vesilahti

Vesilahden kunnan lokipolitiikka

Kunnanhallitus xx.xx.2022

Sisällysluettelo

1. Johdanto 2

2. Lokitietojen hallinnan vaatimukset 3

3. Lokienhallinta Vesilahden kunnassa 3

3.1 Lokienhallinnan periaatteet 3

3.1.1 Lokitiedon määritelmä ja tarkoitus 4

3.1.2 Lokitietojen käytön perusteet 4

3.2 Lokienhallinnan toteuttaminen 6

3.2.1 Lokitietojen kerääminen ja lokien sisältö 6

3.2.2 Lokien säilytys 7

3.3 Lokienhallinnan organisointi ja vastuut 8

3.3.1 Käytönvalvonnan roolit 8

3.3.2 Käytönvalvonta 9

3.3.3 Käytönvalvonnan kulku 11

4. Raportointi 12

1. Johdanto

Tässä lokipolitiikassa määritellään Vesilahden kunnan periaatteet, vastuut ja toimintatavat lokitietojen keräämiselle ja käsittelylle. Lokipolitiikka on hyväksytty Vesilahden kunnan kunnanhallituksessa. Lokipolitiikan asiakirjaa ylläpitää kunnan tietosuojavastaava.

2. Lokitietojen hallinnan vaatimukset

Lokitietojen hallinnasta säädetään lainsäädännössä laajasti, mm.

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuojalaki (1050/2018)
- Rikoslaki (297/2003)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (94/2022)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki sosiaalihuollon asiakasasiakirjoista (254/2015)
- Laki sosiaalihuollon asiakasasiakirjoista annetun lain muuttamisesta (785/2021)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Laki sähköisen viestinnän palveluista (917/2014)

Lisäksi tietosuojavaltuutettu, Terveyden ja hyvinvoinnin laitos, Valvira ja Kyberturvallisuuskeskus ovat antaneet aiheeseen liittyviä ohjeita, jotka on lainsäädännön lisäksi otettu huomioon tätä lokipolitiikkaa laadittaessa.

3. Lokienhallinta Vesilahden kunnassa

3.1 Lokienhallinnan periaatteet

3.1.1 Lokitiedon määritelmä ja tarkoitus

Lokitietoihin kertyy tapahtumista ja muutoksista tietoa, jolla on mahdollista selvittää, mitä, miksi ja milloin tapahtui. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöistä kirjataan lokiin. Lokien hallinnalla ja lokitiedon käsittelyllä tarkoitetaan lokitiedon keräämistä, säilyttämistä, katselua, analysointia, seurantaa, luovutusta, tuhoamista ja raportointia.

Lokienhallinnan tarkoitus on pystyä todentamaan tapahtuman kulku, osapuolet, kiistämättömyys, mahdolliset tunkeutumisyritykset, poikkeamat, häiriöt ja suorituskykyongelmat. Lokitietojen perusteella pyritään varmistamaan käyttäjien ja rekisteröityjen oikeusturva.

3.1.2 Lokitietojen käytön perusteet

Lokitietoja ei saa käyttää työntekijöiden työskentelyn yleiseen valvontaan, vaan niiden käytölle tulee aina löytyä peruste. Nämä tulee ottaa huomioon tietojärjestelmien lokienhallintakyvykkyyksiä selvitettäessä. Vesilahden kunnassa lokeja voidaan kerätä esimerkiksi seuraaviin tarkoituksiin:

Loki	**Lokin sisältö**	**Käyttötarkoitus**
Pääsynvalvonta	Käyttäjään liittyviä tietoja, onnistuneet ja epäonnistuneet yritykset käyttää järjestelmää tai tietoja.	Järjestelmän käytön ja turvallisuuden valvonta, jäljitettävyys, osoitusvelvollisuus.

Käyttö- ja muutosloki	Käytön kohteeseen liittyvät tiedot, käyttäjän tiedot.	Käytönvalvonta, jäljitettävyys, osoitusvelvollisuus.
Virhe- ja varoitusloki	Järjestelmässä, sovelluksessa tai tapahtumassa havaittujen virheiden tiedot.	Toimintahäiriöiden ja virheiden havaitseminen ja korjaus.
Viestintäloki	Viestinvälitykseen liittyvät tiedot, esim. käyttäjän nimi tai muu tunnus, aikaleima, päätelaitteen tiedot, sijaintitieto.	Viestintäjärjestelmän vikatilanteiden selvittäminen, tietoturvapoikkeamatilanteen hallinta, viestintätapahtuman toteen näyttäminen.
Tietoturvaloki	Tietoverkkojen ja tietojärjestelmien tietoturvaan liittyvä tapahtuma.	Tunkeutumisten ja poikkeamatilanteiden havaitseminen.
Järjestelmäloki	Käyttöjärjestelmän tai palvelimen sisäiset tapahtumat, niihin liittyvät prosessit ja virheet.	Tietojärjestelmien ja palvelinten valvonta ja ylläpito, virheiden havaitseminen ja korjaus.
Transaktioloki	Tietokantatapahtumien tiedot, kuten kirjoitus-, muutos-, poisto- ja lukuoperaatiot.	Tietokantamuutosten tekijän selvittäminen.
Ylläpitoloki	Esim. tallennettuihin lokitietoihin kohdistuvat toimenpiteet.	Oikeusturvan toteutuminen, jäljitettävyys, osoitusvelvollisuus.
Haltijaloki	Kenelle tietty laite, ohjelma, lisenssi, ip-osoite tai nettiosoite on ollut annettuna tiettynä ajankohtana.	Tieto voidaan yhdistää suoraan henkilöön tai organisaatioon tai järjestelmään.

Sovelluslokit	Tietoa sovelluksen sisäisistä prosesseista, niiden käynnistymisissä, toimenpiteissä ja virhetilanteissa.	Virhetilanteiden ja tietoturvapoikkeamien selvittäminen.
Verkon yhteyslokit (palvelutarjoaja)	Mm. reitittimet ja palomuurit keräävät tietoa, mistä osoitteesta on mennyt liikennettä mihin osoitteeseen. Korkeamman protokollatason lokista näkyy myös mihin tietoliikenneporttiin liikenne on kohdistunut.	Virhetilanteiden ja tietoturvapoikkeamien selvittäminen.

3.2 Lokienhallinnan toteuttaminen

Kunnan lokitietoja tuottavat tietojärjestelmät tulee tunnistaa. Uusia tietojärjestelmiä hankittaessa tulee määritellä lokienhallintaan tarvittavat kyvykkyydet.

3.2.1 Lokitietojen kerääminen ja lokien sisältö

Lokitietoja tuotetaan ja kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista. Kerättävän lokitiedon sisältö perustuu tarpeellisuusarviointiin. Lokitietojen tulee sisältää riittävän laajat tiedot lokin käyttötarkoitusta varten esim. seuraavista asioista:

- Lokitiedon aikaleima eli päivämäärä ja kellonaika
- Tapahtuman aikaleima eli päivämäärä ja kellonaika (lokitiedon ja tapahtuman aikaleima voivat joskus myös erota toisistaan)
- Tapahtuman tunniste
- Tietojärjestelmän (tai laitteen tai sovelluksen) tunnistetiedot
- Tapahtuman kohdetta kuvaavat tiedot

- Käyttäjän (ihmis- tai laitekäyttäjän) tunnistetiedot
- Millä oikeuksilla ja valtuuksilla tapahtuma tehtiin
- Mitä tapahtui ja onnistuiko tapahtuma
- Tapahtuman tyyppi, kuten laatiminen, muuttaminen, kirjautuminen tai järjestelmän kaatuminen
- Tapahtuman tila (onnistuiko vai epäonnistuiko tapahtuma ja miksi se mahdollisesti epäonnistui)
- Tapahtuman merkitys tai prioriteetti
- Tapahtuman kuvaus

Seuraavien tietojen tallentamista lokitietoihin on vältettävä:

- Henkilötunnus
- EU:n tietosuoja-asetuksen tarkoittamat erityiset henkilötiedot
- Luottokorttinumerot
- Salasanat tai niiden tiivisteet
- Järjestelmien väliset käyttöavaimet
- Valtuutustiedot
- Henkilöiden välisen viestiliikenteen sisältö

Lokitietoja saavat käsitellä vain ne henkilöt, joiden työtehtäviin se kuuluu. Tämän vuoksi lokirekistereihin pääsy on rajoitettu vain tietyille henkilöille. Lokitietojen valvontaa suorittavilla henkilöillä on oikeus ja velvollisuus käyttää lokirekisteriin kertyviä tietoja suorittaessaan henkilötietojen käsittelyyn liittyvää valvontaa (tiedon käyttöä).

3.2.2 Lokien säilytys

Lokitiedot ovat todisteena jostakin tapahtumasta, jolloin on tärkeää huomioida, että lokitietoja ei saa oikeudettomasti käsitellä, tuhota tai muuttaa niiden sisältöä. Periaatteena on, että olemassa olevia tietojärjestelmien lokimerkintöjä ei pidä koskaan pystyä muuttamaan, vaan

virheellisen merkinnän korjaamisesta pitää syntyä uusi lokimerkintä. Säilytysvaatimukset (säilytysaika ja paikka), lokitietojen eheys ja muuttumattomuus tulee taata.

Lokien säilytysajat

- Virhe- ja varoitusloki säilytetään vianselvitykseen tarvittavan ajan
- Viestintäloki 10 vuotta
- Tietoturvaloki 10 vuotta
- Järjestelmäloki 3 kk
- Pääsynvalvontaloki 10 vuotta
- Käyttö/muutosloki sote 12 vuotta
- Käyttö/muutosloki muut 5 vuotta
- Transaktioloki 3 kk
- Ylläpitoloki 5 vuotta

Lokien tuhoaminen säilytysajan päätyttyä

Tietosuoja-asetuksen mukaan henkilötiedot tulee hävittää sen jälkeen, kun tiedot eivät ole rekisterinpitäjän kannalta enää tarpeellisia. Rekisterinpitäjän tarve lokirekisteritietojen säilyttämiseen kestää niin kauan kuin suojattavalla on mahdollisuus esittää oikeudellisia vaatimuksia luvattomien henkilötietojen käsittelyn johdosta. Vaatimukset ovat rikos- ja/tai vahingonkorvausoikeudellisia. Lokitietojen tuhoamisen käytännöt tulee selvittää ja sopia ohjelmistotarjoajan kanssa.

3.3 Lokienhallinnan organisointi ja vastuut

3.3.1 Käytönvalvonnan roolit

Rekisterinpitäjän rooli

Rekisterinpitäjän on huolehdittava, että tietosuojalainsäädännön mukaisia tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Henkilötietojen käsittelyssä noudatettavia periaatteita ovat käyttötarkoitussidonnaisuus, tietojen minimointi,

täsmällisyys, säilytyksen rajoittaminen, lainmukaisuus, kohtuullisuus, läpinäkyvyys, eheys ja luottamuksellisuus sekä sisäänrakennettu tietosuoja.

Käyttäjän rooli

Käyttäjän näkökulmasta kyse on työtehtäviä varten annettujen käyttöoikeuksien jälkikäteisvalvonnasta. Lokivalvonta on käyttäjän oikeusturva. Käyttäjä on vastuussa siitä, että on noudattanut tietosuoja-asetuksessa annettuja velvoitteita ja tietosuojaan liittyviä ohjeita.

Esihenkilön rooli

Esihenkilöt osallistuvat lokitietojen tulkintaan ja arviointiin. Esihenkilöt voivat tehdä valvontapyyntöjä työntekijöistä, osallistua kuulemistilaisuuteen ja antaa huomautuksen tai varoituksen tarvittaessa.

Tietosuojavastaavan rooli

Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän asiantuntijana. Tietosuojavastaava osallistuu suunnitteluun, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutusten toteutukseen. Tietosuojavastaavalla on myös velvollisuutena toimia ohjauksessa ja neuvonnassa asiakkaan suuntaan.

3.3.2 Käytönvalvonta

Työsuhteen alkaessa jokainen työntekijä hyväksyy Tampereen seudun tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen ja tekee tietosuojan verkkotentit.

Valvonta tapahtuu seuraavista lähtökohdista:

- Asiakaslähtöinen eli asiakas tekee valvontapyynnön
- Viranomaislähtöinen
- Esihenkilö tai organisaation työntekijä tekee valvontapyynnön

- Satunnaisvalvonta.

Asiakkaalla on oikeus saada kirjallisesta pyynnöstä lokirekisterin perusteella maksutta tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja, ja mikä on ollut käytön tai luovutuksen peruste. Prosessissa:

1) Tietopyyntö osoitetaan kirjaamoon
2) Kirjaamo välittää tietopyynnön tietosuojavastaavalle
3) Tietosuojavastaavalla ja tietojärjestelmän pääkäyttäjällä on oikeus pyytää ohjelmiston tarjoajalta tarvittava lokitieto ja tehdä tarvittava lokitiedon tulkinta ja arviointi
4) Mahdollisesta jatkoselvittelystä ja toimenpiteistä vastaa tietosuojavastaava
5) Asiakkaalta voidaan vaatia lisäselvitystä
6) Informointi.

Asiakkaalla ei ole oikeutta saada lokitietoja, jos lokitietojen antamisesta saattaisi aiheutua vakavaa vaaraa asiakkaan terveydelle tai hoidolle tai jonkun muun oikeuksille. Kielteisestä päätöksestä on tehtävä kirjallinen päätös. Asiakkaalla on oikeus saada vain pyyntöä edeltävien kahden vuoden aikana kertyneet lokitiedot. Pidemmältä ajalta saa lokitiedot vain, jos siihen on jokin erityinen syy.

Tietojärjestelmien tietojen käsittelyn jälkikäteisvalvonta tapahtuu pääasiassa lokitietojen perusteella. Valvonnassa tarkastetaan näkymien (asiakirjojen) avaukset, katselut, tallennukset ja ajankohta. Valvonnassa seurataan epätavallisena ajankohtana tehtyjä tietojen käsittelyjä. Lokitietoja voidaan verrata esim. vastaaviin työaikatietoihin ja asiointitietoihin.

Selvityspyyntöön perustuva valvonta

Kun rekisteröity, viranomainen tai muu henkilö tekee rekisterinpitäjälle käyttölokirekisterin selvityspyynnön rekisteriin tallennettujen tietojen käytöstä, käynnistyy selvitysprosessi tietosuojavastaavan toimesta yhteistyössä järjestelmän pääkäyttäjien ja toimittajan kanssa. Selvitystyön perusteella tietosuojavastaava antaa pyytäjälle kirjallisen selvityksen tietojen käytöstä ja käytön perusteista.

Jos selvityspyynnön esittää kansallinen rekisterinpitäjä, esim. Kela, tietosuojavastaava antaa kirjallisen selvityksen tietojen käsittelystä organisaation sisällä kyseisen rekisterin vastuuhenkilölle, joka laatii vastauksen.

Valvontasuunnitelma

Suunnitelman mukaan satunnaisotantavalvontaa toteutetaan säännöllisin välein.

- Valitaan lokitiedostoajon kohteeksi satunnaisotanta työntekijöistä ja tiettynä ajanjaksona tehdyt haut.
- Valitaan lokitiedostoajan kohteeksi satunnaisotanta asiakkaita. Tehdään pistokokeena.
- Valitaan lokitiedostoajon kohteeksi henkilöitä, joiden tiedetään olleen asiakassuhteessa organisaatioon ja joilla on korkeampi riski joutua rekisteritietojen luvattoman käytön kohteeksi.

Rekisteritietojen kyselyn yhteydessä tehdään aina organisaatiossa selvitys pyynnön kohteena olevista tiedoista. Tarvittaviin toimenpiteisiin ryhdytään, jos joku työntekijä on lainvastaisesti katsonut, käyttänyt tai luovuttanut henkilö-, asiakas- ja potilastietoja. Yksittäiset työntekijät vastaavat omasta toiminnastaan viime kädessä työ-, rikos- ja vahingonkorvausoikeudellisten sanktioiden uhalla. Mahdolliset väärinkäytösepäilyt selvitetään ennalta määriteltyjä menettelytapoja noudattaen ja rangaistaan yhdenmukaisesti (katso liite 1). Lokivalvonnan lisäksi valvotaan henkilökunnan käyttöoikeuksia.

3.3.3 Käytönvalvonnan kulku

Vaiheet

- lokien tarkastaminen ja tulkinta
- selvityksen pyytäminen työntekijältä
- selvityksen antaminen tietosuojavastaavalle
- asian selvittäminen ja kuuleminen

- asiasta päättäminen
- vastauksen antaminen.

4. Raportointi

Tietosuojavastaava raportoi henkilötietojen valvonnasta. Tietotilinpäätöksellä raportoidaan edeltävänä vuonna suoritetusta henkilötietojen käytön valvonnasta ja mahdollisista epäkohdista tietosuojassa. Tietosuojavastaavat raportoivat valvontaviranomaisille tietosuojan väärinkäytösepäilyissä. Lokiseurantaan liittyvät asiakirjat säilytetään 12 vuotta. Raporttien ja selvitysten säilyttämisestä vastaa tietosuojavastaava tiedonohjaussuunnitelman mukaisesti.

Liite 1. Sisäisen käyttölokivalvonnan prosessi ja käyttölokin selvitys pyydettäessä