



ASIANAJOTOIMISTO AKG OY

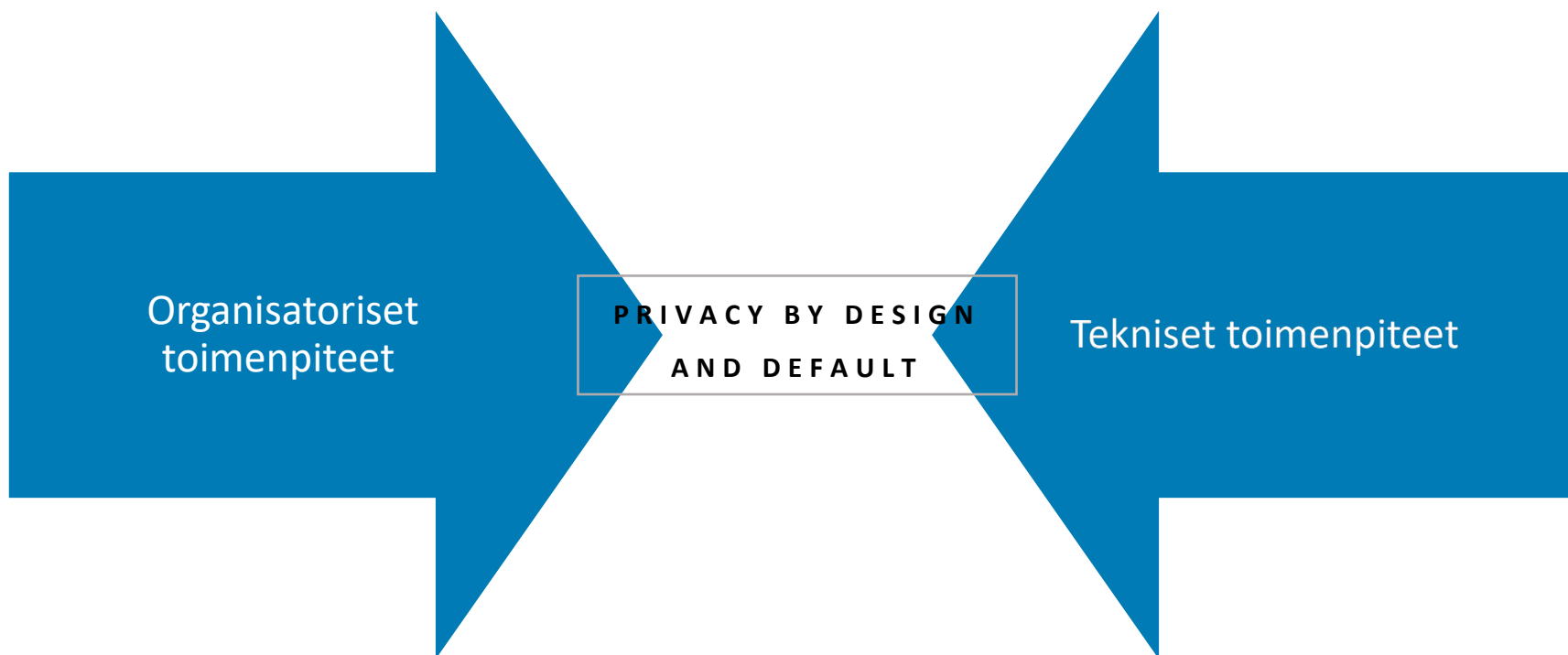
Yrityksen vastuut sekä velvoitteet tietosuoja-asetuksen osalta

GDPR-tietoisku 4.11.2020

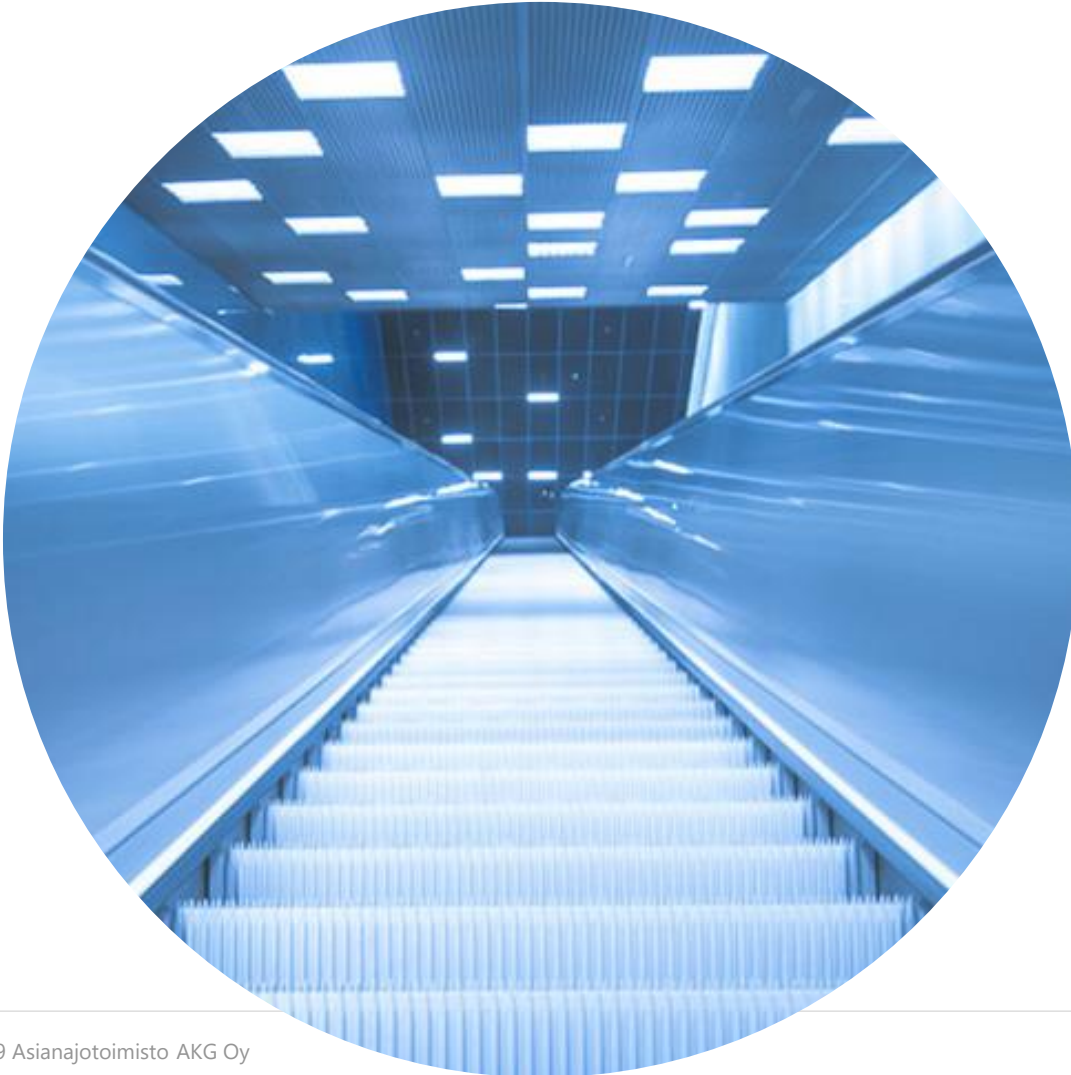
Lauri Mäki, osakas, asianajaja

Asianajotoimisto AKG Oy

Sisäänrakennettu ja oletusarvoinen tietosuoja



Riskipohjainen lähestymistapa



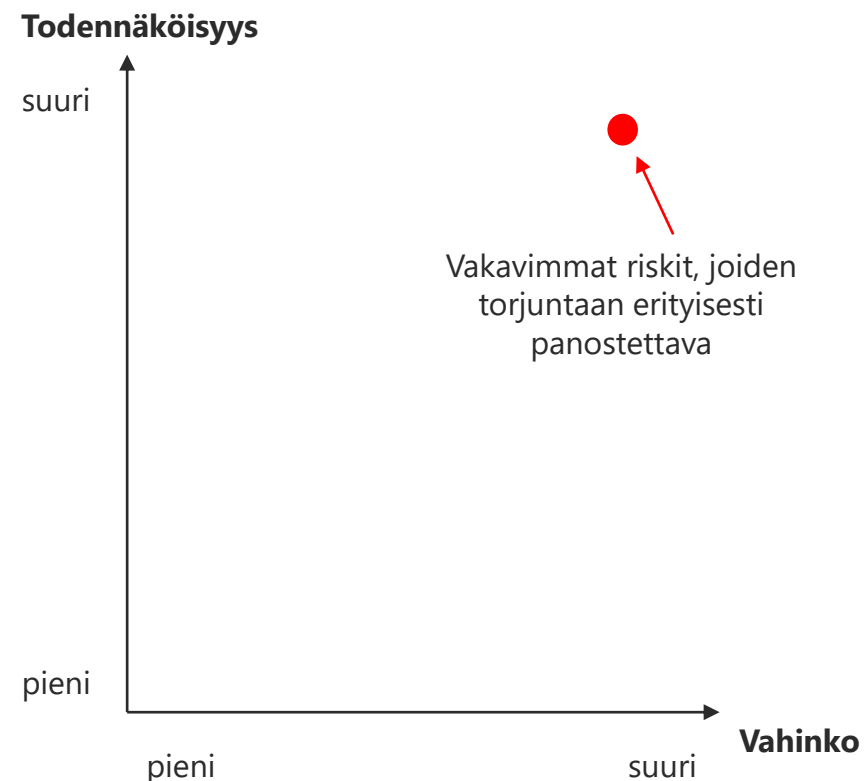
- Riski =
skenaario, jolla kuvataan tapahtumaa ja sen seurauksia sekä arvioidaan näiden vakavuutta ja todennäköisyyttä.
- Riskinhallinta =
koordinoitua toimintaa, jolla ohjataan ja valvotaan organisaatiota riskien osalta.
- Riski koostuu seuraavista tekijöistä: 1. tapahtumasta, 2. tapahtuman todennäköisyydestä ja 3. tapahtuman seurauksien vakavuudesta eli aiheutuvasta vahingosta.
- Tietosuoja-asioissa lähtökohtana on riskipohjainen lähestymistapa, johon liittyy riskien arviointi ja ongelmien ennaltaehkäisy.
- Riskit otettava huomioon sisäänrakennettua ja oletusarvoista tietosuojaa toteutettaessa.

Riskipohjainen lähestymistapa

- Toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.
- Ihmisille ilmoitettava, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin heidän oikeuksilleen ja vapauksilleen.
- Riskejä tulisi arvioida niiden ihmisten näkökulmasta, joiden henkilötiedoista on kysymys.
- Yritykselle aiheutuvia vahinkoja ovat mm. menetettävien tietojen arvo, maineelle, brändille ja luotettavuudelle aiheutuva vahinko sekä mahdolliset vahingonkorvaukset/sanktiot.

Ks. lisää esim. täältä:

<https://shop.almatalent.fi/uusi-tietosuojalainsaadanto>



Vaikutustenarviointi ja ennakkuuleminen

VAIKUTUSTENARVIOINTI

- Mikä on vaikutustenarviointi?
 - Jatkuva prosessi, jossa tarkastellaan tietosuojan toteuttamiseksi suunniteltuja toimenpiteitä, suojatoimia ja mekanismeja, joiden avulla lievennetään henkilötietojen käsittelystä aiheutuvia riskejä.
 - Kuva ja arvioi käsittelyn tarpeellisuutta suhteessa riskeihin.
 - Varmistaa tietosuoja-asetuksen noudattamisen henkilötietojen käsittelyssä.
 - Helpottaa tietosuoja-asetuksen mukaisen osoittamisvelvollisuuden käytännön noudattamista.
 - Oleellinen osa riskienhallintaa.
- Milloin se tulee tehdä?
 - Jos henkilötietojen käsittely aiheuttaa todennäköisesti luonnollisen henkilön oikeuksien kannalta korkean riskin, ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitus.
 - Käsittelyssä tapahtuu muutoksia, esimerkiksi otetaan käyttöön uutta tietojenkäsittelytekniikkaa. Huom. automaattinen päätöksenteko.
 - Aina pakollinen, kun yritys käsittelee laajamittaisesti arkaluontoisia henkilötietoja.
- Vaikutustenarvioinnin tekeminen
 - Toteuttamisesta vastaa rekisterinpitäjä.
 - Tehtävä ennen kuin henkilötietoja aletaan käsitellä.
 - Sisällettävä vähintään: järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksesta; arvio käsittelytoimien tarpeellisuudesta ja oikeasuhtaisuudesta tarkoituksiin nähden; arvio riskeistä, joiden takia vaikutustenarviointi tehdään; sekä suunnitellut toimenpiteet riskeihin puuttumisesta.

Ks. lisää esim. täältä:

Vaikutustenarviointi ja ennakkuuleminen

ENNAKKOKUULEMINEN

- Ketä pitää kuulla?
 - Valvontaviranomaista, eli Suomessa tietosuojavaltuutettua.
- Milloin pitää kuulla?
 - Jos vaikutustenarviointi osoittaa, että henkilötietojen käsittelyyn liittyy suuri riski, eikä rekisterinpitäjä pysty toteuttamaan riittäviä toimenpiteitä riskien lieventämiseksi.
 - Kuuleminen on tehtävä ennen kuin henkilötietoja aletaan käsitellä.
- Toimitettavat tiedot
 - Rekisterinpitäjän tulee toimittaa valvontaviranomaiselle kuulemista varten seuraavat tiedot: eri vastuutahojen vastualueet, suunnitellun henkilötietojen käsittelyn tarkoitus, toteutetut suojatoimet, tietosuojavastaavan yhteystiedot, vaikutustenarviointi ja muut viranomaisen pyytämät tiedot.
 - Valvontaviranomainen antaa kirjalliset ohjeet rekisterinpitäjälle tai henkilötietojen käsittelijälle pääsääntöisesti kahdeksan viikon kuluessa kuulemispyynnöstä.

Ks. lisää esim. täältä:



Sopimukset, velvoitteet ja dokumentaatio

SOPIMUKSET

- Tietojenkäsittelysopimukset
 - Rekisterinpitäjän ja käsittelijän välille on laadittava sopimus (Data Processing Agreement; "DPA")
 - Tietosuoja-asetus edellyttää erityisesti tiettyjä ehtoja (GDPR 28 (3) artikla)
 - Vastuut ja vahingonkorvaukset usein neuvotteluissa keskiössä
 - Sovittava myös kustannusten jako ja maksut
- Luovutus sopimukset
 - Henkilötietojen luovuttaminen vs. henkilötietojen käsittely
 - Henkilötietojen luovuttamisen edellytykset varmistettava
 - Luovutus sopimuksen sisältö
 - Kyseessä on luovutus
 - Informointivelvoitteet
 - Rekisteröityjen oikeudet
 - Mitä, milloin, miten?

Ks. lisää esim. täältä:

Sopimukset, velvoitteet ja dokumentaatio

VELVOITTEET

OSOITUSVELVOLLISUUS SIITÄ, ETTÄ LAINMUKAISUUS, KOHTUULLISUUS JA LÄPINÄKYVYYS TOTEUTUVAT

Organisatorisia?

- ✓ Tietojen minimointi
- ✓ Täsmällisyys

Käyttötarkoitussidonnaisuus

Teknisiä?

- ✓ Säilytyksen rajoittaminen
- ✓ Eheys ja luottamuksellisuus



Sopimukset, velvoitteet ja dokumentaatio

DOKUMENTOINTI



- Osoitusvelvollisuus – dokumentoinnin suuntaviivana.
- Dokumentteja
 - Seloste käsittelytoimista
 - Periaatteet ja mahdolliset tietosuojaa koskevat laajemmat toimintaperiaatteet
 - Informointikäytännöt
 - Oikeusperusteen dokumentointi
 - Muut sisäiset ja ulkoiset ohjeistukset
 - Riskiarvioita koskeva dokumentaatio sekä toteutetut tekniset ja organisatoriset suojatoimenpiteet
 - Sisäiset ja ulkoiset ohjeet rekisteröidyn oikeuksien toteuttamiseksi
 - Ohjeet henkilötietoja käsitteleville työntekijöille ja henkilötietojen käsittelijöille
 - Sisäiset tarkastukset ja auditoinnit
 - Vaikutustenarviointeja koskeva dokumentaatio
 - Henkilötietojen tietoturvaloukkausten dokumentointi ja tätä koskeva prosessi
 - Tietosuojavastaavan asemaan ja tehtäviin liittyvä dokumentaatio
 - Henkilötietojen käsittelyyn liittyvät sopimukset, luovutus sopimukset ja rekisterinpitäjien väliset sopimukset
 - Henkilötietojen siirtoa kolmansiin maihin koskeva dokumentaatio



Ks. lisää esim. täältä:

<https://tietosuoja.fi/osoitusvelvollisuus>



ASIANAJOTOIMISTO AKG OY

Kiitos!
AKG – Ratkaisu.

Lauri Mäki, osakas, asianajaja
lauri.maki@akg.fi
p. 040 723 0984