

EU:n tietosuoja-asetus ja käytännön toimet

Aamukahvikoulutus, 16.1.2018

OTM, FM Kimmo Kajander



LUKANDER RUOHOLA HTO

ASIANAJOTOIMISTO • ADVOKATBYRÄ • ATTORNEYS AT LAW

Vuodesta 1994

Liikejuridiikkaa

30 asiantuntijaa

Henkilökohtaisesti

Pienistä Suuriin

Toimialatuntemus
ja kansainvälisyys

Helsingissä, Turussa,
Salossa ja Kuopiossa

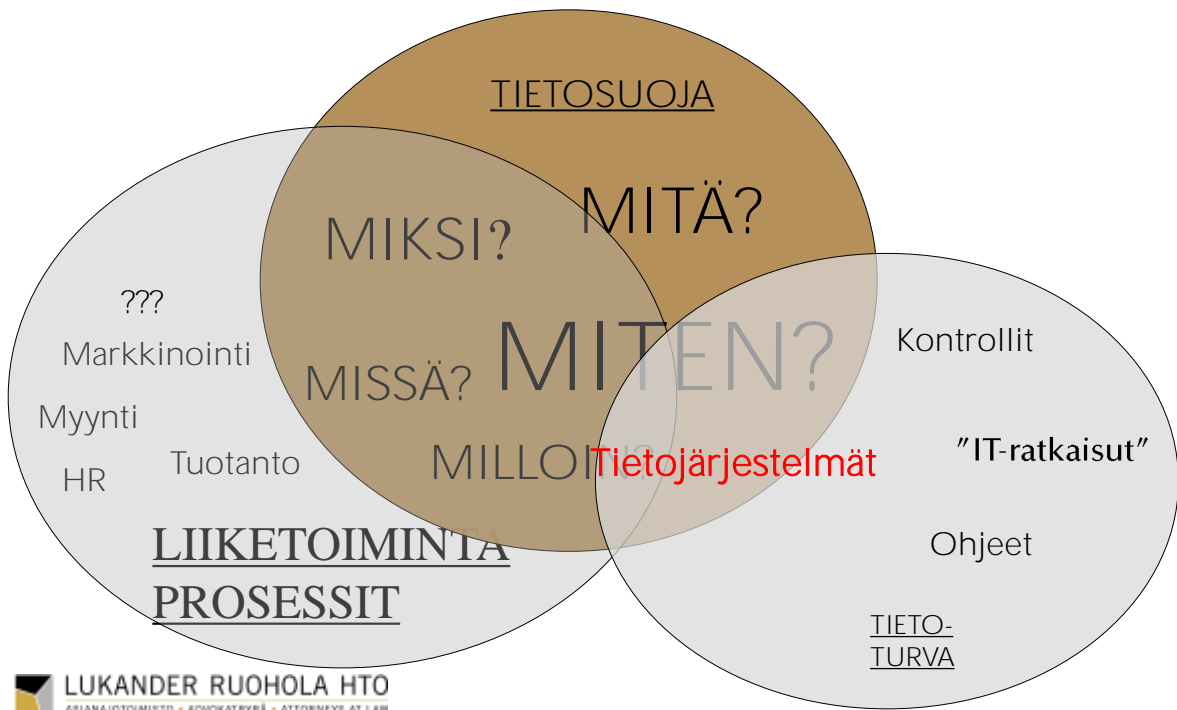
LUKANDER RUOHOLA HTO

ASIANAJOTOIMISTO • ADVOKATBYRÄ • ATTORNEYS AT LAW

EU:n tietosuoja-asetus ja käytännön toimet

- Tietosuoja-asetus hyvin lyhyesti ja mikä muuttuu?
- Sopimukset, HR, markkinointi ja järjestelmät
- Käytännön toimet organisaatiossa

Tietosuoja-asetus hyvin lyhyesti ja mikä muuttuu?



Tietosuoja

- Tietosuoja siis tarkoittaa ihmisten oikeutta omiin tietoihinsa
- Henkilötietoja ovat kaikki sellaiset tiedot, jotka voidaan yhdistää henkilöön tai tämän perheeseen
- Tietosuoja-lainsäädäntö määrittelee mitä henkilötietoa saa kerätä sekä miten saa käsitellä sekä kenelle sen saa näyttää
- Vakiintunut jako tietoturvaan (*information security*) ja tietosuojaan (*data protection*)
- **Tietosuoja ≠ Tietoturva**
 - Saatavuus tai käytettävyys (engl. *availability*)
 - Luottamuksellisuus (engl. *confidentiality*)
 - Eheys (engl. *integrity*)

Vrt. *Kiistämättömyys* tai *rehellisyys* tai *aitous*

Tietosuoja lainsäädännössä

• [Perustuslaki \(ja EU:n perusoikeuskirja\)](#)

• [Henkilötietolaki \(kumotaan\)](#) on henkilötietojen käsittelyn yleislaki. Lain säännöksiä sovelletaan kaikkeen henkilötietojen käsittelyyn, ellei muissa laeissa ole vastaavia erityissäännöksiä. Henkilötietolailla on myös saatettu voimaan Euroopan Unionin henkilötietodirektiivi.

• [Lakia viranomaisten toiminnan julkisuudesta](#) sovelletaan henkilötietojen luovuttamiseen viranomaisen henkilökäsitteistä

• [Laki yksityisyyden suojasta työelämässä](#) on koottu keskeisimmät työelämän tietosuojakäsitteet

• [Tietoyhteiskuntakaari](#) turvaa viestinnän luottamuksellisuutta ja yksityisyyden suojaa sähköisessä viestinnässä

• [Euroopan unionin antamia tietosuojaä koskevia kansainvälisiä normeja ja ohjeita](#)

• [Eri lainsäädännössä viittauksia ja täsmennyksiä tietosuojaan liittyen](#)

• **TULOSSA: Tietosuoja-asetus ja uusia direktiivejä (2018)**



7

EU:n Tietosuoja-asetus

- Velvoitteet voimaan **25.5.2018** alkaen, asetus annettu huhtikuussa 2016
- EU:n kattava ja yhteinen tietosuoja-laki
- Perustuu paljolti nykyiseen tietosuojadirektiiviin
- Muuttaa Suomessa lainsäädäntöä ja osin virkamieskoneistoa
- Koskee EU-kansalaisten tietoja käsitteleviä, myös ulkomaisia toimijoita
- Pääpaino on *lisätä velvoitteita ja ennakoisvelvollisuutta* lisäämällä sanktioita ja keskittämällä valtaa
- Helpottaa toimintaa EU-alueella, luo uusia mahdollisuuksia?
- **OSOITUSVELVOLLISUUS ja SISÄÄNRAKENNETTU TIETOSUOJA**



8

Keskeiset termit

Henkilötieto (art. 4)

- **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

Henkilörekisteri (art. 4)

- mitä tahansa **jäsenneltyä henkilötietoja sisältävää tietojoukkoa**, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, **hajautettu** tai toiminnallinen tai maantieteellisin perustein jaettu,

Käsittely (art. 4)

- **toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin** joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakuja, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista,

Keskeiset termit

Rekisterinpitäjä (art. 4)

- **luonnollista henkilöä tai oikeushenkilöä**, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa **määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot**

Henkilötietojen käsittelijä (art. 4)

- **luonnollista henkilöä tai oikeushenkilöä**, viranomaista, virastoa tai muuta elintä, joka **käsittelee henkilötietoja rekisterinpitäjän lukuun**

Periaatteet ja lainmukaisuus

Käsittelyä koskevat periaatteet (art. 5)

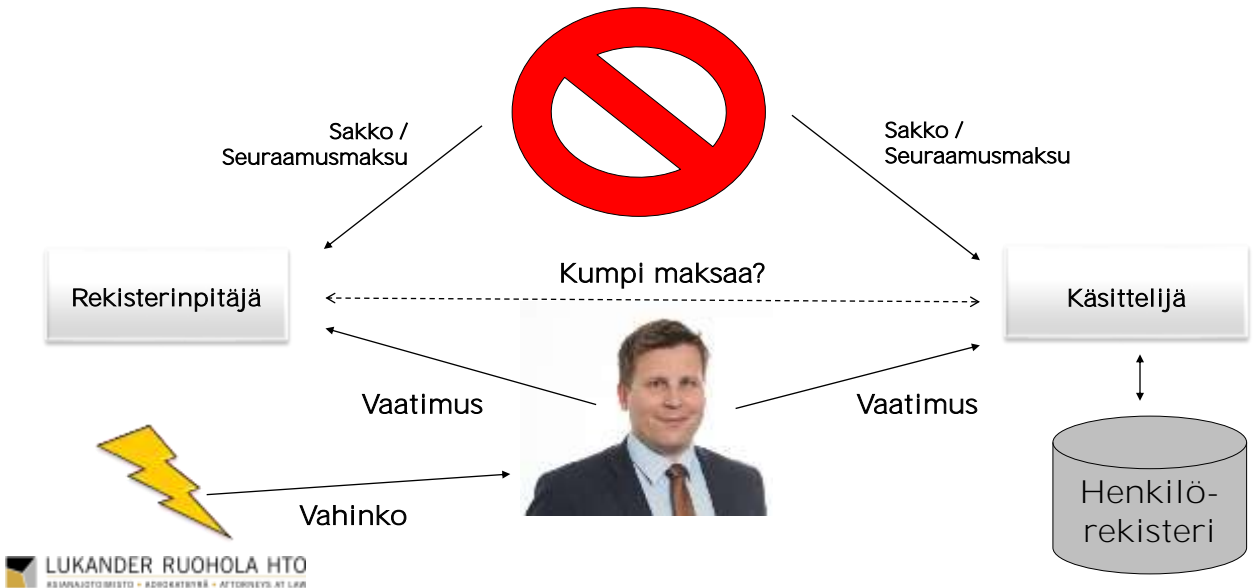
- Kohtuullisuus, **lainmukaisuus** ja läpinäkyvyys lainmukaisuus,
- **käyttötarkoituksidonnaisuus**
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- **OSOITUSVELVOLLISUUS**

Käsittelyn *lainmukaisuus* (art. 6)

- Sopimuksen täytäntöönpano
- **Suostumus**
- Lakisääteinen velvoite
- Elintärkeiden etujen suojele
- Yleinen etu tai julkinen tehtävä
- Rekisterinpitäjän tai kolmannen oikeutettu etu

Sopimukset, HR, markkinointi ja järjestelmät

Vaikutukset sopimukseen?



Vastuun jakautuminen

- Keskeistä tietoa käsittelevien osapuolten välillä
 - Käsittelyn oikeuttamisperuste + käsittelyn turvallisuus
 - Rekisterinpitäjän antamat dokumentoidut ohjeet
- Sovittava vastuista ja reagointivielteistä
 - Art. 82: pelkkä sopimus alihankkijan/käsittelijän kanssa ei vapauta yhteisvastuusta ulkopuolisiin nähden
- Art. 82 mukaan käsittelijä vastuussa, jos ei ole noudattanut rekisterinpitäjän ohjeita tai lain säännöksiä
- Rekisterinpitäjä tai käsittelijä vastuusta vapaa omalta osaltaan, jos osoittaa, ettei millään tavoin ole vastuussa vahingon aiheuttaneesta tapahtumasta

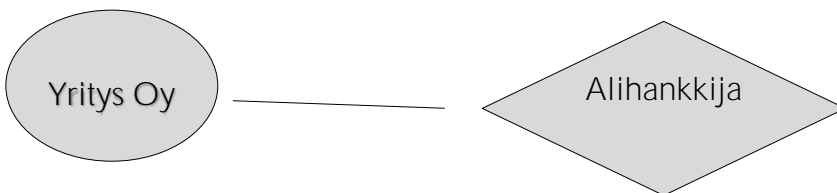
Esimerkki

”Itse kun tekee saa juuri sellaisen kuin tulee...”



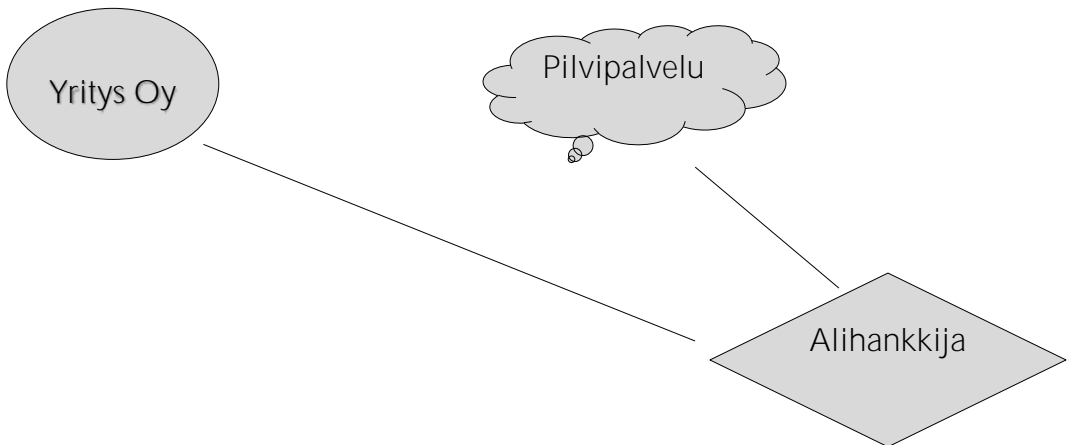
Esimerkki

”Alihankintasuhde luo aina roolijaon rekisterinpitäjään ja henkilötiedon käsitteijään”



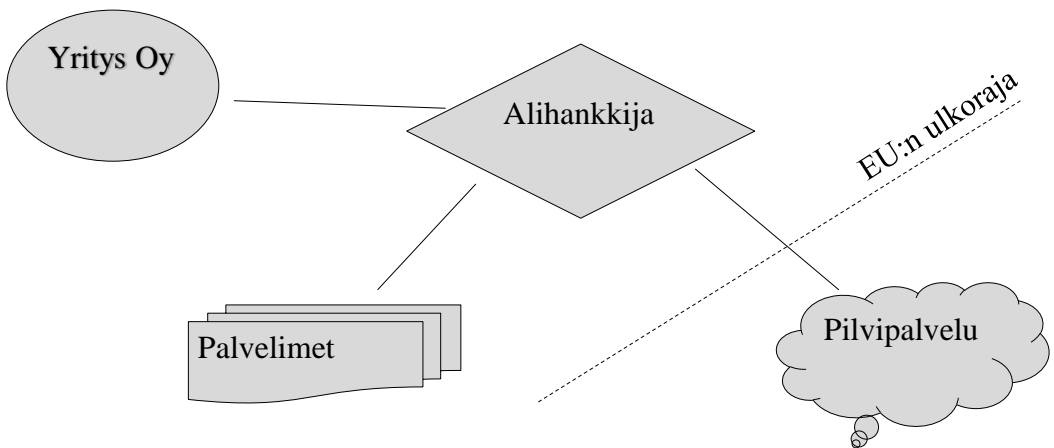
Esimerkki

”Käytätkö sinä tai alihankkijasi pilvipalvelua alihankintaketjun jatkeena?”



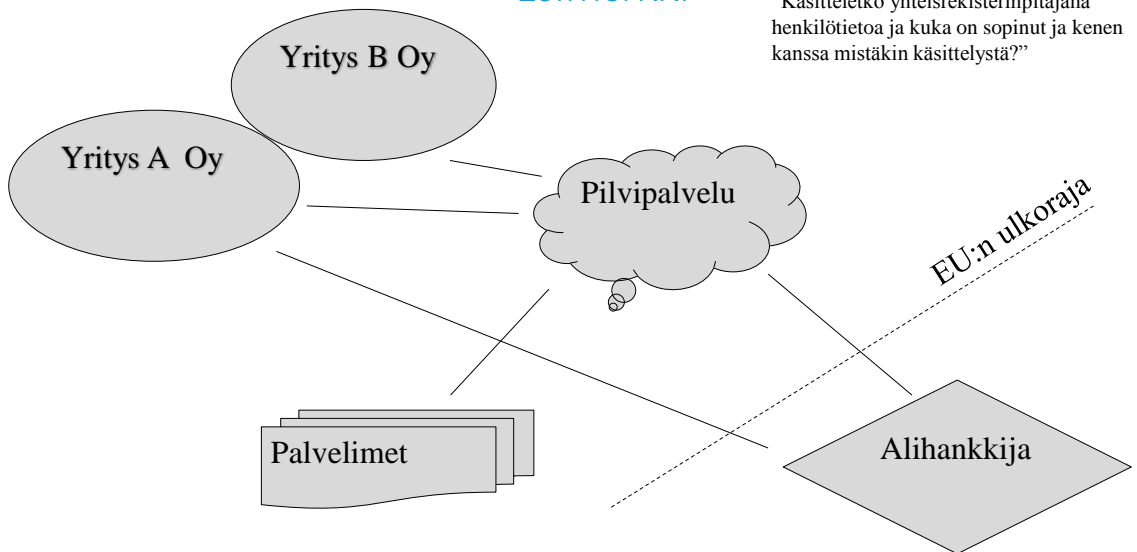
Esimerkki

”Tietosuoja-asetus edellyttää, että EU-kansalaisten henkilötietoja voidaan siirtää kolmansiin maihin vain, jos nämä maat takaavat riittävän tietosuojan tason”



Esimerkki

”Käsitteletkö yhteisrekisterinpitäjänä henkilötietoa ja kuka on sopinut ja kenen kanssa mistäkin käsittelystä?”



Vaikutukset sopimukseen?

Tietosuojasta sopiminen 1/2

- Tunnista sopimuksen henkilötietouloottuvuus
- Kuka huolehtii tietosuojasta
 - Käsitteilyn oikeuttamisperuste + käsittelyn turvallisuus
- Tunne ja varmista koko toimitusketju
- Sovi vahingonkorvausvastuista ja eri vahinkotyypeistä
- **Alihankintaan tarvitaan aina rekisterinpitäjän kirjallinen ennakkolupa!**
- Pelkkä (sopimus)paperi ei suojele
 - ”Köyhällä ei ole varaa puolustautua tai maksaa”
 - pelkkä sopiminen ei vapauta vastuusta ulkopuolisiin nähden
 - » **OSOITUSVELVOLLISUUS**

Vaikutukset sopimukseen?

Tietosuojasta sopiminen 2/2

- Tietosuojaosio/Iilite, jossa sovitaan esim.
 - Artiklaan 28 mukaiset asiat
 - Määritelmät ja lainsäädännön noudattaminen
 - Tietoturva & tietoturvuotoihin reagointi
 - IT- ja muut tietojenkäsittelysäännöt
 - Rekisteröityjen ihmisten oikeudet
 - Henkilötiedon käsittely: Tiedon omistajuus, anonymisointi, pseudonymisointi, poistaminen, luovutukset, siirtäminen, alihankkijat, arvioinnit ja auditoinnit
 - Vahingonkorvausmääritelmät ja vastuut jos ei muualla sovittu

Henkilöstöhallinto

- Työsuhteen aikana
 - Laki tietosuojasta työelämässä
 - Työnantaja saa käsitellä ainoastaan työsuhteen kannalta välttämättömiä henkilötietoja
- Rekrytointi
 - **Tarkoitussidonnaisuus!!!**
 - Tietojen säilytysaika?
 - "Googlaus"
 - Tavallaan Ok, mutta muista yhdenvertaisuus ja...
 - "Työantajan tai tämän edustajan tulee kerätä tiedot ensisijaisesti työntekijältä tai työnhakijalta itseltään, muiden tietojen suhteen tarvitaan suostumus" (Laki yksityisyyden suojasta työelämässä 4§)
- Työsuhteen päättymisen jälkeen
 - 24kk kanneaika
 - 10v Työtodistus
 - 50v palkkatiedot?!?

Esimerkki

Henkilöstötutkimus

Sairaspoissaolot

Henkilöstöluettelo

Palkkakirjanpito

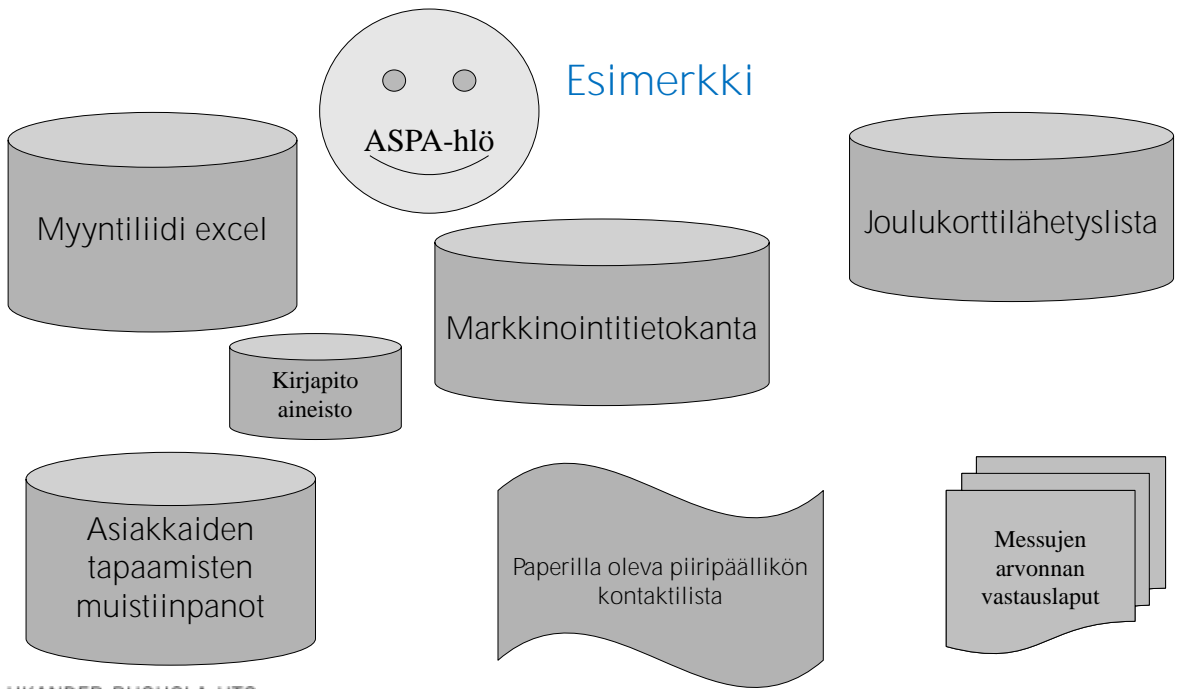


Pikkujoulujen ilmoittautumislista

Markkinointi

- Asiakasrekisteri on eri asia kuin markkinointirekisteri
 - Usein selvä ero, joskus veteen piirretty viiva
- Suoramarkkinointirekisterin pitäminen on sallittua, mutta henkilöllä oikeus pyytää itseään poistettavaksi
- Eri säännöt B2B ja B2C markkinoinnissa
- Suoramarkkinointi sisänsä sallittua, mutta
 - Sähköinen suoramarkkinointi
 - EI ilman kuluttajan lupaa
 - EIKÄ jos yritys on kieltänyt
- Entä evästeet eli ns. cookies?
 - Tulossa uusi asetus täsmentämään...

Esimerkki



Tietojärjestelmät

Tietosuoja ja Tietojärjestelmät

- Liiketoimintaprosessit toimivat tietojärjestelmien varassa
- Tietojärjestelmiä ei ole kuitenkaan suunniteltu tietosuojan näkökulmasta
- ”rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta.” (a24)
- Nykytietojärjestelmät ≠ oletusarvoinen ja sisäänrakennettu tietosuoja (a25)
- Tietosuoja-asetus tulee asettamaan huomattavia haasteita vanhoille ympäristöille

Tietojärjestelmä on ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmistoista koostuva järjestelmä, jonka tarkoituksena on tietojen käsittelyn avulla tietoa tai helpottaa jotain toimintaa tai tehdä se ylipäätään mahdolliseksi.

Tietojärjestelmä – Wikipedia
<https://fi.wikipedia.org/wiki/Tietojärjestelmä>



27

Tietojärjestelmiltä (ainakin) vaadittavat mekanismit

- Tietojen siivoaminen tiedon elinkaaren mukaan (a5: ”Säilytyksen rajoittaminen”)
- Henkilötietojen käsittelyn arvioimiselle (a5: osoitusvelvollisuus)
 - Esim. mahdolliset tiedon käsittelyn lokit, järjestelmäarkkitehtuuri
- Suostumus annettava nimenomaisesti ja antajan ymmärrettävä merkitys ja voitava myös peruuttaa (art. 7)
- Iän vahvistus: ikäraja 16v, mutta voidaan sallia kansallisesti ikärajaksi 13v (art. 8)
- Tiedot, joita rekisteröidylle on toimitettava (a13 ja a14)
- Omien tietojen tarkastaminen (a15)
- Tietojen oikaiseminen (a16)
- Oikeus tulla unohdetuksi (a17)
- Käsittelyn rajoittaminen (a18)
- Muutosten ilmoittaminen myös muille joille henkilötietoja on luovutettu (a19)
- Oikeus siirtää tiedot (*koneluettavasti*) toiseen järjestelmään (art. 20)
- Tietoturvaloukkausilmoitukset (a33 ja a34)
- Vahinkojen minimoiminen (a82)
- Jne...

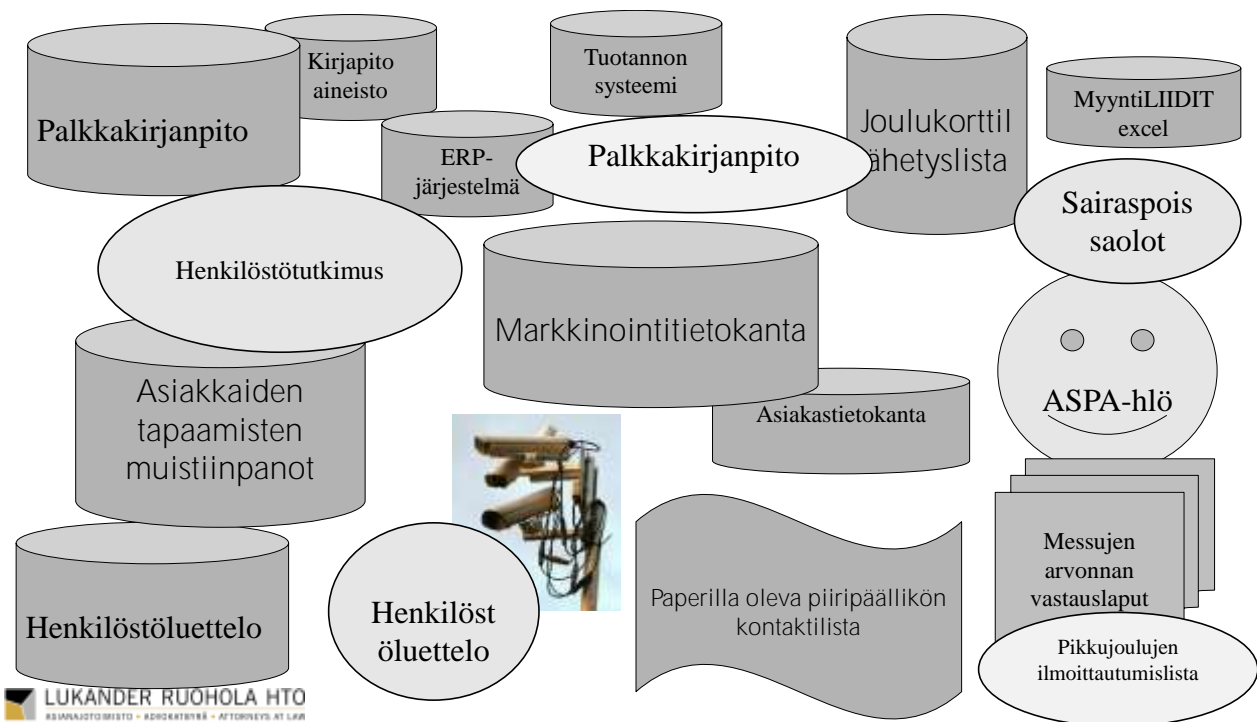


28

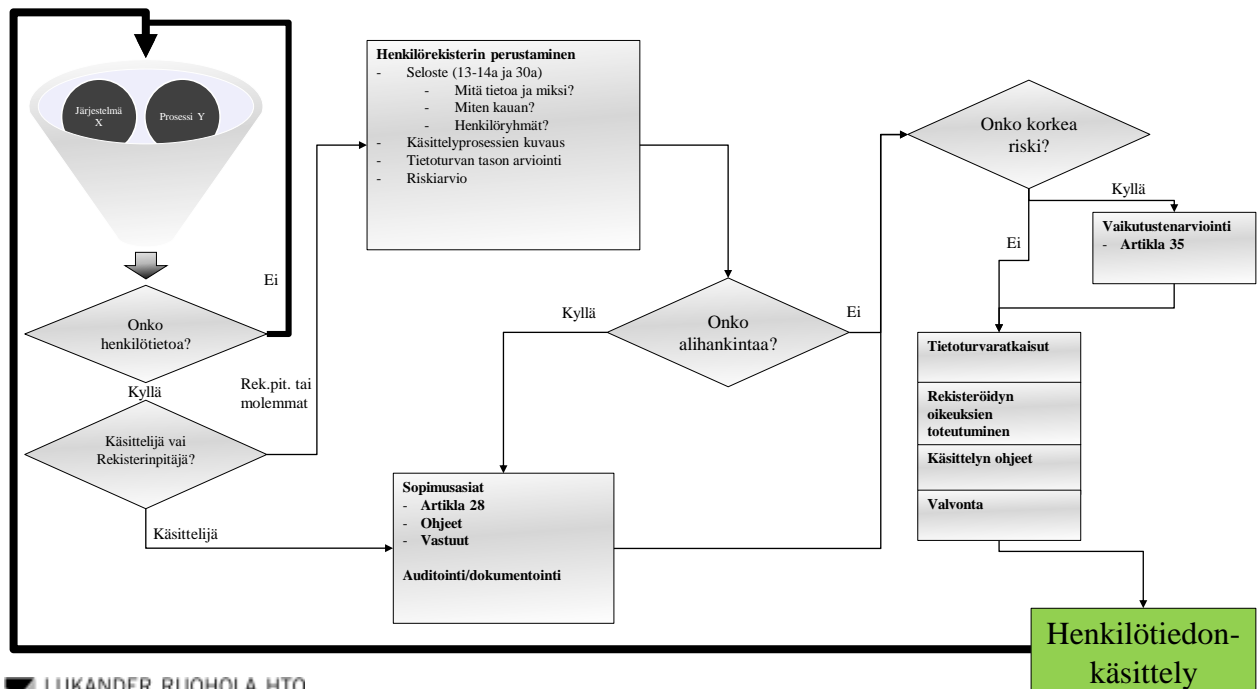
Käytännön toimet organisaatiossa

Käytännön toimet, kolme pääaluetta:

1. Henkilötiedon ja henkilörekisterien sekä ulkoistustilanteiden tunnistaminen
2. Tietosuojaselosteet, vaikutustenarviointi(?), tietosuojavastaava(?), tietoturva, järjestelmien muutokset, sopimusten tarkastaminen, ohjeet ja prosessit
3. Henkilötiedon elinkaaren hallinta ja henkilötietoprosessien jatkuva ylläpito (esim. vuosikello, tietotilinpäätös)



LUKANDER RUOHOLA HTO
 ASIANAJOTOIMISTO • ADVOKATITRYB • ATTORNEYS AT LAW



LUKANDER RUOHOLA HTO
 ASIANAJOTOIMISTO • ADVOKATITRYB • ATTORNEYS AT LAW

Tietosuojaselosteet

- Uuden asetuksen myötä nykyiset rekisteriselosteet muuttuvat tietosuojaselosteiksi
 - Joitakin sisällöllisiä muutoksia
 - Useita eri käyttötarkoituksia (mm. a13, a14)
 - Joitakin koskee vielä laajemman selosteen laatimisvelvoite (a30)
- Jos et aio tehdä mitään muuta, niin käy ainakin nykyiset selosteet läpi ja laadi puuttuvat selosteet!

Tietosuojavastaava

- Tietosuojavastaava on uusi virallinen rooli, jonka tarkoitus on toimia rajapintana rekisterinpitäjän ja valvojan viranomaisen välillä
- Suurimman osan ei tarvitse nimittää
- Edellyttää laajamittaista tai erityisen korkean riskin henkilötietoa
- Voi olla myös ulkoinen taho
- Jos oma henkilö, osittain korotettu irtisanomissuoja
- Toimivaltuudet suoraan asetuksista
- Pääasiassa tehtävä valvoa ja varmistaa, että rekisterinpitäjän tietosuojatunnus – ei henkilökohtaisesti kuitenkaan vastaa siitä

Vaikutustenarviointi (DPIA)

- Asetuksen 35 artiklan mukaan on henkilörekisteriin liittyen tehtävä erityinen vaikutustenarviointi
 - ” Jos tietyn tyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle. Yhtä arviota voidaan käyttää samankaltaisiin vastaaviin korkeita riskejä aiheuttaviin käsittelytoimiin.
- Asetuksessa luettelo vaikutustenarvioinnin tuloksena syntyvistä asiakirjoista
- Ei koske suurinta osaa henkilörekistereistä
- Riskiarvio perustuu rekisterinpitäjän omaan arvioon – ja myös vastuu jää sitä myötä rekisterinpitäjälle
- Eri aloilla saattaa jatkossa olla suosituksia velvoitteeseen liittyen

Tietoturva 32 artikla - Käsittelyn turvallisuus

1. ”Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten:
 - a) henkilötietojen pseudonymisointi ja **saltaus**
 - b) **kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus**
 - c) **kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa**
 - d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi

Tietoturva

33 artikla - Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

1. Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys.

2. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.



37

KESKUS- KAUPPAKAMARI

ETUUSU | MITÄ TEEMME? | LAITSHUONE | MEDIA | KAUPPAKAMARIT | KAUPPAKAMARI 100 | IHTEISTIEDOT

Keskuskauppakamarilta Tietoturvaopas yrityksille

28.11.2016 | ARTIKLA AUJOTIEDOKSI

Keskuskauppamari on julkaissut tämän Tietoturvaopas yrityksille. Se on käytännöllinen opas, joka sisältää ohjeita ja yksinkertaisia ohjeita yrityksen tietoturvan parantamiseksi. Opas tarjoaa toimivan mallin kaikenkokoisille yrityksille siitä, miten lähteä liikkeelle tietoturvaasioiden selvittämistä ja ratkaisemista.



<https://kauppakamari.fi/2016/11/29/keskuskauppakamarilta-tietoturvaopas-yrityksille/>



38

Henkilötiedon elinkaari

- Henkilötieto ei ole vain passiivista dataa - sen on liityttävä aina (liiketoiminta)prosessiin
- Prosessilla on aina alku ja loppu – samoin yksittäisellä henkilötiedolla rekisterissä
- Vain hallitsemalla henkilötiedon elinkaari voidaan todella taata tietosuoja
- Elinkaareen vaikuttaa käyttötarkoitus ja rekisteröidyn oikeudet
- Elinkaari sekä henkilörekisterillä että henkilötiedolla

KÄSITTELYÄ ENNEN

- Sisäänrakennettu ja oletusarvoinen tietosuoja
- Huomioi tulevat muutokset
- Käsitteilyn tarkoitus, kesto, henkilöryhmät, oikeusperuste
- Tietoturvatoimet
- Ohjeet henkilöstölle + mahdolliset käytäntösäännöt
- Vaikutustenarviointi?
- Tietosuojavastaava?
- Rekisteröidyn informointi
- Sertifiointit?
- Tietojenkäsittelysopimus
- YT-menettely

KÄSITTELY

Tiedon määrä

- Suostumusten hallinnointi (tarvittaessa)
- Ylläpidä
 - Ohjeistukset ja rekisteriselosteet
 - Käytäntösäännöt ja sertifikaatit
 - Osoituskyky (esim. tietotilinpäätös)
 - Tietoturva ja kyky reagoida poikkeamiin
- Hallinnoi
 - Käsitteilytoimia
 - Tiedon määrää (säilytysajat ja perusteet)
 - henkilötiedon luovutuksia
 - KV-tiedonsiirtojen hallinta
 - Tiedon sijainti ja tietoturvaso
- Rekisteröidyn oikeudet
 - Korjaus/poisto/tarkastus/kielto-oikeus
 - Oikeus siirtää tiedot koneluettavasti
- Ilmoitukset tietoturvaloukkauksista
 - Viranomaiset ja rekisteröity

KÄSITTELYN JÄLKEEN

- Tietojen siirto myös koneluettavasti
- Henkilötietojen hävittäminen
- Tietojen siirto toiseen rekisteriin
- Arkistoitavien henkilötietojen hävittäminen myöhemmin

t

Tietosuoja vuosikello

- Tietosuoja ei ole projekti vaan
 - Jatkuva tapa toimia
 - Osa liiketoimintaprosesseja
- Vuosikelloajattelu on (vain) yksi tapa jäsenellä toistuvaa tekemistä
 - Tyypillisesti osa taloushallintoa ja markkinointia
 - Toimii myös tietosuojaan käynnistysprojektin runkona
- Päätaoite jaksottaa työ siten, että vuoden aikana kaikki tulee hoidettua, jotta
 - tietosuoja on kunnossa ja
 - on uskottava kyky osoittaa tietosuojavaatimustenmukaisuus
- Tietotilin päätös on looginen lopputulos kellon kierroksesta



41



Tietotilinpäätös

- Perinteistä tilinpäätöstä vastaava vuosiselonteko tietojenkäsittelystä
- Keino osoittaa tietosuojan taso ja tietojenkäsittelyn tilanne
- (Tieto)johtamisen työkalu

- Esimerkkejä ja aineistoa:
 - <http://vrk.fi/tietotilinpaatos>
 - <https://www.trafi.fi/tietopalvelut/tietotilinpaatos>
 - http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetun toimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Tietotilinpäätös

- Mitä tietoon liittyviä prosesseja ja mitä tietovarantoja organisaation hallussa on
- Yleinen kuvaus organisaation tietoarkkitehtuurista
- Organisaation hallussa olevien tietojen laatu ja käytettävyys
- Tietojenkäsittelyyn liittyvät menettelytavat ja periaatteet
- Tietojen suojaustaso ja keskeiset periaatteet
- Tietojenkäsittelyn ja –käytön valvonta ja kontrollit
- Rekisteröityjen oikeuksien toteuttaminen
- Tulossa olevat tai jo havaitut organisaationi liittyvät muutokset sekä niihin liittyvät kehittämistoimet
- Tietosuojan organisointi

Esimerkki projektirunko

1. Vastuuta tietosuoja johtoryhmätasolle!
2. Tutustu uuteen tietosuoja-asetukseen
3. Arvioi henkilötietojen käsittelyn tilanne ja tunnista henkilörekisterit
4. Sopimukset, tietosuojakulttuuri ja organisointi
5. Varmistakaa myös käytännön mekanismit esim. IT:n osalta
6. Luokaa prosessi asetuksen asettamien vaatimusten täyttämiseksi ja vaadittavan dokumentaation sekä käytänteiden ylläpitämiseksi

Projektin lopputuotteet (ainakin)

- **Tietosuojatilmi/henkilöt nimetty**
 - Monialainen (Ainakin: johto/yleishallinto, henkilöstöhallinto, IT, viestintä)
- **Lista henkilörekistereistä ja niihin kuhunkin liittyen**
 - henkilörekisteriä koskeva tietosuojaseloste (a13-14 ja a30)
 - tiedon elinkaari ja hajautusnäkökulma
 - arvio tiedon kriittisyydestä
 - (mahdollinen) vaikutustenarviointidokumentti
 - henkilörekisteriä koskeva sisäinen dokumentaatio
 - Tietoturva-asiat
 - Rekisterin kehityspolku esim. tietojärjestelmien muutosprojektisuunnitelmat
 - Rekisterin ylläpitomalli ("asiakasrajapinnat", "puhtaanapito" ja dokumentaatiovastuut)

- **Ulkoistustilanteissa lisäksi huolehdi ja dokumentoi**
 - rekisteriä koskeva sopimus ja sen yhteensopivuus 28 artiklan kanssa
 - Alihankintaa koskevat ohjeet ja vastuunrajaukset
 - alihankkijan auditointi ja siihen liittyvä dokumentaatio
 - Riittävät tiedot ulkoistuksesta myös tietosuojaselosteessa
- **Henkilötietoprosessi**
 - Kriisisuunnitelma
 - Tiedotussuunnitelma
 - Palautussuunnitelma
 - Jatkuvuussuunnitelma
 - Tiedon elinkaarimallit
 - Vuosikello yms.