YLÖJÄRVI

Ylöjärven kaupungin lokipolitiikka

YLÖJÄRVI

Sisällysluettelo

Sisällys

Johdanto

Tässä lokipolitiikassa määritellään Ylöjärven kaupungin periaatteet, vastuut ja toimintatavat lokitietojen keräämiselle ja käsittelylle. Lokipolitiikka on käsitelty / käsitellään kaupungin johtoryhmässä, yhteistoimintamenettelyssä kaupungin yhteistoimintaryhmässä ja hyväksytään kaupunginhallituksen päätöksellä. Asiakirjaa on työstetty yhteistyössä Tampereen kaupunkiseudun muiden kehyskuntien kanssa. Asiakirjaa päivitetään tarpeen mukaan. Lokipolitiikkaa sovelletaan kaupungin käytössä oleviin sovelluksiin ja tietojärjestelmiin, joissa käsitellään kaupungin rekisteripidon alaista tietoa.

1 Lokitietojen hallinnan vaatimukset

Lokitietoihin liittyvistä asioista säädetään lainsäädännössä muun muassa seuraavissa laeissa:

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuojalaki (1050/2018)
- Rikoslaki (297/2003)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Laki sähköisen viestinnän palveluista (917/2014)

Yksityisyyden suojasta työelämässä annetun lain 21 §:n mukaisesti työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnassa ja hyvinvointialueella annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin.

Tietojärjestelmien tuottamien lokitietojen käyttöön voi liittyä asiasta ja tilanteesta riippuen valvonnallisia piirteitä (esim. satunnaisotanta tietojärjestelmän lokitiedoista taikka useista kirjautumisyrityksistä tuleva ilmoitus).

Tiedonhallintalain 17 §:n mukaisesti “viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.”

2 Lokienhallinta Ylöjärven kaupungissa

2.1. Lokienhallinnan periaatteet

2.1.1. Lokitiedon määritelmä ja tarkoitus

Lokeihin tallentuvia kirjauksia voivat olla esimerkiksi tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä. Lokitietoihin kertyy tapahtumista ja muutoksista tietoa, joiden avulla on mahdollista selvittää, mitä tapahtui, miksi ja milloin. Lokien hallinnalla ja lokitiedon käsittelyllä tarkoitetaan lokitiedon keräämistä, säilyttämistä, katselua, analysointia, seurantaa, luovutusta, tuhoamista ja raportointia.

Lokitietojen käyttötarkoituksena on ennen kaikkea tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen perusteella pyritään varmistamaan käyttäjien, rekisteröityjen ja ylläpitäjien oikeusturvan toteutuminen. Lokia voidaan käyttää myös tilastotarkoitusta varten esimerkiksi tiedonluovutusten seurantaan ja teknisten ongelmien selvittämiseen.

2.1.2 Lokitietojen käytön perusteet

Lokitietoja ei käytetä työntekijöiden työskentelyn yleiseen valvontaan. 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	Tieto voidaan yhdistää suoraan henkilöön tai organisaatioon tai järjestelmään.

	on ollut annettuna tiettynä ajankohtana.	
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

2.2. Lokienhallinnan toteuttaminen

2.2.1. Lokitietojen kerääminen ja lokien sisältö

Lokitietoja tuotetaan ja kerätään ennen kaikkea tietojärjestelmän käytöstä ja tietojen luovutuksista. Lokitietojen tulee sisältää riittävän laajat tiedot lokin käyttötarkoitusta varten mahdollisuuksien mukaan seuraavista asioista:

- Lokitiedon aikaleima eli päivämäärä ja kellonaika
- Tapahtuman aikaleima 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 (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
- Järjestelmien väliset käyttöavaimet
- Valtuutustiedot
- Henkilöiden välisen viestiliikenteen sisältö

Lokitietoja käsittelevät vain ne henkilöt, joiden työ- tai virkatehtäviin asia kuuluu. Tämän vuoksi lokirekistereihin on hyvin rajoitettu pääsy.

2.2.2. Lokien säilytys

Lokitiedot ovat dokumentointi jostakin tapahtumasta. 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 tulee syntyä uusi lokimerkintä.

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 luvattoman henkilötietojen käsittelyn johdosta. Lokitietojen arkistoinnin ja tuhoamisen käytännöt tulee selvittää ja sopia järjestelmätoimittajan kanssa.

2.3. Lokienhallinnan organisointi ja vastuut

2.3.1. Toimijat lokipolitiikan noudattamisessa

Lokipolitiikan noudattamisesta vastaavat osaltaan kaikki kaupungin osastot ja toimijat tehtäviensä mukaisesti. Rekisterinpitäjän, esihenkilön, käyttäjän, pääkäyttäjän, tietoturvavastaavan ja tietosuojavastaavan rooleja lokipolitiikan toteuttamisessa voidaan hahmottaa seuraavasti:

Rekisterinpitäjä

Rekisterinpitäjän tulee huolehtia siitä, että tietosuojalainsäädännön mukaisia tietosuojaperiaatteita noudatetaan henkilötietojen käsittelyvaiheissa. Henkilötietojen käsittelyssä noudatettavia periaatteita ovat mm. käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, lainmukaisuus, kohtuullisuus, läpinäkyvyys, eheys ja luottamuksellisuus sekä sisäänrakennettu tietosuoja.

Esihenkilö

Esihenkilö osallistuu tarvittaessa lokitietojen tulkintaan ja arviointiin.

Esihenkilön velvollisuutena on selvittää ja huolehtia selvittämisestä, mikäli esimerkiksi heräisi kysymys henkilötietojen käsittelyn liittymisestä työntekijän / viranhaltijan työtehtäviin. Esihenkilö tekee tarvittaessa läpikäyntipyynnön sekä tilanteen sitä edellyttäessä muiden toimenpiteiden toteuttamisesta. Esihenkilöiden tehtävänä on myös valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita ja että tietojärjestelmiin on kulloiseenkin työnkuvaan kuuluvat käyttöoikeudet ja tarpeettomat oikeudet poistetaan tai käyttöoikeus päätetään.

Käyttäjä

Käyttäjä on vastuussa siitä, että hän noudattaa työnantajan tietosuojaan ja tietojärjestelmien käyttöön liittyviä ohjeita. Kaupungin jokainen työntekijä ja viranhaltija on allekirjoittanut tietojen ja

tietojärjestelmien käyttö- ja salassapitositoumuksen, jossa henkilö on muun ohella sitoutunut käsittelemään vain työtehtäviensä edellyttämiä tietoja ja sitoutunut olemaan käsittelemättä ”esim. omia, työtovereideni, lähiomaisteni tai julkisuuden henkilön tietoja, mikäli työtehtäväni eivät sitä edellytä”.

Pääkäyttäjä

Tietojärjestelmän pääkäyttäjä on keskeinen toimija lokipolitiikan käytönvalvonnan toteutumisessa ja esimerkiksi käyttöoikeushallinnan ylläpitämisessä.

Tietoturvavastaava

Tietoturvavastaava toimii rekisterinpitäjän asiantuntijana omalta osaltaan mm. osallistuen toiminnan suunnitteluun, ohjeiden valmisteluun ja ylläpitoon sekä aihepiirin koulutusten toteutukseen. Tietoturvavastaava osallistuu osaltaan yksittäisen tapauksen selvittämiseen asian edellyttämässä laajuudessa.

Tietosuojavastaava

Tietosuojavastaava toimii rekisterinpitäjän asiantuntijana. Tietosuojavastaava osallistuu suunnitteluun, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutusten toteutukseen. Tietosuojavastaava osallistuu osaltaan yksittäisen tapauksen selvittämiseen asian edellyttämässä laajuudessa.

2.3.2. Käytönseuranta

Tietojärjestelmien tietojen käsittelyn jälkikäteisseuranta tapahtuu pääasiassa lokitietojen perusteella. Seurantaa ja muita toimenpiteitä voidaan toteuttaa satunnaisotantana tai esimerkiksi saadun ilmoituksen tai havainnon perusteella.

Tarvittaviin lisätoimenpiteisiin ryhdytään, mikäli ilmenisi viitteitä esimerkiksi oikeuksien vastaisesta tietojen katselusta, tietojen käyttöä tai tietojen luovutusta. Esihenkilö ja rekisteristä vastaavat tahot käyvät lokitiedot läpi tietosuojavastaavaa ja tietoturvavastaavaa tarpeen mukaan konsultoiden. Mikäli rekisteritietojen käsittelyssä havaitaan tietosuojapoikkeama, joka edellyttää viranomaisilmoituksia, laaditaan asiasta tarvittavat viranomaisilmoitukset. Jos käytössä havaitaan väärinkäytös, käynnistetään asiassa tilanteen edellyttämät toimenpiteet. Myös käyttöoikeuksia voidaan tapauskohtaisesti rajoittaa tai ne voidaan sulkea selvitystyön ajaksi.

Lokiseurantaan liittyvät asiakirjat säilytetään tiedonohjaussuunnitelman mukaisesti.