TIETOSUOJAPOLITIIKKA: SUOMEN BIOANALYYTIKKOLIITTO RY

TIETOSUOJAPOLITIIKAN TARKOITUS JA TAVOITTEET

Suomen Bioanalyytikkoliitto ry on sosiaali- ja terveysalan ammattijärjestö, joka ajaa jäsentensä ammatillisia etuja. Suomen Bioanalyytikkoliitto ry:n hallituksen 19.5.2018 vahvistaman toimintaperiaatteiden mukaisesti henkilötietojen rekisterinpitäjänä Suomen Bioanalyytikkoliitto ry (jäljempänä Liitto) on sitoutunut suojelemaan yksilön oikeuksia ja vapauksia, kun heidän henkilötietoja käsitellään.

Tämän tietosuojapolitiikan tarkoitus on määritellä ne pääperiaatteet, vastuut ja toimintatavat, joita noudatetaan henkilötietoja käsiteltäessä.

Tavoitteena on varmistaa, että Liitto luotettuna yhdistyksenä noudattaa EU:n tietosuoja-asetuksen, kansallisen lainsäädännön ja muun henkilötietojen käsittelyä koskevan lainsäädännön asettamien vaatimusten mukaisia velvoitteita ja, että lainsäädännön noudattaminen on osoitettavissa dokumentaation avulla.

TIETOSUOJAPOLITIIKAN NOUDATTAMISVELVOLLISUUS

Liiton jäsenet (johto, työntekijät, harjoittelijat sekä vierailijat) ovat velvollisia noudattamaan tietosuojapolitiikkaa sekä muita yhdistystoimintaan läheisesti liittyviä tietoturvaa ja tietosuojaa koskevia käytäntöjä, sääntöjä ja ohjeita. Jos henkilötietojen käsittely tehdään Liiton lukuun, tätä tietosuojapolitiikkaa tulee noudattaa riippumatta siitä missä tietoa säilytetään ja huolimatta siitä kuka omistaa käsittelyyn käytetyt välineet. Tietosuojapolitiikkaa tulee myös noudattaa aina, kun henkilötietojen käsittelyyn käytetään Liiton tietojärjestelmiä tai muita tietotekniikkaresursseja.

MÄÄRITELMÄT

Tietosuojalla tarkoitetaan yksilön (rekisteröidyn) yksityisyyden ja luottamuksen turvaamista sekä henkilötietojen suojaamista luvattomalta käsittelyltä. Henkilötietojen käsittelyn on aina tapahduttava yksilöityä tarkoitusta varten ja laillisen perusteen nojalla.

Henkilötiedolla tarkoitetaan kaikkia tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Henkilötietoja ovat tai voivat olla esimerkiksi nimi, osoite, henkilötunnus, paikkatieto, IP-osoite, muu verkkotunniste, valokuva, tieto ruokavaliosta, terveystieto tai muu tieto, joka yksin tai yhdistettynä muuhun tietoon kertoo jotain tietystä henkilöstä.

Arkaluonteisilla henkilötiedoilla tarkoitetaan tietoja, joista ilmenee henkilön rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisiä tai biometrisiä tietoja, joista henkilö voidaan yksiselitteisesti tunnistaa, terveystietoja taikka tietoja luonnollisen henkilön seksuaalista käyttäytymisestä ja suuntautumisesta.

Pseudonymisoidulla tiedolla tarkoitetaan tietoa, joka on käsitelty niin, ettei tietoa voi enää suoraan yhdistää tiettyyn henkilöön käyttämättä lisätietoja.

Anonymisoidulla tiedolla tarkoitetaan tietoa, joka on käsitelty siten, ettei sen yhdistäminen henkilöön ole enää mahdollista.

Henkilötietojen käsittelyä on esimerkiksi henkilötietojen tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku ja tietojen lähettäminen sähköpostilla tai muutoin.

JULKISUUSPERIAATE

Henkilötietojen suojaa koskevan lainsäädännön lisäksi Liitto voi olla velvollinen luovuttamaan henkilötietoja sisältäviä tietoja sivullisille, joka on yleensä viranomainen tai siihen rinnastettava taho.

Roolit ja vastuut tietosuojan toteuttamisessa

Liiton johdolla on tietosuoja-asioiden yhdistystasoinen vastuu. Tietosuojan ja tietoturvan ohjeistuksen sekä koulutuksen laatimisesta ja tarjoamisesta vastaavat tietosuojavastaava ja tietoturvapäällikkö apunaan tietosuojatyöryhmä sekä henkilöstöhallinto, jonka jäsenet kukin oman vastuu- ja osaamisalueensa osalta osallistuvat ohjeistuksen ja koulutuksen laatimiseen ja tarjoamiseen.

Alueyhdistyksillä on velvollisuus varmistaa, että yhdistyksissä noudatetaan tietosuojalainsäädäntöä ja tätä tietosuojapolitiikkaa. Puheenjohtajat voivat delegoida tietosuoja-asioiden hallinnoinnin tietosuoja-asioiden yhteyshenkilöille, mutta oikeudellinen vastuu on tällöinkin johtajalla.

Henkilörekisterin vastuuhenkilöksi tulee yleensä nimetä asianomaisesta toiminnosta vastaava henkilö. Henkilörekisterin vastuuhenkilö on velvollinen varmistamaan vastuullaan olevan henkilörekisterin osalta, että henkilötietojen käsittely on suunniteltu tietosuojaperiaatteet huomioiden ja tietosuojavelvollisuuksien noudattamisesta huolehditaan tarvittavin teknisin ja organisatorisin toimenpitein.

Henkilörekisterin yhteyshenkilöksi nimetään henkilörekisterin käytännön hallinnoinnista vastaava(t) henkilö(t), esimerkiksi järjestelmän pääkäyttäjä(t). Yhteyshenkilö vastaa mm. henkilörekisterin ja tietosuojadokumentaation ajantasaisuudesta ja rekisterin käyttämisestä Liiton tehtäviin.

Liiton tietosuojavastaava toimii Tehyn tietosuojavastaava, joka vastaa tietosuoja-asioiden neuvonnasta ja opastuksesta, seuraa tietosuoja-asetuksen ja tämän tietosuojapolitiikan noudattamista sekä raportoi poikkeamista johdolle. Tietosuojavastaava toimii valvontaviranomaiselle, tietosuojavaltuutetulle, ilmoittamamana tietosuojayhteyshenkilönä.

Liiton tietoturvapäällikkö toimii Tehyn tietoturvapäällikkö, joka vastaa tietojärjestelmien tietoturvallisuuteen ja muutoin tietoturvaan liittyvästä neuvonnasta ja opastuksesta sekä ilmoitettujen tietoturvapoikkeamien käsittelystä

Jokainen työntekijä ja järjestelmien ja palveluiden käyttäjä on velvollinen osallistumaan omalta osaltaan tietosuojan toteuttamiseen, ylläpitämiseen ja valvontaan mm. noudattamalla tietoturvamääräyksiä.

Henkilötietojen käsittely Liitossa

Liitossa käsitellään tietoja jäsenistä ja Liiton kanssa työskentelevistä yhteistyössä toimivista henkilöistä, kuten entisistä ja nykyisistä jäsenistä ja työntekijöistä, koulutukseen osallistuvista henkilöistä ja yhteistyökumppaneista. Henkilötietoja tulee käsitellä tämän tietosuojapolitiikan mukaisesti ja seuraten hyväksyttyjä suunnitelmia, joissa määritellään käsittelyperusteet ja tarkoitukset, joiden mukaisesti Liiton käsittelee ja säilyttää henkilötietoja.

Liiton toiminnassa voi olla tarve käsitellä arkaluontoisia henkilötietoja, kuten tietoja terveydentilasta sairausloman yhteydessä tai tietoja toimintarajoitteisuudesta tapahtuma järjestelyiden yhteydessä. Arkaluonteisten tietojen ollessa kyseessä pyydetään käsittelyyn erillinen suostumus, jos lainsäädäntö sitä edellyttää.

Tietosuojan toteuttaminen Liitossa

Sisäänrakennettu ja oletusarvoinen tietosuoja

Kaikessa henkilötietojen käsittelyssä tulee noudattaa seuraavia tietosuojan perusperiaatteita:

- henkilötiedon käsittelyllä on lainmukainen käsittelyperuste;
- henkilöille, joiden tietoja käsitellään, annetaan riittävät tiedot käsittelystä; Artikla 30 ja 13/14

- käsittely rajoitetaan käyttötarkoituksen mukaisesti;
- käsittelyssä noudetaan tietoturvaa koskevia määräyksiä;
- työntekijät, jotka käsittelevät henkilötietoja, ovat suorittaneet tietosuojakoulutuksen;
- niille henkilöille, joiden henkilötietoa käsitellään, annetaan tehokkaat mahdollisuudet toteuttaa oikeuksiaan ja heidän pyyntöihinsä reagoidaan viivytyksettä;
- henkilötietojen käsittelyn riskejä arvioidaan käsittelyn kohteena olevan henkilön näkökulmasta, riskit minimoidaan - esimerkiksi pseudonymisoinnin avulla - ja toteutetaan käsittelyä koskeva vaikutustenarviointi, jos riskit ovat suuret;
- käsitellään vain tarpeellisia henkilötietoja;
- huolehditaan tietojen oikeellisuudesta;
- noudatetaan sisäänrakennetun tietosuojan periaatetta;
- tietojenkäsittelytoimet dokumentoidaan;
- henkilötietoja säilytetään vain käyttötarkoituksen edellyttämän ajan;
- tietojenkäsittelyn toimintatapoja arvioidaan säännöllisesti.

Sisäänrakennetun tietosuojan periaatteen toteuttamiseksi tietosuojaperiaatteet ja -vaatimukset tulee huomioida henkilötietoja käsiteltäessä määrittelyvaiheesta koko tietojen elinkaaren ajan. Tämä tarkoittaa muun muassa seuraavaa:

Liiton työntekijät tai alihankkijat, jotka ovat vastuussa uusien tai merkittävästi muuttuneiden henkilötietoja käsittelevien järjestelmien määrittelemisestä ja suunnittelusta ottavat huomioon henkilötietojen suojan ja suoritettavat tarpeelliset riskien- ja/tai vaikutustenarvioinnit

Työntekijöiden, yhteistyökumppaneiden, palveluiden käyttäjien, verkkosivuilla vierailevien ja muiden rekisteröityjen henkilötietoja käsittelevät yksinomaan ne henkilöt, joiden työtehtäviin se kuuluu. Käyttö- ja lukuoikeudet tietojärjestelmiin määritetään ja myönnetään aina työtehtävän edellyttämässä laajuudessa vain niille henkilöille, jotka tarvitsevat ko. tietojärjestelmän sisältämän henkilörekisterin tietoja heille annetun tehtävän hoitamiseksi.

Henkilötietojen käsittelystä informoiminen

Henkilötietojen käsittelystä annetaan tietosuoja-asetuksen edellyttämä informaatio verkkosivuilla julkaistavissa tai muutoin rekisteröityjen tietoon saatettavissa tietosuojailmoituksissa. Kunkin henkilörekisterin vastuuhenkilö on myös velvollinen huolehtimaan siitä, että rekisteristä on laadittu Liiton sisäinen tietosuojaseloste.

Henkilötietojen oikeellisuudesta huolehtiminen

Henkilörekisteritietojen ajantasaisuudesta ja oikeellisuudesta tulee huolehtia. Liiton työntekijöitä koskevien henkilörekisteritietojen ajantasaisuuden varmistamiseksi jokainen työntekijä vastaa palkanmaksua varten antamiensa henkilökohtaisten tietojen sekä muiden ilmoittamiensa tietojen oikeellisuudesta ja ajantasaisuudesta. Työsuhteen aikana työntekijän tulee ilmoittaa em. tietoja koskevat muutokset henkilöstöpalveluiden kulloinkin voimassa olevan ohjeistuksen mukaisesti. Jäsenrekisteritietojen ajantasaisuuden varmistamiseksi jäsenen tulee tarkistaa henkilötietojensa oikeellisuus ja päivittää henkilötietonsa portaalissa tarvittaessa. Muiden henkilörekisterien osalta tietojen päivityksistä sovitaan rekisteröityjen kanssa tai tiedot päivitetään julkisia rekistereitä hyödyntämällä (esim. Väestötietojärjestelmän kautta).

Henkilötietojen säilytysajat

Liitto säilyttää henkilötietoja tiedonohjaussuunnitelman mukaisesti. Tiedonohjaus-suunnitelmassa on lueteltu eri prosesseissa syntyvät asiakirjat tai tiedot, sekä niiden:

- Säilytysajoissa noudatetaan Tehy ry:n säilytysaikoja. Kun tiedonohjaussuunnitelman mukainen säilytysaika on ohi, tulee asiakirjat hävittää turvallisesti tietoaineiston hävittämisestä annetun ohjeistuksen mukaisesti.

Henkilötietojen käsittelyn ulkoistaminen

Liitto voi rekisterinpitäjänä ulkoistaa osan henkilötietojen käsittelytoimistaan ulkopuoliselle käsittelijälle. Ulkopuoliseksi henkilötietojen käsittelijäksi valitaan sellaisia kumppaneita, jotka noudattavat hyvää henkilötietojen käsittelytapaa sekä täyttävät EU:n tietosuoja-asetuksen vaatimukset. Liiton ja palveluntarjoajan välille laaditaan kirjallinen sopimus, jossa määritellään henkilötietojen käsittelyn kohde, tarkoitus sekä muut tietosuoja-asetuksen edellyttämät tiedot.

Automaattinen päätöksenteko

Henkilön tai henkilön suorituksen arviointien tuloksena ei tehdä päätöksiä automatisoidusti, vaan esimerkiksi siten, että Liiton henkilökunnan jäsen valvoo automaattisen arvioinnin tuloksia.

TIETOTURVA

Jokaisen Liitossa henkilötietoja käsittelevän tulee omalta osaltaan varmistaa, että henkilötietoja säilytetään turvallisesti ja henkilötietoja ei anneta kolmannelle osapuolelle vahingossa tai tarkoituksella lainvastaisella tavalla. Eheyden, luottamuksellisuuden ja käytettävyyden varmistamiseen pyritään sekä tietoteknisien ratkaisujen, että prosessien avulla. Vastuu eheyden, luottamuksellisuuden ja käytettävyyden toteutumisesta on jokaisella henkilötietoja käsittelevällä.

Perustan tiedon suojaamiselle (eheys ja luottamuksellisuus) antavat Liiton tietoaineiston käsittelysäännöt. Tietoaineiston käsittelysäännöissä kuvataan toimintatavat, joiden avulla estetään aineiston joutuminen ulkopuolisten käsiin. Käsittelysäännöt sisältävät ohjeet esimerkiksi tiedon salaukseen eri tilanteissa. Tietoaineiston käsittelysäännöt koskevat tietoa sen kaikissa olomuodoissa, esimerkiksi tietojärjestelmissä, dokumentissa, tulostettuna, varmuuskopiona jne. Turvaluokitellun tiedon sijoittaminen johonkin tietojärjestelmään edellyttää, että tietojärjestelmä täyttää turvaluokan vaatimukset.

TIETOTURVAPOIKKEAMIA KOSKEVA ILMOITUSVELVOLLISUUS

Tietoturvapoikkeama on tapahtuma, jonka seurauksena Liiton vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai käytettävyys vaarantuu. Jokaisella on velvollisuus raportoida tietoturvapoikkeamasta. Tietoturvapoikkeamia ovat esimerkiksi muistivälineiden tai laitteiden katoaminen sekä merkittävät haittaohjelmat. Tapahtuneesta tai epäillystä tietoturvapoikkeamasta on välittömästi ilmoitettava ottamalla yhteyttä Liiton tietoturvaryhmään, esimerkiksi sähköpostilla osoitteeseen security@tehy.fi, tai muutoin tietoturvaryhmän ohjeistuksen mukaisesti. Tietoturvaryhmä käsittelee Liittoa koskevat tietoturva- ja tietosuojapoikkeamailmoitukset, avustaa poikkeamien ratkaisemisessa, mm. tutkimalla mahdolliset tietomurrot

Tietosuoja-asetuksen mukaisesti Liiton tietosuojavastaava ilmoittaa ilman aiheetonta viivästystä ja viimeistään 72 tunnin sisällä tietosuojavaltuutetulle, jos tapahtuu henkilötietojen tietoturvaloukkaus, joka todennäköisesti aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Jos tapahtuu henkilötietojen tietoturvaloukkaus, joka todennäköisesti aiheuttaa korkean riskin henkilöille, ilmoittaa tietosuojavastaava viivytyksettä asianomaisille henkilöille.

HENKILÖTIEDON SIIRTÄMINEN EU:N JA EUROPEAN ECONOMIC AREA -ALUEEN (EEA) ULKOPUOLELLE

Liiton tietosuojapolitiikkana on noudattaa erityistä huolellisuutta, jos henkilötietoa siirretään EU:n ja European Economic Area -alueen (EEA) ulkopuolelle maihin, jotka eivät tarjoa EU:n tietosuoja-asetuksen mukaista tietosuojaa. Henkilötiedon siirtäminen EU:n ja EEA-alueen ulkopuolelle tulee toteuttaa tietosuoja-asetuksen vaatimusten mukaisesti.

REKISTERÖITYJEN TIETO-, TARKASTUS- JA MUUT TIETOSUOJAPYYNNÖT

Henkilötietojen suojaan kuuluu mm. jokaisen oikeus tutustua hänestä kerättyihin tietoihin ja saada tiedot korjatuiksi tai tietyin rajoituksin poistetuiksi. Liitossa on määritetty toimintaprosessi ja toteutettu

rekisteröityjen tieto- tarkastus-, korjaus- ja poistamispyyntöjä varten sähköinen menettely, jota ylläpitää tietosuojavastaava.

Koulutus ja ohjeistus

Liiton henkilötietojen rekisterinpitäjänä pyrkii varmistamaan, että henkilökunta on tietoinen tietoturvan heille asettamista vaatimuksista ja vastaa koulutuksen ja ohjeiden tarjoamisesta. Jokaisen henkilökunnan jäsenen tulee tutustua henkilötietojen käsittelyä koskevaan ohjeistukseen. Verkkokoulutuksen tai muun koulutuksen suorittaminen ennen henkilötietojen käsittelemistä voidaan edellyttää, jos työtehtävät sitä vaativat.

Tietosuojailmoitukset, käytännesäännöt- ja ohjeet, koulutusmateriaalit ja muu tietosuojainformaatio julkaistaan Liiton omilla verkkosivuilla.

Tietosuojapolitiikan vastainen menettely

Henkilöä, joka huomaa, ettei tietosuojapolitiikkaa ole noudatettu hänen henkilötietojensa käsittelyssä, pyydetään asian korjaamiseksi ottamaan yhteyttä Liiton tietosuojavastaavaan sähköpostitse tietosuojavastaava@tehy.fi.Henkilöllä on myös oikeus saattaa Liiton toiminnan lainmukaisuus Tietosuojavaltuutetun toimiston arvioitavaksi.

Tietosuojapolitiikan voimaantulo ja ylläpito

Liiton hallituksen puheenjohtaja on hyväksynyt tämän henkilötietojen suojaa koskevan politiikan henkilökuntaa, varsinaisia jäseniä ja muita yhteisön jäseniä sitovaksi säännöstöksi 19.5.2018. Liiton tietosuojavastaava vastaa siitä, että tietosuojapolitiikka pysyy ajankohtaisena ja sitä tarkistetaan muutostarpeita vastaavaksi.