Tietosuojainfo

Tietosuojavastaava Tapani Rinne, Salon kaupunki

6.3.2018

www.salo.fi

EU:n yleinen tietosuoja-asetus

- Tullut voimaan 5/2016, kansallinen soveltaminen alkaa 25.5.2018
- Asetus siis voimassa, eikä muutoksia sisältöön tule; Soveltamisohjeita tulee sekä kansallinen tietosuojalaki, jossa säädetään mm. kansallisen liikkumavaran piiriin kuuluvista asioista
- Asetus, eli sovelletaan suoraan toisin kuin 1995 henkilötietodirektiivi, joka on nykyisen henkilötietolain taustalla
- Oikeus henkilötietojen suojaan tunnustettu perusoikeudeksi (esim. EU:n perusoikeuskirja), siksi rekisterinpitäjän suojausvelvollisuus on vahva
- Uudella asetuksella pyritään takaamaan ihmisten oikeus henkilötietojen suojaan myös digitaaliaikana
- Suomeen uusi viranomainen, kansallinen tietosuojavirasto; mm. neuvoo, ohjaa, valvoo

Henkilötieto ja käsittely

- **Luonnollista henkilöä** tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat **merkinnät**, jotka voidaan **tunnistaa** häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.
- Suora ja epäsuora tunnistaminen, tallennettu mille alustalle tahansa
- Lainsäädäntöä ei sovelleta yksityishenkilön yksityiseen käyttöön tapahtuvaan henkilötietojen käsittelyyn
  - Henkilötietojen julkaisu oma kokonaisuus
- Henkilötietojen **käsittely**: keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä
- Todennäköisesti tulossa paljon tilanteita, joissa viimekädessä oikeuskäytäntö ratkaisee, että oliko kyseessä henkilötieto ja oliko toiminta käsittelyä

5 kohtaa jotka hoidettava kuntoon – Yksi näkemys

- Seuraavaksi käsitellään 5 tietosuojaan ja henkilötietojen käsittelyyn liittyvää asiaa joista voi aloittaa tietosuoja-asetuksen vaatimuksiin valmistautumisen
- Vaikka kaikki 5 olisi hoidettu, henkilötietojen käsittelyn dokumentaatio ja ylläpito sekä valvontajärjestelmä olisi kunnossa, ei se silti tarkoita että organisaatio on vaatimusten mukainen
- Henkilötietojen käsittelyn ja tietosuojan tulee olla oletusarvoista ja sisäänrakennettua (privary by design/privacy by default)
- Vaatii jatkuvaa kehittämistä, valvontaa, raportointia ja dokumentointia

1. Henkilötietovarantojen selvitys

- Mitä henkilötietoja organisaatio käsittelee?
- Mitä henkilörekistereitä organisaatiolla on. Analogiset, sähköiset; laaja näkökulma eli esim. verkkokansiot, tietokoneiden kovalevyt jne.
- Mitkä ovat henkilörekistereitä ja mitkä otteita varsinaisesta rekisteristä
- Mitä tietoja rekistereissä on.
  - Millaisia rekistereitä organisaatiolla on? Mitä käsittelytarkoituksia, lainmukaisuuden peruste
  - Henkilötietoryhmät – Varsinkin erityiset henkilötietoryhmät (ent. arkaluontoiset henkilötiedot)
  - Käsittelyn tarkoitus (selkeästi dokumentoitu, että miksi henkilötietoja kerätään ja käsitellään. Muita tarkoituksia ei voi olla)
  - Käsittelytoimet tulee kertoa selosteessa
  - Jos palveluja tuotetaan lapsille, täytyy selosteiden ja kuvausten olla selkeitä ja kielellä jonka lapsikin ymmärtää!
- Kuvaukset lyhyesti ja selkeästi. Ei 10 sivuisilla selosteilla

Henkilötietojen käsittelyn lainmukaisuus

- Henkilötietoja saa käsitellä, jos vähintään yksi peruste täyttyy
  - Rekisteröidyn suostumus (suostumuksen edellytykset Art. 7)
  - Sopimuksen täytäntöön panemiseksi ja rekisteröity osapuolena
  - Lakisääteisen velvoitteen täyttämiseksi
  - Elintärkeiden etujen suojaaminen
  - Yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi
  - Oikeutettujen etujen toteuttamiseksi

2. Rooli henkilötietojen käsittelyssä

- Missä roolissa organisaatio käsittelee henkilötietoja?
- Rekisterinpitäjällä eri vastuut kuin henkilötietojen käsittelijällä
  - Jos rekisterinpitäjä niin huolehdittava kaikista vaatimuksista **ja** henkilötietojen käsittelijöistä
  - Jos henkilötietojen käsittelijä, niin huolehdittava ettei selkeästi riko lakia ja noudattaa rekisterinpitäjän ohjeita
- Sama taho voi toimia useissa rooleissa; palveluntuottajana henkilötietojen käsittelijä ja oman toiminnan ylläpitäjänä rekisterinpitäjä
- Viimekädessä rekisterinpitäjä on aina vastuussa, rekisterinpitäjällä todistustaakka, että tietosuojasta on huolehdittu
  - Vaikka organisaatiolla ostettuna palveluna tietosuojavastaava, tietosuojavastaava ei ole vastuussa
  - Kannattaa kuitenkin nimetä henkilö, jonka vastuulla tietosuoja on. (Kirjallisesti)

Rooli henkilötietojen käsittelyssä

- Roolien sekoittumista tulee välttää, siksi hyvä sopia kirjallisesti, ohjeistaa kirjallisesti, kouluttaa ja pitää kirjaa koulutuksista, testeistä jne.
- Myös yksityisen ja organisaation edustajan välinen rooli voi olla ongelmallinen
- Yksityishenkilöä koskee eri lainsäädäntö kuin henkilötietojen käsittelijää organisaation edustajana
  - Esim. organisaation järjestämissä vapaa-ajantilaisuuksissa voi roolin määrittely olla vaikeaa
  - Organisaation työkalujen käyttö omaan käyttöön; älylaitteet, kamerat, tietokoneet jne. (esim. sormenjälkitunnistus älylaitteessa, jonka omistaa organisaatio → biometrinen tieto → erityinen henkilötietoryhmä)
- Ei välttämättä ongelmaa, mutta kannattaa huomioida riskit

3. Henkilötietojen käsittelyn periaatteet

- Kun on selvitetty, että mitä henkilötietoja kerätään ja käsitellään, tulee määritellä miten henkilötietoja käsitellään
- Rekisterinpitäjällä on osoitusvelvollisuus, että henkilötietojen käsittelyn periaatteita noudatetaan
- Kansallinen viranomainen voi vaatia dokumentaation tarkastettavaksi
- Laadittuja periaatteita on noudatettava, henkilöstö on koulutettava ja toimintaa valvottava → Dokumentaatio

Periaatteet

- Lainmukaisuus, eheys ja läpinäkyvyys
  - Käsittelylle tulee olla lainmukainen peruste, käsittelyn tulee olla kohtuullista ja läpinäkyvää, eli rekisteröidyllä on oikeus saada tietoja käsittelystä
- Käyttötarkoitussidonnaisuus
  - Henkilötietoja saa käsitellä tiettyä käyttötarkoitusta varten eikä henkilötietoja voi käsitellä muuta tarkoitusta varten kuin mihin ne ovat kerätty
- Minimointi
  - Kerätyt henkilötiedot tulee olla olennaisia ja rajoitettu siihen, mikä on tarpeellista suhteessa käyttötarkoitukseen
  - Ylimääräisiä henkilötietoja ei saa kerätä/Käsitellä. Esim. viranhaltijapäätöksissä vain olennaiset, julkaisukelpoiset tiedot. Muut asiaan vaikuttavat esim. käyttörajoitetussa liitteessä

Periaatteet

- Täsmällisyys
  - Tietojen tulee olla täsmällisiä ja päivitettyjä
  - Kaikki kohtuulliset toimenpiteet toteutettava ettei käsittelyn tarkoituksiin nähden epätarkkoja tai virheellisiä tietoja ole
- Säilytyksen rajoittaminen
  - Säilytettävä vain käsittelyyn nähden tarvittavan ajan siinä muodossa, josta rekisteröity on tunnistettavissa
  - Ei koske yleisen edun perusteella tapahtuvaa, arkistointitarkoituksiin, tieteellisiä-, tai historiallisia tarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaa säilyttämistä… Edellyttäen että vaatimukset täyttyy
- Eheys ja luottamuksellisuus
  - Käsittelyn pitää tapahtua tavalla, jolla varmistetaan asianmukainen turvallisuus, mm. häviäminen, tuhoutuminen, vahingoittuminen, luvaton ja/tai lain vastainen käyttö on estetty

4. Rekisteröidyn oikeudet

- **Miten toteutetaan rekisteröidyn oikeudet!**
- Kun henkilötietoja saadaan rekisteröidyltä, on rekisterinpitäjän toimitettava tietoja:
  - Rekisterinpitäjän ja edustajan identiteetti ja yhteystiedot
  - Tietosuojavastaavan yhteystiedot
  - Henkilötietojen käsittelyn tarkoitus ja oikeusperuste
  - (mahdolliset oikeutetut edut)
  - Henkilötietojen vastaanottajat tai vastaanottoryhmät(luovutukset)
  - (henkilötietojen siirrosta kolmanteen maahan tai muualle → suojatoimet, minne asetettu saataville jne.)
  - Henkilötietojen säilytysaika ja ajan määrityskriteerit
  - Oikeus saada pääsy henkilötietoihin, pyytää oikaisua, poistoa, käsittelyn rajoitusta, vastustaa käsittelyä tai siirtää tiedot järjestelmästä toiseen

Rekisteröidyn oikeudet

- Oikeus peruuttaa suostumus, mikäli henkilötietojen käsittely perustuu rekisteröidyn suostumukseen
- Oikeus tehdä valitus valvontaviranomaiselle
- Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset
- (Jos henkilötietojen käsittelyyn liittyy automaattista päätöksentekoa ja/tai profilointia. Näissä tapauksissa merkitykselliset tiedot käsittelyn logiikasta, ko. käsittelyn merkittävyys ja mahdolliset seuraukset)
- Mahdolliseen jatkokäsittelyyn liittyvät samat tiedot ennen jatkokäsittelyä, silloin kun henkilötietoja aiotaan käsitellä edelleen muuhun tarkoitukseen kuin siihen mihin henkilötiedot on kerätty

Rekisteröidyn oikeudet

- Jos tietoja ei saada rekisteröidyltä itseltään on toimitettava edellä mainittujen lisäksi tiedot:
  - Kyseessä olevat henkilötietoryhmät
  - Mistä henkilötiedot on saatu sekä tarvittaessa, onko tiedot saatu yleisesti saatavilla olevista lähteistä
- Tiedot on toimitettava kohtuullisen ajan kuluttua, mutta viimeistään kuukauden kuluttua henkilötietojen saamisesta
- Jos henkilötietoja käytetään viestintään rekisteröidyn kanssa niin tiedot on toimitettava viimeistään silloin kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran

Milloin tiedottamisvelvollisuutta ei ole

- Edellä mainittuja ei tarvitse soveltaa tietyin ehdoin:
  - Tietojen toimittaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa
  - Varsinkin jos henkilötietojen käsittely tapahtuu yleisen edun mukaisia arkisto- tieteellisiä, historiallisia tai tilastollisia tarkoituksia varten.
  - Tietojen hankinnasta tai luovutuksesta säädetään rekisterinpitäjään sovellettavassa unionin tai jäsenvaltion lainsäädännössä
  - Tiedot on pidettävä luottamuksellisina, koska niitä koskee unionin tai jäsenvaltion lainsäädäntöön perustuva vaitiolovelvollisuus, kuten lakisääteinen salassapitovelvollisuus
  - Tiedot on jo toimitettu rekisteröidylle

Rekisteröidyn oikeus saada pääsy tietoihin

- Rekisteröidyllä on oikeus saada vahvistus että häntä koskevia tietoja käsitellään tai että ei käsitellä.
- Jos käsitellään niin rekisteröidyllä oikeus saada pääsy tietoihin sekä:
  - Käsittelyn tarkoitus
  - Käsiteltävät henkilötietoryhmät
  - Vastaanottajat ja vastaanottajaryhmät
  - Säilytysaika ja kriteerit
  - Tiedon alkuperäinen lähde
  - Automaattisen päätöksenteon ja/tai profiloinnin olemassaolo
  - Henkilötietojen siirrot
  - Haluttaessa jäljennös käsiteltävistä henkilötiedoista
  - Jäljennös ei saa vaikuttaa haitallisesti muiden oikeuksiin tai vapauksiin

Rekisteröidyn oikeuksia

- Rekisteröidyllä on oikeus pyytää tietojen oikaisua → ilman aiheetonta viivytystä epätarkat ja virheelliset tiedot oikaistava.
- Joissakin tapauksissa oikeus vaatia puutteellisten tietojen täydentämistä (otettava huomioon tarkoitus joihin tietoja käsitellään)
- Tietyissä tapauksissa rekisteröity voi vaatia henkilötietojen poistamista
- Tietyin ehdoin rekisteröidyllä on oikeus vaatia käsittelyn rajoitusta → Koskee myös henkilötietojen poistamista(esim. rekisteröity vastustaa tietojen poistamista, koska tarvitsee oikeudellisen vaateen puolustamiseksi
- Oikeus saada tieto rajoitetun käsittelyn päättymisestä
- Rekisterinpitäjä on ilmoitusvelvollinen, jos henkilötietoja oikaistaan, poistetaan käsittelyä rajoitetaan. Ilmoitus on tehtävä kaikille tahoille joille henkilötietoja on luovutettu. Paitsi jos mahdoton tai kohtuuton vaivaa. Nämä vastaanottajat ilmoitettava mikäli rekisteröity vaatii.

Oikeus tietojen siirtoon

- Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle
- Jos henkilötietojen käsittely perustuu suostumukseen
- Käsittely suoritetaan automaattisesti
- Jos se on teknisesti mahdollista, tiedot on oikeus saada siirrettyä rekisterinpitäjältä toiselle suoraan
- Ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin
- Oikeus ei saa rajoittaa oikeutta tulla unohdetuksi

Vastustamisoikeus

- Rekisteröidyllä on oikeus vastustaa käsittelyä henkilökohtaisen erityisen tilanteen perusteella milloin tahansa, jos käsittely toteutetaan yleisen edun, julkisen vallan käytön tai oikeutettujen etujen toteuttamiseksi. Esim. profilointia
- Koskee myös tieteellisiä ja historiallisia tutkimustarkoituksia sekä tilastollisia tarkoituksia varten. Paitsi jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi
- Tiettyjä tapauksia jolloin rekisterinpitäjällä on silti oikeus käsitellä henkilötietoja
- Suoramarkkinointia varten käsittelyä rekisteröidyllä on milloin tahansa oikeus vastustaa. Mukaan lukien profilointi suoramarkkinointia varten.
- Kun rekisteröityyn ollaan 1. kerran yhteydessä, yllä mainitut oikeudet on saatettava rekisteröidyn tietoon ja esitettävä selkeästi ja muusta tiedosta erillään
- Sähköisen viestinnän tietosuojalainsäädäntö otettava huomioon

Automatisoidut yksittäispäätökset

- Rekisteröidyllä on oikeus olla joutumatta sellaisten päätösten kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin ja jolla on häntä koskevia oikeusvaikutuksia
- Ei sovelleta jos
  - Päätös on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten
  - Perustuu rekisteröidyn nimenomaiseen suostumukseen
  - Jos käsittely on hyväksytty rekisterinpitäjään sovellettavassa lainsäädännössä ja rekisteröidyn oikeudet ja vapaudet taataan
  - Ei saa perustua erityisiin henkilötietoryhmiin

Tietoturvaloukkauksista ilmoittaminen

- Rekisteröidylle on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä
  - Kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille
- Ilmoitusta ei vaadita jos:
  - Rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja loukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole ymmärrettävissä ellei ole lupa päästä tietoihin(esim. salaus, anonymisointi jne.)
  - Rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan että korkea riski ei enää toteudu
  - Ilmoitus vaatisi kohtuutonta vaivaa. Tällaisissa toimenpiteissä käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä
- Jos ilmoitusta ei ole vielä tehty, valvontaviranomainen voi voi vaatia ilmoituksen tekemistä tai päättää että joku edellä mainituista kohdista täyttyy, arvioituaan kuinka todennäköinen suuri riski on

5. Sopimukset

- Kuka vastaa ja mistä
- Kuka käsittelee henkilötietoja – Kolmannet osapuolet ja sopimukset niiden kanssa
- Sopimuksissa otettava tietosuoja huomioon (Osoitusvelvollisuus)
- Ei riitä että noudatetaan Suomessa voimassa olevaa lainsäädäntöä → Miten lakia noudatetaan
- Joko suoraan sopimukseen tietosuojasta lausekkeet tai tietosuojaliite/tietosuoja ja tietoturvaliite
- Kuntaliiton materiaalia voinee käyttää pohjana
  - http://shop.kunnat.net/product_details.php?p=3362

Sisään rakennettu ja oletusarvoinen tietosuoja

- Henkilötietojen käsittelyssä tulee noudattaa sisään rakennetun ja oletusarvoisen tietosuoja periaatteita
  - Tietosuojan tulee siis olla oletusarvo, jonka kautta organisaation toiminta/kehitys ym. On tehtävä
- Esimerkkejä oletusarvoisesta tietosuojasta:
  - Henkilötietojen keruun ja käsittelyn minimointi
  - Käyttäjäpiirin tehokas rajaaminen (käyttövaltuudet ja pääsynvalvonta)
  - Säilytysaikojen määrittely ja vanhentuneen tiedon poistaminen (Tiedonhallinta ja tiedonohjausprosessit)
  - Pseudonymisointi
  - Anonymisointi
  - Tiedon salaaminen (kryptays)

Sisäänrakennettu ja oletusarvoinen tietosuoja

- Tietoturva
- Rekisteröidyn oikeuksien toteuttaminen
- Käyttäjäystävälliset asetukset
- Tietosuojavastaavan rooli
- Vaikutustenarvioinnit (DPIA ja riskilähtöisyys)

Kiitos!

Tapani Rinne, Tietosuojavastaava, Salon kaupunki
tapani.rinne@salo.fi
044 778 2031