SUOMEN MOTORISTIT RY FINLAND



**24.4.2018**

**GDPR eli EU:n tietosuoja-asetus, mikä se on ja mitä se tarkoittaa**

**Ketä se koskee ja miten**

Käytännössä kaikkia organisaatioita, jotka tallentavat ja käyttävät toiminnassaan yksilöiviä henkilötietoja. Yhdistysten osalta lähinnä jäsentietoja, oman organisaation tietoja ja mahdollisesti muuten vapaaehtoistoiminnassa mukana olevien tietoja.

Käytännössä muutokset nykyiseen verrattuna eivät ole järkyttävän isoja, monet periaatteet säilyvät ennallaan, mutta tietosuoja-asetus tuo myös uusia tietosuojaa ja henkilötietojen käsittelyä koskevia velvoitteita, joihin rekisterinpitäjien ja henkilötietojen käsittelijöiden on valmistauduttava. Tietosuoja-asetuksen rikkomisesta voi seurata ensin huomautus, sitten varoitus, jonka jälkeen henkilötietojen käsittelykielto ja viimeisimpänä sakko.

Keskeistä ja uutta tietosuoja-asetuksessa on muun muassa riskiperusteinen lähestymistapa ja rekisterinpitäjän osoitusvelvollisuus. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy. Rekisterinpitäjän osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän on pystyttävä osoittamaan, että se noudattaa tietosuoja-asetusta.

Suurin työtä aiheuttava muutos on dokumentointi. Rekisteriselosteet on laitettava ajan tasalle ja ne on oltava selvästi näkyvillä. Myös rekisteröidyn oikeus saada tietonsa nähtäväkseen laajenee samoin oikeus tulla unohdetuksi (tietojen poistaminen rekisteröidyn pyynnöstä, tätä säätelee myös kirjanpitolaki varsinkin palkattujen työntekijöiden osalta).

**Koska se on ajankohtaista**

Asetus on astunut voimaan 25.5.2016, mutta sille on määritelty 2 vuoden siirtymäaika 25.5.2018 saakka. EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa. Tietosuoja-asetusta (General Data Protection Regulation,GDPR) sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn.

**Suomen Motoristit ry (SMOTO)**
Kuusimäenkatu 21
33560 Tampere

Laskutusosoite:
Suomen Motoristit ry
c/o Liisa Leino
Varttivuorentie 51
21180 Livonsaari

**www.smoto.fi**
info@smoto.fi
Y-tunnus 1485223-9
Rekisterinumero 151.543

Tietosuoja-asetusta täydennetään ja täsmennetään kansallisella lainsäädännöllä. Oikeusministeriön asettama työryhmä on ehdottanut mietinnössään uutta kansallista tietosuojalakia, joka tulisi voimaan 25.5.2018, kun myös tietosuoja-asetusta ryhdytään soveltamaan.

Henkilötietojen käsittely on suunniteltava ja dokumentoitava. Dokumentointi koskee henkilötietojen keräämistä, niiden käyttötarkoitusta, käsittelyä ja sitä kenellä on oikeus käsitellä henkilötietoja. Jokaisesta henkilötietoja sisältävästä rekisteristä on tehtävä rekisteriseloste, josta ilmenevät edellä mainitut seikat.

**Tietosuoja-asetuksen ja tietojen käsittelyn periaatteita**

Rekisterinpitäjä = se taho, joka määrittää tietojen käsittelyn tarkoituksen ja keinot, eli se, jonka toimeksiannosta ja tarpeita varten rekisteriä pidetään (esim. SMOTO).

Rekisteritietojen käsittelijä = se todellinen tietoja tallentava, kokoava tai säilyttävä taho (esim. ulkopuolinen palveluntarjoaja).
Huomattavaa on se, että rekisterinpitäjä ei voi siirtää vastuutaan rekisterin käsittelijälle.

Tunnistettavien henkilötietojen määritelmä muuttuu. Aiemmin tunnistettavat tiedot olivat käytännössä nimi ja henkilötunnus, nyt tunnistettaviin henkilötietoihin kuuluvat

- Henkilötunnus
- Nimi
- Osoite
- Puhelinnumero
- Sähköpostiosoite
- IP-osoite
- Pankkitilinumero
- Jäsenmaksut
- Järjestelmän käyttäjien käyttäjätunnukset ja myös nimet (käyttäjähallinta)
- Jäsennumero ja sukupuoli eivät ole yksinään ole henkilötietoja, mutta muuttuvat sellaisiksi, jos ne yhdistetään johonkin muuhun henkilötietoon.

Rekisterinpitäjän on huolehdittava siitä, että tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Tietosuojaperiaatteiden mukaan henkilötietoja on

- Käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi, henkilötietojen luovuttajan tulee tietää mihin käyttötarkoitukseen tietoja kerätään ja luovuttajalle tulee taata asianmukainen yksityisyys tietoja kerätessä
- Käsiteltävä luottamuksellisesti ja turvallisesti. Rekisterinpitäjän keräämiä tietoja ei saa käyttää perusteettomasti tai aiheuttaa niiden käsittelyllä haittaa kyseiselle henkilölle
- Kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Rekisterinpitäjällä pitää olla laillinen peruste kerätä ja käyttää henkilötietoja (esim. yhdistyksen jäsenrekisteri) Titoja on kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden.
- Tietoja on päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä. Rekisterinpitäjän tulee varmistua henkilötietojen oikeellisuudesta ja pitää tiedot ajan tasalla
- Säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Rekisterinpitäjän tulee määritellä kuinka kauan eronneen jäsenen tai toimihenkilön tietoja säilytetään. Palkatun henkilökunnan osalta säilytysajan määrittää kirjanpitolaki.
- Rekisterinpitäjällä on oltava tietojen käsittelyyn ja säilytykseen soveltuvat välineet, joilla voidaan varmistaa, että säilytettävien tietojen turvallisuus ei vahingossa pääse vaarantumaan. Rekisterinpitäjän tulee varmistaa, että tietoturva on riittävä kyseisten tietojen säilyttämiseksi ja olla tietoinen mahdollisista tietoturvauhista,
- Rekisterinpitäjän tulee vastata tehokkaasti kaikkiin mahdollisiin tietoturvaa uhkaaviin tapahtumiin ja olla tietoinen kuka on vastuussa tietoturvan tasosta
- Henkilökohtaisia tietoja ei ole luvallista lähettää EU:n alueen ulkopuolelle, ellei kyseisten henkilötietojen riittävää tietoturvaa ja kyseisen henkilön oikeuksia ja vapauksia voida taata.

**Tietosuoja-asetukseen valmistautuminen**

Valmistautuessasi tietosuoja-asetukseen:

- Selvitä, pitääkö organisaatioosi nimittää tietosuojavastaava (pitää jos käsitellään henkilötietoja).
- Selvitä, miten organisaatiossasi käsitellään henkilötietoja. Käy läpi kaikki henkilötietojen käsittelyn vaiheet keräämisestä hävittämiseen ja dokumentoi ne. Varmista, että organisaatiosi noudattaa nykyisin sovellettavaa henkilötietolakia.
- Selvitä, millä perusteella organisaatiosi käsittelee henkilötietoja. Henkilötietojen käsittelylle on oltava aina laista löytyvä peruste.
- Arvioi, millaisia riskejä henkilötietojen käsittelyyn liittyy organisaatiossasi. Selvitä, miten riskejä voitaisiin minimoida. Ryhdy toimenpiteisiin, jotka vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Esimerkiksi silloin, kun henkilötietojen käsittelyyn kohdistuu todennäköisesti korkea riski, on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi.
- Selvitä, miten organisaatiosi noudattaa tietosuoja-asetuksessa määriteltyjä rekisteröityjen oikeuksia. Selvitä myös, miten rekisteröityjen pyyntöihin tällä hetkellä vastataan. Päivitä prosessit tietosuoja-asetuksen vaatimusten mukaisiksi.
- Huolehdi tietoturvasta. Valmistaudu ilmoittamaan henkilötietojen tietoturvaloukkauksista.
- Varmista, että toimeksiantosopimukset vastaavat asetuksessa säädettyjä ehtoja, jos organisaatiosi on ulkoistanut henkilötietojen käsittelyyn liittyviä tehtäviä. Ota tietosuoja-asetus huomioon myös muissa sopimuksissa ja hankinnoissa.
- Määrittele johtava valvontaviranomainen, jos organisaatiosi toimii usean EU:n jäsenmaan alueella. Suomessa se on tietosuojavaltuutettu.
- Selvitä, miten organisaatiosi on huomioitava lasten erityisasema. Jatkossa lapsi tarvitsee huoltajan tai muun vanhempainvastuunkantajan suostumuksen tai valtuutuksen tietoyhteiskunnan palveluiden käyttöön. Suomessa ikäraja ei ole vielä selvillä, mutta se on vähintään 13 ja enintään 16 vuotta.