

1/3/2018

Tietosuoja ja MLL:ssa noudatettavia käytänteitä



MANNERHEIMIN
LASTENSUOJELULIITTO

Lapset ensin.

Yleinen tietosuoja-asetus (GDPR)

- Tullut voimaan 25.4.2016
- Soveltaminen alkaa 25.5.2018
- Nykyisen henkilötietolain pääpiirteet säilyvät
- Muutos tuo tullessaan uusia velvoitteita rekisterinpitäjille ja oikeuksia rekisteröidylle
- Tietosuoja laki valmisteilla (Täytäntöönpanotyöryhmän mietintö julkaistu 21.6.2017)
- Työryhmä: Kansallisten lainsäädäntötoimien tarpeen arviointi ja lainmuutosten valmistelu

Asetuksen tarkoitus

- Asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä.

Asetuksen soveltamisala

- Sovelletaan aina, kun henkilötietoja käsitellään järjestön tai yrityksen tietojärjestelmissä
- Sovelletaan automaattiseen henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn, kun ne muodostavat rekisterin osan tai niiden on tarkoitus muodostaa rekisterin osa
- Manuaalinen käsittely: asiakaskortisto tai sen osa
- Koskee siten käytännössä kaikkia järjestöjä ja yrityksiä; esim. yksikin asiakas tai työntekijä

Mikä on henkilötieto?

- **Tunnistettua tai tunnistettavissa olevaa henkilöä koskevat tiedot, jotka voidaan liittää häneen.**
 - Nimi, osoite, sähköposti, henkilötunnus, syntymäaika, henkilönumero, sukupuoli, ammatti, kuvataallinen, äänitallinen, IP-osoite, laiteID, sormenjälki, rekisteritunnus ovat henkilötietoja, jos tieto voidaan tunnistaa tiettyä henkilöä koskevaksi.

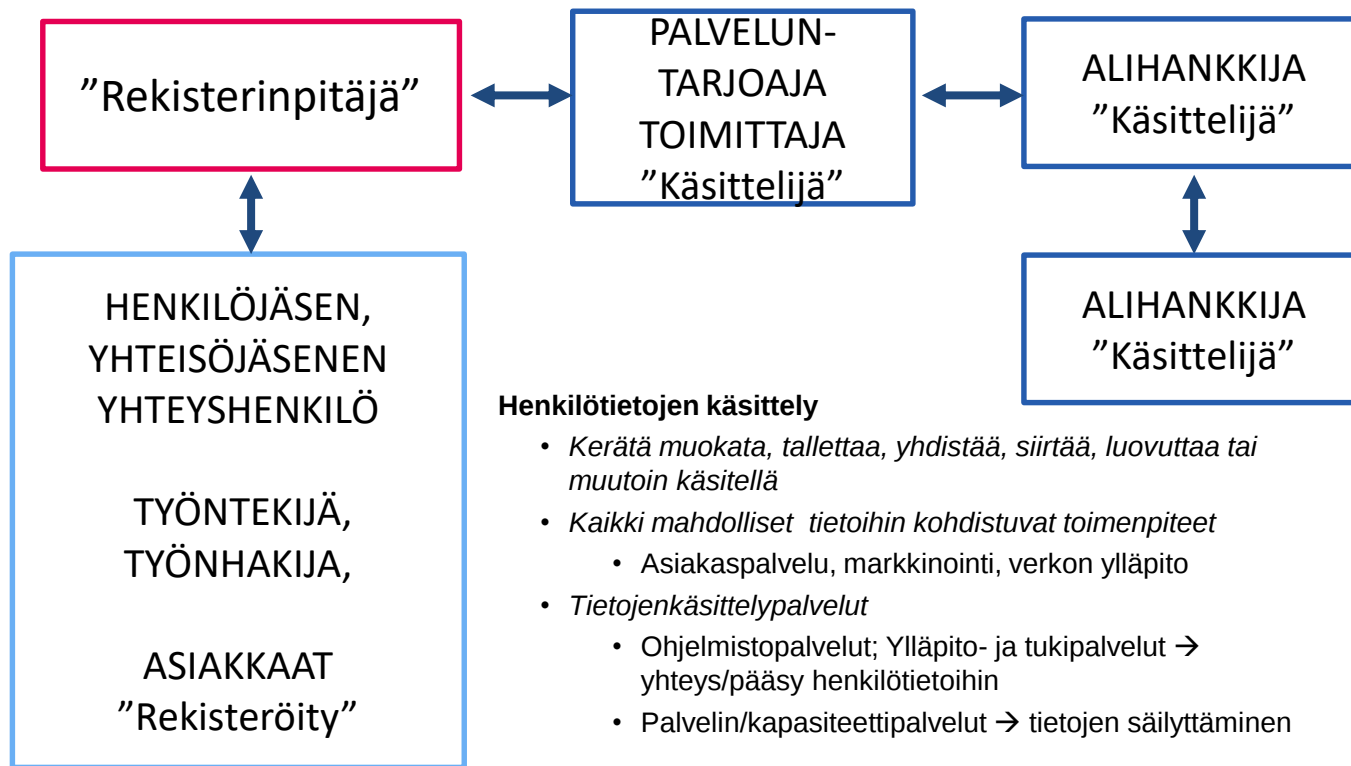
Termejä: Rekisteröity ja rekisteri

- **Rekisteröity.** Henkilötietojen käsittelyn kohteena oleva henkilö.
 - Työntekijät, työnhakijat, yhdistyksen henkilöjäsenet
- **Rekisteri.** Mitä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla henkilöä koskevilla perusteilla.
 - Jäsenrekisteri (jäsenluettelo; nimi ja kotipaikka)
 - Markkinointirekisteri, tapahtuman osallistujalista

Termejä: Roolit

- **Rekisterinpitäjä.** Yritys/yhteisö/henkilö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
 - Ensisijaisessa vastuussa.
- **Käsittelijä.** Rekisterinpitäjän lukuun työskentelevä taho, jonka tehtäviin henkilötietojen käsittely kuuluu.
 - Toimeksianto-, alihankinta- tai yhteistyösuhteessa tietojen käsittelyyn osallistuva taho.

Esimerkki rooleista henkilötietojen käsittelyssä



Käsittelyperusteet

- **Suostumus**
- **Sopimus**
- **Lakisääteiset velvoitteet**
- Elintärkeä etu
- Yleinen etu
- **Oikeutettu etu**
 - (suositelluin käsittelyperuste)

Osoitusvelvollisuus

- **Organisaatiolla on oltava kyky osoittaa noudattavansa asetusta henkilötietoja käsitellessä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä.**
- **Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia.**
- Tietosuoja-asetuksen mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on pääsääntöisesti ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista.

Tiedon elinkaari

SUUNNITTELU

- Peruste ja käyttötarkoitus, säilytysajat, hävittäminen, ohjeistus ja käytännöt



YLLÄPITO

- Virheettömyys, tietoturva, ohjeistuksen noudattaminen ja valvonta, rekisteröidyn oikeudet



PÄÄTTYMINEN

- Säilytysaikojen noudattaminen, velvollisuus tietojen säilyttämiseen, hävittäminen ja arkistointi

Rekisterinpitäjältä vaaditut toimenpiteet (1)

- **Organisaation on tietosuoja-asetuksen vaikutuksia arvioidessaan hahmotettava kokonaiskuva henkilötietojen käsittelyn nykytilasta.**
- **Organisaatio voi esimerkiksi kuvata**
 - mitä henkilötietovarantoja sen hallussa on
 - miten tietosuojaperiaatteet on otettu huomioon
 - toimintaan liittyvät henkilötietovirrat (Missä? Mitä? Kuka käsittelee?)
 - henkilötietojen käsittelyn oikeusperusteet
 - miten tietoturvasta on huolehdittu ja
 - miten henkilötietojen käsittelyyn liittyvä riskienhallinta on toteutettu.

Rekisterinpitäjältä vaaditut toimenpiteet (2)

- Kun henkilötietojen käsittelyn nykytila on kartoitettu, tulisi selvittää, mitä konkreettisia muutoksia ja toimenpiteitä tietosuoja-asetuksen sääntely henkilötietojen käsittelylle tarkoittaa.
- **Tietosuoja-asetuksen velvoitteiden edellyttämien toimenpiteiden laatu ja laajuus riippuvat esimerkiksi organisaation käsittelemistä henkilötiedoista, käsittelyyn kohdistuvasta riskistä ja nykyisistä käytännöistä.**
- Organisaatioiden johdon on oltava tietoinen lainsäädännössä tapahtuvista muutoksista sekä niiden vaikutuksesta organisaationsa eri toimintoihin.

Palvelut lapsille

- Lapsille palveluita tarjoavien rekisterinpitäjien on huomioitava, että tietosuoja-asetus antaa henkilötietolaista poiketen erityistä suojaa lapsien henkilötiedoille.
- Selvitä, miten organisaatiosi on huomioitava lasten erityisasema. Lasten tietoja käsiteltävä erityisellä huolellisuudella ja mietittävä, mitä tietoja on tarve kerätä ja kuinka kauan niitä on tarve säilyttää.
- *Some ja sähköiset palvelut:*
 - *Tilanne 1.3.2018: Hallituksen esityksen mukaan tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle edellyttäisi, että lapsi on vähintään 13-vuotias. Tätä nuoremmalla lapsella olisi oltava vanhempien suostumus esimerkiksi sosiaalisen median ja muiden henkilötietojen antamista edellyttävien palvelujen käyttämiseen. Rekisterinpitäjän vastuulla olisi tarkistaa, että suostumus on olemassa.*
http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojaalaki-taydentaisi-eu-n-tietosuoja-asetusta

Henkilötietojen kerääminen

- **Yhdistyksen tarkoitus ja toiminta määrittävät henkilötietojen keräämisen tarpeet ja perusteet.**
 - Henkilötietojen keräämisen ja muun käsittelyn tulee aina olla asiallisesti perusteltua yhdistyksen toiminnan kannalta.
 - Paras tapa on kerätä kutakin jäsentä koskevat tiedot jäseneltä itseltään > mll.fi > Liity jäseneksi
 - ... ja velvoittaa hänet ilmoittamaan mahdolliset muutokset yhdistykselle – MLL:ssa jäsenpalveluun, jasenpalvelu@mll.fi tai mll.fi > Jäsenyys > Muutokset jäsentietoihin

Jäsenluettelo ja muut rekisterit

- Yhdistyksen toiminnan tueksi tarvitaan jäsenluetteloiden lisäksi usein muita mm. yhteystietoja sisältäviä luetteloita, kuten osallistujalistoja.
- Yhdistyksen toiminnasta riippuen voi myös olla asiakasrekisterityyppisiä rekistereitä, joiden sisältö voi olla hyvinkin laaja. **Oleellista on, että kerättävien tietojen tarpeellisuus pitää aina pystyä perustelemaan.**

Rekisteröidyn oikeudet - huoneentaulu (tietosuojaaluetuutettu)

- Oikeus saada läpinäkyvää informaatiota
- Oikeus saada pääsy tietoihin (tarkastusoikeus)
- Oikeus tietojen oikaisemiseen (virheen oikaisu)
- Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Oikeus omin henkilötietojen käsittelyn vastustamiseen
- Oikeus tulla informoiduksi tietoturvaloukkauksista
- Oikeus saada valvontaviranomaiselta apua
- Oikeus luottaa tietoturvaan

Tietosuojaseloste (1) / Dokumentaatiovelvoite

- Tietosuoja-asetuksen mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on pääsääntöisesti ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista
- Selosteen on asetuksen mukaan oltava kirjallisessa muodossa

Tietosuojaseloste (2)

1) Rekisterinpitäjän on ylläpidettävä selostetta, jossa on:

- a) rekisterinpitäjän yhteystiedot
- b) käsittelyn tarkoitukset
- c) kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- d) henkilötietojen vastaanottajien ryhmät, joille tietoja luovutetaan
- e) tarvittaessa tiedot henkilötietojen siirtämisestä 3. maahan
- f) tietoryhmien poistamisen suunnitellut määräajat
- g) yleinen kuvaus teknisistä ja organisatorisista turvatoimista.

Mitä toimenpiteitä vaatii yhdistykseltä?

- **Kartoita nykytilanne**
 - Asiakirja-aineistojen läpikäynti
 - Mitä henkilötietoja käsitellään? Mistä tiedot on kerätty ja mihin niitä luovutetaan? Kerää esim. excel-listaus (malli Yhdistysnetissä)
 - Rekisterit / listaukset / luettelot ym., jotka sisältävät henkilötietoja → **poista vanhat ja tarpeettomat!**
 - Kirjaa käsittelyn peruste ja vaiheet keräämisestä hävittämiseen → Dokumentoi tiedon elinkaari (excel).

Mitä toimenpiteitä vaatii yhdistykseltä?

- **Informointi rekisteröidyille** ja selosteet (mallit Yhdistysnetissä)
- Suunnittele miten rekisteröityjen pyyntöihin vastataan
- Varmista, että yhdistyksellä on henkilötietojen käsittelyn **ulkoistussopimukset** kunnossa, jos käytätte ulkoisia palveluntarjoajia
 - **HUOM! Yhdistyksen jäsenrekisteriä koskeva sopimus MLL:n keskusjärjestön kanssa päivitetään keväällä 2018**
 - Käytä aina jäsenrekisterin ajantasaisia tietoja. Tuhoa tiedot, kun tarve on ohi

Järjestelmät ja niiden käyttö

- **Laite- ja ohjelmaympäristöt**, ovatko tietoturvallisia?
 - Esim. pilvipalveluiden yhteiskäyttö, miten käyttäjähallinta on toteutettu?
- **Tietojen kerääminen pitää perustua tarpeeseen** ja sellaista tietoa ei pidä kerätä, jolle ei ole tarvetta
 - Jatkuva arviointi tarpeista

Miten selvitän, mitä pitää tehdä?

- Kansallinen lainsäädäntö
 - Käsittelyssä eduskunnassa
- Tietosuoja-valtuutetun www-sivut
 - www.tietosuoja.fi
 - Ohjeita ja vastauksia yleisimpiin kysymyksiin
- MLL:n Yhdistysnetti
- Kysyttävää? Kommentoitavaa? Ota yhteyttä!
 - tietosuoja@mll.fi