KOUVOLA

# Lokipolitiikka

Kouvolan kaupunki

KOUVOLA

**Sisällysluettelo**

# 1 Johdanto

Mikäli tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista, lokitietojen kerääminen on lakiperusteista. Tiedonhallintalain 17 § edellyttää tällöin keräämään lokitietoja, joiden avulla seurataan tietojärjestelmässä olevien tietojen käyttöä, tietojen luovutusta ja selvitetään tietojärjestelmän teknisiä virheitä.

Tämä lokipolitiikka linjaa Kouvolan kaupungilla noudatettavat vastuut, periaatteet ja toimintatavat Kouvolan kaupungin palvelutuotannossa käyttämiensä järjestelmien ja palveluiden lokitietojen käsittelyssä ja keräämisessä sekä ohjaa lokitietojen käyttöä Kouvolan kaupungin tietosuojan ja tietoturvan toteutumisen varmistamiseksi.

Kouvolan kaupungin lokipolitiikan omistaa kaupunginhallitus. Lokipolitiikka dokumenttia ylläpitää Kouvolan kaupungin tietohallinto.

# 2 Ohjaavat vaatimukset

Lokipolitiikan lisäksi Kouvolan kaupungin digitaalisen turvallisuuden politiikka ja tietosuojapolitiikka ohjaavat lokien käsittelyä.

Lokipolitiikkaa laadittaessa on huomioitu seuraavat lait ja asetukset:

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

Lisäksi on otettu huomioon Tietosuojavaltuutetun ohjeistus, Vahti 2009, Valtiovarainministeriön suosituskokoelma 2020 ja Kyberturvallisuuskeskuksen aiheeseen liittyvä ohjeistus.

# 3 Lokipolitiikan soveltamisala

Tämä lokipolitiikka koskee koko kaupunkiorganisaatiota ja sen henkilöstöä. Myös Kouvolan kaupungille palveluita tuottavien organisaatioiden on sitouduttava noudattamaan Kouvolan kaupungin lokipolitiikkaa. Lokitietojen käsittelyä täsmennetään palvelutuottajien kanssa laadittavissa sopimuksissa.

Kouvolan kaupungilla lokipolitiikka liittyy tietoturvan, tietoturvan hallinnan ja prosessien toteuttamiseen. Lokien käsittelyä täsmennetään järjestelmäkohtaisissa ohjeistuksissa, Digiturvamalli-järjestelmän selosteissa sekä perehdyttämällä.

# 4 Lokienhallinnan tavoitteet ja periaatteet

Lokilla tarkoitetaan tiedostoa, johon tietojärjestelmän tapahtumat tallentuvat automaattisesti aikajärjestykseen. Lokitiedot voivat olla myös manuaalisesti kerättäviä merkintöjä (esimerkiksi vierailijaloki). Jokaiselle kerättävälle lokitiedolle on oltava peruste.

Lokitiedon käsittelyllä tarkoitetaan lokitiedon keräämistä, säilyttämistä, katselua, analysointia, seurantaa, luovutusta, tuhoamista ja raportointia. Lokienhallinnalla todennetaan tapahtuman kulku, osapuolet, lokitietojen kiistämättömyys, mahdolliset tunkeutumiset, poikkeamat ja järjestelmän toimivuus.

Lokien kerääminen ja käsittely perustuvat lakiin. Ennen tietojärjestelmän lokitiedon keräämisen aloittamista, on selvitettävä ja kuvattava lokitietojen keräämisen toteutus, käyttötapa sekä kerättävien ja käsiteltävien lokitietojen tarpeellisuus. Tietojärjestelmähankintojen suunnitteluvaiheessa tulee tunnistaa ja huomioida tietojen suojaaminen sekä tarve kerätä lokitietoja.

Lokien tuottamalla tiedolla edesautetaan myös järjestelmän ylläpitäjien ja käyttäjien oikeusturvan toteutumista. Kouvolan kaupungin henkilöstöä informoidaan oikeusturvasta sekä henkilöstöön kohdistuvista käsittelytoimenpiteistä YT-menettelyssä sekä kaupungin informointiasiakirjoissa.

Kouvolan kaupungilla lokitietojen käsittelyoikeudet ovat pääsääntöisesti järjestelmän omistajalla ja järjestelmän vastuuhenkilöllä/pääkäyttäjällä yhdessä (ks. kappale 5 Organisointi ja vastuut).

**Tiedonhallintalain mukaan on kerättävä vähintään seuraavia lokitietoja:**

- Virhe- ja varoituslokit
  - Tekninen loki, joka sisältää tietoja järjestelmässä havaituista virheistä ja varoituksista, joita hyödynnetään teknisissä korjaavissa toimenpiteissä.

- Käytönvalvonta- ja viestintälokit
  - Sisältää käytön kohteeseen liittyviä tietoja.
  - Saattaa sisältää henkilötietoja.
  - Lokista tyypillisesti ilmenee käyttäjän identifioiva tieto, sekä mitä toimia käyttäjä on kohdistanut käytön kohteen tietovarantoihin.
  - Kerättävät tiedot virheiden selvittelyyn, yksilön etujen, oikeuksien ja velvollisuuksien sekä oikeusturvan toteuttamiseksi tai virkavastuun todentamiseksi.

- Tiedon luovutuslokit
  - Sisältää tiedot henkilö- ja muiden tietojen luovutuksesta eri rekisterien tai rekisterinpitäjien välillä, esimerkiksi järjestelmien välisissä integraatioissa. Luovutuslokitiedoilla varmistetaan, että luovuttamiselle on ollut laillinen peruste.

- Muut lokityypit
  - Järjestelmistä voidaan tarvittaessa kerätä myös muita lokitietoja, joiden osalta tarpeellisuusarvio tehdään jokaisen järjestelmähankinnan kohdalla.

**Lokitietojen keräämisen tavoitteita ovat mm.:**

- hyvän tiedonhallintatavan varmistaminen
- tietojärjestelmien ylläpidon ja vianselvityksen helpottaminen
- tietoturvallisuuden valvonnan avustaminen
- asiakkaiden ja oman henkilökunnan oikeusturvan varmistaminen
- väärinkäytösten ja asiakasväittämien todentamisen helpottaminen

# 5 Organisointi ja vastuut

Lokitietojen käsittelyn tulee perustua työtehtäviin liittyviin tarpeisiin. Tämä edellyttää roolien ja vastuiden huolellista suunnittelua. Lokitietojen käsittelyssä on noudatettava erityistä huolellisuutta, ja jokainen lokienhallinnan kanssa työskentelevä on vastuussa omasta työstään ja lokipolitiikan toteutuksesta annetun ohjeistuksen mukaisesti.

Kouvolan kaupunginhallitus

- Hyväksyy lokipolitiikan.
- Kokonaisvastuu tietoturvasta on kaupunginhallituksella.
- Kaupunginhallituksen alaisuudessa toimivat viranomaiset ovat käsiteltävien tietovarantojen omistajia. Kaupunginhallitukselle kuuluu kaupungin toiminnan lakien, viranomaismääräysten ja lokipolitiikan mukaisten toimien toteuttamisen ja ylläpidon vaatimien taloudellisten sekä henkilöresurssien tarpeiden täyttäminen.

Järjestelmän omistaja

- Järjestelmien omistajia ovat kunnan viranomaiset, joille on annettu toimivalta ja velvollisuus tiettyjen tehtävien hoitamiseen omalla toimialallaan.
- Järjestelmien vastuuhenkilöitä ovat toiminnasta vastaavat viranhaltijat.
- Järjestelmien omistajat ja vastuuhenkilöt vastaavat lokien suunnittelusta, tarveperusteen määrittelemisestä, toteuttamisesta sekä näiden dokumentoinnista omistamiensa järjestelmien osalta, osana järjestelmän määrittely-, kehitys- ja hankintavaiheita.

Tietohallintojohtaja, tietoturvavastaava

- Vastaa kaupungin lokitietojen keräämisen tietoturvaedellytysten toteutumisesta ja vaatimustenmukaisuudesta.
- Vastaa lokipolitiikkaan liittyvien prosessien ja menettelytapojen toteuttamisen seuraamisesta, kehittämisestä ja ylläpitämisestä.
- Seuraa ja ohjeistaa lokien dokumentointi-, toteuttamis- ja kehittämistyötä.

Tietosuojavastaava

- Seuraa tietosuojaperiaatteiden toteutumista.
- Osallistuu henkilötietojen tietoturvapoikkeamien käsittelyyn.

Järjestelmän vastuuhenkilö/pääkäyttäjä

- Vastaa järjestelmän tuottaman lokin ohjeistuksen mukaisesta käsittelystä.

# 6 Lokienhallinnan toteuttaminen

Lokienhallinnan käytännön toteutuksissa noudatetaan viranomaisohjeistusta. Lokitiedon keräämisen vaatimukset määritellään järjestelmähankintojen yhteydessä, kuten muutkin toiminnalliset vaatimukset. Tietojärjestelmistä luodaan järjestelmä- ja lokikohtaisesti Digiturvamalli-järjestelmään seloste. Seloste sisältää yleisen kuvauksen tietojärjestelmästä, tietojärjestelmän keräämät erilaiset lokityypit, lokitietojen säilytyspaikan, säilytysajan, tiedon lokitietojen mahdollisesta luovuttamisesta järjestelmästä toiseen sekä käyttöoikeudet.

Huomioitavia lokiasioita tietojärjestelmän ylläpidossa ja hankinnassa:

- Lokilähteet, lokien käyttötarkoitus ja lokien säilytysaika.
    - Suunnitellaan lokien elinkaari, ml. lokitietojen tietoturvallinen hävittäminen.
    - Säilytysaika määräytyy käyttötarkoituksen mukaan.
- Lokitietojen luokittelu.
    - Lokitietojen käyttötarkoitus ohjaa säilytysaikaa ja muuta käsittelyä.
- Sisältävätkö lokit henkilötietoja.
    - Henkilötiedot muodostavat henkilörekisterin, jolloin tulee huolehtia rekisteröityjen informoinnista (tietosuojaseloste/informointiasiakirja). Informointiasiakirjassa tulee huomioida myös lokitiedot.
- Lokitiedon tallennuspaikka ja suojaus.
    - Lokitietojen tietoturvavaatimukset ovat vähintään samantasoiset kohdejärjestelmän kanssa.
    - Lokitiedon eheys ja muuttumattomuus on turvattava.
- Käyttöoikeudet lokitietoihin.
- Lokitapahtumien valvonta ja analysointi.
    - Tämä voidaan toteuttaa myös teknisesti.
    - Tiedonhallintalain 13 § edellyttää tietoturvallisuuden seurantaa.
- Lokitiedon käsittelyn perustelut ja määriteltyihin lokitapahtumiin reagointi.
- Huomioidaan vaatimuksenmukaisuus ja osoitusvelvollisuus.

**Lokitietojen säilytysaika**

Lokitietojen tarkat säilytysajat kirjataan järjestelmä- ja lokikohtaisesti Digiturvamalli-järjestelmään. Lokien säilytysajat ja säilytykseen liittyvät vaatimukset vaihtelevat käyttötarkoituksen mukaan. Sosiaali- ja terveydenhuollon käytönvalvontalokien säilytysaika on 12 vuotta ja muiden henkilötietojärjestelmien käytönvalvontalokien 10 vuotta. Virhe-, varoitus-, käytönvalvonta-, viestintä- ja tiedonluovutuslokien sekä muiden lokityyppien säilytysaika vaihtelee suojattavan kohteen mukaan, yleensä kuuden ja 24 kuukauden välillä.

**Lokitietojen luovuttaminen**

Lokitiedot ovat salassa pidettäviä, eikä kaupunki pääsääntöisesti luovuta niitä. Lokitietoja voidaan luovuttaa muille viranomaisille, mm. poliisille, mikäli kyseessä on tietoturvapoikkeamien tai rikosten selvittely. Muilla viranomaisilla voi sovittaessa olla yhteiskäyttöinen tunnus lokien lukemiseksi. Tarvittaessa lokitiedot otetaan tutkinnan ajaksi talteen erilliseen salattuun sijaintiin. Lokitietojen luovuttamisen hyväksyy tietovarannon omistaja tai vastuuhenkilö.

**Käyttökelpoisesta lokista ilmenevät vähintään seuraavat:**

- Aikaleima (milloin tapahtuma oli)
- Tapahtuma (mitä tehtiin tai yritettiin tehdä)
- Toimija (kuka teki)
- Käyttöoikeus (millä valtuuksilla tapahtuma tehtiin)
- Tapahtuman lähde (mistä muutostieto on peräisin)
- Tapahtuman kohde (mihin tietoon tai järjestelmään kohdistui)
- Tapahtuman tietoturvamerkitys (onnistui/epäonnistui, syy)

**Lokitietoihin on vältettävä tallentamasta:**

- Henkilötunnuksia
- Erityisiä henkilötietoja (ns. arkaluonteiset tiedot)
- Luottokorttinumeroita
- Salasanoja, ei edes tiivistemuotoisia
- Järjestelmien välisiä käyttöavaimia ja salaisuuksia
- Valtuutustietoja
- Henkilöiden välisen viestiliikenteen sisältöä
- Lähdekoodia
- Erityisen korkeaa turvallisuudentasoa edellyttäviä tietoja

**Poikkeamien käsittely**

Näistä periaatteista on mahdollista poiketa dokumentoidusti ja riskiarvion pohjalta. Poikkeamat hyväksyy lokipolitiikan omistaja.

# 7 Käsitteet

| | |
|---|---|
| Digiturvamalli-järjestelmä | Tiedonhallintalain mukainen tiedonhallintamalli. |
| Eheys | Toteutuu lokissa, kun kaikki alkuperäiset lokimerkinnät esiintyvät muuttumattomina täsmälleen kerran lokissa. |
| Erityiset henkilötiedot | Tarkoittaa arkaluonteisia tietoja, muun muassa ammattiliiton jäsenyys, terveystiedot, etninen alkuperä. |
| Henkilötieto | Kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. |
| Informointiasiakirja | Asiakirjan tarkoituksena on, että rekisteröity saa kattavan ja selkeän kuvan henkilötietojen käsittelyn kokonaisuudesta. |
| Integraatio | Tiedonsiirto eri järjestelmien välillä. |

| | |
|---|---|
| Kirjautuminen | Tunnistautuminen järjestelmään, voi tapahtua automaattisesti tai syöttämällä käyttäjätunnus ja salasana. |
| Loki | Rekisteri johon lokitiedot tallentuvat aikajärjestyksessä. |
| Lokilähde | Tietojärjestelmä, jossa kirjautuu tapahtumatietoja automaattisesti. |
| Lokitieto | Tietojärjestelmän muistiin automaattisesti kirjautuva tapahtumatieto. |
| Lähdekoodi | Ohjelmointikielellä toteutettu ohjelman täydellinen kuvaus tekstimuodossa. |
| Osoitusvelvollisuus | Rekisterinpitäjän on osoitettava noudattavansa tietosuojalainsäädäntöä. |
| Palvelu | Aineettoman hyödykkeen tuotanto asiakkaalle, esim. ICT-tuki. |
| Palveluntuottaja | Esim. yhtiö tai ammatinharjoittaja, joka tuottaa palvelua sopimuksen mukaan. |
| Prosessi | Ohjattujen toimintojen ketju. |
| Rekisterinpitäjä | Julkinen organisaatio tai organisaation yksikkö, jolla on lainsäädäntöön perustuva vastuu toiminnan tai palvelun järjestämisestä. |
| Tietojärjestelmä | Tiedoista, tiedonkäsittelijöistä, laitteistoista ja ohjelmistoista koostuva kokonaisuus. |
| Tietosuoja | Perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Henkilötietojen käsittely perustuu aina lain mukaiseen käsittelyperusteeseen. |
| Tietoturva | Tietoaineistojen ja tietojärjestelmien suojaaminen mm. organisatorisin ja teknisin toimenpitein. |
| Tietoturvapoikkeama | Odottamaton ja ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palveluiden tietoturvan ja vaikuttaa toimintaan epäsuotuisasti. |
| Tietovaranto | Tietoaineistoja sisältävä kokonaisuus, jota käsitellään tietojärjestelmien avulla tai manuaalisesti. |
| Vastuuhenkilö/pääkäyttäjä | Tietojärjestelmän käyttäjätunnus, jolla on järjestelmän ylläpito-oikeudet. |
| YT-menettely | Työnantajan ja työntekijöiden välinen menettely, jossa käsitellään työntekijän oikeuksiin ja velvollisuuksiin liittyviä kysymyksiä. Joissakin tilanteissa riittää myös pelkkä tiedottaminen työntekijöille. |

## Versiotiedot

| Versio | Kuvaus | Päivämäärä ja muutoksen tekijät | Muutoksen hyväksyjä |
|---|---|---|---|
| 0.1 | Ensimmäinen versio. | 31.3.2022 MK, HP-M, MP, JT, LL | |
| 0.2 | Muokattu: vastuunjakolistausta (roolit, tehtävät, vastuut), politiikan kohdennus tarkennettu Kouvolan kaupungin organisaation mukaiseksi. | 17.11.2022 MK, HP-M, MP, JT, LL, PL | |
| 0.3 | Dokumentin auditoinut Insta Advance Oy. | 9.12.2022 Petri Jurvanen, Jassi Saurio | |
| 0.4 | Auditointikommentit käsitelty. Muutokset kappaleissa 1, 2, 4, 5 ja 7. | 28.12.2022 MK, HP-M, MP, JT, LL | |