# SUOMEN TENNISLIITON OPAS SEUROILLE HENKILÖTIETOJEN KÄSITTELYYN

*Mailapeliyhteistyön konkreettisena mallina Sulkapalloliitto on saanut luvan käyttää tätä Tennisliiton tuottamaa opasta seurojensa ohjeistamiseen.*

Laatinut Henrik Zilliacus
Päivitetty 23.5.2108

## 1. Johdanto

EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation, GDPR) sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa ja se korvaa tällä hetkellä voimassa olevan kansallisen henkilötietolain. Asetus asettaa jonkin verran uusia velvoitteita rekisterinpitäjille ja antaa uusia oikeuksia rekisteröidyille. Tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Sitä ei kuitenkaan sovelleta yksityisen henkilön yksinomaan henkilökohtaiseen tai kotitalouttaan koskevaan toimintaan.

Tässä oppaassa on pyritty esittämään seurojen kannalta keskeisimmät henkilötietojen käsittelyyn liittyvät määräykset mahdollisimman ymmärrettävässä ja selkeässä muodossa ja oppaan tarkoituksena on auttaa seuroja henkilötietojen käsittelyn suunnittelussa, toteuttamisessa ja valvonnassa. Opas ei kuitenkaan sisällä tyhjentävästi kaikkia tietoja henkilötietojen käsittelyyn liittyvistä säädöksistä. Henkilötietojen käsittelyyn liittyvissä epäselvissä tai tulkinnanvaraisissa tilanteissa suosittelemme aina varmistamaan asian joko Tietosuojavaltuutetun toimiston ohjeista tai ottamaan yhteyttä Tietosuojavaltuutetun toimiston neuvontapalveluun.

Tietosuojalainsäädäntö sisältää jonkin verran tulkinnanvaraisia määräyksiä ja tässä vaiheessa kaikkiin tilanteisiin ei voida esittää yhtä oikeaa toimintamallia. Tuleva oikeuskäytäntö näyttää, minkälaisiin tulkintoihin EU:n tietosuoja-asetuksen ja sitä täydentävien kansallisten lakien soveltamisessa päädytään. Lisäksi on huomioitava, että uusi lainsäädäntö voi muuttaa aiempia tulkintakäytäntöjä. Päivitämme tätä ohjetta aina tarpeen vaatiessa.

## 2. Keskeisiä termejä[1]

**Henkilötiedoilla** tarkoitetaan kaikkia henkilöön liittyviä tietoja (esim. nimi, henkilötunnus, yhteystieto tai kuva), joista henkilö voidaan tunnistaa.

**Käsittelyllä** tarkoitetaan kaikkia henkilötietoihin tai tietojoukkoihin kohdistuvia toimia joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, säilyttämistä, muokkaamista, hakua, kyselyä, käyttöä, tietojen luovuttamista, poistamista tai tuhoamista.

**Rekisterillä** tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla.

**Rekisterinpitäjällä** tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

**Henkilötietojen käsittelijällä** tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisteröidyn **suostumuksella** tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

[1] Ks. myös EU:n tietosuoja-asetuksen artikla 4, jossa on lista asetukseen liittyvistä määritelmistä.

## 3. Henkilötietojen käsittelyä koskevat periaatteet[2]

1) Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

2) Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

3) Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

4) Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Kaikki mahdolliset kohtuulliset toimenpiteet on toteutettava sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

5) Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

6) Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

Rekisterinpitäjä vastaa ja sen on pystyttävä osoittamaan, että se noudattaa näitä periaatteita.

## 4. Käsittelyn lainmukaisuus[3]

Henkilötietojen käsittely on lainmukaista, jos vähintään yksi seuraavista edellytyksistä täyttyy:

1) Rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.

2) Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

3) Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.

4) Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi.

5) Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

6) 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.

Jos henkilötietojen käsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn.[4] Rekisteröidyllä on koska tahansa oikeus peruuttaa suostumuksensa. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen

[2] Henkilötietojen käsittelyä koskevat periaatteet on kirjattu EU:n tietosuoja-asetuksen artiklaan 5.
[3] Henkilötietojen käsittelyn lainmukaiset perusteet on kirjattu EU:n tietosuoja-asetuksen artiklaan 6.
[4] Suostumuksen edellytykset on määritelty EU:n tietosuoja-asetuksen artiklassa 7. Suostumusta koskeva kirjallinen pyyntö on mm. esitettävä selvästi erillään muista asioista ja sen on oltava helposti ymmärrettävä. Ennen suostumuksen antamista rekisteröidylle on myös ilmoitettava oikeudesta peruuttaa suostumus.

antaminen. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen.

Kun kyseessä on tietoyhteiskunnan palvelujen[5] tarjoaminen suoraan lapselle ja käsittely perustuu suostumukseen, lapsen henkilötietojen käsittely on lainmukaista, jos lapsi on vähintään 16-vuotias. Jos lapsi on alle 16 vuotta, käsittely on lainmukaista vain siltä osin kuin lapsen huoltaja on antanut siihen suostumuksen. Kansallisesti voidaan säätää tätä tarkoitusta koskevasta alemmasta iästä, joka ei saa olla alle 13 vuotta.[6]

## 5. Rekisteröidyn oikeuksia[7]

1) Rekisteröidyllä on oikeus saada rekisterinpitäjältä tieto siitä, käsitelläänkö häntä koskevia henkilötietoja. Jos henkilötietoja käsitellään, rekisteröidyllä on oikeus saada pääsy henkilötietoihin.

2) Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.

3) Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ”oikeus tulla unohdetuksi” esimerkiksi seuraavissa tapauksissa:[8]

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin.
- Rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta.
- Henkilötietoja on käsitelty lainvastaisesti.

4) Rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä esimerkiksi seuraavissa tilanteissa:[9]

- Rekisteröity kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan ajaksi, jonka kuluessa rekisterinpitäjä voi varmistaa niiden paikkansapitävyyden.
- Käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista.
- Rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

5) Rekisteröidyllä on oikeus siirtää rekisterinpitäjälle toimittamansa häntä koskevat henkilötiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti.

6) Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on milloin tahansa oikeus vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten.

---

[5] Tietoyhteiskunnan palvelu on määritelty Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 (19) 1 artiklan 1 kohdan b alakohdassa. Sillä tarkoitetaan etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluja, joista tavallisesti maksetaan korvaus.

[6] Suomessa tästä asiasta säädetään uudessa tietosuojalaissa, jota koskeva hallituksen esitys 9/2018 on käsittelyssä. Uudessa tietosuojalaissa ikärajaksi on määritelty 13 vuotta.

[7] Rekisteröidyn oikeudet on määritelty EU:n tietosuoja-asetuksen luvussa III. Asetus antaa rekisteröidylle aiempaa vahvemmat ja laajemmat oikeudet. Tähän lukuun on koottu seuran näkökulmasta keskeisiä asioita.

[8] Ks. tarkemmin oikeudesta saada tiedot poistetuksi EU:n tietosuoja-asetuksen artikla 17.

[9] Ks. tarkemmin oikeudesta rajoittaa tietojen käsittelyä EU:n tietosuoja-asetuksen artikla 18.

7) Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia.[10]

## 6. Rekisterinpitäjän velvollisuuksia

EU:n tietosuoja-asetus asettaa rekisterinpitäjälle velvollisuuksia, jotka liittyvät henkilötietojen käsittelyyn sekä käytettäviin teknisiin ratkaisuihin. Osa velvoitteista on suhteutettu siihen, minkälaisia riskejä käsittely aiheuttaa henkilöiden oikeuksille ja vapauksille. Käsittelijän tulee itse arvioida käsittelyynsä liittyvät riskit.[11]

**1) Rekisterinpitäjän vastuu:** Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan EU:n tietosuoja-asetusta. Toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.

**2) Sisäänrakennettu ja oletusarvoinen tietosuoja:** Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että käsitellään vain tarpeellisia henkilötietoja. Toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja ei saateta rajoittamattoman henkilömäärän saataville ilman henkilön myötävaikutusta.

**3) Henkilötietojen käsittelijä:** Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Rekisterinpitäjän ja henkilötietojen käsittelijän on tehtävä käsittelystä kirjallinen sopimus.

**4) Seloste käsittelytoimista:** Rekisterinpitäjän on laadittava seloste henkilötietojen käsittelystä.[12] Seloste on tarkoitettu rekisterinpitäjän omaan käyttöön, mutta selosteessa olevia tietoja voi hyödyntää informointivelvollisuuden täyttämisessä.

**5) Informointivelvollisuus:** Rekisterinpitäjän on toimitettava rekisteröidylle olennaiset henkilötietojen käsittelyyn liittyvät tiedot. Tiedot on esitettävä selkeässä ja ymmärrettävässä muodossa ja ne on annettava ilmaiseksi. Asetuksessa ei säädetä velvollisuudesta tehdä rekisteriseloste tai muustakaan tietystä muodosta, jolla tiedot tulee antaa. Pääsääntöisesti tiedot tulee kuitenkin antaa kirjallisesti. Jos henkilötiedot kerätään rekisteröidyltä itseltään, käsittelyä koskevat tiedot tulee toimittaa rekisteröidylle silloin, kun tiedot kerätään.[13]

**6) Käsittelyn turvallisuus:** Rekisterinpitäjän ja henkilötietojen käsittelijän on henkilötietojen turvallisuuden varmistamiseksi toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

---

[10] Ks. tästä oikeudesta ja siihen liittyvistä poikkeuksista EU:n tietosuoja-asetuksen artikla 22.

[11] Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista on määrätty EU:n tietosuoja-asetuksen luvussa IV. Ks. myös Tietosuojavaltuutetun toimiston julkaisu Miten valmistautua EU:n tietosuoja-asetukseen s. 16.

[12] Velvollisuus koskee organisaatioita, joilla on yli 250 työntekijää. Seloste on laadittava myös, jos käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittely kohdistuu erityisiin tietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin henkilötietoihin. Seloste kannattaa laatia, vaikka siihen ei olisi velvollisuutta, koska se helpottaa osoittamaan tietosuoja-asetuksen noudattamisen. Selosteesta ja siinä mainittavista asioista on määrätty EU:n tietosuoja-asetuksen artiklassa 30.

[13] Informointivelvollisuudesta on määrätty EU:n tietosuoja-asetuksen artikloissa 12-14. Jos tiedot kerätään muualta kuin rekisteröidyltä, tiedot tulee toimittaa yhden kuukauden kuluessa tai viimeistään, kun tietoja käytetään henkilöön kohdistuvaan viestintään, tai tietoja luovutetaan ensimmäisen kerran. Ks. myös Tietosuojavaltuutetun toimiston ohje Informointivelvollisuuden edellyttämistä tiedoista.

**7) Tietoturvaloukkauksista ilmoittaminen:** Mahdollisesta henkilötietojen tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä toimivaltaiselle valvontaviranomaiselle.[14]

**8) Vaikutusten arviointi ja tietosuojavastaava:** Jos henkilötietojen käsittelyyn liittyy korkea riski, rekisterinpitäjän on tehtävä tietosuojaa koskeva vaikutusten arviointi. Jos rekisterinpitäjän ydintehtävänä on laajamittainen rekisteröityjen säännöllinen ja järjestelmällinen seuranta tai laajamittainen erityisiin henkilötietoryhmiin ja rikostuomioita tai rikkomuksia koskeviin tietoihin kohdistuva käsittely, rekisterinpitäjän on nimitettävä tietosuojavastaava.

## 7. Seuraamuksia asetuksen vastaisesta toiminnasta[15]

**1) Valitus valvontaviranomaiselle:** Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tietosuoja-asetusta.

**2) Valvontaviranomaisen valtuudet:** Kansallinen valvontaviranomainen voi antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle huomautuksen, jos käsittelytoimet ovat olleet asetuksen vastaisia. Viranomainen voi myös määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet asetuksen mukaisiksi, asettaa väliaikaisen tai pysyvän rajoituksen käsittelylle tai määrätä henkilötietojen oikaisemisesta tai poistamisesta.

**3) Hallinnollinen sakko:** Tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä voi seurata hallinnollinen sakko. Sakon määräämisessä otetaan huomioon mm. rikkeen luonne, vakavuus, kesto, tahallisuus, tuottamuksellisuus ja toteutetut toimenpiteet vahingon lieventämiseksi.

**4) Vahingonkorvaus:** Jos henkilölle aiheutuu asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta. Rekisterinpitäjä tai henkilötietojen käsittelijä voi vapautua vahingonkorvausvastuusta, jos se osoittaa, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.

## 8. Henkilötietojen käsittely seurassa

### Esimerkkejä seuran ylläpitämistä henkilörekistereistä ja niihin kerättävästä tiedosta

**1) Jäsenrekisteri:** Yhdistyslain mukaan yhdistyksen jäsenistä on ylläpidettävä luetteloa, johon on merkittävä kunkin jäsenen täydellinen nimi ja kotipaikka. Jäsenrekisteriin voidaan kerätä myös muita tietoja, mutta seuran on arvioitava niiden tarpeellisuus tapauskohtaisesti. Esimerkiksi yhteystietoja tarvitaan yleensä jäsenviestintään, laskutusosoitetta jäsenmaksujen perimiseen, syntymävuotta urheilutoimintaan liittyviin ikärajoihin ja syntymäaikaa samannimisten jäsenten erottamiseen toisistaan. Jäsenrekisterin ylläpitämiseen ei tarvita henkilöiden suostumusta, kunhan rekisteriin kerätään vain jäsenyyden kannalta olennaisia tietoja. Tiedot on poistettava jäsenyyden päätyttyä, ellei käsittelylle ole jotain muuta perustetta.[16]

**2) Rekisteri toimintaan osallistuvista (esim. valmennus, tapahtumat, kilpailut):** Seuralla on yleensä sopimussuhteita toimintaan osallistuvien kanssa. Seura voi ylläpitää rekisteriä sopimuskumppaneistaan eli ns. asiakkaistaan.[17] Rekisteriin voidaan kerätä asiakassuhteen kannalta olennaisia tietoja kuten

[14] Loukkauksesta ei tarvitse ilmoittaa, jos siitä ei todennäköisesti aiheudu henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta myös rekisteröidylle. Ks. ilmoitusvelvollisuudesta ja siihen liittyvistä poikkeuksista EU:n tietosuoja-asetuksen artiklat 33-34.

[15] Oikeussuojakeinoista, vastuista ja seuraamuksista on säädetty EU:n tietotuoja-asetuksen luvussa VIII.

[16] Ks. myös Tietosuojavaltuutetun ohje Yhdistyksen jäsenluettelot ja henkilötietolaki. Huomaa kuitenkin, että opas on laadittu ennen EU:n tietosuoja-asetuksen voimaantuloa ja sisältää osin vanhentunutta tietoa.

[17] Usein seuran jäsenellä on sekä jäsenyys- että sopimussuhde seuraan, jolloin toimintaan liittyviä tietoja voidaan ylläpitää osana jäsenrekisteriä. Muiden kuin jäsenten osalta rekisteriä kutsutaan yleensä asiakasrekisteriksi.

yhteystiedot, ikä, harjoitusaikatoive ja pelitaso. Jokaisen kerättävän tiedon osalta seuran tulee arvioida, onko tieto tarpeellinen ja hävittää vanhentuneet tai turhat tiedot. Sopimukseen perustuvien henkilötietojen käsittelyn osalta ei tarvita henkilön suostumusta niin kauan, kun sopimussuhde on voimassa. Jos seura kuitenkin kerää arkaluonteisia tietoja (esim. tietoja allergioista ruokailuja varten), tulee seuran pyytää suostumus henkilöltä ja tiedot tulee hävittää heti, kun niitä ei enää tarvita.[18]

**3) Yritys/yhteistyökumppanirekisteri:** Yrityksistä pidettävä rekisteri ei itsessään ole henkilörekisteri, mutta yritysten yhteyshenkilöiden tietoja sisältävä rekisteri on henkilörekisteri. Yritysten yhteyshenkilöiden tietoja sisältävän rekisterin ylläpitäminen on sallittua, kun seuralla on yritysten kanssa sopimukset. Rekisteriin voi kerätä sopimussuhteen kannalta olennaisia tietoja.

**4) Sähköinen uutiskirje:** Seura lähettää usein sähköisiä uutiskirjeitä jäsenilleen, muille toimintaan osallistuville, yhteistyökumppaneille ja myös sellaisille, jotka eivät ole mukana seuran toiminnassa. Jos uutiskirjerekisterissä on vain jäseniä, asiakkaita tai yhteistyökumppaneita ja sitä ylläpidetään osana em. rekistereitä, uutiskirjerekisteri ei edellytä erillistä suostumusta.[19] Muiden kuin jäsenten ja asiakkaiden osalta uutiskirjerekisteri edellyttää henkilön suostumusta.

**5) Työntekijä- ja valmentajarekisteri:** Työntekijä- ja valmentajarekistereissä on myös kysymys sopimukseen perustuvista rekistereistä, jotka eivät edellytä rekisteröidyiltä erillistä suostumusta. Rekistereihin voi kerätä työsuhteen kannalta olennaisia tietoja.[20] Lasten kanssa työskenteleviltä on selvitettävä rikostausta, mutta työntekijän henkilötietoihin saa tehdä ainoastaan merkinnät rikosrekisteriotteen esittämisestä ja otteen tunnistetiedoista.[21]

## Tietojen käsittelyssä huomioitavia asioita

**1) Tietojen säilytystapa:** Henkilörekistereitä ei tarvitse säilyttää sähköisessä muodossa, mutta käytännössä suurin osa rekistereistä on tallennettu johonkin sähköiseen muotoon. Seuran tulee varmistaa, että tietojen säilytystapa täyttää tekniset tietoturvavaatimukset (esim. salasanasuojaus, suojattu yhteys, palomuuri).[22] Tietoja saa tallentaa useaan paikkaan (esim. tiedostoja usean työntekijän koneilla), mutta tällöin niitä voi olla hankala hallita. Tästä syystä keskitetty rekisterijärjestelmä on hyvä tapa tietojen säilyttämiselle. Seuran on joka tapauksessa huolehdittava myös siitä, että kaikki tietojen säilytystavat ovat asetuksen mukaisia.

**2) Tietojen käsittely seuran lukuun:** Seurassa on yleensä useita henkilöitä, joilla on pääsy henkilötietoihin (esim. työntekijät, hallituksen jäsenet). Seuran tulee varmistaa, että henkilötietoihin pääsevät käsiksi vain ne henkilöt, joilla on oikeus käsitellä tietoja. Seuran tulee myös ohjeistaa ja valvoa, että henkilötietoja käsittelevät henkilöt käsittelevät niitä lainmukaisesti ja vain sallittuihin tarkoituksiin sekä estää pääsy henkilötietoihin niiltä, joilla ei ole enää oikeutta käsitellä tietoja (esim. vanhat työntekijät tai hallituksen jäsenet).

[18] Ks. erityisiä henkilötietoryhmiä koskevasta käsittelystä EU:n tietosuoja-asetuksen artikla 9.
[19] Käytännössä rekisteriin merkitään se, haluaako henkilö vastaanottaa uutiskirjeitä. On kuitenkin huomattava, että myös jäsenet, asiakkaat ja yhteistyökumppanit voivat kieltää seuraa lähettämästä heille sähköisiä uutiskirjeitä. Ks. sähköisestä markkinoinnista myös laki sähköisen viestinnän palveluista luku 24.
[20] Henkilötietojen käsittelystä työsuhteessa on säädetty laissa yksityisyyden suojasta työelämässä.
[21] Ks. laki lasten kanssa työskentelevien rikostaustan selvittämisestä 7-8 §. Otteesta ei saa ottaa jäljennöstä ja se on palautettava otteen esittäneelle henkilölle viipymättä. Rikosrekisteriotteesta ilmeneviä tietoja ei saa ilmaista muille kuin sellaisille henkilöille, jotka välttämättä tarvitsevat niitä tehdessään päätöstä siitä, annetaanko henkilölle työtehtäviä.
[22] Sulkapalloliiton käyttämä ja jatkossa seuroillekin tarjoama toiminnanohjausjärjestelmä, Suomisport täyttää nämä vaatimukset.

**3) Käsittelyn ulkoistaminen:** Seuralla voi olla tarve ulkoistaa jokin palvelu (esim. taloushallinto), johon liittyy henkilötietojen käsittelyä. Tällöin ulkopuolisesta palveluntarjoajasta tulee henkilötietojen käsittelijä. Seuran tulee tehdä henkilötietojen käsittelystä sopimukset ulkopuolisten palveluntarjoajien kanssa.

**4) Tietojen luovuttaminen:** Henkilötietoja saa luovuttaa vain laillisiin tarkoituksiin ja luovuttamisesta pitää informoida niitä henkilöitä, joiden tietoja luovutetaan. Henkilöillä on oikeus kieltää tietojen luovuttaminen. Henkilötietojen (kuten nimen tai kuvan) julkaiseminen internetissä on sallittua ainoastaan henkilön nimenomaisella suostumuksella. Henkilö voi myös peruuttaa suostumuksen, jolloin tiedot on poistettava internetistä. Päätösvalta tietojen luovuttamisesta on hallituksella, mutta sen tulee noudattaa lainsäädäntöä ja ottaa huomioon henkilöiden oikeus kieltää luovutus.

**5) Tiedote- ja markkinointiviestit:** Seura lähettää yleensä erilaisia tiedotteita ja markkinointiviestejä jäsenilleen ja asiakkailleen. Viestit voidaan jakaa karkeasti kolmeen kategoriaan: 1) toimintaan liittyvät tiedotteet, joissa ei markkinoida uusia palveluita tai tuotteita, 2) sellaisten seuran palvelu- ja tuoteryhmien markkinointi, joita jäsenet ja asiakkaat jo käyttävät[23] ja 3) muiden palveluiden ja tuotteiden markkinointi. Toimintaan liittyviä tiedotteita (ns. jäsen- tai asiakastiedotteita) voi lähettää jäsenille ja asiakkaille ilman suostumusta. Myöskään omien vastaavien palveluiden ja tuotteiden markkinointi ei vaadi suostumusta, mutta markkinointiviestissä tulee selvästi kertoa, miten henkilö voi kieltää markkinointiviestien lähettämisen. Uusien sekä muiden tahojen tarjoamien palveluiden ja tuotteiden markkinointi edellyttää aina suostumusta.[24]

## Kartoitus henkilötietojen käsittelyn nykytilasta

Seuran tulee jatkossa voida itse osoittaa noudattavansa EU:n tietosuoja-asetusta. Seuran tulisi kartoittaa henkilötietojen käsittelyn nykytila ja dokumentoida kartoitus. Tämä auttaa seuraa toimimaan lainmukaisesti ja myös osoittamaan asetuksen noudattamisen. Kartoituksen voi tehdä seuraavasti:

1. Käykää läpi kaikki seuran henkilörekisterit, niiden sisältämät tiedot ja käyttötarkoitukset. Huomatkaa, että rekistereitä voi löytyä myös seuran yksittäisiltä toimihenkilöiltä (esim. valmentajien omat yhteystietolistat). Miettikää, mitkä kaikki rekisterit ja niissä olevat tiedot ovat tarpeellisia. Selvittäkää jokaisen rekisterin käsittelyperuste (suostumus, sopimus, oikeutettu etu vai joku muu) sekä käyttötarkoitukset ja perustelkaa kerättävien tietojen tarve. Arvioikaa myös käsittelyyn liittyvät tekniset ja inhimilliset riskit.

2. Selvittäkää, kuinka pitkään tietoja säilytetään. Hävittäkää turhat rekisterit ja tiedot.

3. Miettikää, mitä teknisiä ratkaisuita henkilörekisterien ylläpidossa käytetään. Varmistakaa, että ne täyttävät tietoturvavaatimukset.

4. Selvittäkää ne prosessit, miten tietoja voidaan luovuttaa rekisteröidylle itselleen tai muille osapuolille. Miettikää myös, miten tietojen pyytäjä voidaan tunnistaa.[25]

5. Tehkää seloste henkilötietojen käsittelytoimista ja huolehtikaa siitä, että rekisteröityjä informoidaan tietojen käsittelystä. Selosteen laatimisessa voitte käyttää apuna Tennisliiton mallia. Tiedot käsittelystä kannattaa lähettää rekisteröidyille sähköpostitse ja julkaista seuran verkkosivuilla.

[23] Tällaiseksi lasketaan kaikki vastaavat palvelut esim., kun talvikauden valmennuksessa mukana oleville markkinoidaan kesäkursseja.
[24] Laki sähköisen viestinnän palveluista 200 §.
[25] Yleisiä luovutustilanteita ovat esimerkiksi tietojen luovuttaminen liiton pelaajarekisteriin, tietojen luovuttaminen kilpailuun ilmoittautumisen yhteydessä, muiden jäsenten tai seurojen kyselyt tai yhteistyökumppanien markkinointitarkoitukset.

6. Käykää läpi kaikki ne henkilöt, jotka käsittelevät seuran henkilötietoja. Ohjeistakaa henkilöitä ja valvokaa, että ohjeita noudatetaan. Huolehtikaa, että pääsy tietoihin estetään niiltä, jotka eivät enää ole oikeutettuja tietojen käsittelyyn. Seuran on hyvä nimetä henkilö, jonka vastuulla henkilötietojen käsittelyn valvonta on.

7. Käykää läpi kaikki ulkopuoliset palveluntarjoajat, jotka käsittelevät seuran henkilötietoja. Tehkää sopimus palveluntarjoajien kanssa. Voitte apuna käyttää Tennisliiton mallisopimuspohjaa.

8. Päivittäkää tarvittaessa toimintamalleja ja ohjeistuksia.

## 9. Lähteet ja julkaisut

### Lainsäädäntöä

EU:n tietosuoja-asetus http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Laki sähköisen viestinnän palveluista https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#L24P200

Laki yksityisyyden suojasta työelämässä https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

### Tietosuojavaltuutetun toimiston julkaisuja

Tietosuojavaltuutetun toimiston sivut löytyvät osoitteesta http://www.tietosuoja.fi/fi/. Sivuilla on julkaistu tietosuojaan liittyviä oppaita ja lomakkeita.

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

Yhdistyksen jäsenluettelot ja henkilötietolaki
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqOozpn/Yhdistyksen_jasenluettelot_ja_henkilotietolaki.pdf

Informointivelvollisuuden edellyttämät tiedot
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/4dCR8ypI9/Informointivelvoitteen_edellyttamat_tiedot.pdf

### Tennisliiton mallit

Tennisliiton mallit löytyvät osoitteesta http://www.tennis.fi/seurat/eun-tietosuoja-asetus/.