Kymsote

Kymenlaakson
sosiaali- ja terveyspalvelut

Tietosuojapolitiikka

2020

Sisällysluettelo

1. Johdanto 1
2. Ohjaavat vaatimukset 2
3. Tietosuojan tavoitteet ja periaatteet 2
4. Tietosuojan organisointi ja vastuut 3
5. Tietosuojan toteuttaminen 4
6. Versio ja päivityshistoria 5
Liitteet 5

1. Johdanto

Tämä tietosuojapolitiikka linjaa vastuut, periaatteet sekä toimintatavat, joita noudatetaan Kymsoten tietosuojan toteutuksessa ja kehityksessä. Tietosuojapolitiikka koskee kaikkea henkilötietojen käsittelyä, jossa Kymsote toimii rekisterinpitäjänä tai henkilötietojen käsittelijänä. Tietosuojapolitiikka otetaan käyttöön koko konsernin laajuisesti koskien myös tytäryhtiöitä.

Kuntayhtymän SOTE – ja muiden henkilötietojen rekisterinpito perustuu Kymsoten hallintosääntöön sekä perustamisasiakirjaan.

Politiikka on katselmoitu Tietoturva- ja tietosuojaryhmässä ja YT-ryhmässä, hyväksytty Kymsoten johtoryhmässä sekä annettu Kymsoten hallitukselle tiedoksi.

Tietosuojapolitiikka on julkinen asiakirja ja se on saatavilla Kymsoten verkkosivuilta. Tietosuojapolitiikkaa päivittää ja ylläpitää Kymsoten Tietoturva- ja tietosuojaryhmä.

2. Ohjaavat vaatimukset

Tietosuojapolitiikan ohella tietosuojan toteuttamista ohjaa myös Kymsoten tietoturvapolitiikka.

Tietosuojapolitiikkaa laadittaessa on huomioitu seuraavat lait ja asetukset:

- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuojalaki (1050/2018)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sosiaalihuollon asiakaskirjoista (254/2015)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)

Lisäksi on otettu huomioon Tietosuojavaltuutetun, Terveyden ja hyvinvoinnin laitoksen, Valviran ja Kyberturvallisuuskeskuksen aiheeseen liittyvä ohjeistus.

3. Tietosuojan tavoitteet ja periaatteet

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot.

Tietosuojan tarkoituksena on turvata tiedon kohteen (data subject) yksityisyys sekä edut, oikeudet ja vapaudet sekä oikeusturva. Henkilötietojen käsittelyn on aina perustuttava lainmukaiseen perusteeseen, joten tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Kaikessa henkilötietojen käsittelyssä on noudatettava EU:n yleisen tietosuoja-asetuksen, kansallisen tietosuojalain ja käsiteltävää henkilötietoa koskevan erityislainsäädännön säädöksiä. Rekisterinpitäjän tulee pystyä osoittamaan, että henkilötietoja käsitellään tietosuoja-asetuksen mukaisesti ottaen huomioon käsittelyn riskit. Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden suunnittelua, käytännön toteuttamista ja näiden valvontaa sekä näiden kaikkien vaiheiden dokumentointia.

Tietosuoja on osa Kymsoten toimintakulttuuria, joka huomioidaan kaikessa tekemisessä alkaen henkilöstön rekrytoinnista kattaen myös työsuhteen jälkeiset salassapitovelvollisuudet. Kaikessa henkilötietojen käsittelyssä korostuu huolellisuus. Tietosuojan vaatimukset huomioidaan jo suunnittelu- ja valmisteluvaiheessa kaikissa hankinnoissa ja sopimuksissa sekä osana niiden ylläpitoa ja toteuttamista.

Kymsoten henkilötietojen käsittelyssä noudatetaan EU:n yleisen tietosuoja-asetuksen artikla 5 periaatteita.

- lainmukaisuus
- kohtuullisuus
- läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- osoitusvelvollisuus

Toiminnassa huomioidaan rekisteröidyn oikeudet, joita ovat:

- oikeus saada informaatio henkilötietojen käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot (suostumuksen peruuttaminen)
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen (suostumuksen perusteella kerätyt tiedot)
- olla joutumatta automaattisen päätöksenteon kohteeksi ilman laillista perustetta

Rekisteröidyn oikeus tulla unohdetuksi ei koske lakisääteisten tehtävien hoitamiseen liittyvää henkilötietojen käsittelyä vaan mahdollisia vapaaehtoisuuteen perustuvia henkilötietorekisterejä.

Henkilötietoja suojattaessa on suojattava tiedon luottamuksellisuuden lisäksi tiedon eheys ja saatavuus. Päätökset on tehtävä ja kontrollit rakennettava riskilähtöisesti siten, että kyseessä olevien lakien vaatimukset tulevat täytetyksi. Lisäksi on täytettävä viranomaisten asettamat erilliset vaatimukset. Mikäli ohjaavaa ja velvoittavaa sääntelyä ei ole, on toimenpiteet perustettava oikein mitoitettuun riskienhallintaan.

4. Tietosuojan organisointi ja vastuut

Hallintojohtaja vastaa Kymsoten tietosuojasta. Kymsoten Tietoturva ja tietosuojaryhmä toimii hallintojohtajan apuna kuntayhtymän tietosuojan kehityksessä sekä seurannassa.

Tietosuojavastaavan tehtävänä on tietosuojan toteutumisen ohjaaminen ja seuranta ja hänet on otettava mukaan ajoissa tietosuojaa koskevien asioiden valmisteluun. Tietosuojavastaavalla on oikeus ja velvollisuus puuttua havaitsemiinsa tietosuojaan liittyviin epäkohtiin sekä raportoida tekemistään havainnoista organisaation ylimmälle johdolle.

Henkilötietoja sisältävien käsittelyjen kokonaisuuksien tietosuojasta vastaa sen kyseisen nimetty rekisterin rekisterinpitäjä.

Jokainen esimies vastaa omien alaistensa perehdyttämisestä, ohjaamisesta, kouluttamisesta ja seurannasta.

Jokainen työntekijä palvelussuhteesta riippumatta on vastuussa omasta työstään ja tietosuojan toimeenpanosta annetun ohjeistuksen ja tietosuojaperiaatteiden mukaisesti.

Henkilötietojen käsittelytehtäviä voidaan ulkoistaa palveluntuottajien vastuulle. Näissä tapauksissa palveluntuottajalla on vastuu sopimukseen kirjattujen tietosuojavelvoitteiden täyttämisestä ja Kymsotella palveluntuottajan sopimusvelvoitteiden täyttymisen seurannasta. Ulkoistettuun henkilötietojen käsittelyyn liittyvät vastuuhenkilöt sekä Kymsoten että palveluntuottajan puolella määritellään sopimuskohtaisesti.

Projektipäällikkö varmistaa projektin tietosuojan toteutumisen ja raportoi tietosuojan toteutumisesta rekisterinpitäjälle.

5. Tietosuojan toteuttaminen

Tietosuojan toimeenpanoa ohjataan ohjeistuksen, koulutuksen sekä tietosuojaprosessien avulla. Kymsoten tietosuojaprosessit on kuvattu IMS -tietojärjestelmässä.

Tietoturvalla ja tietosuojalla pyritään tiedon laadun ja eheyden koskemattomuuden säilyttämiseen sekä tiedon luottamuksellisuuden suojaamiseen teknisin ja hallinnollisin keinoin. Teknisiä keinoja ovat esimerkiksi käyttöoikeudet, toimitilojen turvaaminen ja hallinnollisia keinoja käyttöoikeuksien määritteleminen ja dokumentoiminen, henkilöstön ohjeistaminen ja kouluttaminen.

Yleinen tietosuoja-asetus ei yksiselitteisesti aseta mitään teknologia- tai menetelmävaatimuksia. Käsittelyn turvallisuudessa huomioitavia ratkaisuja ovat tiedon:

- salaaminen
- anonymisointi
- pseudonymisointi
- varmentaminen
- palauttaminen
- toteutettujen tietoturvatoimenpiteiden testaaminen.

Kymsotessa laaditaan kaikesta henkilötietojen käsittelystä:

- Seloste käsittelytoimista
- Henkilötietojen käsittelyn riskien arviointi ja tarvittaessa vaikutustenarviointi
- Rekisteröidyn informointi

Tietosuojapolitiikan velvoitteet ovat voimassa riippumatta työskentelypaikasta. Tietosuojan on toteuduttava samantasoisesti niin etätöissä kuin Kymsoten toimitiloissa. Pääsy henkilötietoja sisältäviin tietoihin on ensisijaisesti rajattava ainoastaan EU:n tai ETA alueen sisäiseksi.

Jos henkilötietojen käsittely aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta todennäköisesti korkean riskin, on rekisterinpitäjän toteutettava ennen käsittelyn aloittamista tietosuojaa koskeva vaikutustenarviointi.

Alihankkijoiden, yhteistyökumppaneiden ja eri henkilötietojen käsittelijöiden vastuut on varmistettava sopimusteknisesti. Henkilötietojen käsittelyyn liittyvissä järjestelmähankinnoissa ja -projekteissa laaditaan käsittelytoimien kuvaus ja riskien arviointi.

Tietojen käsittelyssä noudatetaan Kymsoten henkilötietojen käsittelyn yleisohjetta sekä muita tietosuojaohjeita.

Tietosuojaan kohdistuvaa poikkeamaa käsitellään tietoturvaloukkaus-prosessin mukaisesti tietoturvaloukkausilmoituksena.

Tietosuojaan liittyvä koulutus on jatkuvaa ja kattaa koko työsuhteen elinkaaren. Myös sopimuskumppanit ja alihankkijat tulee velvoittaa huolehtimaan oman henkilöstönsä kouluttamisesta.

Tietosuojan toteutuksen seurantaa suoritetaan aktiivisesti ja havaitut poikkeamat käsitellään Kymsoten prosessien mukaisesti. Seurantaa toteutetaan myös lokipolitiikan määrittämän aktiivisen valvonnan avulla.

Lisätietoja ja käytännön ohjeistusta löydät:

- Kymsoten intranetistä (Etusivu > Meidän tapamme toimia > Tietosuoja)
- Omalta esimieheltä
- Tietosuojavastaavalta
- Tietosuojavaltuutetun toimistosta: https://tietosuoja.fi/

Versio ja päivityshistoria

Muutoshistoria			
Versio	**Päivä**	**Tekijä**	**Kuvaus**
0.1		Kymsoten asiantuntijat ja Huld OY	Asiakirjan pohja ja luonnosversio tehty
0.2	4.6.2020	Tietoturva- ja tietosuojaryhmä	Asiakirja esitelty ja käyty läpi
0.3	12.11.2020	YT-toimikunta	Asiakirja esitelty ja käyty läpi
0.4	17.11.2020	Työsuojelutoimikunta	Asiakirja esitelty ja käyty läpi
1.0	1.12.2020	Kymsote Jory	Politiikka hyväksytty

Liitteet

Liite 1, Terminologia – kuvaukset tietosuojaan ja tietoturvaan liittyvistä käsitteistä