

Lokipolitiikka

Paimion Kaupunki

Sisällysluettelo

1. Johdanto	2
2. Soveltamisala	2
3. Lainsäädännöllinen ja normatiivinen viitekehys	2
4. Lokituksen käyttötarkoitus ja tavoitteet.....	2
5. Lokitettavat tapahtumat	3
6. Lokitietojen sisältö	3
7. Lokituksen tietosuojaperiaatteet.....	3
8. Lokitietojen säilytys ja elinkaaren hallinta	3
9. Lokitietojen suojaaminen	3
10. Lokien seuranta ja valvonta	4
11. Lokitietojen käyttö ja luovutus.....	4
12. Tietoturvaloukkaukset ja poikkeamat	4
13. Vastuut ja roolit.....	4
14. Koulutus ja ohjeistus	4
15. Poliitiikan ylläpito ja muutokset.....	4

1. Johdanto

Tämän lokipolitiikan tarkoituksena on määritellä Paimion kaupungin periaatteet, vaatimukset sekä toimintatavat tietojärjestelmien ja teknisten ympäristöjen lokitukselle. Poliitiikan tavoitteena on varmistaa henkilötietojen ja muiden tietovarantojen lainmukainen, turvallinen ja jäljitettävä käsittely sekä täyttää tiedonhallintalain (906/2019) ja EU:n yleisen tietosuoja-asetuksen (EU 2016/679) vaatimukset.

Lokitus on keskeinen osa kaupungin tietoturvaa, tietosuojaa ja sisäistä valvontaa. Poliitiikka täydentää Paimion kaupungin tietoturva- ja tietosuojaperiaatteita (= tietoturva- ja tietosuojapolitiikka).

2. Soveltamisala

Tätä politiikkaa sovelletaan kaikkiin Paimion kaupungin tietojärjestelmiin ja sovelluksiin, palvelin- ja pilviympäristöihin, työasemiin ja päätelaitteisiin siltä osin kuin ne käsittelevät kaupungin tietoja sekä integraatioihin ja tietoliikenneyhteyksiin.

Poliitiikka koskee kaupungin henkilöstöä, luottamushenkilöitä sekä palveluntuottajia ja toimittajia siltä osin kuin ne käsittelevät kaupungin tietoja.

3. Lainsäädännöllinen ja normatiivinen viitekehys

Lokitus perustuu erityisesti seuraaviin säädöksiin ja ohjeisiin:

- Tiedonhallintalaki (906/2019)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Julkisuuslaki (621/1999)
- Mahdollinen erityislainsäädäntö (esim. sosiaali- ja terveydenhuolto, varhaiskasvatus ja perusopetus)
- ISO/IEC 27001 ja 27002
- VAHTI-ohjeistukset

4. Lokituksen käyttötarkoitus ja tavoitteet

Lokitus tarkoittaa lokitietojen tallennusta ja hyödyntämistä. Lokitietoa tarvitaan selvittämään mitä, miksi ja milloin jotakin tapahtui. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta.

Lokituksen tavoitteena on:

- varmistaa tietojen käsittelyn lainmukaisuus ja jäljitettävyys
- tukea tietoturvan ja tietosuojan toteutumista
- mahdollistaa väärinkäytösten, virheiden ja poikkeamien havaitseminen
- tukea tietoturvaloukkausten selvittämistä ja raportointia
- edesauttaa järjestelmän ylläpitäjien ja käyttäjien oikeusturvan toteutumista
- täyttää rekisterinpitäjän osoitusvelvollisuus

5. Lokitettavat tapahtumat

Lokitettavia tapahtumia ovat järjestelmien niin mahdollistaessa vähintään:

- käyttäjien tunnistautumiset ja kirjautumiset
- käyttöoikeuksien myöntäminen, muuttaminen ja poistaminen
- henkilötietojen katselu, muokkaus ja poistaminen
- tietojen luovutukset ja siirrot
- järjestelmien keskeiset hallinnolliset ja ylläpidolliset toimenpiteet
- järjestelmän normaalin käytön estävät virhe- ja poikkeamatilanteet
- tietoturvaa- tai tietosuojaa uhkaavat tapahtumat

6. Lokitietojen sisältö

Lokitietojen tulee sisältää järjestelmien niin mahdollistaessa vähintään:

- käyttäjän yksilöivä tunniste
- aikaleima
- suoritettu toimenpide
- kohdejärjestelmä tai tietovaranto
- tarvittaessa tekniset lisätiedot (esim. IP-osoite)

7. Lokituksen tietosuojaperiaatteet

Lokituksessa noudatetaan EU:n yleisen tietosuojasetuksen (EU 2016/679) periaatteita:

- käyttötarkoitussidonnaisuus
- tietojen minimointi
- luottamuksellisuus ja eheys
- henkilöstön yksityisyyden suoja

Lokitietoja ei käytetä työntekijöiden jatkuvaan tai perusteettomaan seurantaan.

8. Lokitietojen säilytys ja elinkaaren hallinta

Lokitietojen säilytysajat määritellään käyttötarkoituksen ja lainsäädännön perusteella. Tarpeettomat lokitiedot poistetaan järjestelmän niin salliessa automaattisesti.

9. Lokitietojen suojaaminen

Lokitiedot suojataan asianmukaisilla teknisillä ja hallinnollisilla toimenpiteillä:

- käyttöoikeuksien rajaaminen
 - lokien eheydensuoja
 - salaus levossa ja siirrossa
 - lokien eriyttäminen tuotantodatan käsittelystä
- 
- A decorative graphic at the bottom of the page consisting of several overlapping, flowing blue waves of varying shades, extending across the width of the page.

10. Lokien seuranta ja valvonta

Lokitietoja seurataan säännöllisesti ohjeistuksia noudattaen ja siinä voidaan tukeutua automaattihälytyksiin. Seurannan voi myös käynnistää tietojärjestelmän rekisteristä vastaava, tietoaineistosta vastaava viranhaltija tai kaupungin tietosuojavastaava.

Poikkeamat käsitellään kaupungin tietoturvapoikkeamaprosessin mukaisesti.

11. Lokitietojen käyttö ja luovutus

Lokitietoja saavat käsitellä vain henkilöt, joille työtehtäviin liittyen on annettu oikeus lokin käyttöön. Lokitietojen käyttö dokumentoidaan. Luovutukset viranomaisille perustuvat lakiin.

12. Tietoturvaloukkaukset ja poikkeamat

Lokitus tukee tietoturvaloukkausten havaitsemista, selvittämistä ja raportointia. Lokitietoja käytetään osana loukkausten vaikutusten arviointia.

13. Vastuut ja roolit

Paimion kaupungin rekisterinpitäjiä ovat kaupunginhallitus sekä kunkin tehtävän tai toiminnan järjestämisestä vastaava lautakunta. Rekisterinpitäjälle kuuluvat vastuut on määritelty EU:n tietosuoja-asetuksessa 2016/679.

- Henkilötietojen käsittelyn lainmukaisuutta valvoo tietosuojavastaava.
- Lokituksen teknisestä toteutuksesta vastaa tietohallinto tarvittaessa järjestelmän pääkäyttäjää konsultoiden.
- Järjestelmäkohtaisista vaatimuksista vastaavat järjestelmätoimittajat.

14. Koulutus ja ohjeistus

Henkilöstölle järjestetään koulutusta tietosuojaan ja tietoturvaan liittyvistä velvoitteista.

Henkilöstöä informoidaan, että tietojärjestelmässä käynnit sekä järjestelmässä tehdyt tapahtumat kirjautuvat lokitietoihin ja käyttöä valvotaan.

15. Poliitiikan ylläpito ja muutokset

Tämä politiikka käsitellään kaupungin yhteistyöryhmässä ja hyväksytään kaupunginhallituksessa. Poliitiikka tarkistetaan säännöllisesti ja aina merkittävien muutosten yhteydessä.