POHJOIS-POHJANMAA
COUNCIL OF OULU REGION

Pohjois-Pohjanmaan liiton tietoturva- ja tietosuojasääntö

Maakuntahallitus 23.5.2022 § 82

POHJOIS-POHJANMAA
COUNCIL OF OULU REGION

Sisällys

Johdanto

Tietoturva- ja tietosuojasääntö määrittää ne periaatteet, toimintatavat ja vastuut, joita noudatetaan Pohjois-Pohjanmaan liiton tietoturva- ja tietosuojatyön toteuttamisessa ja kehittämisessä. Sääntö toimii perustana kuntayhtymän tietoturvaa ja tietosuojaa koskeville toimintaohjeille, joiden tehtävänä on tarkentaa säännössä annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa.

Tietoturva- ja tietosuojasääntöä ja sen perusteella annettuja ohjeita ja määräyksiä noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia kuntayhtymän palveluksessa olevia viranhaltijoita, työntekijöitä ja luottamushenkilöitä. Tietoturva- ja tietosuojatyössä onnistuminen edellyttää kuntayhtymän johdon ja henkilöstön sitoutumista tietoturvatyön tukemiseen sekä tietoturvan edistämiseen. Tietoturva ja tietosuoja ovat osa koko organisaation jokapäiväistä toimintaa.

Tietoturva- ja tietosuojasääntö on julkinen asiakirja ja se on saatavilla Pohjois-Pohjanmaan liiton verkkosivuilta.

Tietoturva ja tietoturvatyön tavoitteet

Tietoturvalla tarkoitetaan eri muodossa olevien tietojen suojaamista erilaisilta uhkatekijöiltä. Tietoturvan tavoitteena on tila, jossa tietotekniikkaa ja muita menetelmiä voidaan käyttää tietojen keräämiseen, käsittelyyn ja säilyttämiseen mahdollisimman tietoturvallisesti, sekä käytettävissä olevan tiedon oikeellisuuden, saatavuuden ja luottamuksellisuuden varmistamiseksi.

Tietoturvatyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvallisuudesta huolehtiminen edellyttää tiedon elinkaaren kaikkiin vaiheisiin sekä näiden aikana tiedon käsittelyyn käytettyihin välineisiin, järjestelmiin ja menetelmiin kohdistettuja oikein valittuja ja toteutettuja toimenpiteitä sekä tietoa käsittelevien henkilöiden toiminnan ohjaamiseen tarkoitettuja sääntöjä ja ohjeita sekä koulutusta.

Tietoturvatyön tavoitteena on hallita tiedon käsittelyä uhkaavia riskejä, turvata liiton toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden luvaton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot.

Pohjois-Pohjanmaan liiton tietoturvatoiminta on suunnitelmallista ja systemaattista. Tietoturvallisuuden suunnittelussa ja hallinnassa otetaan huomioon tietojen saatavuus, eheys ja luottamuksellisuus.

- Saatavuus: tiedot ovat kaikkien niitä tarvitsevien saatavilla viivytyksettä ajasta ja paikasta riippumatta käyttöoikeuksien puitteissa.
- Eheys: tiedot on suojattu siten, ettei niitä voi muuttaa tahallisesti tai tahattomasti siten, että niiden luotettavuus vaarantuu, tai ainakin tällaiset muutokset voidaan havaita.
- Luottamuksellisuus: tieto on vain niiden käyttävissä, joilla on siihen oikeus, ja että tietojen luvaton käyttö havaitaan sekä siihen reagoidaan.

Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

Pohjois-Pohjanmaan liitossa on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta (Tiedonhallintalaki 12 §). Vaatimus tarkoittaa sitä, että viranomaisen on esimerkiksi osana organisaation riskienhallinnan suunnittelua arvioitava ja päätettävä, onko tietyissä tehtävissä toimimisen edellytyksenä luotettavuuden arviointi.

Arvioinnin tuloksena voi olla, että erityistä luotettavuutta vaativia tehtäviä ei viranomaisessa ole. Samoin viranomaisen ei tarvitse vaatia esim. luottotietojen selvittämistä, vaikka yksityisyydensuojasta työelämässä annetun lain 5a § mukaiset edellytykset siihen täyttyisivät. Viranomainen voi harkita ovatko sen muut riskienhallintatoimenpiteet riittäviä, jolloin erityisestä luotettavuudesta varmistuminen ei ole tarpeen.

Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

Pohjois-Pohjanmaan liitossa on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan, sekä selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti (Tiedonhallintalaki 13 §).

Tietoturvallisuus varmistetaan laatimalla ja ylläpitämällä tietohallintoa koskeva riskienhallintasuunnitelma Pohjois-Pohjanmaan liiton sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti. Riskienhallintasuunnitelma sisältää tietoturvan vaarantuessa toteutettavat jatkuvuudenhallinnan toimenpiteet. Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys varmistetaan riittävällä järjestelmien testauksella sekä jatkuvuudenhallinnan toimenpiteiden harjoittelulla säännöllisesti.

Tietojen siirtäminen tietoverkossa

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla, eli vahvaa

sähköistä tunnistusta käyttämällä ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja (Tiedonhallintalaki 14 §).

Tietoaineistojen turvallisuuden varmistaminen

Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein sen tietoaineistojen turvallisuus (Tiedonhallintalaki 15 §). Tietoaineistot suojataan teknisiltä ja fyysisiltä vahingoilta käyttämällä viranomaisen järjestelmiä käyttöohjeiden mukaisesti, sekä säilyttämällä paperiasiakirjat asianmukaisissa toimisto- tai arkistotiloissa. Henkilöstöltä edellytetään huolellista ja asianmukaista asiakirjojen ja työvälineiden käsittelyä. Kaikkia henkilöstön käytössä olevia käyttäjätunnuksia, järjestelmiä ja asiakirjoja tulee käsitellä annettujen ohjeiden mukaisesti.

Tietojärjestelmien käyttöoikeuksien hallinta

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina (Tiedonhallintalaki 16 §).

Pohjois-Pohjanmaan liiton käytössä olevien tietojärjestelmien käyttöoikeudet määritetään tehtävittäin, ja käyttöoikeudet myönnetään ja poistetaan ilman erillistä hakemusta sen mukaisesti missä tehtävässä henkilö toimii. Erillisellä hakemuksella myönnetään ainoastaan sellaiset käyttöoikeudet, joihin henkilöllä ei ole tehtäväkohtaisesti määritettyjä oikeuksia. Käyttöoikeudet myönnetään aina vain tehtävän tosiasiallisen hoidon ajalle.

Esihenkilöt vastaavat vastuualueensa henkilöstön tehtävämuutosten ja palvelussuhteen päättymisen ilmoittamisesta tietojärjestelmien pääkäyttäjille, jotta käyttöoikeudet pystytään pitämään ajantasaisina.

Lokitietojen kerääminen

Pohjois-Pohjanmaan liiton on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista (Tiedonhallintalaki 17 §). Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

Pohjois-Pohjanmaan liitossa lokitiedot kerätään niistä tietojärjestelmistä, joihin kirjaudutaan käyttäjäkohtaisella käyttötunnuksella, ja joissa käsitellään henkilötietoja tai salassa pidettäviä tietoja. Lokitiedot muodostavat henkilötietovarannon, joka on kuvattu Pohjois-Pohjanmaan liiton tiedonhallintamallissa.

Henkilötietojen kerääminen ja käsitteleminen

Kaikessa henkilötietojen keräämisessä ja käsittelemisessä on noudatettava EU:n tietosuoja-asetusta ja kansallista tietosuojalakia. Lisää tietoa säädöksistä ja henkilötietojen määritelmästä tietosuojavaltuutetun internet-sivuilta.

Henkilötietojen keräämisen tulee aina perustua tiettyyn etukäteen määritettyyn yksilöityyn ja lailliseen tarkoitukseen. Henkilötietoja on kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden.

- Henkilötietojen käsittelylle täytyy olla oikeutettu käsittelyperuste.
- Henkilötietojen keräämisen täytyy tapahtua vain etukäteen nimettyä tarkoitusta varten.
- Henkilötiedoille täytyy määrittää etukäteen säilytysaika tai säilytyskriteerit.
- Rekisteröidylle täytyy antaa henkilötietoja kerätessä keskeiset tiedot tietojen käsittelystä.
- Rekisteröidyltä tulee pyytää suostumus henkilötietojen keräämiseen, jos se perustuu vapaaehtoisuuteen.

Henkilötietojen käsitteleminen on sallittua ainoastaan etukäteen määritettyyn tarkoitukseen ja vain sen ajan, kun tietoja niitä tarvitaan kyseisessä tarkoituksessa. Henkilötiedot täytyy säilyttää suojattuna asiattomalta katselulta ja käsittelyltä. Rekisterinpitäjän täytyy huolehtia rekisteröidyn oikeuksien toteutumisesta.

- Henkilötietoja käsitellään vain siihen tarkoitukseen, johon ne on kerätty.
- Henkilötietoja saavat katsella ja käsitellä vain ne, joiden työtehtäviin se kuuluu.
- Henkilötiedot on säilytettävä käyttöoikeuksilla tai muilla asianmukaisilla keinoilla suojattuna.
- Rekisteröidyllä on oikeus pyytää nähtäville hänestä kerätyt tiedot, sekä oikeus pyytää tietojen oikaisemista tai suostumuksella annettujen tietojen poistamista.

Kerätyt henkilötiedot on poistettava viivytyksettä, kun niiden käyttötarve on päättynyt. Henkilötietojen käyttöä tai säilyttämistä ei saa jatkaa toisessa tarkoituksessa kuin mihin ne on alun perin kerätty.

- Yksittäisen rekisteröidyn tiedot on poistettava, jos hän pyytää niiden poistamista oikeutetusti.
- Yksittäisen rekisteröidyn tiedot on poistettava, kun kyseistä rekisteröityä koskeva tietojen käyttötarve päättyy.
- Kaikki kerätyt henkilötiedot on hävitettävä niille määritetyn käyttötarpeen ja säilytysajan päätyttyä.
- Kaikki henkilörekisteristä muodostetut kopiot (tiedostot, sähköpostit) on hävitettävä.

Tietoturvan ja tietosuojan organisointi ja vastuut

Tietoturvan ja tietosuojan organisointi ja johdon vastuut perustuvat Pohjois-Pohjanmaan liiton hallintosääntöön. Maakuntajohtajalla on kokonaisvastuu maakunnan liiton tehtävien yhteensovittamisesta (Hallintosääntö 13 §). Hallinto- ja henkilöstöjohtaja toimii hallinnon vastuualueelle kuuluvan tietohallinnon hallinnollisena esimiehenä,

sekä vastaa tehtävien taloudellisesta ja tuloksellisesta hoidosta ja asetettujen tavoitteiden saavuttamisesta (Hallintosääntö 10 §). Tietohallintopäällikkö vastaa tietoturvan ja tietosuojan toteuttamisesta ja toimeenpanosta tehtävänkuvansa mukaisesti.

Tietoturvan ja tietosuojan käytännön toimenpiteet kuvataan pääsääntöisesti erikseen annetuissa ohjeissa sekä Pohjois-Pohjanmaan liiton sisäisen valvonnan ja riskienhallinnan ohjeen mukaisesti laaditussa riskienhallintasuunnitelmassa. Riskienhallintasuunnitelma sisältää kuvauksen riskienhallinnan toimenpiteistä ja niiden vastuista, sekä jatkuvuudenhallinnan toimenpiteistä ja vastuista.

Tietoturvan ja tietosuojan viestintä ja kehittäminen

Pohjois-Pohjanmaan liiton sisäisestä ja ulkoisesta tietoturva- ja tietosuojatiedottamisesta vastaa tietohallintopäällikkö yhdessä viestintä- ja hallintopäällikön kanssa. Kriisitilanteissa viestinnästä vastaa maakuntajohtaja.

Pohjois-Pohjanmaan liitto huolehtii henkilöstön riittävästä tietoturva- ja tietosuojaosaamisesta koulutuksilla ja tiedottamisella. Uudet työntekijät perehdytetään tietoturva- ja tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään henkilötietoja.

Tietosuojaa ja -turvaa koskeva lainsäädäntö ja ohjeistus

- EU:n tietosuoja-asetus
- Tietosuojalaki
- Tiedonhallintalaki
- Pohjois-Pohjanmaan liiton hallintosääntö
- Pohjois-Pohjanmaan liiton sisäisen valvonnan ja riskienhallinnan ohje