EU:n tietosuoja-asetus

GDPR – Mitä se on?

- General Data Protection Regulation – Yleinen tietosuoja-asetus
- EU-parlamentin ja Neuvoston asetus 2016/679 annettu 27.4.2016, toimeenpano alkaa toukokuussa 2018 (25.5.2018).
  - Korvaa kansalliset ja aikaisemmat eurooppalaiset lainsäädännöt
  - Ei vaadi/edellytä kansallisten hallitusten antamaa lainsäädäntöä
- Henkilötietojen käsittelyn tulee olla tietosuoja-asetuksen mukaista.
- Asetuksella säädellään mm. henkilötietojen keräämistä, käsittelyä ja luovuttamista sekä näihin liittyviä oikeuksia ja velvollisuuksia.
- Asetuksesta seuraa rekisterinpitäjille ja henkilötietoja käsitteleville tahoille uusia velvollisuuksia ja vastuita. Tulevia uudistuksia ovat muun muassa rekisteröityjen oikeuksien vahvistuminen, riskiperusteinen lähestymistapa, tietoturvaloukkauksista ilmoittaminen ja rekisterinpitäjälle asetettu tilivelvollisuus sekä merkittävät hallinnolliset sakot.
- Ei sovelleta henkilökohtaisessa tai kotitalouskohtaisessa toiminnassa

Tietosuojalaki

- Hallituksen esitys uudeksi tietosuojalaiksi henkilötietojen käsittelyä koskevaksi yleislaiksi.
  - Täydentää ja täsmentää tietosuoja-asetusta. Ehdotettu tietosuojalaki ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain EU:n tietosuoja-asetuksen kanssa.
- Esitys tietosuojalaiksi on annettu 1.3.2018.

Dokumentin tietosisältö

Tässä dokumentissa kuvataan tietosuoja-asetusta ja siihen liittyviä asioita ainoastaan klubin sisäisen toiminnan näkökulmasta.

Suomen Lions-liitto ry:n jäsenrekisteriin ja LCI:n kansainvälisen jäsenrekisteriin liittyvät asiakohdat ovat kuvattuja erillisissä dokumenteissa.

Käytännön toimenpideluettelo klubeille

Klubin tietosuojaprojekti

1. Mitä henkilötietoja jäsenrekisterin lisäksi klubissasi on (sekä paperiset että atk-järjestelmät)
2. Mistä tiedot saadaan tai kerätään
3. Miten ja missä niitä käsitellään
4. Mitä henkilörekistereitä klubissa on (huomioi kaikki mahdollinen)
5. Mitä henkilötietoryhmiä klubissa on
6. Millä perusteella henkilötietoja käsitellään
7. Mitkä ovat riskit henkilötietojen käsittelyssä
8. Miten noudatetaan asetuksessa määriteltyjä rekisteröityjen oikeuksia
9. Miten tietoturvasta huolehditaan nyt ja asetuksen voimaantulon jälkeen
10. Mitä toimeksiantoja ja sopimuksia ulkopuolisten kanssa tarvitaan
    a. Tilitoimistot, ilmoitusmyyntipalvelut, tuotteiden markkinointipalvelut
11. Dokumentoi toimenpiteet
    a. Tietosuojaseloste, mahdolliset ilmoitukset rekisteröidylle, ympäristön ja järjestelmien tietoturva, käyttäjien tietoturvaohjeet, klubin vastuuhenkilöt

GDPR sanastoa

Henkilötieto

Henkilötietoa on kaikki luonnolliseen henkilöön liittyvä tieto, josta henkilö on tunnistettavissa, kuten nimi, puhelinnumero, sähköpostiosoite tai valokuva.

Henkilötietojen käsittely

Henkilötietojen käsittelyä ovat mm. tiedon kerääminen, tallentaminen, säilyttäminen ja hakeminen.
Käsittelyä ei rajoiteta sen sijaintiin, joten se voi kohdistua niin tietokantaan kuin paperiarkistoon.

Henkilötietojen käsittelyä on myös tietojen luovuttaminen tai sen asettaminen muutoin saataville.

Rekisteri

Mikä tahansa henkilötietoja sisältävä jäsennelty tietojoukko, josta määrätyin perustein henkilötiedot ovat saatavilla.

Rekisteri voi olla hajautettu fyysisesti eri tietokoneille eri palveluntuottajilla.

Se voi olla paperilla, Excel tiedostoissa tai tiettyyn asiaan kehitetty ohjelmisto

Rekisterinpitäjä

Klubi, joka säilyttää henkilötietoja ja jolla on oikeus määrätä henkilörekisterin käytöstä.

Rekisterinpitäjä vastaa, että tietoja käsitellään asetuksen mukaisesti.
Klubi on rekisterinpitäjän asemassa myös jäsentietojensa osalta.

Rekisteröity

Henkilö, jonka tietoja on tallennettu rekisteriin.
Rekisteröity voi olla klubin jäsen tai kuka tahansa henkilö, jonka tietoja klubi rekisteröi tietosuojaselosteessa määriteltyyn tarkoitukseen.

Henkilötietojen käsittelijä

Suomen Lions-liitto ja LCI, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun.

Esimerkkejä muista henkilötietojen käsittelijästä klubin näkökulmasta:

- Klubi siirtää jäsentietoja esim. laskutuksesta vastaavalle taholle, henkilötiedot siirtyvät henkilötietojen käsittelijälle (palveluntarjoaja, joka käsittelee henkilötietoja rekisterinpitäjän toimesta).
- Klubi julkaisee kunnan/tietyn alueen asukkaiden yhteystietoja sisältävää palvelukalenteria ja on ulkoistanut julkaisin taiton, henkilötiedot siirtyvät henkilötietojen käsittelijälle.

Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyssä on noudatettava tietosuojaperiaatteita. Tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla. Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Henkilötietojen on oltava rekisterin käyttötarkoituksen kannalta asianmukaisia, olennaisia ja tarpeellisia.

Henkilötietojen käsittelyssä on varmistettava turvallisuus. Tiedot on suojattava luvattomalta ja lainvastaiselta käsittelyltä. Rekisterinpitäjän on varmistettava, että tiedot eivät häviä, tuhoudu tai vahingoitu vahingossa. Suojaamisessa on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

Rekisterinpitäjä vastaa siitä, että henkilötietojen käsittelyn periaatteita on noudatettu. Tarpeen vaatiessa hänen on pystyttävä osoittamaan se. Näyttönä voi toimia dokumentaatio, kuten selosteet, ohjeet ja sopimukset.

Kuusi perustetta henkilötietojen käsittelyyn

Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy.

1. Suostumus (ei kuvattu tässä dokumentissa)
2. Oikeutettu etu (ei kuvattu tässä dokumentissa)
3. Sopimus
4. Lakisääteinen velvoite (ei kuvattu tässä dokumentissa)
5. Elintärkeä tai yleinen etu (ei kuvattu tässä dokumentissa)
6. Julkinen tehtävä (ei kuvattu tässä dokumentissa)

Sopimus

Henkilötietojen käsittely on lainmukaista, kun se on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena.

Henkilötiedon käsittely sopimuksen täytäntöön panemiseksi tarkoittaa käytännössä esimerkiksi klubille annetun osoitteen käyttämistä, jotta klubin tuottama julkaisu voidaan toimittaa rekisteröidylle tai puhelinnumeron julkaisemin klubin julkaisemassa palveluhakemistossa.

Klubin www-sivuilla julkaistavista henkilötiedoista tulee klubissa laatia sopimus menettelytavoista.

- Suositus on, että klubin jäsenten yhteystiedot ovat klubin salasanalla suojatussa jäsenosiossa.
- Mikäli klubi haluaa julkaista kaikkien jäsenten yhteystiedot www-sivujensa julkisella alueella, tulee klubin pyytää suostumus kaikilta klubin jäseniltä.
- Klubi voi kirjata oman sisäisen jäsenrekisterinsä tietosuojaselosteeseen, että julkisella alueella ovat esim. presidentin, sihteerin, jäsenjohtajan ja palvelujohtajan puhelinnumero ja sähköpostiosoite.
- Mikäli jäsen ottaa vastaan piirin tai Suomen Lions-liiton tehtävän, hän samalla antaa suostumuksen siihen, että nimi, puhelinnumero ja lions.fi osoite julkaistaan piirin ja liiton sähköisissä sekä paperisissa julkaisuissa.
  - Tähän liittyvät määritelmät on kirjattu Suomen Lions-liitto ry:n tietosuoja-asetus dokumentaatioon.

Kun tietoa kerätään rekisteröidyltä

Henkilötietojen käsittelyn tulee olla läpinäkyvää, ja rekisteröidyille tulee kertoa, kuinka heitä koskevia tietoja kerätään ja kuinka niitä käytetään. Tiedot tulee antaa tiiviisti, yksinkertaisella ja selkeällä kielellä. Rekisteröityjen tulee saada tiedot maksutta.

Klubin tulee pitää kuvaus henkilötietojen käsittelystä rekisteröidyn saatavilla. Asetuksen mukaan tiedot tulee toimittaa kirjallisesti, suullisesti tai sähköisesti.

Erilaisissa tapahtumissa järjestettävästä arvontaan osallistumisesta ja henkilötietojen käsittelystä voidaan kertoa näyttämällä pyydettäessä rekisteröitävälle dokumentti, jossa kuvaillaan henkilötietojen käyttöä.
Dokumentti tarvitaan, jos arvonnassa kerätään rekisteröitävän henkilötietoja.

Henkilötietojen käyttö muuhun tarkoitukseen

Pääsääntö on, että klubi ei saa käsitellä henkilötietoja muuhun, kuin tietosuojaselosteessa mainittuihin tarkoituksiin.
Mikäli tietoja suunnitellaan käytettävän muihin tarkoituksiin, tulee klubin perehtyä tietosuoja-asetuksen määrittelyihin.

Tietosuojaseloste – Seloste käsittelytoimista

Tietosuoja-asetus velvoittaa klubin tekemään selosteen käsittelytoimista. Tätä tulee pitää yleisesti saatavilla esimerkiksi klubin www-sivuilla.

Klubin tulee tehdä jokaisesta rekisteristä oma seloste käsittelytoimista. Tällaisia rekistereitä ovat sisäinen jäsenrekisteri klubin omaan käyttöön, klubin paikkakunnan palveluhakemistoa varten keräämä asiakasrekisteri tai muu vastaava henkilötietoja sisältävä rekisteri.

Tietosuojaselosteen tietosisältö

- Rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan tai yhteyshenkilön nimi ja yhteystiedot
- Käsittelyn tarkoitukset
- Kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- Henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan (pääsääntöisesti klubi ei saa luovuttaa rekisteröityjen tietoja ulkopuolisille)
- Tietojen poistamisen suunnitellut määräajat
- Mahdollisuuksien mukaan yleinen kuvaus käsittelyn turvallisuuden varmistamiseksi toteutetuista teknisistä ja organisatorisista turvatoimista.

Tietojenkäsittelyn ulkoistaminen

Rekisterinpitäjä voi ulkoistaa henkilötietojen käsittelyn. Ulkoistettuja palveluita ovat esimerkiksi:
- Tilitoimisto, jos esim. hoitaa klubimaksujen laskutuksen tai laskujen suorituksen valvontaa
- Painotalo, jolle klubi on ulkoistanut palveluhakemiston taiton.

Henkilötietojen katsotaan siirtyvän henkilötietojen käsittelijälle eli palveluntarjoajalle, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka huolehtivat asianmukaisista suojatoimista ja varmistavat, että käsittely täyttää tietosuoja-asetuksen vaatimukset. Näin varmistetaan rekisteröidyn oikeuksien suojelu.

Klubin tulee ohjeistaa henkilötietojen käsittelijänä toimivaa palveluntarjoajaa. Ohjeet tulisi antaa kirjallisina ja ovat osa niin sanottua tietojenkäsittelysopimusta, jossa määritetään sekä rekisterinpitäjän että henkilötietojen käsittelijän oikeudet ja velvollisuudet suhteessa käsiteltäviin henkilötietoihin.

Käsittelyn turvallisuus

Rekisterinpitäjän ja henkilötietojen käsittelijän on asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä varmistettava, että käsittelyn turvallisuustaso vastaa riskiä.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin. Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että jokainen, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena siirrettyjä, tallennettuja tai muuten käsiteltyjä henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää tai muuttuu. Tietoturvaloukkaukseksi katsotaan myös tietojen luvaton luovuttaminen sekä luvaton pääsy tietoihin.

Tietosuojaloukkauksesta ilmoittaminen Suomen Lions-liitolle

- Lions-liitossa on päätetty, että klubin on ilmoitettava henkilötietojen tietosuojaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 24 tunnin kuluessa sen ilmitulosta Lions-liitolle. Lions-liitto vastaa tietosuojaloukkauksen informoimisesta eteenpäin.

- Näin ei kuitenkaan tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä henkilöiden oikeuksille ja vapauksille.

- Kun henkilötietojen käsittelijä saa tietää henkilötietojen tietoturvaloukkauksesta, hänen on ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä.

Tietosuojaloukkauksen dokumentointi

- Rekisterinpitäjän (klubin) on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, niiden vaikutukset sekä korjaavat toimet.