Henkilötietojen käsittely 4H-yhdistyksissä

Uusi EU:n tietosuoja-asetus (GDPR) astuu voimaan 25.5.2018. Uusi asetus edellyttää toimia kaikilta henkilörekisterien pitäjiltä.

Uuden asetuksen tarkoituksena on parantaa henkilötietojen suojaa. Asetus ei välttämättä muuta kaikkea henkilötietojen käsittelyyn liittyvää eikä estä tarpeellisten tietojen käsittelyä. Tähänkin saakka rekistereitä on voinut ylläpitää yhdistyksen toiminnan toteuttamiseksi, henkilötietoja on pitänyt käsitellä huolellisesti ja rekistereistä on pitänyt laatia tietosuojaselosteet. Jatkossa yhdistysten on syytä suhtautua entistäkin huolellisemmin kaikkeen henkilötietojen käsittelyyn.

Tämä ohjeistus on tarkoitettu kaiken kokoisille ja erilaista toimintaa ylläpitäville yhdistyksille, joten osa ohjeista ei välttämättä koske jokaista yhdistystä. Lähtökohdat ja velvoitteet ovat kuitenkin samat aivan kaikille. Ohjetta päivitetään tarvittaessa tietosuojaa koskevien asioiden täsmentyessä.

Tietosuoja-asetuksen lähtökohtana on, että tietojen käsittelijät allekirjoittavat salassapitositoumuksen, jotta voidaan varmistua siitä, että kaikki henkilötietojen käsittelijät ymmärtävät tietojen huolellisen käsittelyn merkityksen ja sitoutuvat noudattamaan asiaa koskevia säännöksiä. Tämän ohjeen liitteenä 1on henkilötietojen salassapitoa koskeva sitoumus, joka on tarkoitettu kaikkien yhdistyksessä henkilötietoja käsittelevien henkilöiden allekirjoitettavaksi.

Henkilötietoja ovat kaikki tiedot, joista henkilö voidaan suoraan tai epäsuorasti tunnistaa tai jotka muuten liittyvät johonkin henkilöön. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, ikä, puhelinnumero, osoite, terveystiedot, kuva, pankkiyhteystiedot, tapahtumiin osallistumista koskevat tiedot yms.

Henkilörekisterejä ovat kaikki sähköiset tai muut listat ja materiaalit, myös käsin kirjoittaen ylläpidetyt, joissa henkilötietoja esiintyy.

Keskeisiä uuden lainsäädännön lähtökohtia ovat seuraavat:
1) Tietojen keräämiseen ja käsittelyyn pitää olla laillinen peruste.
2) Tarpeettomia tietoja ei saa kerätä eikä säilyttää pidempään kuin on tarvetta.
3) Tietoja saavat käsitellä vain ne, joilla on siihen tehtävänsä puolesta tarve
ja oikeus.
4) Tietoja tulee käsitellä ja säilyttää huolellisesti ja poistettavat tiedot tulee hävittää turvallisesti.
5) Tietoja ei tule luovuttaa tai saattaa ulkopuolisten tahojen haltuun, mikäli tietojen luovutukseen ei ole laillista perustetta.
6) Rekisteröidyillä on oikeus saada tieto siitä, mitä tietoja organisaatiolla on heistä eri rekis tereissä ja oikeus vaatia poistamaan tiedot, mikäli ne perustuvat hänen antamaansa suostumukseen.

Kuvaa ja ohjeista henkilötietojen käsittely ja käy ohjeet läpi toimijoiden kanssa!

Uuden lainsäädännön merkittävä muutos on se, että nyt jokaisen organisaation on pystyttävä omatoimisesti osoittamaan, että se on hoitanut kaikki lailliset velvoitteensa. Se edellyttää asioiden suunnittelua, dokumentointia ja sen kuvaamista, mitä henkilötietoja yhdistyksessä käsitellään ja minkä vuoksi, miten käsittely tehdään ja ketkä niitä käsittelevät.

Tämän vuoksi yhdistysten on syytä laatia henkilötietojen käsittelystä kuvaus, johon sisältyvät lisäksi ainakin

- Luettelo yhdistyksen rekistereistä
- Rekistereitä koskevat tietosuojaselosteet
- Sopimukset henkilötietoja käsittelevien ulkopuolisten palveluntuottajien kanssa
- Tietojen käsittelijöille annetut tietosuojaa koskevat ohjeet (tämä ohje ainakin)

Kuvauksen tulee olla kaikkien henkilötietoja käsittelevien saatavissa. Se auttaa myös henkilötietojen käsittelijöiden perehdytyksessä.

Tietosuojaan perehdytyksessä voi käyttää apuna tämän ohjeen lisäksi mm. useiden suomalaisten viranomaisten yhdessä laatimaa Arjen tietosuojaa -videota sekä siihen liittyvää aineistoa ja tietosuojatestiä, jotka löytyvät osoitteesta arjentietosuoja.fi.

Henkilötietojen käsittelyyn pitää aina olla laillinen peruste

Vähintään yhdenseuraavista edellytyksistä on täytyttävä, jotta henkilötietojen käsittely ja rekisteröinti on sallittua:

- Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.
    - Tämä lienee tärkein laillinen peruste erilaisten rekisterien pitämiseen.
    - Yhdistyksen taloudellinen tai toiminnallinen oikeutettu etu on rekisteröidä yhdistyslain määräämää laajemmin tietoja jäsenistään, hallituksen jäsenistä, vapaaehtoisista, yhteistyökumppaneista yms.
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi
    - Esim. yhdistyslaki velvoittaa pitämään jäsenluetteloa, veroasiat kirjanpito ja palkanlaskenta asettavat omat velvoitteensa
- Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä
    - Yhdistyksellä voi olla listoja sopimuskumppaneista ja heidän yhteyshenkilöistään.
- Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi

    - Jos yhdistyksellä on palkattuja työntekijöitä, se on oikeutettu käsittelemään esimerkiksi henkilön sairauslomatodistuksia, koska ne vaikuttavat palkanmaksuun sairausajalta, joka on henkilön (elintärkeä) etu.
- Rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
    - Jäsenrekisterin osalta kysytään sinänsä oikeutettuja tietoja ja lisäksi kysytään suostumusta siihen, saako tietoja luovuttaa ulkopuolisille esim. kaupallisiin tarkoituksiin. Sisäiseen viestintään yhdistyksillä on oikeus käyttää jäsenistönsä osoitetietoja, mutta tätä osoitteistoa ei saa osoiterekisterinä jakaa tarpeettomasti eikä ulkopuolisille.
- Mikäli tiedon kerääminen ei perustu muihin oikeuttamisperusteisiin, tarvitaan henkilöltä suostumus tietojen keräämiseksi. Suostumus tulee aina pyytää kirjallisesti ja sen tulee olla nimenomaisesti annettu.
    - Suostumukseen perustuvat tiedot on aina poistettava henkilön pyynnöstä.
    - Henkilötietojen luovuttaminen kolmannelle taholle edellyttää aina suostumusta (paitsi verotiedot tai muut viranomaisille annettavat tiedot)

Selvitä yhdistyksen henkilörekisterit

Henkilörekisterit voidaan jakaa eri ryhmiin seuraavasti:

- *Sähköisiin rekistereihin* kuuluvat kaikki jäsenrekisterit, kirjanpito-ohjelmat, valokuva-arkistot yms. Nämä on yleensä helppo tunnistaa.
- *Manuaalisia rekistereitä* ovat kaikki paperiarkistot ja tulostetut henkilölistat. Tämmöisiä rekistereitä on yleensä useita pienilläkin organisaatioilla.
- "Piilorekisterit" ovat esimerkiksi sähköposteissa olevat henkilölistaukset ja omat excel-taulukot (tietokoneella tai paperilla). Näitä arkisia listoja on eri organisaatioissa useimmiten iso määrä eri henkilöillä. Niidenkin tunnistaminen henkilörekistereiksi on tärkeää, jotta myös niiden osalta noudatetaan tarpeellista huolellisuutta.

Yhdistyksen on syytä listata ja kuvata

- Mitä sellaisia rekistereitä yhdistyksessä on, mistä henkilö on tunnistettavissa
- Miten tiedot on kerätty
- Miten niitä säilytetään
- Miten huolehditaan tietojen oikeellisuudesta (ajantasaisuus)
- kuka niihin pääsee käsiksi
- Luovutetaanko tietoja ja jos, mihin
- Onko tiedon keräämiseen oikeat perusteet
- Kuinka kauan rekistereitä ja niissä olevia tietoja säilytetään
- Miten tiedot poistetaan
- Miten huolehditaan tietoihin liittyvästä tietoturvasta
- Kenelle osoitetaan yhdistykselle mahdollisesti tulevat henkilöiden rekisteritietoja koskevat selvityspyynnöt, korjauspyynnöt ja tietojen poistopyynnöt ja kuka päättää tietojen luovuttamisesta ja poistamisesta.

Siivoa

Yhdistys saa kerätä vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen eli yhdistyksen toiminnan kannalta. Kaikki tarpeettomat rekisterit ja niissä olevat tarpeettomat ja vanhentuneet tiedot tulee poistaa ja hävittää turvallisesti. Papereille olevia jäsenrekisteritulosteita tai muita listoja ei saa laittaa paperinkeräykseen tai muuhun yleiseen jätekeräykseen.

Mitä arkaluontoisempi jokin tieto on, sitä painavampi peruste tarvitaan sen keräämiseen ja säilyttämiseen.

Esimerkiksi henkilötunnuksia tarvitaan vain hyvin harvoin yhdistystoiminnassa. Niitä tarvitaan nimenkirjoittajia ja tilinkäyttöoikeuksia koskeviin ilmoituksiin sekä mahdollisten palkkojen, palkkioiden tai korvausten maksamiseen.

Henkilötunnuksia ei pidä koskaan kerätä tarpeettomasti ja vanhoissa rekistereissä olevat tarpeettomat henkilötunnukset on poistettava.

Käsittele tietoja huolellisesti ja säilytä tiedot turvallisesti

Tietosuojan riskit jaetaan usein kolmeen kategoriaan; teknisiin, inhimillisiin ja fyysisiin riskeihin.

- *Inhimilliset riskit* eli henkilöiden huolimattomuus ja osaamattomuus ovat käytännössä suurimmat vaarat. Tästä syystä on tärkeää, että jokainen yhdistyksessä henkilötietoja käsittelevä on perehtynyt tietosuojaan ja käsittelee henkilörekisterejä ja henkilötietoja huolellisesti ja velvoitteiden mukaisesti. Ja huolehtii näistä velvoitteistaan myös kotioloissa.
- *Teknisiin riskeihin* kuuluvat laitteisiin ja järjestelmiin, tietoyhteyksiin sekä näihin kuuluviin salasanoihin kuuluvat riskit.
- *Fyysiset riskit* eli murtautumiset ja arkistojen säilytys ja tuhoaminen.

Uuden asetuksen mukaan tietoihin pääsy tulee rajoittaa ainoastaan niille henkilöille, joilla on siihen perusteltu syy. Paperit siis säilytetään lukitussa paikassa ja tiedostot suojattuina tietokoneilla tai palvelimilla käyttäjän henkilökohtaisen salasanan takana.

Yhdistyksen tulee päättää ja kirjata, keillä henkilöillä on oikeus käsitellä henkilörekisterien tietoja. Näiden henkilöiden tulee allekirjoittaa ***salassapitositoumus*** *(ohjeen viimeinen sivu).*

Koska hallitus hyväksyy uudet jäsenet, toteaa mm. jäsenmaksun laiminlyöneet eronneiksi ja vastaa jäsenrekisterin oikeellisuudesta, hallituksen jäsenillä on oikeus saada jäsenluettelotiedot, vaikka eivät kaikki varsinaisesti hoidakaan rekisteriasioita.

Mikäli tietoihin kohdistuu tietoturvaloukkaus eli tietoja tuhoutuu tai niitä pääsee asiattomien haltuun, asiasta tulee tehdä viranomaisille ilmoitus. Mikäli loukkauksesta ei todennäköisesti

aiheudu rekisteröidyn oikeuksiin tai vapauksiin kohdistuvaa riskiä, ilmoitusta ei kuitenkaan tarvitse tehdä.

Vaikka tarjolla on monenlaisia pilvipalveluita, viimeinen varmistus yhdistyksen tärkeistä tiedostoista olisi hyvä tehdä vielä jollekin ulkoiselle, ei verkossa olevalle muistille (muistitikulle tai -levylle).

Tee yhdistyksen rekistereistä tietosuojaselosteet

Tietosuojaselosteesta rekisteröity henkilö näkee, miten hänen henkilötietojaan käsitellään ja millaisia oikeuksia hänellä on. Aina kun henkilötietoja pyydetään näiden rekisteriä koskevien tietojen pitää olla henkilön saatavilla. Mikäli tietoja kerätään verkossa, tietosuojaselosteen pitää olla saatavilla samassa paikassa, missä tietoja pyydetään esimerkiksi linkkinä verkkosivuilla.

Lähtökohtaisesti jokaisesta rekisteristä pitää tehdä oma rekisteriselosteensa. Mikäli tiedot ovat samassa paikassa (mapissa, taulukossa, listassa) tai ne voidaan muutoin ymmärtää yhdeksi rekisteriksi, niistä voidaan laatia yksi yhteinen tietosuojaseloste, vaikka tietoja käytettäisiinkin useampaan eri tarkoitukseen.

Tietosuojaselosteeseen tarvitaan seuraavat tiedot:

- Rekisterinpitäjä (tämä tarkoittaa rekisterinpitäjää, ei sen teknistä ylläpitäjää)
- Yhteyshenkilö
- Rekisterin nimi
- Tietojen käsittelyn tarkoitus (miksi tieto kerätään)
- Rekisterin tietosisältö
- Säännönmukaiset tietolähteet
- Tietojen säännönmukaiset luovutukset / ketkä pääsevät käsittelemään tietoja
- Tietojen siirto EU / ETA –alueen ulkopuolelle
- Rekisterin suojauksen periaatteet
- Tarkastusoikeus
- Tieto siitä, että rekisteröidyllä on oikeus vaatia tietojen korjausta
- Muut henkilötietojen käsittelyyn liittyvät rekisteröidyn oikeudet

Tietosuojaselosteen perusmalli on liitteenä 2.

Tee sopimukset tietojen käsittelijöiden kanssa

Jos jokin ulkopuolinen taho tuottaa henkilötietojen käsittelyyn liittyviä palveluita, kyseisen tahon kanssa tulee tehdä sopimus, jossa määritellään henkilötietojen käsittelyyn liittyvät molempien osapuolten velvoitteet.

4H-yhdistyksillä voi olla muitakin palvelusopimuksia koskien sellaisia palveluita, joissa käsitellään henkilötietoja. Tällaisia voi olla esim. nettisivujen tai vastaavien palvelutoimittajien

kanssa tehdyt sopimukset (esim. Yhdistysavain), jotka sisältäessään jäsensivuominaisuuksia ja mahdollisuuden lähettää kaikille jäsenille massajakeluja sisältävät vähintään jäsenten nimi- ja sähköpostiosoitetiedot.

Yhdistyksen on hyvä tiedustella ja edellyttää käyttämiltään palvelutuottajilta tällaista sopimusta (lisäliitettä vanhaa sopimukseen). Nämä liitteet ovat useimmiten niin pitkiä, että niitä ei kannata ruveta itse tekemään.

Jäsenille tiedottaminen ja markkinointi

Jäsenille tiedottaminen yhdistyksen tapahtumista ja toiminnasta on sallittua edelleenkin. Tietosuojaselosteessa tulee todeta, että henkilön osoitetietoja käytetään yhdistyksen viestintään.

Sähköposteja lähetettäessä osoitteet on aina piilotettava ellei esimerkiksi hallituksen tai muun pienen ryhmän osalta ole toisin sovittu.

Suoramarkkinointiin tulee aina olla henkilön ennakkosuostumus. Suostumus tulee pyytää kirjallisesti ja sen on oltava vapaaehtoinen, yksilöity ja yksiselitteinen. Suostumusta ei voi antaa vaikenemalla tai valmiiksi rastitetuilla ruuduilla.

Suostumus pitää pystyä myös peruuttamaan milloin tahansa. Takautuvasti suostumuksia ei tarvitse pyytää, mutta kaikilla on oltava mahdollisuus poistaa suoramarkkinointilupa milloin vain.

Tietojen tarkastaminen, korjaaminen ja niiden poistaminen

Rekisteröidyillä on oikeus saada tietää ja tarkastaa häntä koskevat rekisteritiedot. Tietosuoja-asetuksen mukaan rekisterin pitäjän tulee tätä varten pystyä pyynnöstä antamaan henkilölle tiedot siitä, mitä tietoja hänestä on kerätty ja miten tietoa on käsitelty.

Henkilöllä on vaatia, että häntä koskevat tiedot korjataan, mikäli niissä on virheitä.

Henkilöllä on oikeus kieltää tietojensa käyttö ja voi hän pyytää halutessaan, että häntä koskevat tiedot poistetaan. Tämä tarkoittaa sellaisia tietoja, joiden kerääminen perustuu henkilön suostumukseen (esim. suoramarkkinointikielto).

Tietoja ei koskaan saa luovuttaa ilman, että kysyjä on tunnistettu. Puhelimitse tai sähköpostitse tulleiden pyyntöjen perusteella tietoja ei siis voi luovuttaa, jos luovuttaja ei varmuudella tunnista henkilöä.

Lisätietoja

Viranomaisten laatima Arjen tietosuojaa -video tukimateriaaleineen sekä siihen liittyvä tietosuojatesti löytyvät osoitteesta arjentietosuoja.fi.

EU on laatinut tammikuussa 2018 tietosuojasta oman tiedotteen, joka löytyy osoitteesta: https://ec.europa.eu/finland/sites/finland/files/eujus15a-1631-i01_-_data_protection_infographic_-_infographie_fi-v03_lr.pdf.

Tietosuojavaltuutetun toimistolla on runsaasti tietosuoja-asetukseen ja tietosuojaan liittyvää ja varmasti vielä täydentyvää aineistoa, jota löytyy osoitteesta: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html.