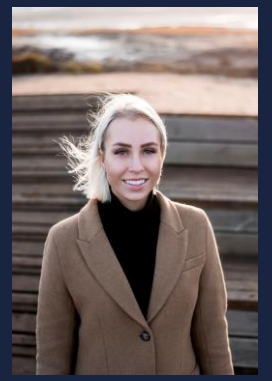
Tietosuojan vaikutustenarviointi

15.6.2022

DLA PIPER

Agenda

1. Mikä on tietosuojan vaikutustenarviointi?
2. Milloin tietosuojan vaikutustenarviointi tulee tehdä?
3. Miten vaikutustenarviointi tehdään?
4. Transfer Impact Assessment
5. Case-esimerkki

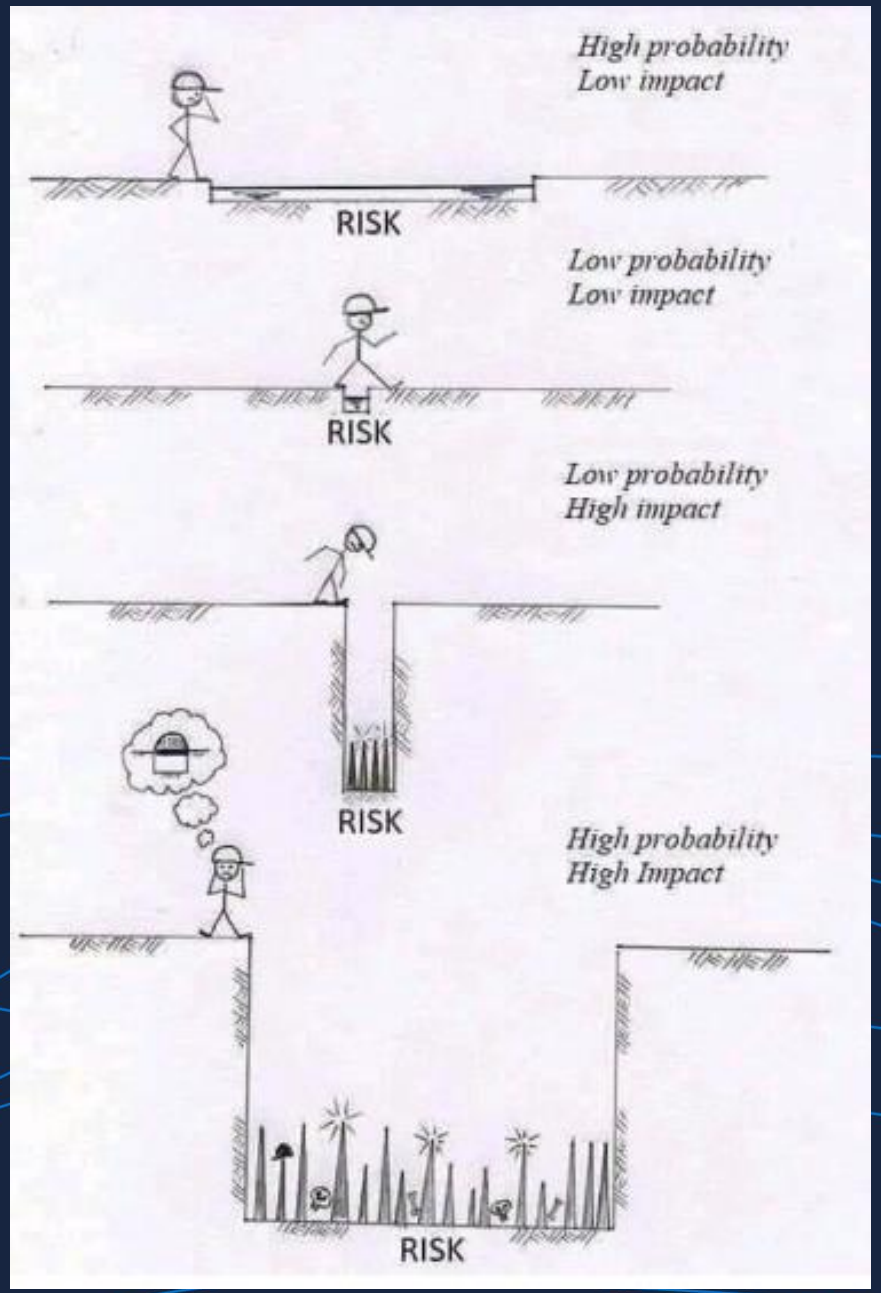


Vera Pallasvesa
Associate Trainee
Asianajotoimisto DLA Piper Finland Oy
+358 45 638 7476
vera.pallasvesa@fi.dlapiper.com

Mikä on tietosuojan vaikutustenarviointi?

Mikä on tietosuojan vaikutustenarviointi?

- Yleinen tietosuoja-asetus asettaa rekisterinpitäjälle velvollisuuden hallita henkilötietojen käsittelyn aiheuttamia riskejä
- Yleisen tietosuoja-asetuksen 35 artiklan mukaan vaikutustenarviointi on tehtävä silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyin oikeuksille ja vapauksille
- Vaikutustenarvioinnin tarkoituksena on tunnistaa ja vähentää henkilötietojen käsittelyyn liittyviä riskejä
- Vaikutustenarvioinnin avulla voidaan tuottaa dokumentaatiota, jolla tietosuojasääntelyn noudattaminen voidaan osoittaa
- Tekemättä jättäminen tilanteessa, jossa vaikutustenarviointi tulisi tehdä, voi johtaa hallinnollisiin seuraamuksiin
- Yhtä vaikutustenarviointia voidaan käyttää useiden käsittelytoimien arviointiin, joiden luonne, laajuus, asiayhteys, tarkoitus ja riskit ovat samankaltaisia



Vaikutustenarvioinnin keskeisenä tavoitteena on tunnistaa, hallinnoida ja minimoida henkilötietojen käsittelyyn liittyviä riskejä

Milloin tietosuojan vaikutustenarviointi tulee tehdä?

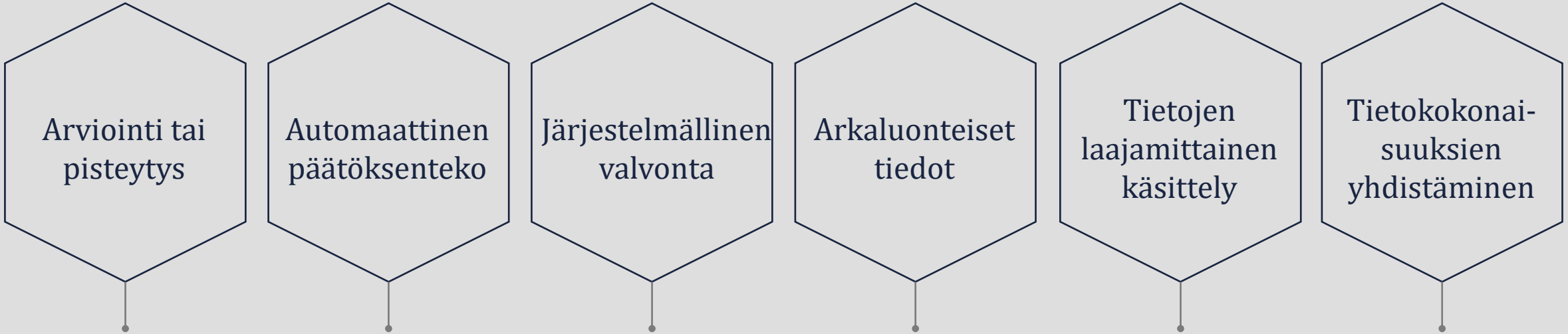
Milloin tietosuojan vaikutustenarviointi tulee tehdä?

Milloin käsittely todennäköisesti aiheuttaa korkean riskin?

- Tietosuoja-asetuksen 35 artikla 3 kohta antaa esimerkkejä tilanteista, joissa vaikutustenarviointi vaaditaan erityisesti:
  - *luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin, joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi;*
  - *laajamittainen käsittely, joka kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin; tai*
  - *yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti.*
- Tietosuoja-asetuksen luettelo ei ole tyhjentävä, ja vaikutustenarviointi voidaan vaatia myös muissa tilanteissa
- Vaikutustenarviointi tulee tehdä ennen käsittelytoimen aloittamista

Milloin tietosuojan vaikutustenarviointi tulee tehdä?

Milloin käsittely todennäköisesti aiheuttaa korkean riskin?



Erityisesti rekisteröidyn työsuorituksen, taloudellisen tilanteen, terveyden, henkilökohtaisten mieltymysten tai kiinnostuksen kohteiden, luotettavuuden tai käyttäytymisen, sijainnin tai liikkumisen arviointi tai pisteytys, mukaan lukien profilointi.

Käsittely, jonka tavoitteena on tehdä rekisteröidyistä päätöksiä, joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi.

Rekisteröityjen tarkkailuun, seurantaan tai valvontaan käytettävä tietojenkäsittely sekä tietojen kerääminen verkkojen välityksellä tai yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti.

Erityiset henkilötietoryhmät sekä rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot.

Rekisteröityjen lukumäärä, käsiteltävien tietojen määrä, käsittelytoimen kesto, käsittelytoimen maantieteellinen ulottuvuus.

Tietokokonaisuuksien yhdistäminen rekisteröidyn kohtuulliset odotukset ylittävällä tavalla.

Milloin tietosuojan vaikutustenarviointi tulee tehdä?

Milloin käsittely todennäköisesti aiheuttaa korkean riskin?

Heikossa asemassa olevia rekisteröityjä koskevat tiedot, esimerkiksi lapsia koskevat tiedot.

Uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen.

Tapaukset, joissa käsittelytoimet estävät rekisteröityjä käyttämästä oikeutta, palvelua tai sopimusta.

Milloin tietosuojan vaikutustenarviointi tulee tehdä?

Milloin käsittely todennäköisesti aiheuttaa korkean riskin?

- Useimmiten kaksi kriteeriä täyttävä käsittely edellyttää tietosuojaa koskevan vaikutustenarvioinnin tekemistä
- Rekisterinpitäjä voi kuitenkin katsoa, että vain yhden näistä kriteereistä täyttävä käsittely edellyttää vaikutustenarvioinnin tekemistä
- Käsittelytoimi voi myös vastata edellä mainittuja tapauksia, ja rekisterinpitäjä voi silti katsoa, ettei se todennäköisesti aiheuta korkeaa riskiä
  - Rekisterinpitäjän on perusteltava ja dokumentoitava syyt, joiden vuoksi se ei tee vaikutustenarviointia
    - Dokumentoinnin tulee sisältää tietosuojavastaavan näkemykset
- Velvoite tehdä vaikutustenarviointi voi myös seurata kansallisesta lainsäädännöstä
  - Esimerkiksi tietosuojalain 31 §:n historiallisessa ja tieteellisessä tutkimuksessa sekä tilastoinnissa määrätyistä rekisteröidyn oikeuksista poikkeaminen

Milloin tietosuojan vaikutustenarviointi tulee tehdä?

Tietosuojavaltuutetun päätös käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi

- Tietosuoja-asetuksen 35 artikla 4 kohta asettaa lisäksi valvontaviranomaiselle velvoitteen julkaista luettelo käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi
- Tietosuojavaltuutetun toimiston julkaisema luettelo on saatavilla heidän verkkosivuillaan, se ei ole tyhjentävä
- Luettelon mukaan seuraavien käsittelytoimien yhteydessä tulee tehdä vaikutustenarviointi:
  - Biometriset tiedot
  - Geneettiset tiedot
  - Sijaintitiedot
  - Poikkeaminen rekisteröidyn informoinnista tietosuoja-asetuksen 14.5 artiklan nojalla
  - Whistleblowing

Miten vaikutustenarviointi tehdään?

Miten vaikutustenarviointi tehdään?

- Yleisen tietosuoja-asetuksen 35 artikla 7 kohta asettaa vähimmäisvaatimukset vaikutustenarvioinnille
- Vaikutustenarvioinnin on sisällettävä vähintään:
  - järjestelmällisen kuvauksen suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, lisäksi tarvittaessa rekisterinpitäjän oikeutetut edut;
  - arvion käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta;
  - arvion rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä;
  - suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että yleistä tietosuoja-asetusta noudatetaan

Miten vaikutustenarviointi tehdään?

Tietosuojavaltuutetun toimiston työkalu

- Tietosuojavaltuutetun toimisto on julkaissut sivuillaan Excel-työkalun vaikutustenarvioinnin tekemisen tueksi
- Työkalu sisältää:
  - Käsittelytoimen yleiset tiedot
  - Kuvaus käsittelytoimesta
  - Käsittelyn tarpeellisuus ja oikeasuhtaisuus
  - Tietosuojaperiaatteet
  - Käsittelijät ja siirrot
  - Rekisteröidyn oikeudet
  - Uhat
  - Riskien arviointi
  - Yhteenveto
  - Hyväksyminen
  - Jatkotoimenpiteet

Miten vaikutustenarviointi tehdään?

- Yleinen tietosuoja-asetus ei vaadi vaikutustenarvioinnin julkaisemista, rekisterinpitäjä voi kuitenkin hyödyntää tehtyä vaikutustenarviointia toteuttaessaan henkilötietojen käsittelyn läpinäkyvyyttä, esimerkiksi julkaisemalla yhteenvedon vaikutustenarvioinnista
- Jos rekisterinpitäjä ei pysty lieventämään havaittuja riskejä hyväksyttävälle tasolle, vaan vaikutustenarvioinnista käy ilmi korkeita jäännösriskejä, rekisterinpitäjän on pyydettävä valvontaviranomaiselta käsittelyä koskevaa ennakkokuulemista
  - Tällöin vaikutustenarviointi on toimitettava valvontaviranomaiselle
- Valvontaviranomainen antaa rekisterinpitäjälle ja käsittelijälle kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi
  - Tarvittaessa valvontaviranomainen voi ennakkokuulemisen yhteydessä käyttää myös toimivaltuuksiaan, kuten varoitusta
  - Rekisteripitäjän ja käsittelijän on toteutettava ohjeen mukaiset toimenpiteet ennen käsittelyn aloittamista, jotta käsittely voidaan katsoa lainmukaiseksi
- Rekisterinpitäjän tulee säilyttää tehty vaikutustenarviointi ja säännöllisesti arvioitava sen päivitystarve

Transfer Impact Assessment

Transfer Impact Assessment

TIA

- Käsittelytoimesta aiheutuvaa riskiä arvioitaessa tulisi ottaa myös huomioon tietojen siirrot EU/ETA-alueen ulkopuolelle
- *Schrems II* tuomion jälkeen käsittelytoimille, joissa on tietojen siirtoja EU/ETA-alueen ulkopuolelle tuli lisävaatimuksia
  - Tietojen siirron huomioinen vain vaikutustenarvioinnissa ei ole riittävä
  - Tietosuojan vaikutustenarvioinnin lisäksi rekisterinpitäjän tulisi toteuttaa erillinen arvio käsittelytoimen tietojen siirrosta, ns. transfer impact assessment, TIA
  - Huomioitavat kriteerit tulevat EDPB:n 1/2020 antamasta suosituksesta
  - TIAn tarkoituksena on arvioida säilyykö EU:n tietosuojalainsäädännön mukainen tietosuojan taso siirrettäessä henkilötietoja kolmanteen maahan
  - Jos arvio osoittaa että tietosuojan taso laskee siirron yhteydessä, on rekisterinpitäjän otettava käyttöön täydentäviä suojatoimia
  - Erityisen ongelmallisia ovat maat, joissa lainsäädäntö mahdollistaa viranomaisten pääsyn henkilötietoihin

DLA Piper Data Transfer Metodologia

Case-esimerkki

Seuraamusmaksu vaikutustenarvioinnin tekemättä jättämisestä

- Vuonna 2020 Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi 16 000 euron seuraamusmaksun Kymen Vesi Oy:lle vaikutustenarvioinnin tekemättä jättämisestä
- Kymen Vesi Oy käsitteli työntekijöiden sijaintietoja paikantamalla ajoneuvoja ajotietojärjestelmän avulla
- Sijaintietoja käytettiin mm. työajanseurantaan
- Rekisterinpitäjä ei ollut tehnyt vaikutustenarviointia ennen käsittelytoimen aloittamista
- Kyseessä oli heikommassa asemassa olevien rekisteröityjen sijaintietojen käsittely ja sijaintietojen käyttäminen järjestelmälliseen valvontaan
- Huom! Työntekijät lasketaan heikossa asemassa oleviksi rekisteröidyiksi ainakin suhteessa valvontatarkoituksiin suoritettavaan henkilötietojen käsittelyyn

Kiitos!