Kymenlaakson hyvinvointialue

Lokipolitiikka

2023

Sisällysluettelo

Johdanto

Tämä lokipolitiikka linjaa vastuut, periaatteet sekä toimintatavat, joita noudatetaan Kymenlaakson hyvinvointialueen (jatkossa hyvinvointialue) lokitietojen käsittelyssä ja keräämisessä. Lokipolitiikka ohjaa lokitietojen käyttöä hyvinvointialueen tietosuojan ja tietoturvan toteutumisen varmistamiseksi.

Tätä lokipolitiikkaa sovelletaan kaikkiin hyvinvointialueen hallinnoimiin tietojärjestelmiin koskien myös tytäryhteisöjä ja pelastustoimea soveltuvin osin.

Politiikka on hyväksytty Kymenlaakson hyvinvointialueen aluehallituksessa.

Lokipolitiikka on julkinen asiakirja ja se on saatavilla Kymenlaakson hyvinvointialueen verkkosivuilta sekä Intra/työn tukena/tietoturva ja tietosuoja sivulta. Lokipolitiikkaa päivittää ja ylläpitää hyvinvointialueen Tietoturva- ja tietosuojaryhmä.

1. Ohjaavat vaatimukset

Lokipolitiikan ohella lokien käsittelyä ohjaavat Kymenlaakson hyvinvointialueen tietoturva- ja tietosuojapolitiikat.

Lokipolitiikkaa 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 (784/2021)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (94/2022)
- 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 viranoimaisen toiminnan julkisuudesta (621/1999)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Laki sähköisen viestinnän palveluista (917/2014)

Lisäksi on otettu huomioon Tietosuojavaltuutetun, Terveyden ja hyvinvoinnin laitoksen, Valviran ja Kyberturvallisuuskeskuksen aiheeseen liittyvä ohjeistus, sekä tiedonhallintalautakunnan suositukset. Hyvinvointialueelle käytetään turvallisuusverkkoa, jonka asettamat tietoturvallisuuden erillisvaatimukset otetaan huomioon turvallisuusverkon käytössä ja käyttöön liittyvissä ICT-ratkaisuissa.

2. Lokienhallinnan tavoitteet ja periaatteet

Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin, eli lokitetaan.

Lokitiedon käsittelyllä tarkoitetaan lokitiedon keräämistä, säilyttämistä, katselua, analysointia, seurantaa, luovutusta, tuhoamista ja raportointia.

Lokin käyttötarkoitus vaikuttaa lokien käsittelyyn. Lokipolitiikka ottaa huomioon seuraavat lokityypit ja käyttötarkoitukset.

- SOTE ja muiden henkilötietojen käsittelyyn liittyvät käytönvalvontalokit.
- Vianselvitykseen ja palvelutason seurantaan liittyvät tekniset lokit.
- Tietoturvallisuuden seurantaan liittyvät tietoturvalokit.
- Viestinvälitykseen liittyvät välitystiedot eli viestintälokit.

Lokienhallinnalla pyritään varmistamaan kyky todentaa tapahtuman kulku, osapuolet, kiistämättömyys, mahdolliset tunkeutumiset ja poikkeamat, järjestelmän toimivuus sekä käyttäjien ja rekisteröityjien oikeusturva.

Kymenlaakson hyvinvointialueella lokien käsittelyä ohjaavat seuraavat periaatteet:

- Lokitietojen käsittelyn tarvelähtöisyys
- Luottamuksellisuuden säilyttäminen
- Eheyden säilyttäminen
- Henkilötietojen minimoiminen
- Vastuiden eriyttäminen
- Säännöllinen valvonta
- Lokien systemaattinen käyttö ja seuranta
- Lokienhallinnan keskittäminen
- Säilytysaikojen noudattaminen

Lokitietoja ei saa käyttää työntekijöiden työskentelyn yleiseen valvontaan vaan niiden käytölle tulee aina löytyä edellä mainittujen käyttötarkoitusten mukaiset perusteet.

Sähköisten viestien ja välitystietojen (viestintälokit) käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

3. Lokienhallinnan organisointi ja vastuut

Tietohallintojohtaja vastaa hyvinvointialueen lokipolitiikasta. Tietoturva- ja tietosuojaryhmä toimii Tietohallintojohtajan apuna lokipolitiikan kehityksessä ja seurannassa.

Käytönvalvonnan lokien käytännön toteutuksesta päättää Tietoturva- ja tietosuojaryhmä.

Jokainen lokienhallinnan kanssa työskentelevä palvelussuhteesta riippumatta on vastuussa omasta työstään ja lokipolitiikan toimeenpanosta annetun ohjeistuksen mukaisesti. Vianselvitys-, palvelutaso-, tietoturvallisuus- ja viestintälokien käsittely tulee perustua edellisessä luvussa kuvattuihin käyttötarkoituksiin oman työtehtävään liittyen. Tarvittaessa lokienkäsittelystä päättää Tietoturva- ja tietosuojaryhmä.

Kymenlaakson hyvinvointialueelle palveluita tuottavien organisaatioiden henkilöstö pitää sopimusteknisesti velvoittaa noudattamaan hyvinvointialueen lokipolitiikkaa.

4. Lokienhallinnan toteuttaminen

Kaikki SOTE ja muiden henkilötietojen käytönvalvonnan lokitus keskitetään lokienhallintajärjestelmään. Käytönvalvonnan lokien osalta tulee ottaa huomioon keskitetyn lokienvalvontajärjestelmän vaatimukset lokiformaateille. Käytönvalvonnan lokien seuranta tulee olla aktiivista ja siinä voidaan tukeutua mm. automaattihälytyksiin.

Järjestelmähankintojen yhteydessä määritellään hankittavan tai kehitettävän tietojärjestelmän toiminnalliset ja muut vaatimukset. Tässä yhteydessä tulee määritellä myös loki- ja tietoturvavaatimukset, jotka ovat yhtä olennainen osa laadukasta ja toimivaa tietojärjestelmää kuin muutkin vaatimukset.

Lokienhallinnan käytännön toteutuksissa noudatetaan viranomaisohjeistusta. A-luokan tietojärjestelmissä noudatetaan THL:n toiminnallisia ja tietoturvavaatimuksia. Muissa tietojärjestelmähankkeissa voidaan noudattaa esimerkiksi Kyberturvallisuuskeskuksen sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimuksia. Pelastuslaitoksen tietojärjestelmähankkeissa lokienhallinnan käytännön toteutuksissa noudatetaan julkisen hallinnon turvallisuusverkoille kohdistettuja tietoturvavaatimuksia.

Lokien säilytyksen tietoturvavaatimukset ovat vähintään samantasoiset kuin kohdejärjestelmän. Mikäli suuri määrä lokitietoja kohdistetaan samaan paikkaan, on syytä noudattaa korotetun tason tietoturvavaatimuksia. Lokitiedon eheys ja muuttumattomuus tulee turvata.

Lokienhallinnan työtehtäviä suunnitellessa on vältettävä vaarallisten työyhdistelmien syntyä eli esimerkiksi henkilö ei voi käsitellä ja poistaa omia lokitietojaan.

Lokien yleinen sisältö koostuu seuraavista merkinnöistä:

- aikaleima
- tapahtuma
- toimija
- käyttöoikeus
- tapahtuman lähde
- tapahtuman tietoturvamerkitys

Lokien muodostamisessa tulee mahdollisuuksien mukaan hyödyntää järjestelmien oletus (default) lokeja. Mikäli lokiformaatti määritellään erikseen, tulee suosia yleisiä rakenteisia formaatteja.

Lokitietoihin on vältettävä tallentamasta:

- henkilötunnuksia
- EU:n tietosuoja-asetuksen tarkoittamia erityisiä henkilötietoja
- luottokorttinumeroita
- salasanoja tai salasanojen tiivisteitä
- järjestelmien välisiä käyttöavaimia ja salaisuuksia
- valtuutustietoja
- henkilöiden välisen viestiliikenteen sisältöä

Henkilötiedot tekevät lokista henkilötietorekisterin.

Lokien säilytysajat ja säilytykseen liittyvät vaatimukset vaihtelevat käyttötarkoituksen mukaan. Sosiaali- ja terveydenhuollon käytönvalvontalokien säilytysaika on 12 vuotta ja muiden henkilötietojärjestelmien käytönvalvontalokien 10 vuotta.

Tietoturva-, välitystieto-, vianselvitys- tai palvelutason seurannan lokien säilytysaika vaihtelee suojattavan kohteen mukaan, yleensä kuuden kuukauden ja 5 vuoden välillä.

Lokien säilytysaikoja päätettäessä tulee ottaa huomioon:

- Tietoaineiston alkuperäisen käyttötarkoituksen mukainen tarpeellisuus viranomaisen toiminnassa;
- Luonnollisen henkilön tai oikeushenkilön etujen, oikeuksien, velvollisuuksien ja oikeusturvan toteuttaminen ja todentaminen;

- Sopimuksen tai muun yksityisoikeudellisen oikeustoimen oikeusvaikutus;
- Vahingonkorvausoikeudelliset vanhentumisajat; ja
- Rikosoikeudelliset vanhentumisajat.

Keskitetyn lokienhallinnan piirissä olevat lokit on säilytysajan päättymisen jälkeen tuhottava viipymättä tietoturvallisella tavalla.

5. Lisätietoja

Lisätietoja ja käytännön ohjeistusta löydät:

- helppi24
- Kymenlaakson hyvinvointialueen tietohallinto
- THL:n Olennaiset toiminnalliset ja tietoturvavaatimukset
- Kyberturvallisuuskeskuksen Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset
- Kyberturvallisuuskeskuksen ohje Näin kerää ja käytät lokitietoja
- Tiedonhallintalautakunta: Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta
- Vahti Lokiohje
- Laki julkisen hallinnon tiedonhallinnasta/suosituskortti 17 § lokitietojen kerääminen

6. Versio ja päivityshistoria

Muutoshistoria			
Versio	**Päivä**	**Tekijä**	**Kuvaus**
0.1	28.11.2022	Kymenlaakson hyvinvointialueen asiantuntijat ja Huld Oy	Ensimmäinen versio
0.2	29.11.2022	Kymenlaakson hyvinvointialueen asiantuntijat ja Huld Oy	Kommenttien perusteella täydennetty versio
0.3	7.12.2022	Kymenlaakson hyvinvointialueen asiantuntijat ja Huld Oy	Viimeistelty versio hyväksyttäväksi

1.0	01-02/2023	Aluehallitus/YT toimikunta	Hyväksytty