Krogerus

EU:N YLEINEN TIETOSUOJA-ASETUS
SUOMEN GOLFLIITON OHJEISTUS SEURAJÄSENILLE

1.4.2018

1 JOHDANTO

1.1 Yleistä

Yleistä tietosuoja-asetusta ryhdytään soveltamaan 25.5.2018. Tietosuoja-asetuksen tavoitteena on parantaa mm. henkilötietojen suojaa ja rekisteröityjen oikeuksia, yhtenäistää tietosuojasääntelyä EU:ssa sekä lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. Suomenkielinen versio tietosuoja-asetuksesta löytyy täältä.

Suomen Golfliiton seurajäsenten ja kenttäyhtiöiden muodostamat golfyhteisöt käsittelevät henkilötietoja toimintansa yhteydessä, joten tietosuoja-asetuksen tuomien velvoitteiden tunteminen on erittäin tärkeää. Henkilötietojen käsittelyn asianmukaisuus on mm. tärkeää asiakasluottamuksen ylläpitämiseksi. Tietosuoja-asetus tulee laajentamaan myös viranomaisten mahdollisuuksia puuttua yritysten henkilötietojen käsittelyyn, mikäli sitä ei tehdä lain edellyttämällä tavalla ja mahdollistaa myös merkittävien seuraamusten määräämisen yritykselle.

Tietosuoja-asetus soveltuu käytännössä aina, kun henkilötietoja käsitellään tietojärjestelmissä. Tämän lisäksi se koskee myös ns. manuaalista käsittelyä, eli käsittelyä muussa kuin automaattisessa muodossa, jos henkilötiedot muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa (käytännössä siis silloin, kun tiedot on järjestelty tietyn logiikan mukaan siten, että tarvittaessa tiettyä henkilöä koskevat tiedot on kohtuudella löydettävissä). Tällainen tilanne voi olla käsillä esim. paperisen kortiston tai arkiston osalta.

Tietosuoja-asetuksen lisäksi henkilötietoja käsiteltäessä huomioon tulee ottaa myös kansalliset lait, kuten tietoyhteiskuntakaari, työelämän tietosuojalaki sekä kansallinen tietosuojalaki.

Tämän ohjeistuksen tarkoituksena on auttaa golfyhteisöjä oman toimintansa läpikäynnissä ja päivittämisessä tietosuoja-asetuksen valossa. Ohjeistus ei kata tyhjentävästi kaikkia tietosuojaan ja tietosuoja-asetukseen liittyviä velvoitteita, mutta ohjeistuksessa on kuvattu golfyhteisöjen kannalta keskeisimpiä velvoitteita.

1.2 Keskeiset määritelmät

Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Määritelmä on laaja ja henkilötietoja ovat myös muut kuin esim. pelkästään henkilön nimi, henkilötunnus, osoite ja yhteystiedot. Henkilötiedon määritelmän täyttymiseksi riittää, että jonkin tiedon voidaan katsoa liittyvän tiettyyn henkilöön.

Erityisillä henkilötietoryhmillä tarkoitetaan henkilötietoja, joista ilmenee esimerkiksi rotu tai etninen alkuperä, poliittinen vakaumus, ammattiliiton jäsenyys tai terveyttä koskevia tietoja. Tällaisten tietojen käsittelyn sallittavuus on rajatumpaa ja käytännössä mahdollista vain tilanteissa, joissa laki velvoittaa kyseisten tietojen käsittelyyn tai niiden käsittelyyn on saatu henkilön nimenomainen suostumus.

Henkilötietojen käsittelyllä tarkoitetaan käytännössä kaikkia henkilötietoihin kohdistuvia toimenpiteitä, kuten henkilötietojen keräämistä, tallentamista, järjestämistä, käyttöä, säilyttämistä ja muuttamista.

Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot ("mitä, miksi ja miten"). Rekisterinpitäjä on lähtökohtaisesti vastuussa henkilötietojen käsittelystä. Käytännössä rekisterinpitäjänä toimii käsittelytilanteesta riippuen usein joko kenttäyhtiö tai jäsenseura. Tietosuoja-asetus tuntee myös ns. **yhteisrekisterinpitäjän** käsitteen. Tämä tarkoittaa sitä, että vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot. Yhteisrekisterin osalta osapuolten tulisi tietosuoja-asetuksen 26 artiklan mukaisesti sopia keskinäisellä järjestelyllä vastuiden ja velvoitteiden jakautumisesta erityisesti informoinnin ja rekisteröidyn oikeuksien toteuttamisen osalta. Käytännön toiminnasta riippuen yhteisrekisterinpitäjiä voivat joissain tilanteissa olla mahdollisesti esimerkiksi kenttäyhtiö ja jäsenseura. Yhteisrekisterinpitäjyys tarkoittaa esimerkiksi sitä, että seura ja kenttäyhtiö yhdessä määrittelevät sen, mitä tietoja esimerkiksi golfyhteisön asiakkaista kerätään sekä sen, mitä kyseisillä tiedoilla tehdään ja mihin tarkoituksiin niitä käytetään. Arvioidessa yhteisrekisterin olemassa oloa, tulee miettiä onko kyse todellisesta yhteisrekisterinpitäjyydestä vai siitä, että rekisterinpitäjät jakavat tietoja keskenään ja käyttävät tietoja omiin tarkoituksiinsa.

Henkilötietojen käsittelijällä taas tarkoitetaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Käytännössä henkilötietojen käsittelijä on esim. ulkopuolinen palveluntarjoaja, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällainen tilanne voi tulla kyseeseen esimerkiksi silloin, jos golfyhteisöllä on käytössä pilvipalvelu, jossa säilytetään henkilötietoja tai jos golfyhteisö on esimerkiksi ulkoistanut palkkahallintonsa. Myös esimerkiksi seuran tai kenttäyhtiön lukuun palveluja tuottava yhtiö, kuten tilitoimisto, IT-palvelujen tuottaja tai opetuspalveluja tuottava yritys, voi olla henkilötietojen käsittelijä, mikäli tämän toiminnan yhteydessä käsitellään sellaisia henkilötietoja, joiden osalta rekisterinpitäjä on seura tai kenttäyhtiö.

Rekisteröity on se henkilö, kenen henkilötietoja käsitellään. Rekisteröityjä voivat esimerkiksi olla asiakkaat, potentiaaliset asiakkaat, yhteistyökumppaneiden yhteyshenkilöt ja rekisterinpitäjän työntekijät.

2 HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT PERIAATTEET

Keskeisenä lähtökohtana asianmukaisen tietosuojan toteuttamisessa on tietosuojalainsäädännön yleisten periaatteiden noudattaminen, jotka tulisi huomioida kaikessa rekisterinpitäjän toiminnassa. Tietosuojalainsäädäntö rakentuu alla olevien seitsemän keskeisen periaatteen ympärille.

1. **Lainmukaisuus, kohtuullisuus ja läpinäkyvyys** tarkoittavat sitä, että henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

    - **Käytännön toimenpiteitä:** Golfyhteisöjen tulee varmistaa, että kaikelle henkilötietojen käsittelylle on jokin alla kohdassa 3 mainittu käsittelyperuste. Golfyhteisöjen pitää myös huolehtia, että kohdassa 4 viitatut informointivelvoitteet täytetään eli rekisteröidyille annetaan tietoja siitä, miten tietoja käsitellään ja heille kerrotaan esimerkiksi kohdassa 4 mainitussa tietosuojaselosteessa käsittelyyn sovellettava käsittelyperuste.

2. **Käyttötarkoitussidonnaisuus** tarkoittaa, että henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

    - **Käytännön toimenpiteitä:** Golfyhteisöjen pitää määritellä kaikelle käsiteltävälle henkilötiedolle käyttötarkoitus eli se, miksi ja mitä varten henkilötietoja käsitellään. Tämä käyttötarkoitus tulee myös informoida rekisteröidyille (esim. tietosuojaselosteella, ks. kohta 4). Lähtökohtaisesti tietoja saa käsitellä vain tähän ennalta määriteltyyn käyttötarkoitukseen. Esimerkkejä käyttötarkoituksista voi olla markkinointi, asiakassuhteen hoitaminen, työnantajan velvoitteiden hoitaminen tai palvelujen tuottaminen.

3. **Tietojen minimointi** tarkoittaa, että henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

    - **Käytännön toimenpiteitä:** Golfyhteisön tulee käydä läpi sen keräämät ja käsittelemät henkilötiedot ja arvioida, onko kaikille henkilötiedoille tarvetta aiottujen käyttötarkoitusten toteuttamiseksi. Tiettyjä tietoja on esimerkiksi tarpeen kerätä ja käsitellä jäsensuhteen hallinnoimiseksi, mutta näitä tietoja läpikäydessä tulisi esittää kysymys siitä, ovatko kaikki tähän asti kerätyt tiedot tarpeellisia tämän (tai mahdollisesti muun) tarkoituksen vuoksi. Jos tarpeettomia tietoja ilmenee, tulisi ne lähtökohtaisesti poistaa.

4. **Tietojen täsmällisyys** tarkoittaa, että henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä.

    - **Käytännön toimenpiteitä:** Golfyhteisön tulisi pyrkiä siihen, että käsiteltävät henkilötiedot ovat ajantasaisia ja oikein. Hyödyllistä voi olla suunnitella prosessi, jonka avulla tiedot voidaan pitää ajantasaisina ja tarvittaessa korjata virheelliset tiedot. Golfyhteisöjen käsittelemien jäsentietojen osalta tällainen prosessi voi olla esimerkiksi jo käytössä oleva toimintamalli siitä, että jäsentä pyydetään tarkastamaan NexGolfissa olevat tietonsa uuden kauden alkaessa. Yhtä ainoaa oikeaa tapaa tämän periaatteen toteuttamiseksi ei kuitenkaan ole, vaan mahdolliset prosessit tulee suunnitella kunkin golfyhteisön omaan toimintaan sopiviksi käsittelytoimintoihin liittyvät erityispiirteet huomioiden.

5. **Tietojen säilytyksen rajoittaminen** tarkoittaa, että henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

    - **Käytännön toimenpiteitä:** Kaikille henkilötiedoille tulisi määritellä säilytysaika tai vähintäänkin kriteerit sille, kuinka pitkään tietoja säilytetään (tiettyjä tietoja voi olla tarpeen käsitellä esimerkiksi koko jäsenyyden ajan). Tämän säilytysajan pitäisi olla perusteltavissa aiottujen käyttötarkoitusten näkökulmasta ja säilytysajat on informoitava

rekisteröidyille esim. tietosuojaselosteella. Säilytysajan umpeutuessa tulee tiedot lähtökohtaisesti poistaa. Välttämättä tarkan säilytysajan (kuten 5 vuotta niiden keräämisestä) määrittely ei aina ole mahdollista, vaan joidenkin tietojen osalta säilytysaika voi olla sidottuna esimerkiksi jäsenyyteen siten, että tiettyjä tietoja käsitellään koko jäsenyyden ajan.

6. **Tietojen eheys ja luottamuksellisuus** tarkoittaa, että 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.

    - **Käytännön toimenpiteitä:** Golfyhteisön tulisi varmistaa se, että henkilötietoja säilytetään tietoturvallisesti (esim. järjestelmän tietoturvallisuus tai paperisen aineiston säilyttäminen lukitussa tilassa). Henkilöstöllä tulisi olla tämän tehtävät huomioon ottaen asianmukainen salassapitovelvollisuus. Pääsyä henkilötietoihin tulisi käyttövaltuuksin rajoittaa siten, että vain ne henkilöt pääsevät käsiksi henkilötietoihin, keiden työtehtävien hoitamisen kannalta se on tarpeellista.

7. **Osoitusvelvollisuus** tarkoittaa sitä, että rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että yllä olevia periaatteita on noudatettu ja että tietosuojavelvoitteet on muutoinkin huomioitu.

    - **Käytännön toimenpiteitä:** Golfyhteisön tulee ylläpitää asianmukaista dokumentaatiota ja toimintamalleja. Tämä tarkoittaa esim. tietojenkäsittelysopimusten päivittämistä, tietoturvaloukkauksien dokumentointia ja tietosuojaselosteiden laatimista ja ylläpitämistä. Golfyhteisö voi myös harkita yhteisön oman tietosuojapolitiikan laatimista, jossa kuvataan sitä, miten tietosuoja huomioidaan yhteisön toiminnassa. Asetus ei kuitenkaan nimenomaisesti velvoita tällaisen tietosuojapolitiikan laatimiseen.

3 KÄSITTELYN OIKEUSPERUSTEET

Lähtökohtana kaikelle henkilötiedon käsitellylle on se, että sille pitää olla laissa säädetty käsittelyperuste. Näitä käsittelyperusteita ovat alla luetellut kuusi perustetta, joista vähintään yhden on oltava käsillä:

1. Rekisteröity on antanut suostumuksensa. Suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen. Suostumuksen tulee olla myös vapaasti peruutettavissa milloin tahansa.

2. Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Esimerkiksi työntekijöiden henkilötietojen käsittelyn voidaan katsoa perustuvan tietyiltä osin työsopimuksen täytäntöönpanoon (esim. palkanmaksu ja siihen liittyvä käsittely). Sopimuksen täytäntöönpanoon liittyvää käsittelyä voi olla myös se, kun henkilö esim. varaa

itselleen lähtöajan tai vuokraa itselleen golfauton taikka bägivaraston ja tähän liittyen käsitellään henkilön henkilötietoja.

3. Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Tällainen lakisääteinen velvoite voi olla käsillä esim. yhdistyksen jäsenluettelon ylläpitämisen osalta[1] tai osan työsuhteeseen liittyvän käsittelyn osalta.

4. Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Tämä käsittelyperuste kohdistuu lähinnä "hätätapauksiin" (tajuton henkilö tuodaan sairaalaan) eikä tämän soveltuminen yleisesti ottaen tule todennäköisesti kyseeseen golfyhteisön toiminnan yhteydessä.

5. Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Tämä käsittelyperuste ei ole erityisen relevantti golfyhteisöjen osalta (koskee lähinnä viranomaistoimintaa).

6. Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi. Oikeutettuun etuun perustuva käsittely siten edellyttää ennakolta tehtävää intressipunnintaa. Tällainen intressipunninta on suositeltavaa laatia huolella ja dokumentoida mm. rekisterinpitäjän osoitusvelvollisuudesta johtuen. Käytännössä "oikeutetut edut" -käsittelyperuste jättää rekisterinpitäjälle tiettyä harkintavaltaa siitä, millaisiin tilanteisiin kyseistä käsittelyperustetta voidaan soveltaa. Tyypillisesti oikeutettujen etujen mukaiseksi käsittelyksi voidaan katsoa esimerkiksi henkilötietojen käsittely markkinointitarkoituksiin. Myös esimerkiksi erilaiset asiakastyytyväisyyskyselyihin tai markkinatutkimuksiin liittyvä henkilötietojen käsittely voidaan tyypillisesti toteuttaa rekisterinpitäjän oikeutettujen etujen perusteella. Vastuu oikeutettujen etujen olemassaolon arvioinnista on rekisterinpitäjällä. Lainsäädännössä ei ole tarkemmin rajattu sitä, mikä voidaan katsoa oikeutetuksi eduksi vaan tämä edellyttää tapauskohtaista harkintaa.

Suostumus on vain yksi käsittelyn oikeusperuste eikä se välttämättä ole tarkoituksenmukaisin käsittelyperuste kaikkiin tilanteisiin ottaen huomioon mm. sen, että suostumus on aina vapaasti peruutettavissa. Jos suostumus peruutetaan, tulee myös suostumukseen perustunut käsittely lopettaa.

Jos henkilötietoja käsitellään suostumuksen perusteella, tulee kiinnittää huomiota suostumuksen pyytämistapaan. Suostumus on annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella tai suullisella lausumalla, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn. Rekisteröity voi esimerkiksi rastittaa ruudun vieraillessaan internetsivustolla. Suostumusta ei voi antaa vaikenemalla, valmiiksi

[1] Yhdistyslain (26.5.1989/503) 3 luvun 11 §:n 1 momentti: "Yhdistyksen jäsenistä on hallituksen pidettävä luetteloa. Luetteloon on merkittävä kunkin jäsenen täydellinen nimi ja kotipaikka."

rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta. Suostumuksen olisi katettava kaikki käsittelytoimet, jotka toteutetaan samaa tarkoitusta tai samoja tarkoituksia varten. Jos käsittelyllä on useita tarkoituksia, suostumus olisi annettava kaikkia käsittelytarkoituksia varten. Jotta suostumuksen voidaan katsoa olevan "tietoinen" tulee rekisteröidylle olla selkeää, mihin tarkoituksiin hän suostumuksensa antaa, eli käytännössä suostumuksen pyytämisen yhteydessä rekisteröidylle on selkeästi informoitava aiotusta käsittelystä (esim. suostumuslausekkeessa tiiviissä muodossa sekä tarkemmin tietosuojaselosteella).

Yllä kuvatuista suostumukseen liittyvistä velvoitteista johtuen on usein suositeltavaa harkita, soveltuisiko jokin muu käsittelyperuste kuin suostumus (ellei tarkoitus ole, että kyseinen henkilötietojen käsittely on aidosti tarkoitettu vapaaehtoiseen suostumukseen perustuvaksi).

4 INFORMOINTIVELVOITE

Keskeinen velvoite rekisterinpitäjille on informointivelvoite, eli rekisteröidyille tulee kertoa mm. siitä, miten ja mihin tarkoituksiin häntä koskevia tietoja käytetään.[2]

Tietosuoja-asetus edellyttää, että organisaatiot toimittavat rekisteröidylle tietoja tilanteissa, joissa henkilötiedot kerätään suoraan rekisteröidyltä sekä tilanteissa, joissa henkilötiedot kerätään muulta kuin rekisteröidyltä itseltään. Rekisterinpitäjän on toimitettava henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Kun tietoja saadaan muualta kuin rekisteröidyltä itseltään, on kerrottava mm. se, mistä henkilötiedot on saatu. Tiedot on toimitettava kohtuullisen ajan kuluttua mutta viimeistään kuukauden kuluessa henkilötietojen saamisesta. Jos henkilötietoja käytetään viestintään asianomaisen rekisteröidyn kanssa, tiedot on toimitettava viimeistään silloin kun näitä tietoja luovutetaan ensimmäisen kerran. Jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, tiedot on toimitettava viimeistään silloin, kun näitä tietoja luovutetaan ensimmäisen kerran.

Informointivelvoitteiden toteuttamiseksi rekisterinpitäjät usein laativat tietosuojaselosteita rekisteröityjen saataville (esim. verkkosivustolle). Tietosuojaseloste on usein suositeltavaa laatia esimerkiksi kunkin eri "käsittelykokonaisuuden" (kuten työntekijöiden, asiakkaiden ja jäsenien tietojen käsittely) osalta erikseen. Malli tietosuojaselosteesta on toimitettu tämän ohjeistuksen ohessa.[3]

---

[2] Ks. tarkemmin informointivelvoitteisiin sisältyvät tiedot mm. asetuksen 13 ja 14 artikloista.

[3] Tietosuoja-asetuksen 30 artikla vaatii myös tietyissä tilanteissa ylläpitämään selostetta rekisterinpitäjän vastuulla olevista käsittelytoimista. Toimitettua tietosuojaselostepohjaa voidaan käyttää myös tämän velvoitteen täyttämisen yhteydessä. Kaikki laaditut tietosuojaselosteet yhdessä muiden mahdollisten tietosuojan toimintaperiaatteita koskevan dokumentaation kanssa voidaan katsoa täyttävän 30 artiklan edellyttämän selosteen. Selosteen tarkoituksena on, että dokumentaation pohjalta saa ajantasaisen kokonaiskuvan organisaation harjoittamasta henkilötietojen käsittelystä. Tietosuojavaltuutettu on myös julkaissut internetsivuilla mallipohjan, jota voidaan käyttää tällaisen selosteen laatimiseksi. Tietosuojavaltuutetun internetsivut sisältävät myös tarkempaa tietoa siitä, milloin tällainen seloste on laadittava (ks. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/selostekasittelytoimista.html).

Suositeltavaa olisi pitää mm. jäsenten ja muiden asiakkaiden henkilötietojen käsittelyä kuvaava tietosuojaseloste saatavilla esimerkiksi golfyhteisön internetsivuilla. Tämän lisäksi henkilön liittyessä yhteisön jäseneksi tai osakkaaksi, voidaan esimerkiksi tähän liittyvässä sopimuksessa tai ehdoissa kertoa, että tarkempia tietoja henkilötietojen käsittelystä on saatavilla tietosuojaselosteelta (ja kertoa, mistä tietosuojaseloste on saatavilla). Mikäli asiakkaille lähetetään erilaisia automaattisia kyselyitä (kuten Pelaaja Ensin), voi golfyhteisö myös harkita lisäävänsä tässä yhteydessä lähetettävään viestiin linkin tätä käsittelyä koskevaan tietosuojaselosteeseen (esimerkiksi viestin lopussa voi olla teksti "Tarkempaa tietoa henkilötietojesi käsittelystä saat tietosuojaselosteesta: [linkki]."). Käytännössä informointi voidaan kuitenkin toteuttaa monella eri tapaa ja tärkeintä on, että rekisteröidyllä on mahdollisuus saada tietää, miten häntä koskevia tietoja käsitellään.

5 REKISTERÖIDYN OIKEUDET

Tietosuoja-asetus antaa rekisteröidyille entistä enemmän oikeuksia, joiden avulla rekisteröidyt voivat itse valvoa ja vaikuttaa heitä koskevien henkilötietojen käsittelyyn. Rekisteröidyn oikeuksien toteuttaminen on keskeinen rekisterinpitäjän velvoite ja näiden oikeuksien toteuttaminen vaatii valmistautumista ja suunnittelua.

Rekisteröidyn pyyntöihin käyttää tietosuoja-asetuksen mukaisia oikeuksiaan on vastattava lähtökohtaisesti kuukauden kuluessa pyynnön esittämisestä (määräaikaa on tietyissä tilanteissa mahdollista jatkaa enintään kahdella kuukaudella). Tämä tarkoittaa sitä, että esim. tarkastusoikeuden osalta tiedot on toimitettava kuukauden kuluessa pyynnön esittämisestä. Rekisteröidyn oikeuksien käyttämisestä ei saa lähtökohtaisesti periä maksua rekisteröidyltä (elleivät pyynnöt ole ilmeisen perusteettomia tai kohtuuttomia).

5.1 Rekisteröidyn oikeus saada pääsy tietoihin (ns. tarkastusoikeus)

Rekisteröidyllä on oikeus tarkastaa *itseään koskevat*[4] henkilötiedot ja saada niistä jäljennös. Mikäli rekisteröity esittää pyyntönsä sähköisesti, tulee myös annettavat tiedot toimittaa lähtökohtaisesti sähköisessä muodossa. Henkilöllä on oikeus tarkastaa vain itseään koskevat henkilötiedot, eikä siten muiden henkilötietoja voida antaa. Esimerkiksi golfyhteisön asiakas tai työntekijä voi esittää yhteisölle pyynnön siitä, että hän haluaa saada kopion kaikista niistä henkilötiedoista, joita yhteisöllä hänestä on.

Lähtökohtaisesti tarkastusoikeus koskee kaikkia niitä rekisteröidyn henkilötietoja, joita rekisterinpitäjä käsittelee. Tietyissä tilanteissa tarkastusoikeutta on voitu esim. lainsäädännössä rajoittaa tai myös liikesalaisuudet voivat joissain tapauksissa olla peruste olla antamatta kaikkia tietoja. Rekisteröity voi myös halutessaan kohdistaa pyyntönsä esimerkiksi vain tiettyihin häntä koskeviin tietoihin.

Pyyntöjen toteuttamisen lähtökohtana on maksuttomuus, eli rekisteröidyltä ei saa periä mitään maksua pyydettyjen tietojen toimittamisesta. Jos rekisteröity kuitenkin pyytää

[4] Huom., että kyseessä on henkilökohtainen oikeus, eikä siten toista henkilöä koskevia tietoja voida antaa tarkastusoikeuden yhteydessä (esim. lähtökohtaisesti vanhemmat eivät voi tarkastaa täysi-ikäisen lapsen henkilötietoja).

useampia jäljennöksiä toimitettavista tiedoista, voidaan näistä lisäkopioista periä kohtuullinen todellisiin hallinnollisiin kustannuksiin perustuva maksu.

Tarkastusoikeuden yhteydessä rekisteröidylle on myös annetta tiettyjä tietoja[5] siitä, miten häntä koskevia tietoja käsitellään. Käytännössä tarkastuspyynnön yhteydessä voidaan esimerkiksi antaa relevantit tietosuojaselosteet, joissa vaaditut tiedot on kuvattu.

5.2 Oikeus tietojen oikaisemiseen

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

Käytännössä tämä tarkoittaa sitä, että mikäli golfyhteisöjen tietojärjestelmissä on virheellistä tietoa henkilöstä, tulee tällaiset tiedot korjata.

5.3 Oikeus tulla unohdetuksi

Rekisteröidyllä on myös oikeus pyytää henkilötietojensa poistamista tietyissä tilanteissa.[6] Henkilötiedot on poistettava esimerkiksi silloin, jos tietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai jos rekisteröity peruuttaa suostumuksensa eikä käsittelyyn ole muuta laillista perustetta.

Oikeus tulla unohdetuksi ei kuitenkaan ole absoluuttinen. Esimerkiksi silloin, kun tiedot ovat tarpeen seuran tai kenttäyhtiön lakiin perustuvien velvoitteiden täyttämiseksi (esim. velvollisuus antaa työtodistus työntekijälle), ei tietoja tarvitse poistaa.

5.4 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus siirtää rekisterinpitäjälle toimittamansa häntä koskevat henkilötiedot rekisterinpitäjältä toiselle. Tiedot on voitava siirtää jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa[7]. Rekisteröidyllä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, mikäli se on teknisesti mahdollista. Oikeus siirtoon on vain silloin, jos käsittely perustuu suostumukseen tai sopimukseen, ja jos käsittely suoritetaan automaattisesti (eli käytännössä silloin, kun tietoja käsitellään tietojärjestelmässä).

Käytännössä siirto-oikeus tulee kyseeseen varsin harvoin ja kohdistuu todennäköisesti vain varsin suppeaan tietojoukkoon golfyhteisöjen toiminnan osalta.

5.5 Vastustamisoikeus

Rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä tietyissä tilanteissa. Käytännössä vastustamisoikeus tulee kyseeseen silloin, kun tietojen käsittely perustuu rekisterinpitäjän oikeutettuihin etuihin (ks. yllä kappaleessa 3 olevan listan kohta 6).

---

[5] Ks. tarkemmin tietosuoja-asetuksen 15 artikla.

[6] Ks. tarkemmin tietosuoja-asetuksen 17 artikla.

[7] Yleisesti käytettävissä olevan koneellisesti luettavan muodon vaatimuksen voidaan katsoa täyttyvän esimerkiksi CSV-tiedoston kohdalla.

Suoramarkkinoinnin osalta vastustamisoikeus tarkoittaa käytännössä rekisteröidyn oikeutta kieltää hänen tietojensa käsittely markkinointitarkoituksiin, eli tältä osin vastustamisoikeus on absoluuttinen. Mikäli rekisteröity kieltää tietojensa käyttämisen suoramarkkinointiin, ei henkilöön saa enää kohdistaa markkinointitoimenpiteitä.

Mikäli muu kuin markkinointitarkoituksissa tapahtuva käsittely perustuu rekisterinpitäjän oikeutettuihin etuihin, vastustamisoikeuden käyttäminen johtaa siihen, että rekisterinpitäjän pitää uudestaan arvioida oikeutettujen etujen olemassaolo suhteessa rekisteröidyn oikeuksiin ja vapauksiin. Mikäli rekisterinpitäjän *huomattavan tärkeä ja perusteltu syy* (tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi) edellyttää tietojenkäsittelyn jatkamista, ei käsittelyä tarvitse kyseisen rekisteröidyn osalta lopettaa[8].

Mikäli henkilö käyttää vastustamisoikeuttaan, tulee golfyhteisöllä olla mahdollisuus markkinoinnin osalta ottaa vastaan henkilön markkinointikielto ja pystyä varmistumaan, ettei kyseisen henkilön tietoja käsitellä enää markkinointitarkoituksissa. Käytännössä esim. asiakkaan tietoihin pitäisi lisätä tätä koskeva tieto ja markkinointikäytännöissä ennen markkinointiviestin lähettämistä pitäisi varmistaa, ettei henkilö ole kieltänyt häneen kohdistuvaa markkinointia.

5.6 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus saada aktiivinen henkilötietojen käsittely rajoitetuksi asetuksessa luetellussa neljässä eri tilanteessa.[9] Oikeus on olemassa muun muassa silloin, kun rekisteröity esittää henkilötietojen oikaisua tai poistoa koskevan pyynnön, tai jos käsittely on lainvastaista ja rekisteröity vaatii käytön rajoittamista henkilötietojen poistamisen sijaan.

Käytännössä rajoittaminen voi tulla kyseeseen, kun rekisteröity kiistää jonkin tiedon paikkansapitävyyden ja vaatii, että käsittelyä on rajoitettava siksi aikaa, kunnes rekisterinpitäjä on voinut varmistaa tietojen paikkansapitävyyden. Tarkoituksena on siis estää se, ettei mahdollisesti virheellistä tietoa tässä yhteydessä käsiteltäisi. Käsittelyn rajoittaminen voi tulla myös vastaan tilanteessa, jossa rekisteröity vastustaa tietojen käsittelyä, jolloin käsittelyä tulee rajoittaa siksi aikaa, kunnes rekisterinpitäjä on arvioinut sen, syrjäyttävätkö rekisterinpitäjän edut rekisteröidyn edut, eli voidaanko käsittelyä edelleen jatkaa.

Kun henkilötietojen käsittelyä on rajoitettu, ei tietoja saa aktiivisesti käsitellä (eli tietoja saa pelkästään säilyttää).

5.7 Ilmoitusvelvollisuus

Mikäli golfyhteisö oikaisee, poistaa tai rajoittaa henkilötietojen käsittelyä oma-aloitteisesti tai rekisteröidyn pyynnöstä, on tästä ilmoitettava jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Poikkeuksena tästä velvollisuudesta on tilanne, jossa velvollisuus osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa.

---

[8] Muista dokumentoida ja perustella tällainen arvio.

[9] Ks. tarkemmin tietosuoja-asetuksen 18 artikla.

Käytännössä tämä tarkoittaa sitä, että mikäli henkilö käyttää "oikeuttaan tulla unohdetuksi" ja tämän perusteella esim. entisen jäsenen tiedot poistetaan, tulee tästä rekisteröidyn pyynnöstä tulla unohdetuksi ilmoittaa myös niille yhteistyökumppaneille, joille poistamisen kohteena olleita henkilötietoja on mahdollisesti luovutettu.

6 KÄSITTELYN TURVALLISUUS

Osana asianmukaista tietosuojaa on myös tietoturvallisuudesta huolehtiminen. Tietosuojassa on kyse henkilön yksityiselämän suojaamisesta henkilötietoja käsitellessä ja tietoturva puolestaan tarkoittaa tietojen saatavuuden, luottamuksellisuuden ja eheyden turvaamista. Tietosuoja-asetus velvoittaa (asetuksen 32 artikla) rekisterinpitäjät ja henkilötietojen käsittelijät toteuttamaan käsittelyyn liittyvät riskit huomioon ottaen tarvittavat tekniset ja organisatoriset toimenpiteet, jotta käsittelyn turvallisuus voidaan varmistaa (mm. koulutus, palomuurit, salasanasuojaukset, säännölliset päivitykset ja käyttöoikeuksien ja -valtuuksien hallinta).

Käytännössä tämä tarkoittaa varsinaisten tietojärjestelmien tietoteknisen turvallisuuden lisäksi mm. sitä, että pääsyä henkilötietoihin rajoitetaan. Vain niillä henkilöillä tulisi olla pääsy niihin henkilötietoihin, jotka ovat tarpeen henkilön työtehtävien hoitamiseksi. Esimerkiksi caddiemastereilla tulee olla pääsy jäsenten/asiakkaiden henkilötietoihin työtehtäviensä hoitamiseksi (kuten esimerkiksi ajanvarausten tekemiseksi), mutta mikäli heidän työtehtävänsä ei edellytä golfyhteisön työntekijöiden henkilötietoihin pääsyä, ei heillä myöskään tulisi olla pääsyä näihin tietoihin. Golfyhteisöjen pitäisi ottaa tämä huomioon mm. käyttöoikeuksia ja -valtuuksia myönnettäessä. Henkilöstö tulisi myös sitouttaa asianmukaisella tavalla salassapitoon (esim. työsopimuksissa) ja heitä olisi hyvä selkeästi tiedottaa tietosuojaan ja -turvaan liittyvistä velvoitteista (esim. työsuhteen alkaessa). Henkilökunnan kouluttaminen henkilötietojen asianmukaisesta käsittelystä on myös yksi keskeinen toimenpide, jolla käsittelyn turvallisuutta voidaan parantaa.

Tietojärjestelmien lisäksi tietoturvallisuus on syytä huomioida mahdollisen paperisen aineiston osalta (esim. niiden säilyttäminen lukitussa tilassa).

7 TOIMINTAMALLIT JA TIETOSUOJAORGANISAATIO

7.1 Toimintamallit

Tietosuojan toteuttaminen organisaatiossa edellyttää käytännössä erilaisten toimintamallien laatimista ja jalkauttamista henkilöstölle. Tässä kappaleessa on tuotu esille joitain keskeisiä toimintamalleja, joita yrityksellä olisi hyvä vähintäänkin olla.

7.1.1 Markkinointi

Golfyhteisöjen tulee suunnitella markkinointikäytäntönsä siten, että ne täyttävät tietosuojalainsäädännön velvoitteet.[10] Golfyhteisön tulee kiinnittää huomiota siihen, mistä se hankkii markkinoinnissa käytetyt tiedot ja täyttyvätkö keskeiset tietosuojaperiaatteet markkinoinnin yhteydessä.

[10] Suoramarkkinoinnin osalta tulee tietosuoja-asetuksen lisäksi kiinnittää huomiota myös tietoyhteiskuntakaaren (917/2014) velvoitteisiin.

Keskeistä on mm. varmistaa, että:

- markkinointiin käytetyt tiedot on hankittu tietosuojalainsäädännön mukaisesti ja niiden käyttöön on käsittelyperuste (kuten rekisterinpitäjän oikeutetut edut);
- henkilötietojen keräämisestä ja niiden käyttämisestä markkinointiin on informoitu rekisteröityjä;
- yksityishenkilöihin kohdistuvaa sähköistä suoramarkkinointia (esim. sähköpostilla lähetettävä markkinointiviesti) varten on saatu etukäteinen nimenomainen suostumus; ja
- rekisteröidyillä on mahdollista kieltää markkinointi ja tällöin markkinointi voidaan lopettaa.

7.1.2 Rekisteröidyn oikeuksien toteuttaminen

Rekisterinpitäjän olisi suositeltavaa suunnitella valmiiksi prosessi sitä varten, miten rekisteröidyn oikeudet toteutetaan. Valmiiksi suunniteltu prosessi auttaa rekisterinpitäjää toteuttamaan pyynnöt asetuksen mukaisessa määritellyssä ajassa ja vähentää myös pyynnöistä aiheutuvia hallinnollisia rasitteita. Rekisterinpitäjän pitäisi kiinnittää huomioita ainakin seuraaviin seikkoihin:

- Mitkä rekisteröidyn oikeudet voivat kohdistua omaan toimintaamme? Mitä tietoja rekisteröity voi pyytää poistettavaksi? Voidaanko tällaiset tiedot poistaa järjestelmistä?
    - Selvitä ja dokumentoi se, mitkä tiedot kuuluvat tarkastus- ja siirto-oikeuden piiriin. Jos mahdollista, laadi valmiita lomakkeita, joilla tiedot voidaan toimittaa (tai selvitä, onko tietojärjestelmistä mahdollista saada valmiita listauksia tätä varten).
    - Varaudu siihen, että rekisteröity vastustaa käsittelyä, vaatii käsittelyn rajoittamista, peruu suostumuksensa tai pyytää tietojensa poistamista (ns. "oikeus tulla unohdetuksi").
    - Miten varmistetaan, että esimerkiksi markkinoinnin kieltämisen jälkeen tietoja ei enää käytetä markkinointiin?
- Kuka toimii vastuuhenkilönä rekisteröidyn oikeuksien toteuttamisessa ja huolehtii siitä, että ne toteutetaan lain edellyttämällä tavalla (mm. vastataan määräajan puitteissa)? Kuka käytännössä toteuttaa rekisteröidyn pyynnöt?
- Miten rekisteröidyn henkilöllisyys todennetaan eri tilanteissa (esimerkiksi kun pyyntö esitetään paikan päällä tai jos se esitetään sähköpostitse)?
- Miten tiedot toimitetaan rekisteröidylle?
- Miten rekisteröidyn esittämät pyynnöt ja niihin liittyvät vastaukset dokumentoidaan mm. osoitusvelvollisuudesta johtuen?

Selvitä myös missä yhteyksissä rekisteröidyiltä kerätään suostumuksia. Golfyhteisöllä pitäisi olla kyvykkyys hallinnoida suostumuksia siten, että mahdollinen suostumuksen peruuttaminen tulee kirjatuksi, jolloin myös suostumukseen perustuvan käsittelyn tulee loppua. Suunnittele, miten tämä toteutetaan ja millä tapaa rekisteröidyllä on mahdollisuus peruuttaa suostumuksensa. Annetun suostumuksen olemassaolo pitää myös tarvittaessa pystyä osoittamaan.

7.1.3 Tietosuojan tietoturvaloukkaukset

Tietosuoja-asetuksen mukaan rekisterinpitäjällä on tietyissä tilanteissa velvollisuus ilmoittaa henkilötietoihin kohdistuneista tietoturvaloukkauksista viranomaisille ja mahdollisesti myös rekisteröidyille.

Tietoturvaloukkauksella tarkoitetaan tässä yhteydessä tapahtumaa tai toimenpidettä, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Tietoturvaloukkaus voi siten olla varsinaisen tietomurron lisäksi myös esimerkiksi inhimillisestä virheestä tapahtuva henkilötietoja sisältävän viestin lähettäminen väärälle vastaanottajalle.

Ilmoitus viranomaiselle on tehtävä ilman aiheetonta viivästystä, mutta kuitenkin 72 tunnin kuluessa, siitä kun tietoturvaloukkaus havaittiin. Poikkeus tähän ilmoitusvelvollisuuteen on sellainen tietoturvaloukkaus, josta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivästystä myös rekisteröidyille silloin, kun tietoturvaloukkauksesta todennäköisesti aiheutuu korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksen seurauksia ja siitä aiheutuvaa riskiä tulee siten aina arvioida rekisteröityjen näkökulmasta. Tarkempaa tietoa mm. ilmoituksen sisällöstä löytyy tietosuoja-asetuksen 33 ja 34 artikloista (ks. linkki yllä).

Tapahtuneet tietototurvaloukkaukset ja tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet on kuitenkin aina dokumentoitava. Dokumentoinnin tarkoituksena on mm. se, että viranomaiset voivat tarkistaa, onko tietoturvaloukkauksiin liittyviä velvoitteita noudatettu.

Golfyhteisön tulisi suunnitella toimintamalli sille, miten ja kenen toimesta ilmoitukset tehdään ja varmistaa, että henkilökunta ymmärtää mitä tietoturvaloukkaukset ovat ja miten silloin tulee toimia. Tällainen toimintamalli voi esimerkiksi olla se, että henkilökunta ilmoittaa havaitut tietoturvaloukkaukset (tai jos tällaisista on epäilys) yhteisön toimitusjohtajalle, joka arvioi tilanteen ja ryhtyy tarvittaviin toimenpiteisiin.

7.2 Tietosuojaorganisaatio

Golfyhteisön tulisi myös suunnitella tietosuojaorganisaationsa siten, että tietosuojaan liittyvien eri osa-alueiden vastuut olisi jaoteltu nimetyille henkilöille.[11] Organisaation

[11] Tietosuoja-asetus edellyttää tietyissä tilanteissa nimenomaisen *tietosuojavastaavan* nimittämistä. Tietosuojavastaava on nimitettävä lähinnä silloin, kun yrityksen ydintehtäviin liittyy rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai

koosta ja rakenteesta riippuen voi tähän riittää yksikin henkilö. Päävastuu ja kokonaiskuvan hallinta golfyhteisön tietosuoja-asioista on useimmissa tapauksissa suositeltavaa keskittää yhdelle henkilölle, joka voi tarpeellisin osin delegoida tehtäviään.

8 YHTEISTYÖKUVIOT JA ALIHANKKIJAT

Yhteistyökuvioihin liittyvien henkilötietojen käsittelyn osalta on syytä selvittää se, luovutetaanko tai siirretäänkö henkilötietoja ulkopuolisille toimijoille ja missä yhteyksissä käytetään henkilötietojen käsittelijöitä.

8.1 Henkilötietojen käsittelijän käyttäminen

Henkilötietojen käsittelijän käyttämisestä on kyse mm. tilanteissa, joissa käytetään alihankkijaa tai palveluntarjoajaa, joka käsittelee tietoja rekisterinpitäjän ohjeiden mukaan (eli esimerkiksi golfseura määrää käsittelyn keinot ja tarkoitukset).

Tietosuoja-asetus velvoittaa rekisterinpitäjän (artikla 28) laatimaan tietynsisältöisen sopimuksen henkilötietojen käsittelijän (ks. määritelmät yllä) kanssa. Tämä tarkoittaa sitä, että myös olemassa olevia sopimuksia tulee päivittää, mikäli ne eivät ole tietosuoja-asetuksen 28 artiklan mukaisia. Tällaisessa sopimuksessa pitää mm. velvoittaa henkilötietojen käsittelijä avustamaan rekisterinpitäjää sen velvoitteiden ja rekisteröidyn oikeuksien toteuttamisessa (ks. tarkempi lista ko. artiklasta).

Tällaisen sopimuksen tekeminen voi olla tarpeen esimerkiksi tilitoimiston, tilintarkastajayhteisön ja erilaisten IT-palvelujen tarjoajien kanssa (mahdollisesti myös esim. muiden palveluntarjoajien, kuten opetus- tai ylläpitopalveluja tarjoavien yritysten kanssa, mikäli tässä yhteydessä palveluntarjoaja käsittelee henkilötietoja). Työterveyspalveluja tuottavien terveyskeskusten osalta tällainen sopimus ei lähtökohtaisesti ole tarpeen, sillä tyypillisesti työterveyspalveluja tuottavat yritykset toimivat tältä osin itsenäisinä rekisterinpitäjinä.

8.1.1 Käytännön näkökulmia

Henkilötietojen käsittelijän käyttäminen tulee usean golfyhteisön osalta tyypillisesti vastaan esimerkiksi käytettäessä Golfbox, Nexgolf, Pelaaja Ensin, Feelback, Zef sekä Koodiviidakko -palveluita. Tällaisten palveluntarjoajien kanssa tehdyt sopimukset tulee päivittää 25.5.2018 mennessä tietosuoja-asetuksen 28 artiklan vaatimukset täyttäviksi. Tällaisessa sopimuksessa tulee olla sovittuna asetuksen 28(3) artiklan kohdissa a-h mainitut seikat, jonka lisäksi esimerkiksi sopimuksen liitteessä tulee kuvata 1) käsittelyn kohde ja kesto, 2) käsittelyn luonne ja tarkoitus sekä 3) henkilötietojen tyyppi ja rekisteröityjen ryhmät.

Näiden toimijoiden osalta golfyhteisön olisi myös hyvä varmistua siitä, että kyseiset toimijat voivat täyttää sopimuksessa heille asetettavat tietosuojaan ja tietoturvaan

---

jos ydintehtävät muodostuvat laajamittaisesta erityisiin henkilötietoryhmiin (esim. terveystiedot) kohdistuvista käsittelytoimista. Todennäköistä on, ettei golfseuralla tai kenttäyhtiöllä ole velvollisuutta nimittää asetuksen tarkoittamaa tietosuojavastaavaa. Mikäli tietosuojan "vastuuhenkilö" nimitetään golfseuralle tai kenttäyhtiölle, ei tämän henkilön nimikkeenä saisi olla "tietosuojavastaava", sillä tällöin voi syntyä epäselvyys siitä, onko seuralle tai kenttäyhtiölle nimitetty asetuksen tarkoittama tietosuojavastaava.

liittyvät velvoitteet. Tämä on tärkeää siitä syystä, että rekisterinpitäjä on lähtökohtaisesti[12] vastuussa henkilötietojen käsittelystä.

8.2 Henkilötietojen luovuttaminen

Henkilötietojen luovuttaminen on eräänlainen henkilötietojen siirtämisen erityistilanne, jollainen on käsillä silloin, kun tietoja vastaanottava taho käyttää tietoja omiin tarkoituksiinsa eikä siis pelkästään rekisterinpitäjän puolesta ja sen ohjeiden mukaisesti. Henkilötietojen luovuttamisessa on siis kyse tietojen antamisesta yhdeltä rekisterinpitäjältä toiselle. Henkilötietoja luovuttavan rekisterinpitäjän tulee varmistua siitä, että sillä on oikeus luovuttaa henkilötietoja. Tämä edellyttää jonkin käsittelyperusteen olemassaoloa (kuten suostumus tai rekisterinpitäjän "oikeutetut edut"). Luovutuksensaajana oleva rekisterinpitäjä vastaa sen omasta henkilötietojen käsittelystä (toisin kuin käytettäessä henkilötietojen käsittelijää, jolloin tietojen käsittelystä on lähtökohtaisesti vastuussa rekisterinpitäjä). Henkilötietojen luovuttamisesta ei ole lainsäädännöstä tulevaa pakottavaa velvoitetta laatia sopimusta, mutta se on suositeltavaa (luovutussopimuksessa huomioitavat asiat eroavat 28 artiklan mukaisesta sopimuksesta).

Henkilötietojen luovuttaminen voi tulla kyseeseen esimerkiksi silloin, kun jäsenseura luovuttaa keskusrekisterin kautta jäsentietoja golfliitolle ja muille seuroille. Tällaisissa tilanteissa on varmistuttava jonkin käsittelyperusteen olemassaolosta.

Henkilötietojen luovuttamiseksi voidaan katsoa myös se, jos seura tai kenttäyhtiö lähettää omiin asiakastietoihinsa perustuen markkinointiviestintää yhteistyökumppanin puolesta. Nexgolf mahdollistaa luvan keräämisen asiakkaalta tällaiselle tietojen luovuttamiselle. Tässä yhteydessä on tärkeää varmistaa, että sellaisten henkilöiden tietoja ei luovuteta, ketkä eivät ole antaneet lupaa kyseisiin luovutuksiin. Jotta suostumus olisi tietosuoja-asetuksen valossa pätevä, tulee sen muutoinkin täyttää suostumukselle asetetut velvoitteet.

8.3 Kansainväliset tietojen siirrot

Mikäli yhteistyökuvioiden yhteydessä henkilötietoja luovutetaan tai siirretään Euroopan talousalueen ulkopuolelle, tulee tässä yhteydessä ottaa huomioon lainsäädännön erityisedellytykset. Tietojensiirroksi katsotaan jo esimerkiksi se, että tiedot on tallennettuna Euroopan talousalueen ulkopuolella sijaitsevalle pilvipalvelimelle. Yleisen kohdassa 3 mainitun käsittelyperusteen lisäksi vaaditaan siirtoperusteen olemassaoloa, jotta tiedot voidaan tallentaa esimerkiksi Yhdysvalloissa olevalle serverille. Käytännössä yleisin siirtoperuste on laatia EU:n komission hyväksymien mallisopimuslausekkeiden mukainen sopimus tietojensiirrosta yhteistyökumppanin kanssa (myös muita vaihtoehtoja on olemassa ja soveltuvin siirtoperuste on hyvä harkita tapauskohtaisesti)[13].

---

[12] Henkilötietojen käsittelijä voi joutua vastuuseen siinä tilanteessa, että se on toiminut rekisterinpitäjän ohjeiden vastaisesti tai että se ei ole noudattanut henkilötietojen käsittelijöille tietosuoja-asetuksessa asetettuja velvoitteita.

[13] Ks. lisätietoja kansainvälisiä tietojen siirtoja koskevista tietosuoja-asetuksen artikloista 44 - 50.

9 NYKYTILAN ARVIOINTI JA TARVITTAVAT TOIMENPITEET

Ensimmäisenä toimenpiteenä tietosuoja-asetuksen velvoitteisiin varautumisessa on suositeltavaa ryhtyä selvittämään toiminnan nykytilaa ja vastata mm. alla tässä kappaleessa listattuihin kysymyksiin.

- Missä kaikissa yhteyksissä käsitellään henkilötietoja? Mitä henkilötietoja toiminnassa käsitellään/kerätään (käsitelläänkö esim. erityisiä henkilötietoryhmiä kuten terveystietoja)?
- Miksi ja mitä tarkoitusta varten näitä tietoja käsitellään? Ovatko kaikki tiedot tarpeellisia?
- Mistä henkilötiedot saadaan? Luovutetaanko henkilötietoja toisille rekisterinpitäjille?
- Missä tiedot sijaitsevat (excel-taulukoissa, tietojärjestelmissä, paperisissa kansioissa, palveluntarjoajien järjestelmissä, pilvipalveluissa…)?
- Kuinka pitkään ja missä tietoja säilytetään? Miten tietoturvallisuus on huomioitu säilyttämisessä? Milloin ja miten tiedot poistetaan? Miten tietojen elinkaaren hallinta keräämisestä poistamiseen on järjestetty?

Nykytilan arviointi on suositeltavaa dokumentoida sopivalla tavalla. Kun nykytilanne on selvitetty, seuraava askel on ryhtyä soveltamaan tässä ohjeistuksessa kuvattuja tietosuojavelvoitteita käytännön toimintaan ja tarkastella, miltä osin nykykäytännöt eivät mahdollisesti ole lainsäädännön mukaisia ja miltä osin niitä tulee päivittää. Tee erityisesti nämä toimenpiteet:

- Varmista, että tietojen käsittelylle on olemassa jokin käsittelyperuste (ks. tarkemmin kohta 3) ja että ne ovat tarpeellisia aiottuja tarkoituksia varten.
- Huolehdi tietojen elinkaaren hallinnasta ja määrittele tiedoille mm. säilytysajat tai ne kriteerit, joiden perusteella säilytys määräytyy. Tietojen säilytysaika tulisi arvioida sen mukaan, kuinka pitkään tietoja on tarpeen käsitellä aiottujen tarkoitusten toteuttamiseksi.
- Informoi rekisteröityjä tietojenkäsittelystä hyödyntämällä esimerkiksi toimitettua tietosuojaselostepohjaa.
- Suunnittele prosessi rekisteröidyn oikeuksien toteuttamiseksi ja varaudu siihen, että rekisteröidyt käyttävät oikeuksiaan (ks. kohta 7.1.2).
- Kouluta henkilökuntaa siten, että he ovat tietoisia tietosuojaan liittyvistä velvoitteista ja laadi tarvittavia sisäisiä ohjeita ja prosesseja (esim. markkinointikäytännöt ja prosessi tietoturvaloukkausten havaitsemiseksi ja niistä ilmoittamiseksi).
- Laadi asetuksen 28 artiklan mukaiset sopimukset henkilötietojen käsittelijöiden kanssa (ks. lähetteen tarjous).

- Laadi ja ylläpidä tarvittavaa dokumentaatiota osoittaaksesi, että toiminta täyttää tietosuojalainsäädännön velvoitteet (mm. tietosuojaselosteet ja mahdollisten tietoturvaloukkausten dokumentointi sekä soveltuvin osin mahdollinen lyhyt kuvaus tietosuojaorganisaatiosta, mahdollinen prosessikuvaus rekisteröidyn oikeuksien toteuttamisesta, henkilökunnalle laaditut ohjeistukset).