# Opiskelijajärjestö & GDPR

AYY:n yhdistyskoulutus 27.11.2018

Liisa Lähteenaho

**GDPR:n tavoitteena on parantaa luonnollisten henkilöiden oikeusturvaa henkilötietojen käsittelyn osalta.**

# Mikä GDPR?

- GDPR = yleinen EU:n tietosuoja-asetus (General Data Protection Regulation)
- Alettiin soveltaa 25.5.2018 alkaen
- Asetus koskee yrityksiä, julkishallintoa, **yhdistyksiä,** urheiluseuroja ja muita järjestötoimijoita
- Suomessa asetusta täydentää marraskuussa 2018 hyväksytty uusi tietosuojalaki

# GDPR:n keskeiset periaatteet

Ei tehtävälista,
vaan ajattelutavan muutos.

1. Oikeus tulla unohdetuksi
2. Tiedon saanti helpottuu
3. Oikeus saada tieto tietoturvaloukkauksesta
4. Sisäänrakennettu ja oletusarvoinen tietosuoja
5. Tiukemmat seuraamukset rikkomuksista

# Henkilötietojen käsittelyn periaatteet

(Asetuksessa määritellyt)

1. Tietosuojaperiaatteet
2. Suostumus
3. Oikeus tulla unohdetuksi

# Tietosuojaperiaatteet

Henkilötietoja on…

1. käsiteltävä lain mukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
2. käsiteltävä luottamuksellisesti ja turvallisesti
3. kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
4. kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
5. päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
6. säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten.

# Suostumus

- **“Suostumus on yksiselitteinen ja selkeä tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Rekisteröity ei voi antaa suostumustaan vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jotakin tekemättä.”**
- Käytännössä: Yhdistyksessä suostumus henkilötietojen käsittelyyn on kätevintä pyytää uuden jäsenen liittyessä yhdistykseen. Samalla voidaan pyytää paperisella tai sähköisellä lomakkeella suostumus muun muassa jäsenrekisteritietojen keräämiseen, sähköpostilistoille liittämiseen ja muihin tarkoituksiin.

# Oikeus tulla unohdetuksi

- **Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjä poistamaan kaikki itseään koskevat tiedot ilman aiheetonta viivytystä. Oikeus tunnetaan myös nimellä oikeus tulla unohdetuksi.**
- Muistakaa, että tätä oikeutta on kuitenkin rajoitettu! Säännökset, jotka koskevat oikeutta tulla unohdetuksi ovat hyvin selkeät: niissä suojataan ilmaisunvapaus sekä historiallinen ja tieteellinen tutkimus. Ennen henkilötietojen poistamista on siis hyvä miettiä, onko niillä kuitenkin vielä jokin, esimerkiksi sääntömääräinen tai historiankirjoitukseen liittyvä, tarkoitus.

# GDPR:n keskeiset käsitteet

1. Henkilötieto
2. Rekisterinpitäjä
3. Henkilötietojen käsittelijä
4. Tietosuojavastaava

**Kaikki tieto, jonka perusteella luonnollinen henkilö voidaan tunnistaa, on henkilötietoa.**

# 1. Henkilötieto (Personal Data)

**Tietosuoja-asetus ei yksityiskohtaisesti määrittele käsitettä henkilötieto, vaan asetuksen mukaan kaikki henkilöä yksilöivä tieto on henkilötietoa.**

Henkilötietoja ovat esimerkiksi nimi, kotiosoite, valokuva, sähköpostiosoite, sosiaalisen median päivitykset, tilaukset ja ostokset, pankkitiedot, käyttäjätunnus ja salasana, maksukortin numero sekä IP-osoite.

# 2. Rekisterinpitäjä (Data Controller)

**Rekisterinpitäjä on luonnollinen tai oikeushenkilö, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.**

Rekisterinpitäjä on juridisessa vastuussa rekisteristä, määrää rekisterin käytöstä sekä on taho, jonka käyttöä varten rekisteri on luotu.

# 3. Henkilötietojen käsittelijä (Data Processor)

**Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.**

Yhdistyksessä henkilötietojen käsittelijöitä ovat esimerkiksi hallituksen jäsenet ja virkailijat. Joissakin tapauksissa henkilötietojen käsittelijäksi voidaan katsoa myös ulkoistetun palvelun ylläpitäjä, esimerkiksi Google (tapahtumien ilmoittautumislomakkeet) tai Yhdistysavain (jäsenrekisteripalvelu).

# 4. Tietosuojavastaava (Data Protection Officer)

Tietosuojavastaavan tehtäviin kuuluu toimia asiantuntijana ja yhteyshenkilönä tietosuojaan liittyvissä kysymyksissä.

# Pakolliset ja vapaaehtoiset dokumentit

1. Seloste henkilötietojen käsittelytoimista
2. Tietosuojaseloste
3. Tietotilinpäätös

# 1. Pakollinen: Seloste henkilötietojen käsittelytoimista

- **GDPR:n myötä organisaatioiden tulee laatia kirjallinen kuvaus henkilötietojen käsittelystä organisaatiossa. Tätä kuvausta kutsutaan selosteeksi käsittelytoimista.**
- Käsittelytoimia koskevaa selostetta ei ole tarkoitettu käytettäväksi suoraan rekisteröidyn informointiin, mutta sitä voidaan hyödyntää rekisteröidyille suunnatun informaation tuottamisessa.
- Selosteen laatiminen on pakollista tiettyjen edellytysten täyttyessä. Yksi pakollisuuden edellytys  on se, että henkilötietojen käsittely ei ole satunnaista. Yhdistykset käsittelevät henkilötietoja jatkuvasti, eivät satunnaisesti.
- Katso AYY:n malliasiakirja: Tietosuojapolitiikka

# Selosteen sisältö 1/2

- Rekisterinpitäjä
- Tietosuojavastaava
- Tietojen käsittelyn tarkoitus
- Henkilötietojen luovuttaminen ja siirtäminen
- Kuvaus teknisistä ja organisatorisista turvatoimista

# Selosteen sisältö 2/2

- Luettelo henkilörekistereistä ja kuvattuna jokaisen rekisterin ja dokumentin
  - Formaatti:
  - Henkilötietojen käsittelijä:
  - Käsittelyn tarkoitukset:
  - Rekisteröityjen ryhmät:
  - Henkilötietoryhmät:
  - Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin
  - Kuvaus turvatoimista:
  - Tietojen elinkaari:
  - Tietojen julkisuus:
  - Kehityskohteet:

# 2. Pakollinen: Tietosuojaseloste tai vastaava asiakirja

- **EU:n tietosuoja-asetus tai uusi tietosuojalaki eivät edellytä henkilörekisteri- tai tietosuojaselosteiden laatimista. Näiden sijaan tietosuoja-asetus säätää rekisterinpitäjän velvollisuudesta informoida rekisteröityjä henkilötietojen käsittelystä ja tallentamisesta.**
- Tästä aiheesta on ollut liikkeellä aika paljon sekavaa ja vaihtelevaa tietoa, koska GDPR:n soveltamisen alkaessa toukokuussa 2018 Suomessa oli vielä voimassa “vanha” henkilötietolaki. Laki on nyt kumottu, ja sen tilalle on tullut uusi tietosuojalaki.
- Katso AYY:n malliasiakirja: Tietosuojaseloste

# 3. Vapaaehtoinen: Tietotilinpäätös

- **Tietosuojavaltuutettu: “Tietotilinpäätöksen tavoitteena on antaa kuvaus tietojen käsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvan toteutumisesta.”**
- Vaikka tietotilinpäätös ei ole pakollinen, se on hyvä tehdä!
- Alkuun pääsee googlaamalla mallin yhdistyksen tietotilinpäätökseksi - homma on loppujen lopuksi pitkälti olemassa olevien henkilörekistereiden listaamista ja se auttaa pohtimaan riskejä, kehittämiskohteita, koulutustarpeita, yms.

# Kiitos!

Hyvin kirjoitettua lisätietoa Tietosuojavaltuutetun toimistolta:

https://tietosuoja.fi/organisaatiot

AYY:n materiaalit:

https://ayy.fi/yhdistykset/palvelut/koulutus-ja-kurssit/gdpr-asiat-kuntoon/