

Tietosuoja koskeva vaikutustenarviointi (DPIA, 35 artikla)



TIETOSUOJAVALTUUTETUN
TOIMISTO

Heikki Partanen
Ylitarkastaja

- Uusi väline tietosuojaoikeudessa
- Tähän saakka kehitetty PIAna (Privacy Impact Assessment)
- Tukee riskiperusteista lähestymistapaa
- Itsearviointityökalu
- Valvontaviranomaisen roolina ennakkokuuleminen
- Yhdenmukaisen soveltamisen ja kehittämisen uhkana se, ettei ennakkokuulemispyyntöjä tehdä eikä käytäntöä synny

Miksi vaikutusarviointi tulisi tehdä ?

- Asetuksessa säädetty tai sen nojalla määrätty velvollisuus
 - 35 artiklan 1, 3, 4 ja 5 kohdat
 - Ohjeet WP 248:ssa
- Kansallisessa laissa
 - Tietosuojalaki 6 § 10 kohta, 31 § 3 mom
- Lainvalmisteluvaiheessa etukäteen
 - 35 artiklan 10 kohta (yleinen ja erityinen)
- Osana lähtökohtaista ja oletusarvoista tietosuojan toteutusta

Mitä vaikutusten arvioinnilta edellytetään ?

- Asetuksen 35 artiklan 7 alakohta arvioinnin vähimmäisisältö
 - Kuvaus arvioitavasta käsittelystä
 - Arvio käsittely tarpeellisuudesta ja oikeasuhteisuudesta
 - Arvio oikeuksia ja vapauksia koskevista riskeistä
 - Suunnitellut toimenpiteet riskeihin puuttumiseksi
- WP 248 ohjeet
 - Liite 2 tarkastuslista edellä mainituista kohdista

ja miten se tulisi tehdä ?

- Komission aloitteita työkalun kehittämiseksi
 - RFID –sovellusten vaikutusarviointikehys (WP 175 (2010) ja WP 180 (2011))
 - Smartgrid and metering vaikutusten arvioinnin laadintamalli (templete)
 - WP 205 (2013) ja WP 209 (2013)
 - Ensimmäinen versio 3/2014
 - Toinen versio 9/2018 <https://ec.europa.eu/energy/en/data-protection-impact-assessment-smart-grid-and-smart-metering-environment>
- Jäsenvaltioiden valvontaviranomaisen kehittämiä työkaluja
 - CNIL (FR) kehittämä PIA (Privacy Impact Assessment) 2012 ja 2018
 - Methodology, Template ja Knowledge base
 - Puutteet

Miten DPIA tekemistä tulisi edistää ja tukea ?

- Yhteistyö toimialakohtaisesti
 - yhtä arviota voidaan käyttää samankaltaisissa tilanteissa
- Valitun metodologian kokeilu hyvin rajatuissa tilanteissa
 - Esim. henkilötietojen konvertointi toiseen järjestelmään
- Jaettavien resurssien muodostaminen ja jakelu
 - Threat taxonomy (Uhkakuvasto)
 - List of possible controls (Suojauskeinojen kirjasto)
 - GDPR requirements (Tietosuojaperiaatteiden ja -oikeuksien listaus)