

# Tietosuojaohje Journalistiliiton freelancereille

työehtoasiamies Hannu Hallamaa

# Esimerkki sopimusjärjestelystä: vähittäiskaupan kanta-asiakasjärjestelmät ja data-analytiikka

(Lähde: Peter Leonard/ Gilbert + Tobin, IAPP Global Privacy Summit, Washington DC maaliskuu 2013)

## Customer Data Analytics Contract Architecture



> 23.1.2018

# 1. Yleistä: Mitä on tietosuoja?

- Yksityisyyden suojaamista henkilötietoja käsiteltäessä ja siihen kuuluu jokaisen oikeus omiin henkilötietoihin.
- Luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus. Euroopan unionin perusoikeuskirjan ja Euroopan unionin toiminnasta tehdyn sopimuksen mukaan jokaisella on oikeus henkilötietojensa suojaan.
- 25.5.2018 alkaen voimassa EU:n uusi tietosuoja-asetus.
- Asetuksen rikkomisesta jopa 20 milj. € sakko!

# Tietosuoja-asetus koskee organisaatioita

- Asetuksen piirissä ovat yritykset, julkisorganisaatiot ja yhdistykset - vain tilanne, jossa luonnollinen henkilö käsittelee henkilötietoja yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa on asetuksen ulkopuolella.
- Asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

# Milloin tietosuoja-asetus koskee freelanceria?

Osittain kokonaisuudessaan, esimerkiksi näissä käsittelytilanteissa:

- Tiedot yhteistyökumppaneista (yrityksen tiedot eivät ole henkilötietoja, työntekijöiden tiedot ovat)
- Uutiskirjeet ja muu markkinointi
- Tiedot työntekijöistä
- Omien verkkosivujen avulla kerättävät tiedot

# Rekisteripitäjä ja rekisteröity

- Tietosuoja-asetus tarkoittaa 'rekisterinpitäjällä' luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot
- Tietosuoja-asetus: "'henkilötiedoilla' kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja"
- Suomeksi: Rekisteröity on henkilö, jonka henkilötietoja käsitellään

# Milloin tietosuoja-asetus EI koskee freelanceria?

Kun henkilötietoja käsitellään journalistisiin tarkoituksiin:

- Ei velvoitetta tietojen minimointiin: Journalistiset tarkoitukset edellyttävät tyypillisesti laajoja tietovarantoja
- Rekisteröidyllä ei oikeutta vaatia virheellisen tiedon oikaisemista (“täsmällisyys”)
- Ei velvoitetta “säilytyksen rajoittamiseen”, eli tietoa voi säilöä journalistisiin arkistoihin
- Ei vaatimusta normaalille lainmukaiselle käsittelyperusteelle - myös arkaluonteisia tietoja saa käsitellä!

# Milloin tietosuoja-asetus EI koskee freelanceria?

- Asetuksen artiklat 12-22 ja 34 - journalistisen henkilötietojen käsittelyn kohteella ei ole oikeutta tulla informoiduksi tiedonkäsittelystä eikä vaikuttaa siihen!
- Ei velvoitetta laatia selostetta käsittelytoimista
- Journalisti myös vapautettu vaikutustenarvioinnin tekemisestä ja viranomaisten kuulemisvelvoitteesta (35 ja 36 artikla)
- Valvontaviranomaisella ei oikeutta keskeyttää henkilötietojen käsittelyä



Milloin tietosuoja-asetus kuitenkin koskee freelanceria?

Aina kun kysymys on tietojen turvallisesta käsittelystä:

- Journalistinen poikkeus ei vapauta velvoitteesta huolehtia tietoturvasta ja ilmoittaa tietomurrosta tietosuojaviranomaiselle - rekisteröidylle ei kuitenkaan tarvitse ilmoittaa, mutta viranomainen voi velvoittaa niin tekemään.

# Mitä on asetuksen poikkeuksen suojelema journalismi?

- Tietosuojavaltuutetun toimistossa on vuosien 2008-2017 aikana ollut vireillä noin 200 asiaa, jotka ovat koskeneet sananvapauden ilmaisun ja henkilötietojen suojan yhteensovittamista. Viime vuosina merkittävä osa kansalaisten tekemistä kanteluista edellä mainituissa asioissa on liittynyt henkilötietojen julkaisemiseen verkossa ja erilaisissa joukkoviestintävälineissä.

# Mitä on poikkeuksen suojelema journalismi?

- Osa käsiteltävistä asioista on tullut vireille, koska tietosuojavaltuutettu on katsonut, ettei kyseinen henkilötietojen käsittely kuulu henkilötietolain 2 §:n 5 momentin soveltamisalarajauksen piiriin. Tästä esimerkkinä verotustietojen julkaisemiseen liittyvä niin kutsuttu Veropörssi-asia (KHO 2009:82), josta korkein hallinto-oikeus pyysi vuonna 2007 ennakkoratkaisua unionin tuomioistuimelta.

# Mitä on poikkeuksen suojelema journalismi?

- Korkein hallinto-oikeus totesi unionin tuomioistuimen antaman ennakkoratkaisun C-73/07 -perusteella antamassaan ratkaisussa KHO 2009:82 sananvapauden ja henkilötietojen yhteensovittamisen osalta, että henkilötietolain 2 §:n 5 momentin soveltamisalan rajauksen arvioinnin lähtökohtana on se, onko kyseisen toiminnan tarkoituksena tietojen, mielipiteiden ja ajatusten ilmaiseminen yleisölle.

# Mitä on poikkeuksen suojelema journalismi?

- Arvioinnissa on huomioitava, missä määrin toiminta edistää yhteiskunnallisesti kiinnostavaa keskustelua pikemmin kuin pyrkiä keskustelusta irrallaan tyydyttämään yksittäisten henkilöiden uteliaisuutta.
- Henkilötietojen käsittelynä toimituksellista tarkoitusta varten ei kuitenkaan voida pitää tietojen sellaista käsittelyä, jossa toimituksellisessa tarkoituksessa muodostettu henkilörekisteri laajamittaisesti, lähes kokonaisuudessaan ja lähes sellaisenaan, vaikkakin eri osissa ja kunnittain, julkaistaan erillisinä luetteloina.

# Mitä on poikkeuksen suojelema journalismi?

- Koska rekisteröityjen tietojen julkaiseminen tässä laajuudessa rinnastui koko asianomaisen yhtiön toimituksellisessa tarkoituksessa keräämän niin sanotun taustarekisterin julkaisemiseen, kysymys ei ollut pelkästään tietojen, mielipiteiden tai ajatusten ilmaisemisesta.

# Mitä on poikkeuksen suojelema journalismi?

- Demokraattisessa yhteiskunnassa välttämätön, avoin ja yhteiskunnallisesti kiinnostava keskustelu taikka yhteiskunnallisen vallankäytön kontrolli ja arvostelun vapaus eivät edellytä yksittäisiä henkilöitä ratkaisusta ilmenevin tavoin yksilöityjen henkilötietojen julkaisemista siinä laajuudessa. Euroopan ihmisoikeustuomioistuimen suuri jaosto antoi asiassa ratkaisunsa 27.6.2017.

# Mitä on poikkeuksen suojelema journalismi?

- Oikeuskäytännössä on painotettu, että henkilötietojen käsittelyä koskevat poikkeukset koskevat joukkotiedotusyritysten lisäksi kaikkia journalismia harjoittavia henkilöitä.
- Journalismi määritelty hyvin laajasti - käytännössä raja menee juuri Veropörssin tavassa yksinkertaisesti julkaista koko rekisteri sellaisenaan.



## Rekisteröidyt



Parempaa viestintää  
- käsittelystä  
- loukkauksista



Siirto-  
oikeus



Oikeus tulla  
unohdetuksi

Profiloinnin  
kieltäminen

Lapsen henkilötietojen käsittelyn  
rajottaminen

## Rekisterinpitäjät / Käsittelijät



Yhdenmukaiset velvoitteet koko EU:ssa

Riskilähtöisyys

Yhdenmukaisuusmekanismi

'One-stop-shop'

Sakot



Sertifiointimekanismit



Tietosuojavastaava

## 2. Mitä on henkilötietojen käsittely?

- Henkilötietojen käsittelylle pitää aina olla laillinen peruste.
- Käsittelyä ovat kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä on esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

# Mikä on laillinen käsittelyperuste?

- Suostumus
- Sopimus
- Oikeutettu etu
- Lakisääteinen velvoite

# Suostumus

- Rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa tarkoitusta varten. Rekisterinpitäjän tulee dokumentoida saatu suostumus, koska se pitää pystyä todentamaan. Suostumus tulee antaa tarkoituksellisesti, eli sitä ei voi antaa vaikenemalla, valmiiksi rastitetulla ruudulla tai jättämällä jotakin tekemättä.

# Sopimus

- Henkilötietojen käsittely on lainmukaista, kun se on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena. Henkilötiedon käsittely sopimuksen täytäntöön panemiseksi tarkoittaa käytännössä esimerkiksi myyjälle annetun osoitteen käyttämistä, jotta tuote voidaan toimittaa rekisteröidylle.
- Suostumus voi täydentää sopimusta, sopimus tulla suostumuksen rinnalle - eivät sulje toisiaan pois

# Oikeutettu etu

- Henkilötietojen käsittelyn perusteena voi olla oikeutettu etu. Tämä tarkoittaa sitä, että rekisterinpitäjän ja rekisteröidyn välillä on asianmukainen ja merkityksellinen suhde, kuten jäsenyys, asiakkuus tai työsuhde.

# Lakisääteinen velvoite

- Henkilötietojen käsittely on sallittua, kun se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.

# Rekisteröidyn oikeudet

1. Saada läpinäkyvästi tietoa henkilötietojen käsittelystä
2. Saada pääsy omiin tietoihin
3. Tietojen oikaiseminen
4. Tulla unohdetuksi, eli tietojen poistaminen
5. Siirtää tiedot järjestelmästä toiseen
6. Rajoittaa tietojen käsittelyä



# Oikeus saada tietoa henkilötietojen käsittelystä

Rekisteröidyllä on aina oikeus saada tietää, käsitteleeö organisaatio hänen tietojaan. Tämä kattaa oikeuden saada tietoonsa hänestä tallennetut henkilötiedot sekä saada seuraavat tiedot:

- Käsiteltävät henkilötietoryhmät.
- Vastaanottajat tai vastaanottajaryhmät, joille yritys on luovuttanut henkilötietoja tai joille tietoja on tarkoitus luovuttaa.
- Mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos säilytysaikaa ei voi ilmoittaa, tämän ajan määrittämiskriteerit.
- Kaikki tietojen alkuperästä käytettävissä olevat tiedot, jos henkilötietoja ei kerätä rekisteröidyltä.

# Oikeus tietoon henkilötietojen käsittelystä

- Ilmoitus henkilötiedon siirtoa EU:n ulkopuolelle koskevista asianmukaisista toimista.
- Automaattisen päätöksenteon (mukaan lukien profiloinnin) olemassaolo, keskeiset tiedot tietojen käsittelyyn liittyvästä logiikasta sekä käsittelyn merkittävydestä ja mahdollisista seurauksista rekisteröidyille.

Rekisteröidylle tulee myös kertoa, että hänellä on oikeus

- Pyytää rekisterinpitäjältä häntä koskevien henkilötietojen oikaisemista, poistamista tai henkilötietojen käsittelyn rajoittamista.
- Tehdä valitus valvontaviranomaiselle.

# Oikeus tietojen oikaisemiseen

- Rekisteröidyllä on oikeus vaatia, että organisaatio oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.
- Rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys.
- Organisaation tulisi pystyä muokkaamaan rekisterinsä tietoja jälkikäteen, jotta epätarkat tai virheelliset tiedot voidaan korjata

# Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada yritys poistamaan häntä koskevat tiedot eli oikeus tulla unohdetuksi seuraavissa tilanteissa:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin. (jos tietoja ei enää tarvita muun lainsäädännön tai edun nojalla).

# Oikeus tulla unohdetuksi

- Henkilötietojen käsittely perustuu suostumukseen ja rekisteröity peruuttaa antamansa suostumuksen.
- Rekisteröity vastustaa perustelluisti käsittelyä.
- Henkilötietoja on käsitelty lainvastaisesti.
- Henkilötiedot on poistettava lakisääteisen velvoitteen noudattamiseksi.
- Henkilötiedot on kerätty tarjottaessa sähköisiä palveluja suoraan lapselle.

Organisaatiolla voi olla oikeutettu etu henkilötietojen käsittelyyn, jolloin tietoja ei tarvitse poistaa.

# Oikeus siirtää tiedot järjestelmästä toiseen

- Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä yleisesti käytetyssä ja koneellisesti luettavassa muodossa.
- Hänellä on oikeus siirtää kyseiset tiedot toiselle yritykselle tai rekisterinpitäjälle, jos tietojen käsittely perustuu suostumukseen tai sopimukseen ja tietoja käsitellään automaattisesti eli jonkinlaisella ohjelmalla

# Oikeus siirtää tiedot järjestelmästä toiseen

- Jos yritys käsittelee henkilötietoja suostumuksen tai sopimuksen perusteella, tulisi sen päivittää tietojärjestelmänsä sellaisiksi, että niistä voidaan siirtää tietoa toiselle yritykselle. Tämä koskee vain sähköistä tietoa; paperilla olevia tietoja ei tarvitse luovuttaa siirto-oikeuden perusteella.
- Jos tietojen käsittely ei perustu suostumukseen tai sopimukseen, ei rekisteröidyllä ole oikeutta siirtää henkilötietoja järjestelmästä toiseen.

# Oikeus siirtää tiedot järjestelmästä toiseen

- Esimerkiksi työntekijöiden tietoja käsitellään sekä sopimuksen että yrityksen oikeutettujen etujen perusteella. Tällöin siirto-oikeus on olemassa vain sopimukseen liittyvissä tiedoissa, kuten palkkatiedoissa.
- On huomioitava, että siirto-oikeuden kohteena voivat olla vain tiedot, jotka rekisteröity on toimittanut yritykselle.



# Oikeus rajoittaa tietojen käsittelyä

Rekisteröidyllä on oikeus vaatia, että organisaatio rajoittaa hänen tietojensa käsittelyä, kun

- Käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista
- Rekisterinpitäjä ei enää tarvitse henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi

# Oikeus rajoittaa tietojen käsittelyä

- Rekisteröidyn ja organisaation välillä on erimielisyys siitä, syrjäyttävätkö organisaation henkilötietojen käsittelyn oikeutetut perusteet rekisteröidyn vaatimukset, ja odotettaessa asian todentamista rekisteröity on vastustanut henkilötietojen käsittelyä.

Jos käsittelyä on rajoitettu jollain edellä mainitulla perusteella, saa käsittelyä tehdä ainoastaan rekisteröidyn suostumuksella, oikeudellisen vaateen laatimiseksi tai toisen henkilön oikeuksien suojaamiseksi.

# Oikeus vastustaa käsittelyä

- Rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä silloin, kun hän on antanut suostumuksensa tietojen käsittelylle.
- Rekisteröidyllä on oikeus myös milloin tahansa vastustaa sellaista häntä koskevien henkilötietojen käsittelyä, joka perustuu organisaation oikeutettuun etuun tai profilointiin.

# Oikeus vastustaa käsittelyä

- Rekisterinpitäjä ei kiellon jälkeen saa enää käsitellä henkilötietoja.
- Poikkeus: Jos käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut tai jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Oikeusvaade tarkoittaa esimerkiksi kannetta käräjäoikeudessa.

# Oikeus vastustaa käsittelyä

- Perusteltuna syynä voidaan pitää myös työnantajan lakisääteistä velvollisuutta käsitellä työntekijän tietoja. Tällöin tietojen käsittelyä ei voida lopettaa, vaikka työntekijä sitä vastustaisikin.
- Rekisteröidyillä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä suoramarkkinointia varten – mukaan lukien profilointi silloin kun se liittyy suoramarkkinointiin.

# Oikeus vastustaa automatisoituja päätöksiä

- Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn (kuten profilointiin), jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.
- Esim. online-luottohakemuksen automaattinen epääminen tai sähköisen rekrytoinnin käytännöt ilman, että kukaan ihminen osallistuu päätöksentekoon.

# Suoramarkkinoinnista

- Suoramarkkinointia saa harjoittaa jatkossakin, jos vastaanottajille kerrotaan mahdollisuudesta kieltää suoramarkkinointi.
- Sähköisen suoramarkkinoinnin lähettämiseen henkilölle tulee saada suostumus ennalta. Yritykselle lähetettävään mainontaan ei tarvita suostumusta.
- Oikeusperusteena henkilötietojen käsittelyyn suoramarkkinointi varten oikeutettu etu

### 3. Tieto henkilötietojen käsittelystä pitää olla rekisteröityjen saatavilla (informointivelvoite)

- Henkilötietojen käsittelyn tulee olla läpinäkyvää, ja rekisteröidyille tulee kertoa, kuinka heitä koskevia tietoja kerätään ja kuinka niitä käytetään. Tiedot tulisi antaa tiiviisti, yksinkertaisella ja selkeällä kielellä.
- Laatikaa omista rekistereistänne tällaiset tietosuojaselosteet! Liitto toimittaa pohjat!



# Tietosuojaselosteet

Kun rekisteröidyltä kerätään henkilötietoja, rekisterinpitäjän on täytettävä informointivelvoite toimittamalla rekisteröidylle kaikki seuraavat tiedot:

- Peruste eli syy, jonka perusteella henkilötietoja saa käsitellä
- Henkilötietojen käsittelyn tarkoitukset
- Henkilötietojen vastaanottajat tai vastaanottajaryhmät

# Tietosuojaselosteet

- Oikeus peruuttaa suostumus milloin tahansa ilman, että se vaikuttaa suostumuksen perusteella ja ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen
- Onko henkilötietojen antaminen lakisääteinen, sopimukseen perustuva tai sopimuksen tekemisen edellyttämä vaatimus
- Onko rekisteröidyn pakko toimittaa henkilötiedot ja mitä tällaisten tietojen antamatta jättämisestä mahdollisesti seura

# Tietosuojaselosteet

- Automaattisen päätöksenteon eli profiloinnin olemassaolo, merkitykselliset tiedot käsittelyyn liittyvästä logiikasta sekä käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.
- Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle ennen kyseistä jatkokäsittelyä ja annettava asiaan kuuluvat lisätiedot.

# Informointivelvoite kun tietoja ei ole saatu rekisteröidyltä

Rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot viimeistään kuukauden kuluessa henkilötietojen saamisesta tai kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran:

- Mahdollisen tietosuojavastaavan yhteystiedot
- Henkilötietojen käsittelyn tarkoitukset sekä oikeusperuste
- Rekisterissä olevat henkilötietoryhmät
- Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit

# Informointivelvoite kun tietoja ei ole saatu rekisteröidyltä

- Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut
- Oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin
- Oikeus pyytää tietojen oikaisemista tai poistamista tai käsittelyn rajoittamista, oikeus vastustaa käsittelyä
- Oikeus siirtää tiedot järjestelmästä toiseen
- Oikeus tehdä valitus valvontaviranomaiselle
- Mistä henkilötiedot on saatu sekä onko tiedot saatu yleisesti saatavilla olevista lähteistä

# Muista käsittelyn turvallisuus

- Rekisterinpitäjän ja henkilötietojen käsittelijän on asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä varmistettava, esim. pseudonymisointi ja salaaminen, että käsittelyn turvallisuustaso vastaa riskiä.
- Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että jokainen, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

# Tietoturvaloukkaukset

- Tietoturvaloukkauksella tarkoitetaan sellaista tapahtumaa, jonka seurauksena siirrettyjä, tallennettuja tai muuten käsiteltyjä henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää tai muuttuu.
- Myös tietojen luvaton luovuttaminen sekä luvaton pääsy tietoihin on ko. loukkaus.
- Rekisterinpitäjän on ilmoitettava henkilötietojen tietosuojaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle.

# Tietoturvaloukkaukset

- Kun henkilötietojen käsittelijä saa tietää henkilötietojen tietoturvaloukkauksesta, hänen on ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä. Ilmoituksessa on kuvattava tietoturvaloukkaus, mahdollisuuksien mukaan rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietoryhmät ja määrät.
- Kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset



# Tietoturvaloukkaukset

- Kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta
- Kerrottava, miten haittavaikutuksia lievennetään.
- Rekisterinpitäjän on dokumentoitava henkilötietojen tietoturvaloukkaukset, niiden vaikutukset sekä korjaavat toimet. Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa asia.

# Tietoturvaloukkauksesta ilmoitus rekisteröidylle

- Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin henkilöille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.
- Rekisteröidylle annettavassa ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne.
- Samalla on ilmoitettava ainakin tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa.

# Mitä henkilötiedot ovat?



## KERÄÄTKÖ TALLENNATKO KÄYTÄTKÖ HENKILÖTIETOJA?

Sinun on noudatettava sääntöjä.

**Käsitletkö tietoja** toisten  
yritysten puolesta?

Tämä koskee myös sinua.

# Muistilista 1/2

- Käy läpi organisaatiosi tietosuojakäytännöt
- Inventoi organisaatiosi keräämät henkilötiedot: Miksi ne on kerätty? Tarvitaanko tietoja? Säilytetäänkö niitä turvallisesti?
- Päivitä tietosuojaselosteesi
- Varmista kykysi toteuttaa rekisteröityjen oikeudet
- Suunnittele miten toteutat henkilötietojen tarkastuspyynnöt
- Valmistaudu kertomaan tietomurrosta rekisteröidyille ja viranomaisille

## Muistilista 2/2

- Selvitä millä perusteella kulloinkin käsittelet henkilötietoja - lainmukainen peruste pitää löytyä!
- Varmista, että hankit suostumuksen tietojen käsittelyyn asetuksen vaatimusten mukaisesti
- Varmista kykysi raportoida tietovuodoista tietosuojaviranomaiselle
- Dokumentoi, miten rekisteröityjä on informoitu käsittelystä
- Dokumentoi tietojenkäsittelyn turvallisuus
- Laadi salassapitosopimukset henkilökunnan kanssa



Viestintä

- Käytä selkeää kieltä.
- Kerro **kuinka** olet, kun pyydät tietoja.
- Kerro **mitkä** käsitteet heidän tietojaan, **kuinka** kauan niitä säilytetään ja **kenelle** ne luovutetaan.



Varoitus

Tiedota ihmisille tietoturvaloukkauksista, jos heihin kohdistuu vakava uhka.



Suostumus

Pyydä ihmisiltä selkeä suostumus tietojen käsitteelyyn.

Keräätkö tietoja lapsilta sosiaalista mediaa varten? Tarkista ikäraja, joka määrittää, tarvitaanko vanhemman suostumus.



Tarkastelu ja siirto

Anna ihmisille mahdollisuus tarkastella tietojaan ja siirtää ne toiselle yritykselle.



Arkaluonteisten tietojen turvaaminen

Toteuta ylimääräisiä suojatoimia terveyttä, rotua, sukupuolista suuntautunutta, uskontoa ja poliittisia näkemyksiä koskevien tietojen turvaamiseksi.

## Tietosuoja Euroopassa digitaaliajalla



### Parempaa henkilötietojen suojaa



### Enemmän liiketoimintamahdollisuuksia



### Johdonmukaisempi soveltaminen ja tehokas täytäntöönpano

- Yksityshenkilöt ja yritykset voivat saada asiansa käsiteltyä heitä lähellä olevassa tietosuojaviranomaisessa ja tuomioistuimissa
- Keskittetty asiantunteita yksilöille ja yrityksille rajat yltävissä tilanteissa kansallisten tietosuojaviranomaisten yhteistyön ansiosta

Sakot

€ jopa 20 milj. €

TAI

4% vuotuisesta kokonaistulokvahdosta



Euroopan unionin neuvosto  
Pääsihteeri

© Euroopan unioni, 2015.  
Tiedote valmistettu EU:n Eurostatin avulla.

# Vinkkejä ja lisätietoa:

■ Tietosuoja-valtuutetun toimiston sivut: [www.tietosuoja.fi](http://www.tietosuoja.fi)

■ Miten valmistautua EU:n tietosuoja-asetukseen – opas:

[http://www.tietosuoja.fi/material/attachments/tietosuoja-valtuutettu/tietosuoja-valtuutetun-toimisto/opaat/1Em8rT7IF/Miten\\_valmistautua\\_EUn\\_tietosuoja-asetukseen.pdf](http://www.tietosuoja.fi/material/attachments/tietosuoja-valtuutettu/tietosuoja-valtuutetun-toimisto/opaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf)

■ Julkishallinnolle suunnattu Arjen tietosuoja – hanke:

<http://tietosuoja.vahtiohje.fi/fi/#/front>

■ <http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit>

■ Vahti-tietoturvaohje:

[https://www.vahtiohje.fi/c/document\\_library/get\\_file?uuid=c338d07d-ac04-4884-b941-1554d07ae41f&groupId=10229](https://www.vahtiohje.fi/c/document_library/get_file?uuid=c338d07d-ac04-4884-b941-1554d07ae41f&groupId=10229)