Pohjois-Pohjanmaan sosiaali- ja terveysturvayhdistys ry

Käsittele ja säilytä henkilötietoja oikein - EU:n tietosuoja-asetus tuo velvoitteita yhdistyksille

Infon sisältö

1. Mitä EU:n tietosuoja-asetuksella tarkoitetaan
2. Keskeiset käsitteet
3. Rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja vastuut
4. Käsittelyn lainmukaisuus (sis. arkaluonteiset tiedot)
5. Tietojen käsittelyn yleiset periaatteet
6. Rekisteröityjen oikeudet
7. Rekisteröityjen informointi
8. Tietosuojavastaava
9. Valvonta ja sanktiot
10. Tietosuoja-asetukseen valmistautuminen
11. Lisätietoja

Mitä EU:n tietosuoja-asetuksella tarkoitetaan

- EU:n yleisen tietosuoja-asetuksen (GDPR = General Data Protection Regulation) tavoitteena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä henkilötietojen käsittelyssä sekä vahvistaa rekisteröidyn oikeuksia valvoa henkilötietojensa käsittelyä.
- Yhdenmukaistetaan EU:n jäsenvaltioiden tietosuojalakeja ja sääntelyä sekä helpotetaan palveluiden tarjoamista valtioiden välillä, taustalla teknologinen kehitys ja globalisaatio.
- Asetus koskee kaikkia organisaatioita, joissa käsitellään henkilötietoja erilaisissa järjestelmissä/ohjelmistoissa/ohjelmissa/asiakaskortistoissa/ asiakaskortistojen osissa.
- Asetuksen lähtökohta riskiperusteinen. Tämä voi tuoda huomattavaa kilpailuetua asiakaspalveluun, johtamiseen, laatutyöhön ja imagomarkkinointiin.
- EU-tietosuoja-asetus astuu täysimääräisenä voimaan 25.5.2018.

Keskeiset käsitteet

- **Henkilötiedolla** tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa suoraan tai epäsuorasti häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi eli voidaan selvittää, kenestä on kyse. Esim. nimi, puhelinnumero, sähköpostiosoite, henkilötunnus, valokuva, somepäivitys, auton rekisterinumero, IP-osoite, sijaintitieto tai mm. fyysinen, psykologinen ja sosiaalinen tekijä.
- **Henkilötietojen käsittelyllä** tarkoitetaan henkilötietojen keräämistä, tallettamista, jäsentämistä, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista/muokkaamista, hakua, kyselyä, luovuttamista, yhdistämistä, yhteensovittamista, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.
- **Rekisteröidyllä** tarkoitetaan henkilöä, jonka henkilötietoja käsitellään.
- **Rekisterillä** tarkoitetaan jäsenneltyä henkilötietoa sisältävää tietojoukkoa, josta tiedot ovat saatavilla henkilöä koskevin perustein ja tiettyä käyttötarkoitusta varten.
- **Tietosuojaan** kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.

Rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja vastuut

- Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot.
- Rekisterinpitäjällä lopullinen vastuu henkilötietojen käsittelyn lainmukaisuudesta.
- Rekisterinpitäjän on toteutettava riittävät tekniset ja organisatoriset toimet, joilla voidaan varmistaa ja osoittaa, että tietosuoja-asetusta noudatetaan. Tässä otettava huomioon käsittelyn luonne, asiayhteys, tarkoitukset ja käsittelyyn liittyvät riskit.
- Suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Riskejä esim. identiteettivarkaus, maineen vahingoittuminen ja syrjintä.
- Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun.
- Henkilötietojen käsittelijä voi käsitellä henkilötietoja **ainoastaan** rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti.

Käsittelyn lainmukaisuus (sis. arkaluonteiset tiedot)

- Jotta henkilötietoja voisi käsitellä, vähintään yhden käsittelyn edellytyksistä pitää täyttä. Tällöinkin on oikeus käsitellä vain juuri sitä asiaa koskevaa tietoa.
  - Suostumus – rekisteröity on antanut (kirjallisen) suostumuksensa henkilötietojen käsittelyä varten. Suostumuksen oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaus.
  - Sopimus – esimerkiksi tilaus verkkokaupasta. Myyjä tarvitsee asiakkaan tiedot toimittaakseen tuotteen. Koskee myös työsopimusta, työnantajalla on sopimuksen perusteella oikeus käsitellä työntekijän tietoja.
  - Lakisääteisyys – esim. yhdistyksen jäsenistä on lain mukaan oltava jäsenrekisteri.
  - Elintärkeä etu – esim. jälkikäteen selvitetään tuhkarokkoa sairastaneen henkilön kanssa samalla lennolla olleita.
  - Yleinen etu tai julkisen vallan käyttö
  - Oikeutettu etu – tyypillisesti esimerkiksi asiakassuhde tai työsuhde.

Käsittelyn lainmukaisuus (sis. arkaluonteiset tiedot)

- Rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen ja filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset ja biometriset tiedot (yksilön tunnistamista varten), rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta koskevat tiedot, seksuaalinen käyttäytyminen tai suuntautuminen, henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia koskevat tiedot, henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia koskevat tiedot.
- Pääsääntöisesti näitä tietoja ei saa käsitellä, ellei ole erityistä perustetta:
  - Rekisteröidyn antama suostumus. Ei aina riitä, koska rekisteröity ei voi aina kumota kieltoa. Täytyy olla kirjallisena.
  - Sallitaan työlainsäädännössä (esim. sairaslomat, työkyky)
  - Tietojen käsittely on tarpeen esim. oikeudessa
- Tietosuoja-asetuksessa vaatimus on, että erityisesti lasten henkilötietoja on pyrittävä suojaamaan, koska he eivät välttämättä ole kovin hyvin perillä henkilötietojen käsittelyyn liittyvistä riskeistä, seurauksista, asianomaisista suojatoimista tai omista oikeuksistaan.

Tietojen käsittelyn yleiset periaatteet

- **1. Tietosuojaperiaatteet**:
  - Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys – lainmukaiset perusteet käsittelylle, mitä tietoja kerätään ja käsitellään ja miten, tieto rekisterinpitäjästä, riskit, suojatoimet ja rekisteröityjen oikeudet ja näistä kaikista informointi
  - Käyttötarkoitussidonnaisuus – tiedot kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten ja käsittely aina vain tietyn ilmoitetun tehtävän hoitamiseksi. Tarkoituksia esim. asiakassuhteen hoito, suoramarkkinointi, työsuhteen osapuolten oikeuksien ja velvollisuuksien hoito.
  - Tietojen minimointi – vain välttämätön henkilötieto tietojen käsittelyn tarkoituksen kannalta. Tietoja ei saa kerätä eikä käsitellä tarpeettomasti.
  - Tietojen täsmällisyys – henkilötietojen oltava täsmällisiä ja tarpeen mukaan päivitettävä ajantasaisiksi
  - Tietojen säilytyksen rajoittaminen – henkilötietojen säilytysajan tulee olla mahdollisimman lyhyt ja ainoastaan sen pituinen kuin tietojen käsittelyn tarkoituksen toteuttaminen on.
  - Tietojen eheys ja luottamuksellisuus – turvallisuus ja luottamuksellisuus säilytettävä ja suojattava lainvastaiselta käsittelyltä ja vahingoilta (esim. tuhoutuminen, hävittäminen, luvaton pääsy)
  - Rekisterinpitäjän osoitusvelvollisuus – uusi velvollisuus, joka koskee erityisesti rekisterinpitäjää

Tietojen käsittelyn yleiset periaatteet

- Osoitusvelvollisuus:
  - Rekisterinpitäjän on dokumentoitava mitä tietosuojaperiaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa.
  - Näiden pohjalta tulla olla mahdollista muodostaa kuva organisaation henkilötietojen käsittelystä ja tietosuojasta.
  - Dokumentoitava henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteet. Näihin kuuluvat lisäksi mm. tietosuojakäytännöt, selosteet, ohjeistukset, koulutukset, sopimukset, riskit, ongelmatilanteet (tietoturvaloukkaukset) ja rekisteröityjen oikeuksien käyttö. Suuria henkilötietomääriä ja arkaluonteisia tietoa käsitellessä on hyvä tehdä tietotilinpäätös tai henkilötietojen käsittelyä koskeva vuosiraportti.
  - Vähintään tulee dokumentoida tietosuojaorganisaatio/tietosuojavastaava, käsiteltävät henkilötietoryhmät, käsittelyn perusteet, henkilötietojen käyttötarkoitus, miten henkilötietoja käsitellään, tietojen säilyttämisaika, miten rekisteröityjä informoidaan käsittelystä, perustelut arkaluonteisten tietojen käsittelylle ja suostumusten hallinta.

Tietojen käsittelyn yleiset periaatteet

- **2. Sisäänrakennettu ja oletusarvoinen tietosuoja**
  - tietosuojaperiaatteet on huomioitava jo tuotteita/palveluita/sovelluksia/toimintaa suunniteltaessa ja kehittäessä.
  - oletusarvoisesti tulee käsitellä vain kunkin käyttötarkoituksen kannalta tarpeellisia tietoja.
  - mukaan suunnitteluun kaikki henkilötietojen käsittelyn kanssa tekemisissä olevat organisaation edustajat.
- **3. Tekniset ja organisatoriset toimenpiteet**
  - mm. henkilöstön koulutus, ohjeet ja määräykset, salassapitosopimukset, fyysinen ja muu tietoturva, tietojen salaus/rajaus, sertifikaatit
- Huom. dokumentaatio on jatkuva prosessi.

Rekisteröityjen oikeudet

- **Oikeus saada tietoa henkilötietojen käsittelystä** – esim. tietosuojaseloste
- **Oikeus saada pääsy tietoihin** – jäljennös käsiteltävistä tiedoista ja tietosuojaseloste
- **Oikeus tietojen oikaisemiseen** – epätarkat, puutteelliset ja virheelliset tiedot oikaistava tai täydennettävä
- **Oikeus tietojen poistamiseen** eli oikeus tulla unohdetuksi – esim. kun henkilötietoja ei enää tarvita, suostumus peruutettu tai lainvastainen käsittely. Oikeus rajoitettu, esim. työntekijä ei voi tulla unohdetuksi.
- **Oikeus käsittelyn rajoittamiseen** – esim. henkilötietojen paikkansapitävyyden kiistäminen, lainvastainen käsittely, erimielisyydet rekisterinpitäjän kanssa. Tällöin organisaation rajoitettava tietojen käsittelyä, käytännössä esim. tietojen siirto toiseen järjestelmään tai estämällä pääsy tietoihin.
- **Oikeus siirtää tiedot järjestelmästä toiseen** – pohjautuu suostumukseen tai sopimukseen ja henkilötietoja käsitellään automaattisesti, esim. sähköpostitili ja sähköpostitilin osoitekirja

Rekisteröityjen oikeudet

- **Vastustamisoikeus** – voi milloin tahansa vastustaa henkilökohtaisella erityisellä tilanteella omien henkilötietojen käsittelyä, joka pohjautuu oikeutettuun etuun. Toteutetaan poistamalla tiedot tai estämättä pääsy tietoihin.
- **Automatisoituihin päätöksiin ja profilointiin liittyvät oikeudet** – oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka pohjautuu automatisoituun käsittelyyn ja profilointiin ja jolla on häntä koskevia oikeusvaikutuksia tai muita vastaavia vaikutuksia. Vaatii ihmisen käsittelijäksi.
- **Oikeus pyytää tieto sellaisista henkilötietojen vastaanottajista**, joille rekisterinpitäjän on ilmoitettava henkilötietojen oikaisemisesta, poistamisesta ja käsittelyn rajoittamisesta.
- **Oikeus tehdä valitus tietosuojaviranomaiselle** – ohjeistus annettava
- **Oikeus saada tieto tietoturvarikkomuksesta**

Rekisteröityjen oikeudet – huomioitavaa

- Rekisterinpitäjällä velvollisuus toteuttaa rekisteröidyn oikeudet.
- Rekisteröityjen saatavilla on oltava ohjeet siitä, miten oikeudet voi toteuttaa.
- Oikeuksia tulee voida toteuttaa suhteellisen helposti.
- Oikeuksien käyttäjän henkilöllisyyden varmistaminen hoidettava tarvittaessa.
- Pyyntö tulee toteuttaa ilman aiheetonta viivytystä, kuitenkin viimeistään yhden kuukauden kuluessa pyynnön vastaanottamisesta, vaativiin ja määrältään suuriin pyyntöihin voi saada kaksi kuukautta lisäaikaa.
- Toimitus yleisesti käytetty sähköinen muoto, jos rekisteröity ei toisin pyydä.
- Oikeuksien käyttö on rekisteröidylle lähtökohtaisesti maksutonta.
- Jos pyyntö on kohtuuton, toistuva tai perusteeton, organisaatio voi joko kieltäytyä pyynnöstä tai periä kohtuullisen maksun.

Rekisteröityjen informointi

- Rekisteröityjen tulisi saada tieto siitä, miten heistä kerättyjä tietoja kerätään ja miten sekä missä määrin niitä käytetään.
- Tietojen oltava helposti saatavilla ja ne on ilmaistava yksinkertaisella ja selkeällä kielellä
- Helpointa usein kerättävien tietojen kuvaaminen Tietosuojaselosteella. Voidaan informoida myös muulla tavoin.
- Tietosuojaselosteen sisältö:
  - Organisaation identiteetti ja yhteystiedot
  - Tietosuojavastaavan yhteystiedot (jos ei ole, niin muuten tietosuojasta vastaavan tiedot
  - Henkilötietojen käsittelyn tarkoitus ja peruste
  - Henkilötietojen vastaanottajat
  - Siirretäänkö tietoja kolmanteen maahan
  - Henkilötietojen säilytysaika
  - Rekisteröidyn oikeudet
  - Onko henkilötietojen antaminen lakisääteinen taikka sopimuksen tekemisen edellyttämä vaatimus ja tietojen antamatta jättämisen seuraukset
  - Mahdollinen profiloinnin olemassaolo
  - Riskit korkean riskien kohdalla
  - Rekisteröityjen ryhmät ja henkilötietoryhmät

Tietosuojavastaava

- Tietosuojavastaava valvoo tietosuoja-asetuksen noudattamista henkilötietojen käsittelyssä. Toimii organisaatiossa rekisterinpitäjän ja henkilötiedon käsittelijöiden tukena.
- Milloin nimitettävä:
  - rekisterinpitäjä on julkishallinnon toimija (pois lukien tuomioistuimet)
  - ydintehtävät edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
  - henkilötietojen käsittely on laajamittaista, kohdistuu erityisiin henkilötietoryhmiin (kuten terveystietoihin, etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen vakaumukseen tai seksuaaliseen suuntautumiseen) tai rikoksia koskeviin tietoihin.
  - Voidaan vaatia myös muissa tilanteissa
  - Pääasiassa organisaatiossa vain yksi tietosuojavastaava, voidaan nimittää myös ulkopuolinen
- Käytännössä siis silloin kun asiakastietojen käsittely on oleellinen osa ydintoimintaa ja laajamittaista. Esim. jos tarjotaan palveluista asiakkaille/jäsenille ja pidetään heistä rekisterejä tämän perusteella, tietoturvavastaava on hyvä olla olemassa.
- Sen sijaan normaali jäsenrekisterin pitäminen tai palkanmaksu työntekijälle on oheistoiminto, ja silloin tietoturvavastaavaa ei tarvita. Tietoturva on kuitenkin varmistettava kaikissa tapauksissa.
- Omattava ja/tai hankittava riittävä asiantuntemus. Koulutuksesta ei ole olemassa vielä tarkempia määrittelyjä.

Tietosuojavastaava

- Tietosuojavastaavan tehtävät:
  - Antaa rekisterinpitäjälle tai käsittelijälle tietoja ja neuvoja tietosuojalainsäädännön asettamista velvollisuuksista ja rekisteröityjen oikeuksien toteuttamisesta
  - seuraa tietosuojalainsäädännön noudattamista ja rekisterinpitäjän tai käsittelijän henkilötietojen suojaan liittyviä menettelyjä, kuten vastuunjakokysymyksen ja henkilöstön koulutuksen järjestämistä
  - antaa pyydettäessä neuvoja ja valvoa asetuksen 35 artiklan mukaista tietosuojaa koskevaa vaikutustenarvioinnin toteuttamista
  - tekee tarpeen mukaan yhteistyötä valvontaviranomaisen kanssa
  - toimii valvontaviranomaisen yhteyshenkilönä käsittelyyn liittyvissä kysymyksissä
  - tietosuojasta (ja tietoturvasta) kokonaisvastuussa on aina organisaation johto
  - rekisterinpitäjä tai henkilötietojen käsittelijä ei saa antaa tietosuojavastaavalle ohjeita tämän tehtävien hoitamisesta
  - rekisterinpitäjä ei saa erottaa tai rangaista tietosuojavastaavaa tietosuojatehtävien hoitamisen vuoksi
  - mahdolliset muut tehtävät ja velvollisuudet eivät saa aiheuttaa eturistiriitaa (esim. ylempi johto ei todennäköisesti voi toimia tietosuojavastaavana).
  - Tietosuojavastaavalle pitää antaa riittävät resurssit tehtävän toteuttamiseen

Valvonta ja sanktiot

- Tuleva tietosuojavirasto toimii valvontaviranomaisena. Laajat tutkintavaltuudet, oikeus tehdä toteuttaa tarkastuksia, oikeus saada pääsy henkilötietoihin sekä rekisterinpitäjän ja käsittelijän tiloihin, valtuudet antaa varoituksia, huomautuksia, määräyksiä (myös sakkoja) ja rajoituksia.
- Jokaisella rekisteröidyllä oikeus tehdä valitus viranomaiselle, jos rekisteröity katsoo, että häntä koskevien tietojen käsittelyssä rikotaan tietosuoja-asetusta.
- Ilmoitukset valvontaviranomaiselle
  - Tietoturvaloukkauksista ilmoittaminen
  - Ennakkokuuleminen korkean riskin tapauksissa
  - Henkilötietojen siirtäminen kolmansiin maihin tai kansainväliselle järjestölle
  - Muu yhteistyö viranomaisten kanssa.

Valvonta ja sanktiot

- Uusi tietosuoja-asetus tuo valvontaviranomaiselle oikeuden määrätä hallinnollisia sakkoja. Lisäksi vahingonkorvausvastuu ja rikosoikeudellinen vastuu (tietosuojarikos).
- Sakkojen määräämisessä vaikuttavat seuraavat tekijät
  - mitä velvollisuutta on rikottu
  - rikkomisen luonne, vakavuus ja kesto
  - kuinka moneen rekisteröityyn vaikuttaa
  - organisaation korjaustoimet
  - miten tuli tietoon (ilmoittiko organisaatio itse ja missä laajuudessa)
  - enimmäismäärä 20 miljoona euroa tai 4 % organisaation liikevaihdosta
- Tietosuojarikkomuksissa ja epäillyissä rikkomuksissa ilmoita aina 72 tunnin sisällä valvontaviranomaiselle.

Tietosuoja-asetukseen valmistautuminen

- Selvitä, pitääkö organisaatioosi nimittää tietosuojavastaava.
- Selvitä, miten organisaatiossasi käsitellään henkilötietoja. Käy läpi käsittelyn vaiheet keräämisestä hävittämiseen ja dokumentoi ne. Varmista, että henkilötietolakia noudatetaan.
- Selvitä, millä laillisella perusteella organisaatiosi käsittelee henkilötietoja.
- Arvioi, millaisia riskejä henkilötietojen käsittelyyn liittyy organisaatiossasi ja miten riskejä minimoidaan. Ryhdy toimenpiteisiin, jotka vastaavat henkilötietojen käsittelyyn liittyvää riskiä ja tee tarvittaessa vaikutustenarviointi.
- Selvitä, miten organisaatiosi noudattaa tietosuoja-asetuksessa määriteltyjä rekisteröityjen oikeuksia. Selvitä myös, miten rekisteröityjen pyyntöihin tällä hetkellä vastataan. Päivitä prosessit.
- Huolehdi tietoturvasta. Valmistaudu ilmoittamaan henkilötietojen tietoturvaloukkauksista.
- Varmista, että sopimukset vastaavat asetuksessa säädettyjä ehtoja, jos organisaatiosi on ulkoistanut henkilötietojen käsittelyyn liittyviä tehtäviä. Huomioi tietosuoja-asetus myös muissa sopimuksissa ja hankinnoissa.
- 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.
- Määrittele johtava valvontaviranomainen, jos organisaatiosi toimii usean EU:n jäsenmaan alueella.
- Lähde: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Lisätietoja

- EU:n yleinen tietosuoja-asetus
- Oikeusministeriö: Miten valmistautua EU:n tietosuoja-asetukseen?
- Tietosuojavaltuutetun toimisto:
  - EU:n tietosuojauudistus
  - Ohjeita rekisterinpitäjälle EU:n tietosuojauudistukseen
  - Tietosuojan ja tietoturvan ”tee se itse” –tarkastus
- Arjen tietosuojaa –materiaalit ja testit
- Tietosuojatesti.fi: Tietosuojatesti
- Kuntaliitto: Henkilötietojen käsittelyn ehdot –sopimuspohja (Word-tiedosto)
- Tulossa vuonna 2018:
  - Suomen tietosuojalaki
  - Kuntaliiton opas tietosuoja-asetuksen ja erityislakien yhteensovittamisessa