Kuvaus henkilötietojen käsittelytoimista – mitä, milloin ja miksi?

Asianajaja, osakas, CIPP/E Ville Vainio

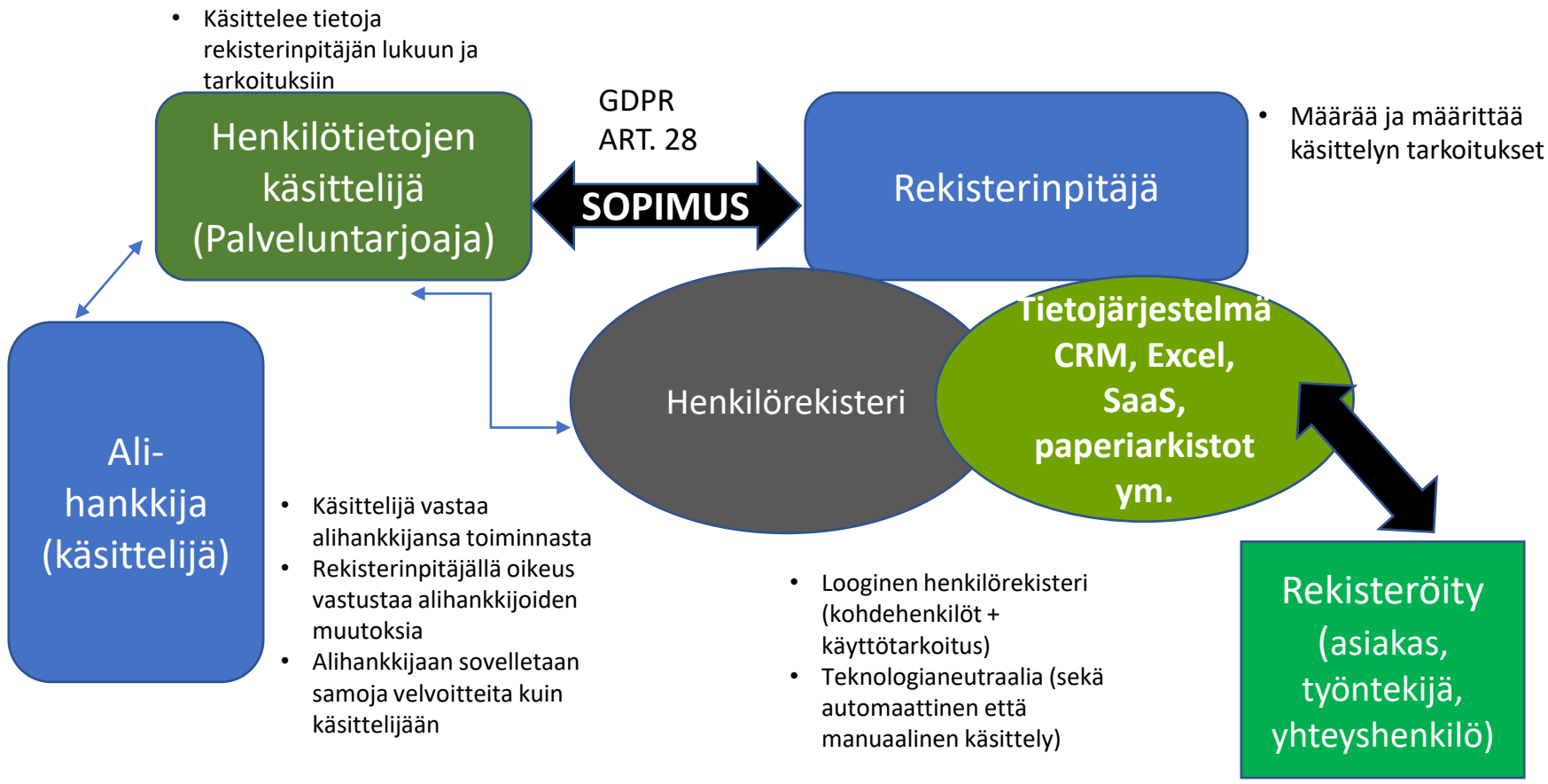
Asianajotoimisto Applex Oy | 25.5.2022

GDPR

- EU:n yleinen tietosuoja-asetus 679/2016 (General Data Protection Regulation) korvasi EU:n aiemman tietosuojadirektiivin 95/46/EY vuodelta 1995
  - Yhdet yhteiset tietosuojapelisäännöt EU-alueelle
  - Sääntelyn tuominen nykypäivään – teknologian kehittyminen
- Asetuksena GDPR on suoraan sovellettavaa EU-lainsäädäntöä
- Soveltaminen alkoi 25.5.2018
- Suomen osalta tietosuoja-asetusta täydentää yleinen tietosuojalaki (1050/2018)
- Suomessa valvontaviranomainen Tietosuojavaltuutetun toimisto, www.tietosuoja.fi

Tietosuojalainsäädännön peruskäsitteet ja toimijat

1) 'henkilötiedoilla' kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella,



Henkilötietojen käsittelyä koskevat periaatteet

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys	Henkilötiedoille on oltava lainmukainen käsittelyperuste Rekisteröityjä on informoitava henkilötietojen käsittelystä
Käyttötarkoitussidonnaisuus	Henkilötietoja saa käsitellä vain ennalta määritettyyn käyttötarkoitukseen
Tietojen minimointi	Vain tarpeellisia henkilötietoja saa käsitellä
Täsmällisyys	Epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
Säilytyksen rajoittaminen	Henkilötietoja saa käsitellä vain määritetyn käyttötarkoituksen ajan
Eheys ja luottamuksellisuus	Suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta

Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että näitä periaatteita on noudatettu!

Applex

Seloste käsittelytoimista

- GDPR 30 artiklan mukainen velvollisuus tarkoittaa, että rekisterinpitäjän ja henkilötietojen käsittelijän on dokumentoiva sen vastuulla olevat käsittelytoimet
- GDPR 30 artiklan mukainen velvollisuus laatia seloste käsittelytoimista liittyy osoitusvelvollisuuden toteuttamiseen
  - Rekisterinpitäjän ja henkilötietojen käsittelijän on ylläpidettävä kuvausta sen vastuulla olevista käsittelytoimista voidakseen osoittaa, että ne ovat GDPR:n mukaisia
  - Palveluntarjoaja-käsittelijöiden pidettävä selostetta rekisterinpitäjä-asiakkaidensa lukuun suorittamista henkilötietojen käsittelytoimista (GDPR 30(2) artikla)
  - Tarkoituksena on, että dokumentaation pohjalta saa ajantasaisen kokonaiskuvan organisaation harjoittamasta henkilötietojen käsittelystä
- Hyödyllinen apuväline, joka mahdollistaa
  - 1) henkilötietojen käsittelijän tai rekisterinpitäjän toteuttamien käsittelytoimien ajantasaisen kuvauksen ja riskienhallinnan
  - 2) asianmukaisten suojatoimien tunnistamisen ja implementoinnin henkilötietojen suojaamiseksi

Applex

Seloste käsittelytoimista ja sen sisältö

- Kirjallinen ja sähköinen kuvaus organisaation tekemästä henkilötietojen käsittelystä, joka on pyydettäessä saatettava valvontaviranomaisen saataville
- Selosteen tulee sisältää:
  - rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan *nimi*
  - käsittelyn *tarkoitukset*
  - *kuvaus* rekisteröityjen ryhmistä ja henkilötietoryhmistä
  - henkilötietojen *vastaanottajien ryhmät*, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä olevat vastaanottajat
  - tarvittaessa *tiedot henkilötietojen siirtämisestä* kolmanteen maahan tai kansainväliselle järjestölle
    - Tieto siitä, mikä kolmas maa tai kansainvälinen järjestö on kyseessä, sekä asianmukaisia suojatoimia koskevat asiakirjat, jos kyseessä on 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto;
  - mahdollisuuksien mukaan *eri tietoryhmien poistamisen suunnitellut määräajat*
  - mahdollisuuksien mukaan *yleinen kuvaus* 32 artiklan 1 kohdassa tarkoitetuista *teknisistä ja organisatorisista turvatoimista*

Applex

TSV:n Excel-mallipohja

Tehtävä, johon tietoja käsitellään	Käsittelyn tarkoitus	(Tarvittaessa) yhteisrekisterinpitäjä ja tämän yhteystiedot	Rekisteröityjen ryhmät	Henkilötietojen ryhmät
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Yhteystiedot
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Pankkitiedot
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Eläketiedot
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Verotiedot
HR	Työsuhde	N/A	Työntekijät	Yhteystiedot
HR	Työsuhde	N/A	Työntekijät	Palkkaustiedot

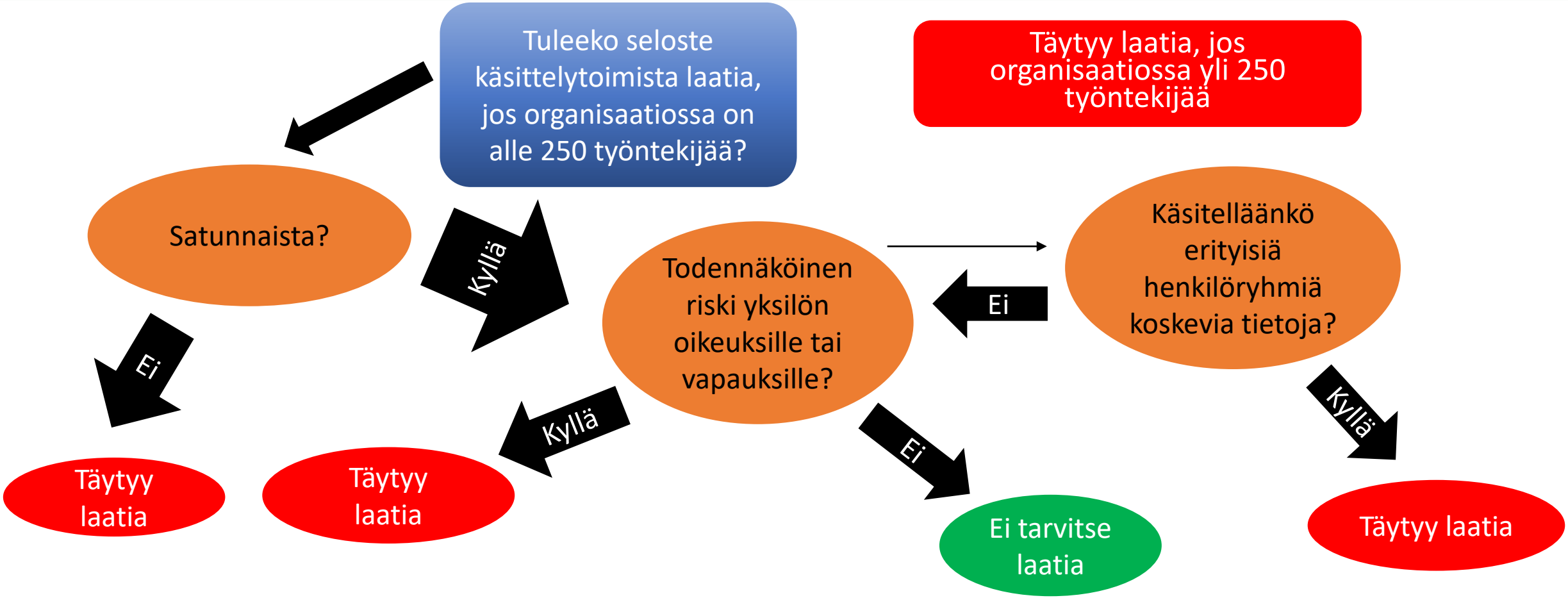
Vastaanottajaryhmät	Viittaus (mahdolliseen) henkilötietojen käsittelijän kanssa solmittuun henkilötietojen käsittelyä koskevaan sopimukseen	Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin	Asianmukaisia suojatoimia koskeva dokumentaatio, jos henkilötietoja siirretään kolmansiin maihin tai kansainvälisiin järjestöihin tietosuoja-asetuksen 49 artiklan 1 kohdan toisessa alakohdassa tarkoitetulla siirrolla	Tietojen säilytysajat, tai sen määrittämisen kriteerit	Kuvaus tietosuoja-aset 1 kohdan mukaisist organisatorisista t
HMRC	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen krypt
HMRC	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen krypt
HMRC	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen krypt
HMRC	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen krypt
N/A	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen krypt
N/A	N/A	N/A	N/A	X vuotta työsuhteen päättymisestä	Tietojen kryptaaminen

Tietosuojavaltuutetun toimisto on julkaissut ohjeen ja Excel-mallipohjan käsittelytoimiselosteesta rekisterinpitäjille ja käsittelijöille: https://tietosuoja.fi/seloste-kasittelytoimista

Milloin seloste käsittelytoimista tulee tehdä?

- Seloste on tehtävä, mikäli…
  - 1) organisaatiossa on yli 250 työntekijää tai
  - 2) työntekijöiden määrästä riippumatta silloin, kun
    - henkilötietojen **käsittely aiheuttaa todennäköisesti riskin** rekisteröidyn oikeuksille ja vapauksille tai
    - henkilötietojen **käsittely ei ole satunnaista** tai
    - käsiteltävät henkilötiedot **sisältävät erityisiä henkilötietoryhmiä tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja**
- Riskiä arvioitaessa huomioitava käsittelyn luonne, asiayhteys, laajuus ja tarkoitukset (perustelukohta 80)
- Rekisterinpitäjän tulisi tehdä henkilötietojen käsittelyyn liittyvä riskianalyysi jo siinä vaiheessa, kun henkilötietojen käsittelyä suunnitellaan. Riskien arviointi on tärkeää, koska rekisterinpitäjään kohdistuvat velvollisuudet kasvavat riskin kasvaessa
- Riskiarvion laatimalla ja sitä ylläpitämällä rekisterinpitäjä voi arvioida toimenpiteiden riittävyyttä

Milloin 30 artikla velvoittaa laatimaan selosteen?



Selosteen laatiminen on kuitenkin aina järkevä toimintatapa → tehokas tietojen hallinta sekä GDPR:n noudattamisen, erityisesti osoitusvelvollisuuden, tehokas toteuttaminen

10 kriteeriä riskien arvioimiseksi

1. Arviointi ja pisteytys (profilointi ja ennustaminen)
2. . Automaattinen päätöksenteko johtaa oikeudellisiin päätöksiin
3. Järjestelmällinen ja laajamittainen valvonta
4. Erityisten henkilötietoryhmien käsittely
5. Laajat käsittelytoimet (tietojen määrä)
6. Yhdistetyt henkilötietokannat
7. Haavoittuvassa asemassa olevat rekisteröidyt
8. Uudet tekniset ja organisatoriset ratkaisut
9. Tiedonsiirrot kolmansiin maihin
10. Käsittely estää rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta

Erityiset henkilötietoryhmät

- Erityisillä henkilötietoryhmillä tarkoitetaan tietoja, joista ilmenee:
  - henkilön rotu tai etninen alkuperä (ei koske kansalaisuutta tai syntymämaata)
  - poliittinen mielipide
  - henkilön kannattamat tai vastustamat ideologiat
  - uskonnollinen tai filosofinen vakaumus
  - ammattiliiton jäsenyys
  - geneettiset tiedot, joista henkilö voidaan yksiselitteisesti tunnistaa
  - henkilötiedot, jotka liittyvät henkilön perittyihin tai hankittuihin ominaisuuksiin, koska ne on saatu kyseisen henkilön biologisesta näytteestä analysoimalla
  - biometriset tiedot, joista henkilö voidaan yksiselitteisesti tunnistaa
  - henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saadut henkilötiedot, joiden perusteella kyseinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa
  - terveyttä koskevat tiedot
  - seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot
- Erityisiin henkilötietoryhmiin kuuluvat tiedot tarvitsevat luonteensa vuoksi erityistä suojausta

Satunnainen käsittely ja todennäköinen riski

- Pienessäkin organisaatiossa todennäköisesti käsitellään säännöllisesti työntekijöitä koskevaa dataa, minkä vuoksi tällaista tietojenkäsittelyä ei voida pitää satunnaisena
  → Tällainen tietojenkäsittely tulee dokumentoida käsittelytoimiselosteessa
- Vakuutusyhtiö, joka työllistää 100 henkilöä, käsittelee säännöllisesti henkilötietoja vahinkotapahtumia, myyntejä ja henkilöstöhallinnollisia asioita käsitellessään
  - Näiden osa-alueiden osalta tapahtuva henkilötietojen käsittely tulee dokumentoida 30 artiklan edellyttämällä tavalla, koska käsittely ei ole satunnaista (vaikka työntekijöitä alle 250)
  - Mikäli tässä yhtiössä tapahtuu ajoittain muunlaista henkilötietojen käsittelyä, esim. tehdään yhtiön sisäinen henkilöstökysely, ei sitä tarvitse dokumentoida osana selostetta

Satunnainen käsittely ja todennäköinen riski

- Jos yhtiö harjoittaa ajoittain asiakastietojen profilointia osana yhtiön riskienhallintaa, tulee sen dokumentoida tällainen toiminta
  - Aiheuttaa *"todennäköisen riskin"* eikä satunnaisuudella ole siten merkitystä
  - Profilointi tuottaa johdettua tietoa yksilöistä, joka voi olla luonteeltaan arkaluontoista
    - → Luo todennäköisen riskin yksilöiden oikeuksille ja vapauksille
- Huomionarvoista on, ettei riskiltä edellytetä erityistä vakavuutta tai suuruutta!
  - → 30 artiklan soveltamiskynnys on siten tältä osin matala
- Rekrytointikampanjoiden yhteydessä kerätyt tiedot sisältävät erityisiin henkilöryhmiin kuuluvaa tietoa → Tietojen käsittelytoimi tulee dokumentoida

Miten 30 artiklan seloste eroaa 13 artiklan informoimisesta/tietosuojaselosteista?

- Rekisterinpitäjän tai henkilötietojen käsittelijän on *pyydettäessä saatettava* seloste käsittelytoimista *valvontaviranomaisen saataville (*GDPR 30(4) artikla*)*
  - ”Peruskuvaus” GDPR:n noudattamisen osoittamiseksi
- Selosteen käsittelytoimista ei siten tarvitse olla julkisesti saatavilla
  - Luonteeltaan organisaation sisäinen ”compliance”-asiakirja
  - Vrt. organisaatioiden nettisivuilla olevat tietosuojaselosteet (GDPR 13 ja 14 artikla)
- Tarkoituksena on, että dokumentaation pohjalta saa ajantasaisen kokonaiskuvan organisaation harjoittamasta henkilötietojen käsittelystä
- Seloste käsittelytoimista voi olla osa laajempaa dokumentaatiota, jolla toteutetaan tietosuoja-asetuksen toimintaperiaatteita → ei tarvitse olla erillinen asiakirja
- Käsittelytoimia koskevaa selostetta ei ole tarkoitettu käytettävän rekisteröidyn informointiin (mutta voi toimia hyvänä pohjana tietosuojaselosteiden laatimiselle!)

Asianajotoimisto Applex Oy

Asianajaja, osakas, CIPP/E Ville Vainio
+358 50 3264454
ville.vainio@applex.fi

Puh. 010 2999 471
info@applex.fi

www.applex.fi