SAMIN ATK-APU

TIETOSUOJA YHDISTYKSESSÄ 10.11.2022

Sami Tervo

Työuraa tietotekniikan, tietosuojan ja tietoturvan parissa yli 30 vuotta. Kymenlaakson liiton palveluksessa tietohallintosuunnittelijana, tietosuojavaltuutettuna ja työsuojeluvaltuutettuna

Tietosuoja yhdistyksissä

- Koskeeko tietosuoja-asetus meidän yhdistystä?
- Informointivelvollisuus ja rekisteröidyn oikeudet
- Rekisterit, rekisterinpitäjä, käsittelijä ja riskienarviointi
- Viestintä, markkinointi, tiedottaminen
- Henkilötunnus
- Kouluttaminen
- https://tietosuoja.fi/usein-kysyttya-yhdistystoiminta
- https://tietosuoja.fi/documents/6927448/10594424/Henkil%C3%B6tietojen+k%C3%A4sittely+yhdistystoiminnassa/3f0e1e72-ec39-a103-4de9-df5a730ed226/Henkil%C3%B6tietojen+k%C3%A4sittely+yhdistystoiminnassa.pdf?t=1620635100143

Koskeeko tietosuoja-asetus yhdistystä ?

- Kyllä koskee. Yhdistyksen koolla ei ole merkitystä; tietosuoja-asetusta tulee noudattaa, jos yhdistys käsittelee henkilötietoja.
- Käsittelemistä on lähtökohtaisesti kaikki henkilötiedoille tehtävät toimet: Kerääminen, säilyttäminen, levittäminen, hakeminen, siirtäminen, muokkaaminen, poistaminen, järjestäminen
- Tietosuoja-asetus ei aseta velvollisuuksia yksityisille henkilöille. Ihminen saa edelleen pitää "henkilörekisteriä" eli vaikka tuttujen nimiä ja puhelinnumeroita kännykässään.

Informointivelvollisuus ja rekisteröidyn oikeudet

- Tietosuojaseloste esim. kotisivuille

Rekisteröidylle on kerrottava:

- kuka rekisterinpitäjä on
- mitä tarkoitusta varten rekisteröidyn henkilötietoja tarvitaan
- kuinka kauan henkilötietoja tarvitaan
- luovutetaanko henkilötietoja eteenpäin tai siirretäänkö niitä ETA-maiden ulkopuolelle
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä
- Lataa malli https://www.invalidiliitto.fi/tietosuoja-asetukseen-liittyvia-kasitteita

Informointivelvollisuus ja rekisteröidyn oikeudet

Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus:

- saada tietoa henkilötietojensa käsittelystä
- saada tutustua tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.

SAMIN ATK-APU

Informointivelvollisuus ja rekisteröidyn oikeudet

- Kun rekisterinpitäjä käsittelee henkilötietoja, sen on toteutettava asianmukaiset toimenpiteet rekisteröityjen tietosuojaoikeuksien toteuttamiseksi. Sen on myös helpotettava rekisteröidyn oikeuksien käyttämistä.
- Rekisteröity ei voi käyttää kaikkia oikeuksia kaikissa tilanteissa. Tilanteeseen vaikuttaa esimerkiksi se, millä perusteella henkilötietoja käsitellään.
- Esim. Et voi vaatia pankkia tai poliisia hävittämää kaikkia tietojasi
- Lisätietoja rekisteröidyn oikeuksista
- https://tietosuoja.fi/rekisteroidyn-oikeudet-eri-tilanteissa

Rekisterinpitäjä ja käsittelijä

- **Rekisterinpitäjä** = Taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai lainsäädännössä rekisterinpitäjäksi vahvistettu taho.
- **Käsittelijä** = Käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.
- Käsittelijä yleensä järjestelmän toimittaja/palveluntarjooja.
- Rekisterinpitäjän työntekijä on osa rekisterinpitäjää, ei erillinen käsittelijä.
- Käsittelijällä ei ole itsenäistä oikeutta käsitellä tietoja.
- HUOM, jos sopimuksessa lukee ” toimittajalla on oikeus käsitellä tietoja omassa toiminnassaan XX tarkoituksessa” Hälytyskellot soimaan!

SAMIN ATK-APU

Rekisterinpitäjä ja käsittelijä

Roolin vaikutus	Rekisterinpitäjä	Käsittelijä
Onko oikeutta käyttää tietoja toimintanne hyväksi?	Kyllä	Ei
Onko oikeutta käsitellä muutoin kuin tilatun palvelun toteuttamiseksi?	Kyllä	Ei
Onko velvollisuutta soveltaa tietosuojalainsäädäntöä?	Kyllä	Kyllä
Soveltuvatko hallinnolliset sakot?	Kyllä	Kyllä
Onko vahingonkorvausvelvollisuutta kolmansille?	Kyllä	Kyllä

SAMIN ATK-APU

Jäsenrekisteri

- Pääsy jäsenrekisteriin tulee olla niillä yhdistyksen toimihenkilöillä, joiden tehtävien hoidon kannalta tämä on tarpeen. Myös yhdistyksen jäsenellä on yhdistyslain mukaan oikeus tutustua jäsenluettelon tietoihin.
- Toimivalta käsitellä jäsenten tietoja päättyy, kun toimihenkilön asema yhdistyksessä lakkaa. Toimihenkilön on luovutettava hallussaan oleva henkilötietoaineisto, eikä hän saa ottaa siitä itselleen kopioita.
- Esim. jäsenlaskutuksen ulkoistamisesta tulee tehdä sopimus, jossa huomioidaan tietosuoja-asetuksen vaatimukset. Ulkoistaminen ei poista yhdistyksen vastuuta.

Jäsenrekisteri

- Jäsenrekisteriä säilytetään huolellisesti suojattuna joko laitteella, joka on kokonaan erillään internetistä, tai hyvän palomuuri- ja virustorjuntaohjelmiston suojaamana. Peruspaketti esim. F-secure
- Henkilötunnus jäsentiedoissa, Yleensä ei voida käyttää. Poikkeuksena on tilanne, jossa jäsen on antanut henkilötunnuksen käyttöön suostumuksensa, käsittelystä on säädetty lailla tai on olemassa muu erityisen tärkeä syy yksiselitteiseen yksilöimiseen, eikä yksilöintiä voi tehdä muutoin kuin henkilötunnuksen avulla.
- Samannimisten erottaminen toisistaan, Syntymävuosi, jäsennumero tai vastaava. Lisäksi voidaan käyttää lisätunnusta (Matti Meikäläinen X erottaminen Matti Meikäläinen Z:stä).

Riskien arviointi

SAMIN ATK-APU

- Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina, ennen kuin se ryhtyy käsittelemään henkilötietoja
- Selvitä mitä rekistereitä tai henkilötietoja yhdistyksellä on käytössään,
- Arvioikaa riskejä riskillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen.

  (**Pseudonymisointi** tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja)

Riskien arviointi

SAMIN ATK-APU

Riskiarvio on tehtävä rekisteröidyn näkökulmasta eli rekisterinpitäjän on arvioitava:

- mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja
- mitä vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä.
- Vahingot voivat olla fyysisiä, aineellisia tai aineettomia.
- **Tietoturvariskien tunnistaminen ja dokumentointi**
- Riskin kuvaus (teema, esim. Tietojen tuhoutuminen vahingossa)
- Riskin vakavuus 1-3 (vähäinen, haitallinen, vakava)
- Riskin todennäköisyys 1-3 (epätodennäköinen, mahdollinen, todennäköinen)
- **Riskin hyväksyttävyys ja käsittely vaihtoehdot:**
- Vähennä riskiä= uusia tehtäviä ja hallintakeinoja riskin pienentämiseksi
- jaa riski= Vakuutus jolla taloudellinen riski jakaantuu.
- vältä riski= keskeytä riskiin liittyvä toiminta jos niitä ei voi muilla toimilla vähentää
- säilytä riski=riskin hyväksyntä tekemättä sille mitään käytä vain jos lieventäminen kalliipaa kuin arvioitu korvaus.

SAMIN ATK-APU

Riskien arviointi

Esim. Kotkanseudun Invalidit ry henkilötietorekisterit:

- Jäsenrekisteri **Kilta** (rooli rekisterinpitäjä). Puutteellinen tunnistautuminen laitteelle, haitallinen, mahdollinen. Pienennä riskiä, Henkilökohtaiset tunnukset koneelle.
- lentopalloilijoiden pelaajaluettelo ja harjoituksiin ilmoittautuminen **Nimenhuuto** (rooli rekisterinpitäjä). Puutteellinen tunnistautuminen järjestelmään, vähäinen, Mahdollinen, Riski säilytetään. Käyttäjien ohjeistus salasanan tasosta ja vaihdosta.
- Taloushallinto, palkanmaksu ja laskutus **Fennoa** (rooli rekisterinpitäjä). Henkilökunta ei ymmärrä vastuuta tietoturvasta, Pienennä riskiä, Tietoturva koulutus
- Järjestelmiin vain henkilökohtaisia käyttäjätunnuksia, Fennoa ja Kilta vahvalla tunnistautumisella.

SAMIN ATK-APU

Viestintä, markkinointi, tiedottaminen

- Yhdistyksen tulee suunnitella tiedotustoimintansa sellaiseksi, että jäsen tietää menettelytavat.
- Sähköposti on lähetettävä niin, että osoitteet ovat piilokopiokentässä eivätkä näy muille jäsenille, ellei yhteystietojen näkymiseen ole erityistä syytä (esimerkiksi jäsenet voivat liittyä vapaaehtoiseen keskusteluryhmään tai sähköpostilistalle, jossa muiden tiedot ovat näkyvillä).
- Yhdistys saa tiedottaa toiminnastaan jäsenille, eikä tiedottamista pidetä suoramarkkinointina. Jäsentietoja ei saa kuitenkaan luovuttaa suoramarkkinointitarkoituksiin ilman jäsenen lupaa.

Viestintä, markkinointi, tiedottaminen

- Yhdistyksen sähköpostiosoite tulisi olla muotoa yhdistys@yhdistys.fi ei henkilökohtainen sähköpostiosoite.
- Sähköposti ja pilvipalvelu kuuluvat yksityisyydensuojaan
- Postilaatikkoon oikeudet sille kuka ko. tehtävää hoitaa ja oikeudet pois sitten kun tehtävän hoito päättyy.
- Näin saapuneet ja lähetetyt viestit säilyvät yhdistyksellä.
- Esim. KSI ry. ksikotka@gmail.com käyttöoikeus sihteeri ja puheenjohtaja
- Hallituksen pilvipalvelu Google Drive levytilan jako samoilla periaatteilla

SAMIN ATK-APU

Henkilötunnuksen käyttö

- Pankkikortilla maksavan asiakkaan henkilöllisyydestä voidaan vaatia selvitystä. Menettely varmistaa sekä asiakkaan että maksunsaajan oikeusturvaa.
- Henkilötunnuksen kysyminen ei ole luotettava tapa selvittää esim. puhelimessa tai internetissä asioivan henkilöllisyyttä.
- Rekisterinpitäjä ei saa rakentaa tunnistamiskäytäntöjään yksinomaan henkilötunnuksen ja nimen kysymisen varaan.
- Henkilötunnusta saa kuitenkin kysyä yhtenä tietona muiden joukossa, kun henkilö soittaa esimerkiksi yrityksen asiakaspalveluun, terveydenhuollon toimintayksikköön tai viranomaiselle.

SAMIN ATK-APU

Henkilötunnuksen käyttö

- Henkilötunnusta ei koskaan pidä käyttää salasanana sähköisissä palveluissa. Salasanan tulee olla vain sinun tiedossasi, mutta henkilötunnuksesi saattaa tietää ulkopuolinenkin henkilö. Salasanan tulee myös olla tarvittaessa vaihdettavissa.
- henkilötunnusta tai sen osaa ei tule käyttää laskun viitenumerossa tai osana viitenumeroa.
- Yleinen hyvän tietojenkäsittelytavan periaate on, ettei kenenkään yksityisyyttä perusteettomasti vaaranneta.

Kouluttaminen

- Henkilöstön ja jäsenistön kouluttaminen tietosuojasta on erinomainen tapa osoittaa tietosuojan vaatimustenmukaisuutta.
- Koulutus on tehokas tapa vähentää yhdistyksen tietosuojaan liittyviä riskejä.
- Tietosuojan kannalta inhimillisillä virheillä voi usein olla vakavat seuraukset koko yhdistykselle ja sen maineelle.
- Kyse on yhdistyksen vastuiden ymmärtämisestä ja näiden mukaan toimimisesta.
- On syytä muistaa että, jokainen meistä on rekisteröity.
- GDPR- ja tietosuojakoulutus on myös omien oikeuksien ymmärtämistä.
- https://tietosuoja.fi

TIETOSUOJAVALTUUTETUN TOIMISTO

SAMIN ATK-APU

KIITOS!

SAMI TERVO & HANNES
040 570 4506
SAMI@SAMINATK.COM