

030218

V-S Piiri / Täyskäsi / Alma

# Tietosuojauudistus



MANNERHEIMIN  
LASTENSUOJELULIITTO

Lapset ensin.

# Uudistuksen tavoite ja tarkoitus

- EU:n tietosuoja-asetuksen tarkoituksena on yhtenäistää tietosuojakäytäntöjä ja helpottaa jokaisen EU:n kansalaisen omien henkilötietojen tallentamisen ja käytön seuraamista.
- Kansallinen lainsäädäntömme täydentyy vielä tämän vuoden aikana, mutta nyt on aika selvittää henkilötietojen käsittelyä omassa yhdistyksessä. Tähänkin asti lainsäädäntö on velvoittanut henkilötietojen huolelliseen käsittelemiseen sekä vain tarvittavien tietojen keräämiseen. Uutta on etenkin osoitusvelvollisuus mikä käytännössä tarkoittaa tarkempaa henkilötietojen käsittelyn kuvaamista ja dokumentointia.

# Mikä on henkilötieto?

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

# 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)
  - Jos asiakirjaa ei voi hakea ym. perustein (pdf, ei metatietoja), asetus ei koske niitä.

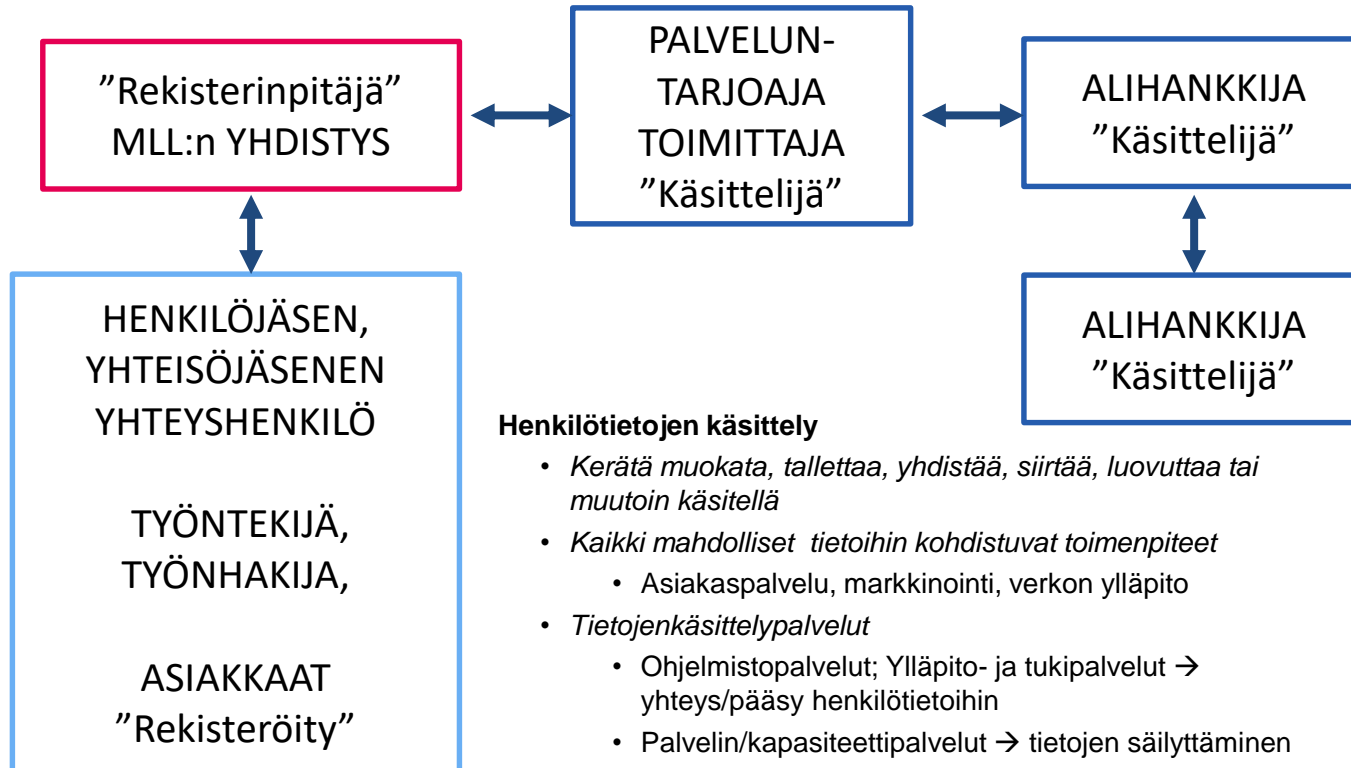
# Tietosuoja-asetuksen soveltaminen

- **Tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä rekisterissä olevien henkilötietojen manuaaliseen käsittelyyn.**
- Asetuksen mukainen henkilötiedon määritelmä on henkilötietolakia yksityiskohtaisempi ja se sisältää konkreettisia esimerkkejä henkilötiedoiksi määriteltävistä tiedoista.

# 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



# Tietosuojaperiaatteet

- **Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys; käyttötarkoitussidonnaisuus; tietojen minimointi; tietojen täsmällisyys; tietojen säilytyksen rajoittaminen; tietojen eheys ja luottamuksellisuus; rekisterinpitäjän osoitusvelvollisuus.**
- Rekisterinpitäjän on huolehdittava siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.



# 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.

# 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 (kuka/ketkä käsittelevät, säilytys yms.) on otettu huomioon, toimintaan liittyvät henkilötietovirrat (siirrot), 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.
- Asetuksen mukaan lapsen henkilötietojen käsittely suostumuksen perusteella suoraan lapselle tarjottavien tietoyhteiskunnan palvelujen tarjoamisen yhteydessä edellyttää vanhempainvastuunkantajan suostumusta tai valtuutusta.
- Asetuksessa lapseksi määritellään alle 16-vuotiaat. Tätä alhaisempi ikäraja, joka voi olla vähintään 13 vuotta, voidaan määritellä kansallisella lainsäädännöllä.

# 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, että yhdistys kerää kutakin jäsentä koskevat tiedot jäseneltä itseltään ja velvoittaa hänet ilmoittamaan mahdolliset muutokset yhdistykselle.

# 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

- Rekisterinpitäjän on toimitettava **henkilötietojen käsittelyä koskevat tiedot** rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa.
- **Tieto toimenpiteistä**, joihin rekisteröidyn pyynnön johdosta on ryhdytty, tulee antaa ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta.

# Rekisteröidyn oikeudet

- **Rekisteröidyn oikeus saada pääsy tietoihin**
  - Asetuksen mukaan rekisteröidyllä on oikeus saada jäljennös häntä koskevista henkilötiedoista
- **Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi**
  - Tietosuoja-asetus takaa rekisteröidylle oikeuden tietojen oikaisemiseen sekä oikeuden tietojen poistamiseen eli oikeuden tulla unohdetuksi.



# Tietosuojaseloste

- Tietosuoja-asetuksen mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on pääsääntöisesti ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista, jotta voidaan osoittaa, että ne ovat asetuksen mukaisia.
- Selosteen on asetuksen mukaan oltava kirjallisessa muodossa ja se on pyydettäessä toimitettava viranomaiselle.
- Seuraa Yhdistysnettiä!

# Valmistautuminen

- **Tiedon omistajuus (vastuhenkilöt)**
  - **Raportointi hallitukselle, sitoutuminen**
  - **Suunnittele henkilötietojen käsittely**
  - **Ohjeista ja valvo**
- 
- **Seuraa Yhdistysnettiä / Tietosuojavaltuutetun ohjeistuksia**

# Valmistautuminen

- **Kartoita nykytilanne**
  - Mitä henkilötietoja käsitellään? Mistä tiedot on kerätty ja mihin niitä luovutetaan?
- **Käsittelyn peruste ja vaiheet keräämisestä hävittämiseen → Dokumentoi.**
- **Selosteet (tarvittaessa), rekisteröidyn informointi**
- **Selvitä miten rekisteröityjen pyyntöihin vastataan**
- **Henkilötietojen käsittelyn ulkoistussopimukset**

# Mitä toimenpiteitä vaatii yhdistykseltä?

- **Edellyttää kykyä tunnistaa henkilörekisteri ja/tai sen osat**
- **Asiakirja-aineistojen läpikäynti**
  - Rekisterit / listaukset / luettelot ym., jotka sisältävät henkilötietoja  
→ **poista tarpeettomat!**
- **Organisaation pitää kuvata:**
  - Henkilötietovarannot ja tietosuojaperiaatteiden huomioiminen
  - toimintaan liittyvät henkilötietovirrat
  - henkilötietojen käsittelyn (oikeus)perusteet
  - miten tietoturvasta on huolehdittu
  - miten henkilötietojen käsittelyyn liittyvä riskienhallinta on toteutettu.
- **Henkilötietovastaavan nimeäminen > kj tiedottaa!**

# Mitä toimenpiteitä vaatii yhdistykseltä?

Selvitä, miten organisaatiosi on huomioitava lasten erityisasema. Jatkossa lapsi tarvitsee huoltajan tai muun vanhempainvastuunkantajan suostumuksen tai valtuutuksen tietoyhteiskunnan palveluiden käyttöön.

Suomessa ikäraja ei ole vielä selvillä, mutta se tulee olemaan 13 ja 16 vuoden välillä. (Tilanne 12/2017.)

# Miten asiat pysyvät kunnossa jatkossa?

- Hyödynnä jäsenrekisterin ajantasaiset tiedot, kun tarvitsset esim. yhteystietoja ja tuhoa tiedot, kun tarve on ohi.
- Tietojen hävittämisen automatisointi
- Haasteita:
  - Kaikkien rekisteritietojen löytäminen luotettavasti eri järjestelmistä / sijainneista.
  - Tietojen poistaminen esim. taulukoista.

# Järjestelmät ja niiden ylläpitämät rekisterit

- Laiteympäristö, onko tietoturvallinen?
  - Yhteiskäyttö: miten käyttäjähallinta toteutettu?
- Tietojen kerääminen pitää perustua tarpeeseen ja sellaista tietoa ei pidä kerätä, jolle ei ole tarvetta
  - Jatkuva arviointi tarpeista
- Tietojen tuhoamiselle on oltava suunnitelma.
  - Pitää pystyä osoittamaan (viranomaiselle) miten prosessi on järjestetty.
- Tietojen tarkastusoikeuden huomioiminen.

# Miten selvitän, mitä pitää tehdä?

- **Kansallinen lainsäädäntö**
  - Käsittelyssä eduskunnassa
- **Tietosuojavaltuutetun www-sivut**
  - [www.tietosuoja.fi](http://www.tietosuoja.fi)
  - Ohjeita ja vastauksia yleisimpiin kysymyksiin.
- MLL:n **Yhdistysnettiin** tulee tiivis ohje, joka ottaa kantaa tavallisimpiin asioihin.
  - **Kerro mieleen tulevat huomiosi!**



# Vastuut ja seuraukset

- **Vahingonkorvausvastuu**
- **Hallinnolliset sakot**
- **Huomautus / korjausvelvollisuus**

# Tietosuoja haltuun!



MANNERHEIMIN  
LASTENSUOJELULIITTO

