Yleinen tietosuoja-asetus (GDPR)

EU:n yleinen tietosuoja-asetuksen (GDPR) soveltaminen alkaa 25.5.2018. Tietosuoja-asetusta täydennetään ja täsmennetään kansallisella lainsäädännöllä. Uuden kansallisen tietosuojalain valmistelu on meneillään, ja se tullee voimaan samalla päivämäärällä kuin asetuksen soveltaminen alkaa.

Asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Asetusta noudatetaan aina, kun henkilötietoja käsitellään järjestön (sis. yhdistyksen) tai yrityksen tietojärjestelmissä tai manuaalisesti, esim. kortistossa.

Asetus koskee myös kaikkia siirtola- ja ryhmäpuutarhayhdistyksiä.

Käsitteitä

Henkilötieto

Kaikenlaiset tunnistettua tai tunnistettavissa olevaa henkilöä koskevat tiedot, jotka voidaan liittää häneen. Lyhyesti: jos tiedon perusteella voidaan tietää tai saada selville, kenestä on kyse, tieto on henkilötieto.
Esimerkki: Kaikki yhdistyksen jäseneen liittyvät tiedot. Jäsenrekisterissä olevan tiedon lisäksi henkilötietoja ovat myös esim. talkoo-/yhteisötyöhön osallistumisen seuranta, listat palkituista jäsenistä, tapahtumiin osallistuneet, …

Rekisterinpitäjä

Taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Henkilörekisteri perustetaan rekisterinpitäjän käyttöä varten ja ko. taholla on oikeus määrätä henkilörekisterin käytöstä.
Esimerkkejä: Siirtola- tai ryhmäpuutarhayhdistys; Siirtolapuutarhaliitto (mm. jäsenyhdistysten toimihenkilöiden osalta)

Käsittelijä

Taho, joka työskentelee rekisterinpitäjän lukuun ja jonka tehtäviin henkilötietojen käsittely kuuluu. Uuden asetuksen myötä vastuu kasvaa.
Esimerkkejä: yhdistyksen käyttämä tilitoimisto; Siirtolapuutarhaliitto lehden osoiterekisterin osalta

Käsittely

Toimintoja, joita kohdistetaan henkilötietoihin. Esim. tiedon kerääminen, tallentaminen, säilyttäminen, muokkaaminen, haut, kyselyt, luovuttaminen, yhdistämine, poistaminen, … aina kun henkilötietoja käytetään.

Suostumus

Mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu henkilötietojen käsittelyyn.

Mitä GDPR muuttaa?

1) Yksilölle enemmän oikeuksia tietoihinsa
   - Pääsy tietoihin, unohtaminen jne.
   - Oikeus saada avoimesti tietoa

2) Rekisterinpitäjälle uusia velvoitteita
   - Turvallisuus, informointi, tietojen minimointi jne.
   - Yhteispeli / vastuu kumppaneista
3) **Rekisterinpitäjällä osoitusvelvollisuus**
   - ”*Enää ei riitä, että sanoo noudattavansa lakeja*”
   - Osoitettava **dokumentoinnilla**
4) Laajemmat viranomaisvaltuudet
   - Saada tiedot, tarkastaa, varoittaa, rajoittaa, sakottaa, …
   - Maksimisanktiot ovat suuria
5) EU:lle yhtenäinen tietosuojakehys
   - Sama luottamus eri maiden toimijoihin
   - Digimarkkinoiden kehittyminen

Henkilötietojen käsittelyn arviointi

Asetus edellyttää, että henkilötietojen käsittelystä tehdään arviointi. Organisaation on hahmotettava kokonaiskuva henkilötietojen käsittelyn nykytilasta: Mitä henkilötietoja on? Miten ja missä yhteydessä kerätään henkilötietoja? Miten tietoturva on hoidettu? Miten riskienhallinta on hoidettu? → Mitä toimenpiteitä tietosuoja-asetuksen sääntely edellyttää?

Toimenpiteet on tehtävä ennen 25.5.2018.

Henkilötietojen käsittelyn periaatteita:

- Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys: Henkilötietojen käsittelyyn on laillinen peruste.
  Yhdistyksen tapauksessa tämä periaate toteutuu automaattisesti, koska yhdistyslaki velvoittaa hallitusta pitämään jäsenluetteloa.

- Käyttötarkoitussidonnaisuus: Tiedot kerätään tiettyä laillista käyttötarkoitusta varten. Tietoja ei saa käsitellä määriteltyjen tarkoitusten kanssa yhteensopimattomalla tavalla.

- Tietojen minimointi: Kerätyt tiedot ovat asianmukaisia ja olennaisia, sekä rajoittuvat siihen, mikä on tarpeen käyttötarkoituksen kannalta.

- Tietojen täsmällisyys

- Tietojen säilytyksen rajoittaminen – elinkaari.
  Tarkoittaa käytännössä esim. sitä, että yhdistyksestä eronneen jäsenen tiedot on hävitettävä tai että jotakin arvontaa tms. varten käytetyt tiedot hävitetään, kun arvonta on suoritettu.

Rekisterinpitäjällä on **osoitusvelvollisuus**. Todistustaakka siirtyy nyt selkeämmin rekisterinpitäjälle, jonka on pystyttävä osoittamaan, että periaatteita on noudatettu.

Sopimukset

Jos henkilötietojen käsittely tehdään jonkinlaisena yhteistyönä, pitää siitä olla kirjallinen sopimus. Sopimuksen sisällölle on asetettu vähimmäisvaatimukset.

Käytännössä tämä tarkoittaa sitä, että yhdistyksen ja Siirtolapuutarhaliiton välille on tehtävä kirjallinen sopimus jäsentietojen toimittamisesta Siirtolapuutarha-lehden postitusta varten. Liitto tekee myös oman kirjallisen sopimuksen painotalon kanssa.

Tietoturva

Rekisterinpitäjän ja henkilötietojen käsittelijän on ennen 25.5.2018 selvitettävä, vastaavatko tietojen suojaamista koskevat käytännöt ja toimenpiteet asetuksen sääntelyä. Rekisterinpitäjän on myös arvioitava riskit ja toimittava näiden riskien lieventämiseksi. Suojaaminen koskee henkilötietojen koko elinkaarta.

Yhdistyksissä on runsaasti tietosuojahaasteita. Esim. henkilöt vaihtuvat ja asiat tehdään kunkin tekijän parhaaksi katsomalla tavalla, henkilötiedot ovat dokumenteissa ja paperilla tai vanhoja jäsentietoja ei hävitetä (mapeissa on listat entisistäkin jäsenistä…).

Rekisteröidyn oikeudet

Tietosuojavaltuutetun määrittely:

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

Rekisterinpitäjällä on velvollisuus toteuttaa rekisteröidyn oikeuksia. Tämä on huomioitava prosessien ja tietojärjestelmien suunnittelussa. Lisäksi on varmistettava, että nykyiset prosessit ja tietojärjestelmät taipuvat muutoksiin.

Rekisteröidyllä on oikeus saada pääsy omiin tietoihinsa. Pyydettäessä rekisteröidylle tulee toimittaa **jäljennös häntä koskevista henkilötiedoista**, lähtökohtaisesti maksutta. Rekisteröidyn pitää esittää pyyntö aina kirjallisesti ja henkilökohtaisesti, mutta määrämuotoa pyynnölle ei ole. Rekisterinpitäjä voi pyytää lisätietoja, jotka ovat tarpeen esim. rekisteröidyn henkilöllisyyden vahvistamiseksi.

Rekisterinpitäjän on toimitettava **henkilötietojen käsittelyä koskevat tiedot** rekisteröidyille tiiviisti ja läpinäkyvästi sekä helposti ymmärrettävässä ja saatavassa muodossa. Tiedot on toimitettava ilman aiheetonta viivytystä – vähintään yhden kuukauden sisällä. Jos tiedot kerätään henkilöltä itseltään, tulee käsittelystä informoida **silloin**, kun tiedot kerätään.

Vahingonkorvaus

Vahinko syntyy, kun rekisteröidyn oikeusturva vaarantuu tai sitä on loukattu. Tästä esimerkkeinä, että tyytymätön jäsen valittaa tietosuojavaltuutetulle, että hän kokee oikeutensa rikotuksi tai että tietoja katoaa tai vuotaa ja ne ilmestyvät esiin väärässä paikassa.

Asetuksen soveltamisen alkamisen myötä tietosuojavaltuutetun toimiston rooli muuttuu neuvoa-antavasta viranomaisesta valvovaksi viranomaiseksi. Valvontaviranomainen voi määrätä hallinnollisia sakkoja rekisterinpitäjälle tai henkilötietojen käsittelijälle tietosuoja-asetuksen rikkomisesta. Hallinnollinen sakko voi olla enintään neljä prosenttia liikevaihdosta. Yhdistyksessä liikevaihtoon lasketaan varsinaisen toiminnan, varainhankinnan sekä sijoitus- ja rahoitustoiminnan tuotot.

Muita mahdollisia seuraamuksia ovat muun muassa varoitukset, huomautukset ja määräykset sekä henkilötietojen käsittelyn rajoittaminen ja kieltäminen.

Lähteet:

- Tietosuojavaltuutetun www-sivut (http://www.tietosuoja.fi/fi/)
- Lakimies Maarit Päivike: EU:n tietosuoja-asetus ja yhdistykset / Visio 31.1.2018
- Ismo Paananen: Tietosuoja järjestön näkökulmasta / webinaarin aineisto

Valmistaudu asetuksen soveltamisen alkamiseen 25.5.2018

Maarit Päivike

1. **Kartoita ja dokumentoi nykytilanne; sitouta toimihenkilöt**
    - Minkälaisia henkilötietoja käsitellään? Mistä tiedot on kerätty ja mihin niitä luovutetaan?
    - Käyttötarkoitus ja käsittelyn peruste → dokumentoi!
    - Selosteet, informointi ja rekisteröidyn oikeuksien toteutuminen
    - Henkilötiedon käsittelyt ulkoistussopimukset

    Mitä pitää **dokumentoida**:
        - Nykytilan arviointi
        - Riski- ja vaikutustenarviointi
        - Ohjeistus käsittelystä. Millä perusteella käsitellään, kuvaus teknisistä ja organisatorisista turvatoimista, miten periaatteet huomioitu?
        - Tietosuojaselosteet: rekisterissä saa olla vain tietoa, joka on etukäteen laaditun suunnitelman mukaista
        - Sopimukset päivitettävä vastaamaan asetuksen vaatimuksia

2. **Varmista yhdistyksesi osaaminen ja resurssit**
    - Vastuu tietosuojasta, tiedon omistajuus
    - Raportointi hallitukselle, henkilötietojen käsittelyn suunnittelu
    - Ohjeistukset, perehdytys ja koulutus, valvonta
    - Valvonta ja prosessi tietoturvaloukkausten ilmoittamiseen

3. **Varmista järjestelmähankintojen osalta, että henkilötietojen käsittely otetaan huomioon jo suunnitteluvaiheessa.**

4. **Seuraa viranomaisten ohjeistusta ja kansallisia muutoksia.**

GDPR kevätsiivous

Ismo Paananen

- Hävitä vanhentuneet tiedot, jotka eivät ole tarpeen
- Pohdi, onko jäljelle jääneiden tietojen käsittelyyn oikeusperuste, ja hävitä tarpeettomat tiedot
- Karsi tietojärjestelmät ja muut tallennuspaikat minimiin, panosta jäsenrekisterin ylläpitoon
- Selvitä kenen kaikkien täytyy päästä tietoihin käsiksi, ja rajaa käyttöoikeudet kunkin tarpeen mukaan
- Poista ylimääräiset käyttäjätunnukset ja katso, että paperit ovat lukkojen takana

Hyödyllisiä linkkejä

Tietosuojavaltuutetun toimiston EU:n tietosuojauudistus -sivut
http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietosuojavaltuutetun toimiston GDPR-ohjeita rekisterinpitäjille
http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle.html

Opas ’Miten valmistautua EU:n tietosuoja-asetukseen
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimiston Rekisteriseloste-sivu
http://www.tietosuoja.fi/fi/index/useinkysyttya/rekisteriseloste.html

Tietosuojavaltuutetun toimiston rekisteriselosteen mallilomakkeet
http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html

Toistaiseksi voimassa olevan lain mukainen opas ’Henkilörekisteriin talletettujen tietojen tarkastaminen’
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/dxJufFmwB/Henkilorekisteriin_talletettujen_tietojen_tarkastaminen_24.11.2014.pdf

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö
http://julkaisut.valtioneuvosto.fi/handle/10024/80098