SOLUTO
IT-palvelut yrityksille

Soluto Oy

EU-tietosuojadirektiivi eli GDPR

Jani-Petteri Pohjonen
3.5.2018

25.5.2018

- EU-tietoturva-asetus (GDPR) :
  - *Asetus koskee kaikkia organisaatioita, joilla on henkilörekistereitä tai jotka käsittelevät henkilörekistereiden tietoja*
  - *Asetus koskee dataa (paperinen tai sähköinen), jonka perusteella ihminen voidaan tunnistaa yksilöllisesti*
  - *Oman tietosuojavastaavan joutuvat nimittämään arkaluonteista henkilötietoa käsittelevät organisaatiot*
    - *Rotu tai etninen alkuperä*
    - *Poliittinen tai uskonnollinen vakaumus*
    - *Ammattiliittoon kuuluminen*
    - *Rikollinen teko, rangaistus tai rikoksen seuraamukset*
    - *Terveystiedot (sairaudet, vammaisuus, jne) tai terveyteen kohdistuvat hoitotoimenpiteet*
    - *Henkilön seksuaalinen suuntautuminen tai käyttäytyminen*
    - *Sosiaalihuollon tarve tai saadut sosiaalihuollon palvelut ja etuudet*
  - *Noudattamisen sijasta myös osoittamisen velvollisuus*
  - *Ilmoitusvelvollisuus viranomaisille 72 h sisällä henkilötietoihin kohdistuneesta tietoturvaloukkauksesta*
  - *Tietosuojasäännösten rikkomisesta viranomaiset voivat määrätä hallinnollisen sakon, joka on 2 prosenttia organisaation edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta.*
- Siirtymäaika loppuu: 25.5.2018

Käsitteet

Henkilörekisteri (rekisteri) = Kaikki rekisterit, listat, kortistot, muistiinpanot, luettelot tai näihin verrattavat rekisterit, joissa on tallennettuna tietoa, jonka perusteella henkilö X pystytään tunnistamaan. Esimerkkejä rekistereistä: Excel –tiedosto, paperiset jäsenlistat, laskutusluettelo, Word –ohjelmistolla kirjoitettu osallistujaluettelo jne. **Se on siis tietokoneelle ja tietojärjestelmiin tallennettu tieto, mutta myös paperille koottu arkisto / kortisto.**

Henkilötieto = kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvä tieto

- Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Rekisterinpitäjä = luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot

Käsittelijä = luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun

Tietoturvaloukkaus = Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin

Esimerkkejä henkilötietorekistereistä

Tapahtumien osallistujat = Esimerkki rekisteristä, johon kerätään henkilöosallistujat tapahtumaan. Rekisterissä on esimerkiksi seuraavat tiedot: Henkilön nimi, osoite, puhelinnumero.

Jäsenmaksut = Rekisteriin kerätään tietoja henkilön jäsenyydestä.

Työntekijärekisteri = Rekisterissä on työntekijän tietoja, kuten nimi, sotu, terveystiedot, puhelinnumero, sähköpostiosoite, palkkatiedot jne.

Markkinointilistat = Rekisteri joka koostu henkilöistä joille lähetetään markkinointimateriaalia. Tämä on esimerkiksi sähköpostimainontaa, kirjepostia, jne.

Varauslistat = Rekisteri johon laite, tila, avain tai muissa näihin rinnastettavissa asioissa kerätään rekisteritietoa, kuten henkilön nimi ja puhelinnumero.

Huomioita rekistereistä

Henkilörekisteriksi EI luokitella seuraavia rekistereitä:

Esimerkiksi:

Varauslista, jossa nimi ”Matti Meikäläinen, Avain 1, mökkiin 3”

Miksi? Tietämällä nimi Matti Meikäläinen ei vielä kerro kenellekään ketä Matti Meikäläistä tämä tieto koskee. Jos varauslistassa olisi ”Matti Meikäläinen, Keskuskatu 15 B 3, 33100 Tampere”, niin kyseessä olisi henkilörekisteri. Tieto ”Keskuskatu 15 B 3” osoittaa Matti Meikäläisen asuinosoitetta, EI viikonlopun varauksessa olevaa tilaa.

Allergialista (esim. tapahtumaan liittyen), jossa lukee ”Maija Meikäläinen, keliakia”, EI vielä täytä henkilörekisterin määritelmää.

Miksi? Koska tieto, että jollakin Maija Meikäläinen-nimisellä henkilöllä on keliakia, ei vielä täytä henkilörekisterin määritelmää. Ei siis pystytä kohdistamaan tietoa juuri tiettyyn Maija Meikäläiseen. Jos kuitenkin rekisterissä lukisi, että ”Maija Meikäläinen, 040 1234 1234, keliakia”,olisi kyseessä henkilörekisteri.

Asiakkaan – jäsenen oikeudet

- Rekisterinpitäjän (liiton, yhdistyksen, seuran) on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan tietojenkäsittelyn asetuksen mukaisuus
  - Toimenpiteet tulee olla dokumentoituna ja ne on tarkistettava ja päivitettävät tarvittaessa
  - Toiminnan oltava riskilähtöistä ja ennakoivaa
  - Kyky todistaa toimenpiteet tarvittaessa viranomaisille, dokumentoinnin ja sertifioinnin kautta

- Rekisteröidyllä henkilöllä (esim. asiakas, jäsen) on vahvempi kontrolli omiin tietoihin
  - Oikeus tulla unohdutuksi
    - Oikeus tietojen korjaukseen ja poistamiseen, jos tietojenkäsittely ei enää tarpeellista tai käsittelylle ei ole enää laillista perustetta.
  - Oikeus saada tiedot yleisesti käytetyssä sähköisessä tai jäsennellyssä muodossa

Mitä tehdä käytännössä? WWW-sivut

Www-sivut ovat käytännössä monille paikka kerätä jäsenilmoittautumisia ja jäsentietoja. GDPR:n eli EU-tietosuojadirektiivin perusteella tietojen kerääminen www-sivuja hyödyntämällä pitää kertoa selkeästi käyttäjälle.

Miten?:

- *Jos sivustolla on jäseneksiliittymislomake, lomakkeeseen pitää lisätä erillinen valinta, jolla käyttäjä hyväksyy (suostumus), että hänen tietojaan kerätään henkilötietojen käsittelyyn.*

- *Jos www-sivuilla käytetään evästeitä (cookies), niiden käytöstä pitää erikseen tiedottaa.*

    - *Läheskään kaikki sivustot eivät käytä evästeitä. Kysy WWW-suunnittelijaltanne käytetäänkö sivustollanne evästeitä. Jos käytetään, luodaan sivustolle erillinen ilmoitus evästeiden käytöstä.*

Mitä tehdä käytännössä? Kilpailutulokset

Kilpailutulokset, jotka sisältävät tiedon ”Matti Meikäläinen, Viialan perhokalastajat, Siika 2 kg, 1. sija” EI täytä henkilörekisterin määritelmää.

Mitä jos nykyisessä kilpailutuloksessa lukee ”Matti Meikäläinen, GSM 040 1234 1234”?

- *Voiko kilpailutulosten rekisteriä – tulostaulua muuttaa niin, että kohdentavat tiedot jätetään pois?*

Mitä tehdä käytännössä? Seuran tietokone tai seuran töihin käytetty henkilökohtainen tietokone

Valtaosalla tai jopa kaikilla seuroilla on joko seuran tai seuran aktiivisten henkilöiden tietokoneilla tallennettuna seuran toimintaan tarkoitettuja henkilötietoja. Tietokoneet tulee olla suojattu tietoturvallisesti.

Miten?

EU –tietosuojadirektiivissä ei suoraan määritellä miten tietoturva pitää olla hoidettu. Määritelmä on ”riittävällä tasolla”.

Miten käytännössä?

- *Virustorjunta-, palomuuriohjelmisto tietokoneelle. Esim. F-Secure Safe*
- *Suojaa tietokoneen kirjautuminen salasanalla*
- *Varmista, että tietokoneelle asentuu tietoturvapäivitykset, esim. Windows –päivitykset jne.*
- *Hoida tietokoneen varmuuskopio, eli tietokoneelle kerätty henkilörekisteri – henkilörekisterit tulee olla varmuuskopioitu*

Mitä tehdä käytännössä? Mitä, kun meillä on jo aikaisemmin kerättyjä rekistereitä? Pitääkö näihin kysyä erikseen jäseniltä lupa?

Rekistereitä, jotka ovat kerätty ennen 25.5.2018, ei tarvitse erikseen hyväksyä jäseniltä – henkilöiltä, vaan voidaan todeta, että henkilöt ovat jo suostuneet henkilötietojen antamiseen. Teidän ei siis tarvitse erikseen lähteä pyytämään erillistä suostumusta jokaiselta jäseneltä henkilörekisterin pitämiseen.

Huomioi kuitenkin, että:

26.5.2018 alkaen asia on toisin. Tällöin Teidän pitää kysyä henkilöltä erillinen suostumus henkilötietojen keräämiseen.

Mitä tehdä käytännössä? Mitä jos joku jäsen haluaa, että kaikki häneen liittyvät tiedot poistetaan seuralta (henkilön oikeus tulla unohdetuksi)?

Tilanteissa, joissa henkilö haluaa tulla unohdetuksi, eli hän haluaa että seuran poistavan kaikki tiedot hänestä.

Huomioi kuitenkin, että:

Seura EI saa poistaa henkilötietoja vaikka henkilö näin toivoo, jos ne ovat ristiriidassa muiden lakien kanssa. Esimerkiksi laskutustietoja ei saa poistaa kirjanpitolain mukaan. Myös sopimustietoja ei saa poistaa.

Tieto, joita Teidän pitää poistaa henkilöön liittyen koskee pääasiassa vain niitä tietoja, joita henkilö on itsestään antanut Teille, kunhan ne eivät ole ristiriidassa ylemmän kanssa.

Rekisteriselosteet

Jokaisen seuran pitää tunnistaa tällä hetkellä ylläpitämänsä henkilörekisterit ja tehdä niistä jokaisesta erillinen rekisteriseloste (jäsenrekisteri ja markkinointirekisteri)

Kts. Liitteenä lähetetty erillinen Excel –tiedosto rekisteriselosteen tekemiseen.

Huomioi kuitenkin, että:

Rekisteriselostetta ei tarvitse toimittaa etukäteen valtion viranomaisille. Se pitää olla valmiina, jos viranomaiset suorittavat tarkastuksen, miten tietosuoja on hoidettu.

Tee rekisteriselosteet nykyisistä henkilörekistereistä heti ja tee niitä lisää sitä mukaa kun rekistereitä muodostuu myöhemmin lisää.

Lisää rekisteriseloste esim. uusien jäsensopimusten liitteeksi tai nähtäville ilmoittautumisten yhteyteen. Näin henkilö pystyy omia henkilötietojaan täyttäessään tarvittaessa tutustumaan tietoon siitä, mihin hänen henkilötietojaan tallennetaan ja käytetään.

Kiitos

Soluto Oy
Jani-Petteri Pohjonen
jani-petteri.pohjonen@soluto.fi
+358 400 866018

www.soluto.fi
www.yritystenverkkokauppa.fi
www.fixu.fi
www.it-vuokraus.fi