsenäinen asema
- ”Irtisanomissuoja”
- Eturistiriidat

Tietosuojavastaavan tehtävät

- Neuvot rekisterinpitäjälle tai käsittelijälle sekä työntekijöille
- Valvoa tietosuoja-asetuksen noudattamista
- Rooli tietosuojaa koskevan vaikutusten arvioinnin tekemisessä ja ennakkokuulemisessa
- Valvontaviranomaisen ja rekisteröityjen yhteyspiste

Huoneentaulu rekisterinpitäjille

1) Kartoita tietojen käsittelyn nykytila ja ota tietosuoja osaksi toimintojen suunnittelua
2) Arvio henkilötietojen käsittelyyn liittyvät riskit ja toimenpiteet niiden minimoimiseksi
3) Tee tarvittaessa tietosuojaa koskeva vaikutustenarviointi ja kuule valvontaviranomaista
4) Selvitä, millä perusteella käsittelet henkilötietoja
5) Tunnista tietosuoja-asetuksen vaatimukset henkilötietojen käsittelyn ulkoistamiselle
6) Selvitä, mitä rekisteröidyn oikeuksia toimintaasi liittyy ja, miten toteutat niitä
7) Jos organisaatiosi toimii usean jäsenvaltion alueella, selvitä johtava valvontaviranomainen
8) Arvio asianmukaiset suojatoimenpiteet ja suojaa koko elinkaari
9) Valmistaudu ilmoittamaan tietoturvaloukkauksista
10) Nimitä tarvittaessa tietosuojavastaava

Lisätietoja

Tietosuojavaltuutetun verkkosivut:

www.tietosuoja.fi

Tietosuoja-asetus teksti:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT