LOKIENHALLINTAPOLITIIKKA

Turun kaupunki

Konsernihallinto
Tietosuojavastaava
7.1.2019

Sisällysluettelo

1. Johdanto

Tietojärjestelmien käyttö ja ylläpito tuottaa paljon erilaista tapahtumatietoa – sekä teknistä että järjestelmän käyttöä kuvaavaa. Yleisesti tällaista tietoa kutsutaan lokitiedoksi. Lokitiedoilla pystytään jäljittämään järjestelmien teknisiä tapahtumia (jolloin lokitieto auttaa järjestelmien ylläpidossa, kehittämisessä ja vian-korjauksessa) tai järjestelmien käyttöä ja tietojen katselua (käyttöloki). Käyttölokitietoja hyödynnetään järjestelmän sidosryhmien – omistajaorganisaation, käyttäjien sekä henkilötietojen osalta rekisteröityjen – oikeuksien turvaamiseen sekä mahdollisten väärinkäytösten selvittämiseen ja ennalta ehkäisyyn.

Lokienhallintapolitiikkaa hallinnoi Turun kaupungin konsernihallinnon tietosuojavastaava. Lokitietojen avulla voidaan valvoa tietojärjestelmien tapahtumia ja käyttöä sekä automaattisesti että manuaalisesti. Tämä lokipolitiikka on käytävä läpi kaupungin yhteistoimintamenettelyssä. Käyttölokien keskitetty kerääminen muodostaa henkilörekisterin, jonka rekisterinpitäjä on Turun kaupunki. Rekisteriselostetta ylläpidetään kaupungin rekisteriselostejärjestelmässä (https://rekisteri.turku.fi).

2. Lokienhallinnasta yleisesti

Jotta kappaleessa 1. mainitut tavoitteet (oikeuksien turvaaminen sekä väärinkäytösten selvittäminen ja ennalta ehkäisy) voidaan saavuttaa, on voitava luottaa siihen, että Turun kaupungin tietojärjestelmien ja tietojen käsittelyn lokitieto on eheää. Eheydellä tarkoitetaan sitä, että kertyneitä lokitietoja ei pidä pystyä muuttamaan eivätkä lokitiedot saa muuttua ilman asianmukaista oikeutta ja oikeutetusti tehtyjä toimenpiteitä. Perusperiaatteena on se, että syntyneitä lokitietoja ei lähtökohtaisesti muokata, vaan virheellisen lokitiedon korjaamisesta syntyy uusi lokimerkintä. Lokit täytyy hävittää heti, kun ne eivät ole enää tarpeellisia.

Turun kaupungin esimiesten vastuulle kuuluu valvoa, että heidän alaisensa noudattavat tietosuoja- ja tietoturvaohjeistusta. Rekisterinpitäjien vastuulla on huolehtia siitä, että tietojärjestelmiin ja muihin tietojen tallennuspaikkoihin on oikeudet ja pääsy vain sellaisilla henkilöillä, jotka niitä työtehtäviensä suorittamiseen tarvitsevat. Rekisterinpitäjä vastaa ja päättää kunkin henkilörekisterin osalta henkilötietojen käytön seurannan tarpeesta, asianmukaisesta henkilötietojen käytön valvonnan toteuttamisesta sekä valvonnan periaatteiden ja käytäntöjen dokumentoinnista.

Lokitietoihin myönnetään pääsy tapauskohtaisesti harkiten vain niille henkilöille, joille lokitietojen katselu on työtehtävien suorittamiseksi välttämätöntä.

Rekisteröidyillä on määrätyin ehdoin oikeus saada tietoa lokeista ja tietojensa katselusta. Prosessi rekisteröityjen tietopyynnöille on kuvattu erillisessä ohjeistuksessa. Mahdolliset rikostutkintoihin ja valvontaviranomaisten selvityksiin liittyvät lokitietojen luovutukset perustuvat aina tapauskohtaiseen harkintaan ja käsittelyyn rekisterinpitäjän ja kyseisen viranomaisen kesken.

3. Yleinen lokiohjeistus

3.1 Lokitietojen muodostuminen operatiivisissa järjestelmissä henkilötietojen käsittelyssä

Operatiivisissa järjestelmissä ja henkilötietojen käsittelyssä lokitietoa täytyy muodostua mahdollisuuksien mukaan alla mainituista tapahtumista.

- Käyttäjien sisään- ja uloskirjautumiset
- Pääkäyttäjän toimenpiteet
    - Aikaleima
    - Sisään- ja uloskirjautumiset
    - Suoritetut komennot
    - Haut henkilötietoja sisältäviin tietueisiin
- Käyttäjän toimenpiteet
    - Aikaleima
    - Sisään- ja uloskirjautumiset
    - Henkilötietojen katselu, lisääminen ja poistaminen
- Integraatiorajapintojen toiminta
    - Aikaleima
    - Henkilötietojen viennit ja tuonnit

3.2 Tietoturvalokitus

IT-infrastruktuurijärjestelmien osalta tietoturvalokitietoa täytyy muodostua mahdollisuuksien mukaan alla mainituista tapahtumista. Vastaava seuranta toteutetaan mahdollisuuksien mukaan myös ulkoisen palveluntarjoajan tuottamissa palveluissa.

- Ydinjärjestelmien lokitus:
    - Ulkoiset DNS-lokit sekä kyselyiden tietosisältö
    - DHCP-lokit
    - Palomuurin tapahtumat
    - VPN-lokit
    - Virustorjuntalokit
    - Domain controllerin tapahtumat
    - Autentikointipisteiden tapahtumat
    - Soveltuvin osin tiedostopalvelinten ja dokumenttienhallinnan tapahtumat
    - Sähköposti- ja viestintäjärjestelmien tapahtumat (tekninen ja viestintäloki)

3.3 Poikkeamien havainnointi

Mikäli lokien hallintaan ja analysointiin käytetään automaattista järjestelmää, voidaan hälytykset muodostaa esimerkiksi alla mainituista tapahtumista. Tarkempi määrittely, jossa tunnistetaan hälytykset muodostavat tapahtumat sekä havainnoinnin kohteena olevat järjestelmät, tehdään erikseen tarvittaessa. Automaattista havainnointia voi toteuttaa kolmas osapuoli.

- Henkilötietojen massaviennit, -poistot ja -muokkaukset
- Toistuvat epäonnistuneet sisäänkirjautumisyritykset
- Virushavainnot
- Järjestelmän pääkäyttäjän haut henkilötietoja sisältäviin tietueisiin
- Paikallisella käyttäjätunnuksella kirjautuminen
- Paikallisen käyttäjätunnuksen luonti

3.4 Lokitietojen säilytys

Lokitiedot tallennetaan valvottavan järjestelmän ulkopuolelle paikkaan, joka on suojattu riittävillä tietoturvakäytännöillä ja -teknologioilla, jotta voidaan taata lokitiedon eheys, luottamuksellisuus ja saatavuus. Lokien tallennusajat sekä menetelmät tallennusaikojen umpeutumisen yhteydessä on dokumentoitava erikseen esimerkiksi järjestelmien tai henkilörekisterien sisäisissä kuvauksissa.

- Henkilörekisterien käyttö- ja luovutuslokien osalta rekisterinpitäjä vastaa siitä, että lokitiedon säilytysaika on määritelty käyttötarkoituksen mukaan ja että lokitietoja kerätään vain tarpeen mukaan. Mikäli toimialakohtaiset tai muut erityislait eivät toisin määrittele, on lokitietojen säilytysaika henkilörekisterien käyttö- ja luovutuslokeissa 10 vuotta. Rekisterinpitäjä voi poiketa tapauskohtaisen harkinnan perusteella edellä mainitusta tallennusajasta erityisen painavien teknisten tai muiden rajoitteiden tai lyhyemmän tallennustarpeen vuoksi.

- Teknistä lokitietoa (käyttöjärjestelmän tai palvelinalustan sisäiset tapahtumat, niihin liittyvät prosessit ja virheet) hyödynnetään esimerkiksi järjestelmien vianselvitykseen, kuormituksen seurantaan sekä tilastointiin. Teknisen lokitiedon ohjeellinen tallennusaika on kolme kuukautta. Järjestelmän omistaja tai rekisterinpitäjä voi poiketa tapauskohtaisen harkinnan perusteella ohjeellisesta tallennusajasta esimerkiksi teknisten rajoitteiden tai lyhyemmän tallennustarpeen vuoksi.

- Tietoturvalokilla valvotaan verkon estettyä tai sallittua toimintaa (palomuuri, IDS/IPS, VPN). Tietoturvalokin säilytysaika on vähintään 2 vuotta.

- Viestintäloki seuraa organisaation viestintävälineiden (esimerkiksi sähköposti- ja pikaviestijärjestelmä) viestintätapahtumia. Tallennettavia tietoja ovat viestintään osallistuvan käyttäjän nimi, käyttäjätunnus, aikaleima sekä käytetyn päätelaitteen tiedot. Viestintälokin ohjeellinen tallennus-

aika on 60 vuorokautta. Viestintäjärjestelmän omistaja tai rekisterinpitäjä voi poiketa tapauskohtaisen harkinnan perusteella ohjeellisesta tallennusajasta esimerkiksi teknisten rajoitteiden tai lyhyemmän tallennustarpeen vuoksi.

- Ylläpitoloki kerää tietoa tallennettuun lokitietoon kohdistuvista toimenpiteistä. Ylläpitolokitiedon eheys on kyettävä varmistamaan lokin tallennusaikana.

3.5 Lokitietojen käyttöoikeudet

Lokitietoihin tulee luovuttaa käyttöoikeudet vain niille henkilöille, jotka niitä työtehtävissään tarvitsevat. Myönnetyt oikeudet on dokumentoitava. Henkilötietoja sisältävä loki on henkilörekisteri. Henkilötietojen käsittely tulee dokumentoida ja kirjata erilliseen lokiin.

Oikeus lokitietojen lukemiseen myönnetään tapauskohtaisen harkinnan perusteella. Myöntämisen voi tehdä lokitiedon omistaja. Lokitietoa saa käsitellä vain ajantasaisen henkilötieto- ja tietosuojalainsäädännön mukaisesti.

Lokitietojen muokkaaminen on kiellettyä. Mahdollisuuksien mukaan muokkaaminen on pyrittävä teknisesti estämään.

Lokitietojen poistamista suositellaan hoidettavaksi automaattisella menettelyllä ennalta sovitun määrittelyn mukaisesti. Mikäli automaattinen poistaminen ei ole mahdollista, voi poiston tehdä rekisterinpitäjän luvalla ja pyynnöstä sellainen henkilö, joka ei itse käytä rekisteriä. Muu kuin edellä mainittu manuaalinen lokitietojen poistaminen on kielletty ja se on mahdollisuuksien mukaan pyrittävä teknisesti estämään.

4. Poikkeukset lokienhallintapolitiikkaan

Mahdolliset tästä politiikasta poikkeavat menettelyt täytyy hyväksyttää kyseessä olevan henkilö- tai muiden tietojen käsittelytoimen vastuuhenkilöllä ennen menettelyn aloittamista. Ennen hyväksyntää on suositeltavaa pyytää asiaan konsernihallinnon tietosuojavastaavan kommentti. Mahdolliset kappaleessa 3.4 määritellyistä tallennusajoista poikkeavat tallennusajat on hyväksytettävä konsernihallinnon asianhallinnassa ennen menettelyn aloittamista.