

17.5.2023 Risto Heikkinen

Tietosuoja - miten käsitellä turvallisesti henkilötietoja

**ALLERGIA
IHO
ASTMA** 

Tietosuojan perusteet (1)

- tietosuoja on perusoikeus
 - perustuslaki § 10: yksityiselämän suoja
 - tietosuojalaki 1050/2018
 - Euroopan parlamentin ja neuvoston asetuksen 2016/679 (yleinen tietosuoja-asetus) kansallinen soveltaminen
 - GDPR = General Data Protection Regulation
- lainsäädäntö määrittelee henkilötietojen käsittelyn periaatteet
 - mitä oikeuksia ja vapauksia rekisteröidyllä on

Tietosuojaan perusteet (2)

- tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselostetta
- rekisteröityjä tulee kuitenkin informoida henkilötietojen käsittelystä: informointivelvoite
 - korostetaan sitä, että tieto käsittelystä tulee ilmoittaa ymmärrettävästi ja selkeästi
 - käytännössä moni kuitenkin tekee vielä tietosuojaselosteen
- organisaatioiden on tehtävä sisäiseen käyttöön seloste henkilötietojen käsittelytoimista
 - auttaa hahmottamaan henkilötietojen käsittelyn periaatteet
 - osoittaa, että henkilötietoja käsitellään lainmukaisesti

Käsitteitä (1)

- henkilötieto
 - kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön
 - tunnistaminen voi olla suoraa tai välillistä
 - henkilötietoja voi olla talletettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella
 - henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen vaatimuksia, kun
 - käsittely on kokonaan tai osittain automaattista (riippumatta tekniikasta) tai
 - tiedot muodostavat rekisterin osan
- henkilötieto ei ole esim. yleinen sähköpostiosoite yhdistysP@gmail.com tai anonymisoitu tieto. Milloin tieto on anonymia, arvioidaan aina tapauskohtaisesti (esim. harvinainen sairaus).

Käsitteitä (2)

- rekisteröity
 - henkilö, jota henkilötieto koskee
- rekisterinpitäjä
 - henkilö, yritys, viranomainen tai yhteisö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot
 - Allergia-, iho- ja astmaliitto on rekisterinpitäjä yhdessä yhdistysten kanssa
- henkilötietojen käsittelijä
 - rekisterinpitäjästä ulkopuolinen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun
- tietoturva vs. tietosuojaja
 - tietoturva on yksi keino toteuttaa tietosuojaa koskevia velvoitteita

Henkilötietojen käsittely (1)

- osoitusvelvollisuus
 - osoitetaan, että ymmärretään tietosuojalainsäädäntö ja että sitä noudatetaan
 - osoitetaan, että ymmärretään henkilötietojen käsittelyn riskin
 - velvollisuus dokumentoida käsittelyyn liittyvien toimenpiteiden tekeminen ja kirjaaminen
 - sisäänrakennettu ja oletusarvoinen tietosuoja
 - esim. tehdään tarvittavat tekniset ja organisatoriset toimenpiteet
 - osoitusvelvollisuuden laajuus riippuu muun muassa organisaation koosta, henkilötietojen määrästä ja siitä, millaisia henkilötietoja rekisterinpitäjä käsittelee.

Henkilötietojen käsittely (2)

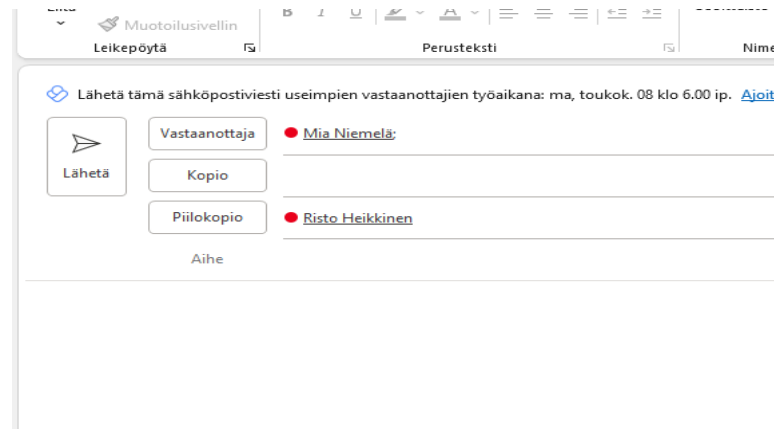
- liiton tietosuojaselosteet ovat vapaasti käytettävissä ja linkitettävissä
 - www.allergia.fi/tietosuojaseloste
 - jäsenrekisteri (Kilta), tapahtumat ja koulutukset, kurssit
- kaikki muu henkilötietojen käsittely tulee kirjata yhdistyksen omaan tietosuojaselosteeseen
- henkilötietoja ovat esim. nimi, yhteystiedot, osoite, puhelinnumero, kaikki terveystiedot (myös ruoka-aineallergiat)
 - terveystietojen käsittely on lähtökohtaisesti kiellettyä, ellei niiden käsittely tapahdu esimerkiksi yhteisön laillisen toiminnan yhteydessä tai ellei niiden käsittelyyn saada suostumusta
 - huomioi, että pelkkä yhdistyksen nimen liittäminen henkilön yhteyteen saatetaan tulkita terveystietojen käsittelyksi

Henkilötietojen käsittely (3)

- milloin yhdistyksessä käsitellään henkilötietoja?
 - uusien jäsenten henkilötiedot
 - <https://kilta.allergia.fi/Lomakkeet/liittymislomake>
 - liiton lähettämät tai itse Killasta haetut tiedot jäsenistä
 - liitosta tiedot lähetetään salatusti
 - tapahtumiin ilmoittautumiset
 - kuka/ketkä kirjaavat? mihin kirjataan? miten säilytetään?
 - annettu neuvonta, jos henkilötietoja kirjataan rekisteriksi (myös jos viestit jäävät sähköpostikansioon)
 - anonymisoitu kirjaaminen ei ole henkilötietojen käsittelyä

Henkilötietojen käsittely (4)

- toinen jäsen voi saada tietää toisen jäsenen nimi- ja kotipaikkatiedot
- sähköinen viestintä
 - jos sähköpostiviesti lähetetään massaviestinä, vastaanottajat pistetään piilokopio-kenttään



- luottamushenkilöiden välisessä viestinnässä voidaan toimia normaalisti

Yhdistyksen oma tietosuojaseloste (1)

- henkilötietojen käsittelyn tarkoitus
 - jäsentietojen käsittely, tapahtumien järjestäminen...
- henkilötietojen käsittelyn oikeusperuste:
 - yhdistyslain velvoite: yhdistyksen tulee pitää luettelo jäsenistään
 - suostumus: tulee pyytää mielellään kirjallisena
 - rekisterinpitäjän oikeutettu etu: rekisterinpitäjän ja rekisteröidyn välillä on jokin merkityksellinen suhde (esim. asiakas ja alainen tai myös jäsen)
 - (elintärkeät edut; yleinen etu ja julkinen valta)

Yhdistyksen oma tietosuojaseloste (2)

- mitä tietoja kerätään
 - yhdistyksen jäsenistä vähintään nimi ja kotipaikka
 - muulle kerättävälle tiedolle tulee olla peruste/tarve (ja suostumus)
 - kannattaa miettiä tarkoin, mitä tietoja kerätään ja miksi
- mistä ja millä keinoin tiedot saadaan
 - ilmoittautumislomake, soitto ym.
- miten tiedot on suojattu
 - konkreettinen kuvaus, esim. tietokoneella salasanan takana, suljetussa kaapissa ym.
- luovutetaanko tietoja muille
 - esim. ravintolaan tai hotelliin tieto ruoka-aineallergioista

Yhdistyksen oma tietosuojaseloste (3)

- miten pitkään tietoja säilytetään
 - yleensä henkilötiedot tuhotaan, kun tapahtuma tai prosessi, jossa tietoja on käsitelty, päättyy.
Anonymisoidun tilastotiedon säilyttäminen on sallittua ja jopa suositeltavaa.
- mitä oikeuksia rekisteröidyllä on
 - esim. oikeus saada nähdä, mitä tietoja on rekisteröity tai oikeus saada poistaa omat tiedot
- yhteystiedot
 - keneen olla yhteydessä omien henkilötietojen käsittelyyn liittyen
 - <https://tietosuoja.fi/>

Henkilötietoja on ...

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

17.5.2023 Risto Heikkinen

Kiitos!

risto.heikkinen@allergia.fi

045 114 4459

ALLERGIA
IHO
ASTMA

The logo consists of the words "ALLERGIA", "IHO", and "ASTMA" stacked vertically in a bold, blue, sans-serif font. To the right of the text is a large, light grey ampersand (&) with a stylized bird in flight integrated into its upper right curve.