KOUVOLAN KAUPUNKI

KOUVOLAN LOKIEN KÄYTÖN SEURANTA JA VALVONTA

Versio	Pvm	Kuvaus	Laatija	Tarkastaja	Hyväksyjä
1.0	15.6.2011	Versio 1.0	Tietohallinto	Tietohallinnon or	Yt-työryhmä
1.0	26.3.2012	Hyväksytty toimintamalli	Tietohallinto	Yt-ryhmä	Kaupunginhallitus
1.1	9.8.2024	Dokumentin päivitys	Tietohallinto	Tiedonhallinnan ohry	Tiedonhallinnan ohry
1.1	8.10.2024	Dokumentin tekstin lakitekninen tarkastus ja korjaus	Tietohallinto	Kaupungin-lakimies	Konsernipalvelui-den johtoryhmä
1.1	11.11.2024 / 25.11.2024	Dokumentin läpikäynti Yhteistyöryhmässä / joryssä	Tietohallinto	Yhteistyöryhmä	Kaupungin johtoryhmä
2.0		Hyväksytty toimintamalli	Tietohallinto	Johtoryhmä	Kaupunginhallitus

1. KÄYTTÄJÄLOKIN TIETOJEN KÄSITTELY

Lokijärjestelmällä tarkoitetaan tässä ohjeessa järjestelmää, jonka tarkoituksena on suojata organisaation tietoturva sekä varmistaa tietosuojan toteutumista ja rekisteröidyn yksityisyyttä. Lokijärjestelmän avulla rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta.

Lokitiedoissa ei kysymys ole yksin tietoturvallisuudesta, vaan organisaation johdon vastuulla olevasta tietojärjestelmien ja niiden tukemien organisaation ydinprosessien kokonaislaadun osasta.

1.1. Oikeusperuste

Tietosuojalain (1050/2018) sekä EU:n yleisen tietosuoja-asetuksen (GDPR, 679/2016) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Lokitietojen käsittelyllä varmistetaan myös organisaation tietoturvaa sekä järjestelmien toimivuutta, jonka osalta kyse on julkisen hallinnon tiedonhallinnasta annetun lain (tiedonhallintalaki, 906/2019) toteuttamisesta. Tiedonhallintalaissa säädetään tietoturvavelvoitteista 4 luvussa.

Tämän tarkoituksen toteuttamiseksi laissa edellytetään, että rekisterinpitäjä toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen ***suojaamiseksi*** asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Sama velvollisuus on myös kaupungin palveluntuottajilla esimerkiksi niillä, jotka itsenäisenä elinkeinonharjoittajana toimivat rekisterinpitäjän lukuun.[1]

Tässä ohjeessa tarkoitettu lokitietojen käsittely tapahtuu siis sekä rekisteröidyn yksityisyyden ja siihen liittyvien oikeuksien että rekisterinpitäjän velvollisuuksien[2] toteuttamiseksi. On huomattava, että pelkkä lokitietojärjestelmä ei yksin vastaa edellä esitettyä, vaan sen ohella rekisterinpitäjän on syytä ryhtyä muihinkin tietoturvallisuuden toteutumisen varmistaviin toimenpiteisiin, kuten[3]

- sopimusjärjestelyt tietojen hankinnasta ja luovuttamisesta,
- käsiteltävien henkilö- ja muiden tietojen laadun varmistamisesta huolehtiminen,
- henkilöstön kouluttaminen,
- käyttöoikeuksien hallinnointi,
- tietotekniset turvallisuusratkaisut

[1] Tietosuoja-asetus (GDPR, 679/2016)
[2] Muun muassa: Tietosuoja-asetus IV luku, tiedonhallintalaki (906/2019) 4 luku.
[3] Tiedonhallintalain vaatimukset (4 luku) sekä tietosuoja-asetuksen osoitusvelvollisuuden toteuttaminen.

- sisäiset valvontajärjestelmät
- vaitiolositoumukset ja tietoturvasitoumukset

On huomattava, että esimerkiksi tietosuojarikos sekä tietomurto ovat kriminalisoituja. Rikoslaissa (39/1889) on säädetty 38 luvussa tarkemmin tieto- ja viestintärikoksista.

Jos lokia tai sitä tuottavaa teknistä järjestelmää on tarkoitus käyttää henkilöstön valvontaan esimerkiksi väärinkäytöstapausten selvittämiseksi, lokin käytöstä on tiedotettava myös käyttäjille[4].

1.2. Käsittelyn tarkoituksen määrittely

Lokitietojen avulla voidaan jäljittää järjestelmän tapahtumia (kuka, mitä milloin), virheitä, väärinkäyttö- ja tietomurtotilanteita ja niiden yrityksiä.[5]

Lokin avulla tapahtuvan henkilötietojen käsittelyn tarkoitus on *valvoa ja tarvittaessa reagoida rekisteröidyn turvaksi, että rekisteröityjä koskevia henkilötietoja käsitellään annettujen ehtojen, määräysten ja lain mukaisesti.* Seurannan tavoitteena on siis käyttäjien, rekisteröityjen sekä ylläpitäjien oikeusturvasta huolehtiminen. Lokia voidaan käyttää myös *tilastotarkoitusta varten* esimerkiksi tiedonluovutusten seurantaan, kustannusten jakoon eri toimipisteille tai toimintayksiköille ja teknisten ongelmien selvittämiseen.

Työntekijöiden tai muiden henkilöiden työ- tai palvelussuhteen ehtojen noudattamisen valvontaan ei lokia tule käyttää, koska sellainen lokitietojen käsittelyn tarkoitus ei ole lain edellyttämällä tavalla yhteensopiva edellä mainitun käsittelyn tarkoituksen kanssa.[6]

Lokia saavat käyttää vain ne henkilöt, joille työtehtäviin liittyen on annettu oikeus lokin käyttöön.

1.3. Informointi

On huolehdittava siitä, että ne henkilöt, joiden tietoja lokiin tallentuu, saavat tietosuoja-asetuksen, tietosuojalain ja yksityisyyden suojasta työelämässä annetun lain[7] tarkoittamalla tavalla tietoonsa lain edellyttämät tiedot mm.;

- rekisterinpitäjästä,
- lokin avulla tapahtuvan henkilötietojen käsittelyn tarkoituksesta,
- rekisteröidyn oikeuksista.

---

[4] Työnantajan on järjestettävä yhteistoimintamenettely, kuten laissa yksityisyydensuojasta työelämässä 21 §:ssä säädetään. Ks. myös tietoyhteiskuntakaaren 18 luvun nk. lex nokia -säännökset.
[5] Laki julkisen hallinnon tiedonhallinnasta (906/2019) 17 §
[6] Yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:ssä säädetään työntekijöihin kohdistuvasta teknisestä valvonnasta ja sen edellytyksistä.
[7] Laki yksityisyyden suojasta työelämässä 21 §. Yhteistoiminnasta annetun lain 6 §. Tietosuoja-asetuksen 13 artikla. Tietosuojalaki 4 §. Informointi suoritetaan osana henkilöstörekisteristä laadittua informointiasiakirjaa, jolla toteutetaan rekisteröityjen tiedonsaantioikeus tietosuoja-asetuksen mukaisesti.

Henkilöitä on informoitava myös siitä, kenen puoleen he voivat kääntyä halutessaan käyttää lakiin perustuvia oikeuksiaan. Riippumatta siitä, kuka lokitietoja pyytää tai kuka oikeuksiaan haluaa käyttää, tulee kaikki tietopyynnöt ohjata kaupungin kirjaamoon, jossa asia kirjataan asianhallintajärjestelmään ja josta asia välitetään oikealle taholle vastattavaksi.

Tietojärjestelmän käyttäjää informoidaan siitä, että heidän tietonsa tallentuvat lokiin. Informointi voidaan toteuttaa esimerkiksi tietojärjestelmän käyttökoulutuksen yhteydessä tai perehdytyksen yhteydessä. Vastuu informoimisesta on rekisterinpitäjällä.

Lokin edellä mainittuun käyttötarkoitukseen ei kuulu tietojen luovuttaminen sivulliselle[8]. Myös tämä on syytä kertoa informointiin oikeutetuille henkilötietoja käsitteleville. Lokiin talletettuja tietoja saa luovuttaa vain silloin, kun tiedon pyytäjällä on lakiin perustuva oikeus saada näitä tietoja.

1.4. Rekisteröityjen oikeudet

Niillä henkilöillä (käsittelijöillä), joita koskevia henkilötietoja lokiin tallentuu, on oikeus tarkastaa tietonsa ja tarvittaessa vaatia virhe oikaistuksi, ellei tarkastusoikeutta ole tapauskohtaisesti rajoitettu.

Kaupungin lokirekisteriin rekisteröityjä tulee informoida edellä esitetyllä tavalla lokin käytöstä. Heillä on myös oikeus luottaa siihen, ettei lokiin tallentuvia tietoja käytetä käyttötarkoituksensa vastaisesti ja että myös loki on suojattu tehokkaasti sivullisilta.

Henkilö, joka on lokia koskevia tehtäviä suorittaessaan saanut tietää toista henkilöä koskevia henkilötietoja, on vaitiolovelvollinen, eikä hän saa ilmaista saamiaan tietoja lainvastaisesti sivulliselle[9].

Rekisteröity, jonka eduksi lokijärjestelmä on luotu, on oikeutettu saamaan tietoonsa sen, kuka häntä koskevia tietoja on käsitellyt julkisuuslain asianosaiselle kuuluvan tiedonsaantioikeuden nojalla. Tämä edellyttää sitä, että vireillä on ollut asiakasta koskeva asia, johon lokitieto on voinut vaikuttaa. Pääsääntöisesti lokitiedot eivät koske asiakasta, vaan työnantajan henkilöstöä eli tiedot koskevat muita henkilöitä. Tämän osalta on siis tapauskohtaisesti harkittava, koskeeko asianosaisen tiedonsaantioikeus lokitietoja vai ei.

Rekisteröity voi tilanteessa, jossa on perusteltu syy epäillä rikosta, saattaa asian tietosuojavaltuutetun tai poliisin tutkittavaksi.

[8] Kaupunki ei pääsääntöisesti luovuta lokitietoja kolmansille osapuolille/ sivullisille. Tiedonluovutukset tapahtuvat lakisääteisesti eri viranomaistoimijoille ja mikäli asiakkaalla tai muulla tietoja pyytävällä taholla on tiedonsaantiin oikeus, voidaan tiedot luovuttaa. Tietojen luovutuksessa huomioidaan mm. julkisuuslain 11 ja 12 § sekä tietosuoja-asetuksen 15 artikla.
[9] Rikoslaki (39/1889) 38 luku 9 § tai muut asiaa koskevat erityissäännökset. Rikoslaista löytyvät myös muut tiedonväärinkäytöksiä koskevat rangaistussäännökset.

1.5. Tallennusaika

Lokitietojen tallennusaika on johdettava lokin käyttötarkoituksesta. Koska lokia pidetään rekisteröidyn hyväksi, voidaan lokiin tallentuvia tietoja säilyttää niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullista vastaan.

Koska henkilötietojen lainvastainen käsittely ja rekisteriin tunkeutuminen ovat kriminalisoituja tekoja, joiden syyteoikeus vanhentuu kahdessa vuodessa, on lokia säilytettävä kahden vuoden aika, ellei aiemmin ole voitu todeta perusteen säilyttämiselle menettäneen merkityksensä. Lokitiedot tulee hävittää turvallisesti!

Tieto lokin säilytysajasta sekä säilytykseen liittyvistä vaatimuksista kirjataan kaupungin tiedonhallintamalliin (Digiturvamalli). Esimerkiksi virhe-, varoitus-, käytönvalvonta-, viestintä- ja tiedonluovutuslokien sekä muiden lokityyppien säilytysaika vaihtelee suojattavan kohteen mukaan, yleensä kuuden ja 24 kuukauden välillä.

1.6. Viranomaisilmoitukset

Lokiin saa tallettaa tietoja vain sellaisista henkilötietoja käsittelevistä, joilla on asiakkuuteen tai palvelussuhteeseen perustuva asiallinen yhteys rekisterinpitäjään. Mikäli lokitiedoista käy ilmi tietosuoja- tai tietoturvapoikkeama, tulee sen, jolla on, tai jolla voi olla vaikutuksia rekisteröityyn tai organisaation toimintaan, laatia havainnosta tai todennetusta tapauksesta lakisääteiset sekä tapauksen muutoin edellyttämät viranomaisilmoitukset esimerkiksi tietosuojavaltuutetun toimistolle, poliisille tai kyberturvallisuuskeskukselle.

1.7. Lokitietojen kerääminen – käytön ja virheiden selvittäminen

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.”*

Kaupungin on huolehdittava siitä, että tiedonhallintalain mukainen lokitus on toteutettu ja että lokitus toimii. Käyttö-, luovutus- ja virhetilanteet on tarvittaessa pystyttävä selvittämään[10].

2. LOKITIETOJEN SEURANTA JA VALVONTA

2.1. Rutiiniseuranta

Kaupungin tietojärjestelmien tietoturvaa sekä tietosuojan toteutumista seurataan ja valvotaan rutiinivalvonnan muotoisesti 1 - 2 kertaa vuodessa. Seurannan käynnistää tietojärjestelmän *rekisteristä vastaava henkilö*

[10] Kuntaorganisaatiossa on hyvä huomata, ettei kuntaorganisaatioita koske vastaavat lokitietovaatimukset tai asiakkaan oikeudet lokitietoihin, kuin esimerkiksi hyvinvointialuetta. Laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) on 10 ja 11 §:ssä säädetty tarkemmin sosiaali- ja terveydenhuollon lokitiedoista sekä asiakkaan oikeudesta lokitietoihin.

(rekisterin vastuuviranhaltija). Hän esittää pyynnön tietojärjestelmän pääkäyttäjälle tai henkilölle, jolla on oikeus päästä lokitietoihin.

Seuranta tehdään satunnaisotantana tietyn päivän tilanteesta, jolloin seurantaan tulevat mukaan kaikki tiettynä päivänä järjestelmää käyttäneet henkilöt (kaupungin järjestelmään käyttöoikeuden omaavat). Selvityksessä varmistetaan myös em. henkilöiden järjestelmän katselu- ja käyttöoikeustasot niin, että tietyn käyttö- tai katseluoikeuden omaavalla tunnuksella ei ole muita kuin sille tarkoitettuja käyttö- tai katseluoikeuksia. Tarkastuksen ja siihen liittyvän raportin tekee rekisteristä vastaava tai hänen nimeämänsä henkilö/henkilöt.

Seuranta voidaan tehdä myös niin, että valitaan tietty määrä satunnaisia asiakkaita, joiden asiakastietoja on käsitelty sovittuna päivänä tai ajanjaksona. Sen jälkeen tarkastetaan, ovatko kaikki em. asiakastietoja käsitelleet henkilöt oikeutettuja asiakkaan tietojen käsittelyyn. Tarkastuksen ja siihen liittyvän raportin tekee rekisteristä vastaava tai hänen nimeämänsä henkilö/henkilöt.

Jos tiedoissa ei ole huomautettavaa, tarkastusraportti arkistoidaan organisaation arkistointisääntöjen mukaisesti. Jos tarkastuksen yhteydessä havaitaan tietosuojan vastainen rekisteröidyn tietojen käyttö, otetaan yhteyttä kaupungin tietosuojavastaavaan sekä ao. henkilön esimieheen, jotka käynnistävät kaupungissa sovitun menettelyn.

2.2. Seuranta ilmoituksen tai havainnon perusteella (ilmoitus joko asiakkaalta tai organisaation oma havainto)

Asiakkaalla on oikeus saada tiedot hänen henkilötietoihinsa tehdyistä kyselyistä sekä niihin liittyvät tiedot kyselytoimien ajankohdista ja tarkoituksista. Tietosuoja-asetuksen 15 art. 1 kohdassa ei kuitenkaan vahvisteta henkilön oikeutta tietoihin, jotka koskevat rekisterinpitäjän niiden työntekijöiden henkilöllisyyttä, jotka ovat suorittaneet kyselytoimet rekisterinpitäjän alaisuudessa ja sen ohjeiden mukaisesti (kaupungin henkilöstö). Asiakas voi pyytää tietojen tarkastusta kirjallisesti siihen tarkoitetulla lomakkeella (kaupungin verkkosivut, tietopyynnöt). Kaupungille saapuvat tietopyynnöt ohjataan kaupungin kirjaamoon, jossa asia kirjataan asianhallintajärjestelmään, jonka kautta asia välitetään oikealle viranomaiselle tai viranomaisen vastuuviranhaltijalle vastattavaksi. Jos rekisteristä vastaava henkilö pitää pyyntöä aiheellisena, pyytää hän tiedot ohjelman pääkäyttäjältä, joka toimittaa tiedot niitä pyytäneelle viranhaltijalle viivytyksettä. Rekisteristä vastaava selvittää tietojen katselun tai luovutuksen perusteet ja huolehtii tietopyyntöön vastaamisesta. Tarvittaessa rekisteristä vastaava käy vastauksen läpi yhdessä asiakkaan kanssa (ml. lokitiedot).

Jos työntekijän havaitaan katselleen tai käyttäneen asiakkaan tietoja asiattomasti, otetaan rekisteristä vastaavan pyynnöstä asianomaiseen tapaukseen liittyvät lokitiedot järjestelmästä. Esimies ja rekisteristä vastaavat käyvät loki- ja rekisteritiedot läpi yhdessä kaupungin tietosuojavastaavan kanssa. Mikäli rekisteritietojen käsittelyssä havaitaan tietosuojapoikkeama, joka edellyttää viranomaisilmoituksia, laatii kaupungin tietosuojavastaava tarvittavat viranomaisilmoitukset. Jos

henkilörekisteritietojen käytössä havaitaan väärinkäytös, käynnistää esimies kaupungissa sovitun menettelyn.

2.3. Erityinen väärinkäyttöuhka

Osana kaupungin omavalvontaa tunnistetaan myös erityisen väärinkäytön uhka. Erityinen väärinkäyttöuhka voi syntyä esimerkiksi tilanteessa, jossa asiakkaana on tunnettu julkisuuden henkilö tai tilanteessa, jossa käsiteltävä asia on yleisesti kiinnostava (rikos, erityinen sairaus tms.). Mikäli on syytä epäillä tai kaupunki saa ilmoituksen mahdollisesta tietojen väärinkäytöstä ja rekisteristä vastaava (vastuuviranhaltija) katsoo tarkastuksen tarpeelliseksi, voi rekisterin vastuuhenkilö käynnistää lokitietojen tarkastuksen ja pyytää ao. uhkaan liittyviä lokitietoja järjestelmän pääkäyttäjältä. Pyynnön yhteydessä on uhka määriteltävä.

Rekisteristä vastaava henkilö tarkastaa lokitiedot ja mikäli tietojen perusteella on syytä epäillä väärinkäytöksiä tai muuta tiedon asiatonta käyttöä, ilmoittaa hän havainnoistaan kaupungin tietosuoja- ja tietoturvavastaaville. Mikäli tarkastuksessa havaitaan tietojen väärinkäyttöä tai muuta asiatonta käyttöä, ilmoittaa rekisteristä vastaava asiasta kaupungin tietoturva- ja tietosuojavastaaville sekä ao. työntekijän esimiehelle, jotka käynnistävät kaupungissa sovitun menettelyn.

Mikäli tietojen tarkastelu tapahtuu kaupungille tulleen ilmoituksen perusteella, laaditaan asiasta tietopyyntöä vastaava vastaus, joka kirjataan kaupungin asianhallintajärjestelmään. Vastauksen antaa rekisteristä vastaava henkilö.

3. TOIMENPITEET VÄÄRINKÄYTÖKSESSÄ

3.1. Kouvolan kaupungin käytäntö

Liitteen 1 mukaan.

3.2. Rikosoikeudellinen vastuu

Henkilötietojen käsittelijä voi väärinkäytöstilanteessa joutua rikosoikeudelliseen vastuuseen, jos väärinkäytös katsotaan joko tietosuojarikokseksi tai muuksi tieto- ja viestintärikokseksi. Rikoslain 38 luvun 9 §:n mukaan tietosuojarikoksesta voidaan rangaista, jos henkilötietoja käsitellään vastoin tietosuojasäännöksiä (esim. käyttötarkoitussidonnaisuus ei täyty) ja väärinkäytös loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa. Tietosuojarikoksena voidaan pitää esimerkiksi asiakastietojen katselua tai selaamista uteliaisuudesta. Tämän lisäksi rikoslaista löytyvät mm. rangaistukset viestintäsalaisuuden loukkauksista sekä tietomurroista.