GDPR – Tietosuoja-asetus

Toukokuun 25. päivä astuu voimaan uusi EU:n laajuinen tietosuoja-asetus – General Data Protection Act, tai ”GDPR”. GDPR korvaa aiemman ruotsalaisen henkilötietolain (personuppgiftslagen, ”PUL”). Monet periaatteet säilyvät ennallaan, mutta GDPR tuo myös uusia tietosuojaa ja henkilötietojen käsittelyä koskevia velvoitteita, joihin muun muassa seurojen on valmistauduttava.

Julkaisemme lähiaikoina RSKL:n kotisivulle lisätietoja asiasta.

Keskeiset käsitteet:

Henkilötieto: Kaikki sellainen tieto, jolla voidaan tunnistaa ja yksilöidä elossa olevia henkilöitä.

- Esim. nimi, osoite, henkilötunnus, sähköpostiosoite, verkkotunnistetiedot, tiedot perheenjäsenistä, valokuvat jne.

Henkilörekisteri: Henkilötietoja sisältävä jäsennelty tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta.

- Esim. RSKL:n tai seurojen jäsenrekisterit ja sähköpostilistat.

Rekisteröity: Rekisterissä oleva tunnistettava tai tunnistettavissa oleva henkilö.

Rekisterinpitäjä: Henkilö, yhteisö, virasto, säätiö tai joku muu, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä.

- Esim. RSKL tai jäsenyhdistys/-seura.

Henkilötietojen käsittelijä: Henkilö, viranomainen, virasto tai joku muu, joka käsittelee henkilötietoja rekisterinpitäjän lukuun, esimerkiksi uutiskirjetyökalun toimittaja.

GDPR lyhyesti

Henkilötietojen käsittelyn on oltava asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Tallennustavalla ei ole merkitystä. Tämä tarkoittaa, että GDPR kattaa kaikki henkilötiedot riippumatta siitä, onko tallennettu rakenteellisena tietokantaan, Word-dokumentissa tai sähköpostissa, tai vaikka tulostettuna paperille.

Lähtökohtana on, että henkilötietojen käsittely on sallittua vain, jos on laista löytyvä peruste tai jos rekisteröity on antanut suostumuksensa. Henkilölle on ilmoitettava siitä, mihin hän suostuu. Yhdistyksen on kyettävä osoittamaan, että suostumus on annettu.
Olemassa olevilta jäseniltä ei tarvitse kerätä ”uutta” suostumusta, kunhan PUL-sääntöjä on seurattu, kun jäsenyys rekisteröitiin ensimmäisen kerran. Jäsen voi milloin tahansa peruuttaa suostumuksensa, ja hänellä on oikeus saada itseään koskevat henkilötiedot poistettua.

(Henkilöllä ei ole oikeutta vaatia henkilötietojen poistamista, jos yhdistyksen käsittely perustuu lakiin, esim. arkistointia koskevissa asioissa.)

Jos seura/yhdistys haluaa käsitellä tietoja toisessa toiminnassa tai jos tietoja on luovutettava kolmansille osapuolille, rekisteröidyltä on oltava nimenomainen suostumus. Tämä voi koskea esimerkiksi tiettyjä yhdistyksen tietoviestejä. Muista, että myös kuva on henkilötieto. Keskeistä ja uutta tietosuoja-asetuksessa on muun muassa riskiperusteinen lähestymistapa ja rekisterinpitäjän osoitusvelvollisuus. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeimpia riskejä henkilötietojen käsittelyyn liittyy. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuoja-asetusta on noudatettu. Henkilötietojen käsittely on suunniteltava ja dokumentoitava.

Jos kyseessä on tietoturvahäiriö, esim. vahingossa tapahtuneesta tietojen menetyksestä, on ilmoitettava se tietosuojaviranomaiselle (Datainspektionen) 72. tunnin kuluessa. Tällaisessa tilanteessa sinun on myös ilmoitettava jäsenille, ja ryhdyttävä toimiin estääkseen samanlaiset tapaukset.
Tietosuoja-asetuksen rikkomisesta voi seurata muun muassa sakkoja tai henkilötietojen käsittelykielto.

Miten valmistautua tietosuoja-asetukseen?

Yhdistysten tulee käsitellä GDPR johtokunnassa ja tehdä toimintasuunnitelma. Seuran/yhdistyksen hallitus on vastuussa sääntöjen mukaisesta henkilötietojen käsittelystä yhdistyksessä.

Toimenpiteet:

- Selvitä, miten seurassa käsitellään henkilötietoja. Käy läpi kaikki henkilötietojen käsittelyn vaiheet: kerääminen, tallentaminen, hallinto, hävittäminen jne. Dokumentoi vaiheet.

- Selvitä, miksi henkilötietoja käsitellään, eli millä perusteella seura käsittelee niitä. Henkilötietojen käsittelylle on aina oltava laista löytyvä peruste. Esim. jäsenrekisterin ylläpitäminen perustuu jäsenen ja seuran väliseen sopimukseen jäsenyydestä. Henkilötietoja ei saa käyttää toisiin tarkoituksiin, ellei ole olemassa laillista perustetta (esim. arkistointia koskevat lait) tai henkilön suostumusta. Tästä seuraa myös, että jos jäsenyys loppuu, niin henkilötiedot on poistettava.

- Selvitä, miten seuran on huomioitava lasten erityisasema: lapsi tarvitsee huoltajan tai muun vanhempainvastuunkantajan suostumuksen tai valtuutuksen tietoyhteiskunnan palveluiden käyttöön.

- Arvioi, millaisia riskejä henkilötietojen käsittelyyn liittyy. Selvitä, miten riskejä voitaisiin minimoida. Huolehdi tietoturvasta.

- Valmistaudu ilmoittamaan henkilötietojen tietoturvaloukkauksista.

Tietosuojaperiaatteiden noudattaminen

On huolehdittava siitä, että tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.

Henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- henkilötietoja ei pidä säilyttää pidempään kuin hoitoa varten tarvitaan.