

EU:N UUSI TIETOSUOJA- ASETUS (GDPR)

Suomen Karateliitto ry

Opas seuroille

2.5.2018

- ▶ EU:n uusi tietosuoja-asetus, jonka tavoitteena on lisätä henkilötietojen käsittelyn avoimutta ja läpinäkyvyyttä. Sillä halutaan vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä.
- ▶ Mikä muuttuu?
 - ▶ Rekisterinpitäjän osoitusvelvollisuus – dokumentointi entistäkin tärkeämpi
 - ▶ Rekisteröidyn oikeudet – erityisesti unohdetuksi tuleminen
 - ▶ Turvallisuuskulttuuri – riskiperusteinen lähestymistapa
 - ▶ Yksityisyyden suojan kunnioitus
 - ▶ Selosteet, kuvaukset ja tekniikka kunnossa, ihmiset sitoutetaan ja sitoutuvat tietosuojaan
 - ▶ Muu turvallisuus (printtaus, suojaamattoman sähköpostin käyttö, tietokoneen näyttö kiinni etc.)
 - ▶ Ei dramatiikkaa – tietoturva pitää vain ottaa vakavasti

MIKÄ ON GDPR?

- ▶ Euroopan Unionin uusi tietosuojasetus tuli voimaan 24.5.2016.
- ▶ Elämme nyt toukokuussa 2018 loppuvaa siirtymäkautta.
- ▶ Asetusta aletaan soveltaa 25.5.2018 alkaen.
- ▶ **Asetus on suoraan sovellettavaa lainsäädäntöä!**
- ▶ Asetus jättää kuitenkin jäsenvaltioille direktiivinomaista kansallista liikkumavaraa. Hallituksen esitys uudeksi tietosuojalaksi on annettu 1.3.2018.
- ▶ Uuden Tietosuojalain vahvistamisen aikataulusta ei ole varmaa tietoa. Tietosuojavaltuutettu lausuu asiasta aikaisintaan syksyllä.
- ▶ Lain säätämisen jälkeenkin jää paljon avoimia kysymyksiä liittyen urheilun käytänteisiin. Olympiakomitea laatii liitoille ja sitä kautta seuroille käytännesäännön, joka valmistuu aikaisintaan loppuvuodesta 2018. Käytännesääntö vastaa kysymyksiin tietosuojasetuksen soveltamisesta urheilun erityispiirteet huomioiden.

MISSÄ MENNÄÄN?

- ▶ **Henkilötieto:** Esimerkiksi henkilön nimi, postiosoite, puhelinnumero, sähköpostiosoite, henkilötunnus, syntymäaika, sukupuoli, paidan koko, kulkuneuvon rekisterinumero, valokuva, videohaastattelu tai kilpailun tulos = kaikki henkilöön liittyvä tieto. Sosiaaliturvatunnuksen kerääminen yksilöintitarkoitukseen on mahdollista, jos se on tarpeellista (kynnys on korkea ja suojausvaatimukset isot). Erityiset henkilötietoryhmät (arkaluontoinen tieto) esim. terveyttä koskevat tiedot. Alle 16-vuotiailla lapsilla erityinen suoja.
- ▶ **Rekisteröity:** Luonnollinen henkilö, jota yllämainittu henkilötieto koskee.
- ▶ **Rekisteri:** Henkilötietojen joukko, jota käsitellään ja josta tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja pienin kustannuksin. HUOM! Asetus ei koske: Toimituksellinen aineisto tai asiakirja, josta ei voi hakea tietoa henkilöä koskevilla perusteilla (linjaus tulee todennäköisesti olemaan esim. pdf ilman metatietoja, käytännössä mm. toimintasuunnitelmat ja kertomukset sekä kilpailutulokset.)
- ▶ **Rekisterinpitäjä:** Taho, joka määrittelee, miksi ja miten henkilötietoja käsitellään, ja miksi rekisteri on syntynyt. Rekisterinpitäjä on vastuussa henkilötietojen käsittelystä.
- ▶ **Käsittelijä:** Henkilö tai taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (esim. henkilöt, joilla käyttöoikeus seuran jäsenrekisteriin tai muihin rekistereihin). Asetuksen myötä käsittelijän vastuu kasvaa! Sopimukset entistä tärkeämmät, kaikki sitoutettava noudattamaan tietoturva-asetusta.
- ▶ **Osoitusvelvollisuus:** Henkilötietoja käsittelevillä rekisterinpitäjillä on velvollisuus osoittaa konkreettisesti dokumentein, että organisaatio toimii tietojen käsittelyssä asetuksen edellyttämällä tavalla.
- ▶ **Tietosuojavastaava:** Vapaaehtoinen nimitys, mutta seurojen on hyvä nimetä tietosuojan yhteyshenkilö. Tietosuojavastaava on organisaation sisäinen asiantuntija tietosuoja-asioissa sekä yhteyspiste rekisteröidyille ja valvontaviranomaisille. Tietosuojavastaavan on oltava riippumaton rekisterinpitäjästä.

KÄSITTEISTÖÄ

- ▶ **Laki** (esim. yhdistyslaki määrää, että yhdistyksen on pidettävä jäsenluettelo)
- ▶ **Sopimus:** Henkilötietoja saa käsitellä siinä tilanteessa, että rekisteröity on jonkin sopimuksen toisena osapuolena, tai kun rekisteröidyn pyynnöstä, sopimusta laadittaessa, on suoritettava henkilötietoihin liittyviä toimenpiteitä.
- ▶ **Oikeutettu etu:** (ei ristiriitaa yksilön perusoikeuksien kanssa). Oikeutetut edut liittyvät sellaisiin toimintoihin kuten esimerkiksi suoramarkkinointi, asiakaspalvelu tai tuote- ja palvelukehitys.
- ▶ **Yleinen etu tai julkinen tehtävä**
- ▶ **Suostumus:** Jos ei muuta oikeusperustetta (suostumuksen on oltava selkeä ja aktiivinen sekä dokumentoitu).

HENKILÖTIETOJEN KÄSITTELYN OIKEUSPERUSTA

- ▶ Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- ▶ Käyttötarkoitussidonnaisuus
 - ▶ Esim. jäsenyys, asiakkuus ja työsuhde.
 - ▶ Tietojen käsittelyn tarkoitus on määriteltävä etukäteen.
 - ▶ Tietoja voi käyttää vain etukäteen määriteltyyn tarkoitukseen.
- ▶ Tietojen keräämisen ja tietojen minimointi
- ▶ Tietojen täsmällisyys
- ▶ Tietojen säilytyksen rajoittaminen
- ▶ Tietojen eheys ja luottamuksellisuus
- ▶ Rekisterinpitäjän osoitusvelvollisuus

TIETOSUOJAPERIAATTEET

- ▶ Rekisterinpitäjällä on oltava kyky osoittaa noudattavansa asetusta henkilötietojen käsittelyssä ja toteuttavansa tietosuojaperiaatteita käytännössä. Kaikki yhteisön henkilörekisterit ja tietojenkäsittelyprosessit täytyy siis olla dokumentoituna (seloste käsittelytoimista)!
 - ▶ Tietojen käsittelyn prosessien ja sisältöjen kuvaus – avoimuus – lisää rekisteröidyn luottamusta
- ▶ Suhteellisuusperiaate (Facebook vs. pieni urheiluseura)

OSOITUSVELVOLLISUUS

- ▶ Oikeus saada läpinäkyvää informaatiota, kun henkilötiedot kerätään (seloste käsittelytoimista).
- ▶ Oikeus päästä tarkastamaan omat tietonsa ja oikeus oikaista omia tietoja.
- ▶ Oikeus poistaa tietoja ja tulla kokonaan unohdetuksi sekä rajoittaa omien tietojen käsittelyä (ei absoluuttinen oikeus)
 - ▶ Henkilötieto hävitetään heti, kun käytön peruste päättyy
 - ▶ Anonymisointi tilastoja varten on mahdollista
 - ▶ Ratkaistavaksi tulee, miten käsitellä esim. kilpailulistoja- ja tuloksia, koulutushistoria-, suoritus- ja edustusoirekistereitä. Näihin kysymyksiin vastaa Urheilun käytäntösääntö.
- ▶ Oikeus tulla informoiduksi henkilötietojen tietoturvaloukkauksista
 - ▶ Velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaisille ja rekisteröidyille
 - ▶ Loukkaus on esimerkiksi henkilötietojen vahingossa tapahtuva tuhoaminen, tietojen häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin
 - ▶ Ilmoitus ilman aiheetonta viivästyä, viranomaiselle viimeistään 72 tunnin kuluessa
- ▶ Lapsilla erityinen suoja (alle 16v.)

REKISTERÖIDYN OIKEUDET

- ▶ Myös tähän asti yhteisöillä on ollut velvollisuus laatia rekisteriseloste/tietosuojaseloste
- ▶ Nyt velvollisuus on vain laajempi
 - ▶ Seloste käsittelytoimista voi olla nimeltään seloste käsittelytoimista – tulossa virallisia malleja!

Mitä selosteen käsittelytoimista tulee sisältää:

- ▶ Mitä tietoja käsitellään sekä käsittelyn oikeusperuste?
- ▶ Miten ja missä tietoja käsitellään (kerääminen, tallentaminen, säilytys ja hävitys)?
- ▶ Kenelle ja mihin tietoja luovutetaan?

SELOSTE KÄSITTELYTOIMISTA

Seuran tulee:

STEPPI 1: Selvittää, mitä henkilötietoja seuralla on hallussa eli kartoittaa käytössä olevat rekisterit ja miten henkilötietoja käytetään?

(Mitä rekistereitä seuroilla mahdollisesti on? Mm. Jäsenluettelo, Jäsenrekisteri, Dan/Poom-rekisteri, Valmentajarekisteri, Koulutusrekisteri, Tapahtumien ilmoittautumislistat, Varustelausekset, Kilpailu- ja testitulokset yms.)

STEPPI 2: Selvittää, kuka henkilötietoja käsittelee ja suunnitella, miten käsittelijät sitoutetaan ja koulutetaan?

- ▶ Ovatko käyttöoikeudet henkilökohtaiset?
- ▶ Kuka hallinnoi käyttöoikeuksia?
- ▶ Käsittelijät sitoutettava sopimuksin!

STEPPI 3: Suunnitella ja toteuttaa, miten tarpeettomat henkilötiedot poistetaan?

STEPPI 4: Laatia jokaisen rekisterin osalta selosteet käsittelytoimista.

STEPPI 5: Kartoittaa kaikkeen tietoturvaan liittyvät riskit seuran toiminnassa.

STEPPI 6: Nimetä seuraan tietosuojavastaava.

Noudattaa julkaisutoiminnassa (internet, some-kanavat) huolellisuutta! Suostumus pyydettävä julkaisuihin (suostumus on aina peruttavissa).

Noudatettava huolellisuutta luovutettaessa henkilötietoja kolmansille osapuolille!

MITÄ SEURAAVAKSI SEUROISSA?

- ▶ Suomen Karateliitto auttaa tietosuoja-asetusta koskevissa kysymyksissä sekä konsultoi tarvittaessa Olympiakomitean erityisasiantuntijaa. Lisätietoa jaetaan seuroille sitä mukaan, kun uuden tietosuojalain käsittely etenee!
- ▶ Uusimmissa seuratyökaluissa, esim. Suomisport ja MyClub, tietosuoja-asetus on huomioitu. Tiesithän, että Suomisporttia pystyy käyttämään seuran jäsenrekisterinä! (www.suomisport.fi)
- ▶ www.tietosuoja.fi
- ▶ www.arjentietosuoja.fi (<http://tietosuoja.vahtiohje.fi/fi/#/front>)

LISÄTIETOJA