Lokienhallintapolitiikka

Tietoturvapäällikkö
9.1.2025
2.2

Sisällys

1. Johdanto

Tämä lokienhallintapolitiikka linjaa vastuut, periaatteet sekä toimintatavat, joita noudatetaan Turun kaupungin lokitietojen käsittelyssä ja keräämisessä. Se ohjaa lokitietojen käyttöä tietosuojan ja tietoturvan toteutumisen varmistamiseksi. Tätä politiikkaa sovelletaan kaikkiin Turun kaupungin käytössä oleviin sovelluksiin ja tietojärjestelmiin, myös ulkoisen palveluntarjoajan tuottamiin, ja sitä hallinnoi kaupungin tietoturvapäällikkö.

2. Ohjaavat vaatimukset

Tämän politiikan taustalla lokien käsittelyä ohjaavat Turun kaupungin tietoturva- ja tietosuojapolitiikat sekä erityisesti seuraavat lait, asetukset ja suositukset:

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuojalaki (1050/2018)
- Arkistolaki (831/1994)
- Rikoslaki (1889/39)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Laki sähköisen viestinnän palveluista (917/2014)
- Tiedonhallintalautakunnan suositukset (vm.fi)
- Suositus tietoturvallisuuden vähimmäisvaatimuksista (valtioneuvosto.fi)

3. Lokienhallinnasta yleisesti

Tietojärjestelmien käyttö ja ylläpito tuottaa paljon erilaista tapahtumatietoa – sekä teknistä, että järjestelmän käyttöä kuvaavaa. Yleisesti tällaista tietoa kutsutaan lokitiedoksi. Järjestelmähankintojen yhteydessä tulee aina määritellä käyttöönotettaviksi myös lokitietovaatimukset.

Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin, eli lokitetaan.

Lokitiedoilla pystytään jäljittämään järjestelmien teknisiä tapahtumia, jolloin lokitieto auttaa järjestelmien ylläpidossa, kehittämisessä, viankorjauksessa sekä tietosuojan hallinnassa ja seurannassa. Tavoitteena on muodostaa aukoton ja eheä todisteketju (audit trail) ko. tapahtumalle.

Lokitiedon käsittelyllä tarkoitetaan lokitiedon keräämistä, säilyttämistä, katselua, analysointia, seurantaa, luovutusta, tuhoamista ja raportointia. Lokin käyttötarkoitus vaikuttaa lokien käsittelyyn.

Lokienhallinnalla pyritään varmistamaan kyky todentaa tapahtuman kulku, osapuolet, kiistämättömyys, mahdolliset tunkeutumiset ja poikkeamat, järjestelmän toimivuus sekä käyttäjien ja rekisteröityjien oikeusturva.

3.1 Ohjaavia käytäntöjä

Lokitietoihin on vältettävä tallentamasta:
- henkilötunnuksia
- EU:n tietosuoja-asetuksen tarkoittamia erityisiä henkilötietoja
- luottokorttinumeroita
- salasanoja tai salasanojen tiivisteitä

- järjestelmien välisiä käyttöavaimia ja salaisuuksia
- valtuutustietoja
- henkilöiden välisen viestiliikenteen sisältöä

Lokien käsittelyn periaatteet:
- Lokitietojen käsittelyn tarvelähtöisyys
- Luottamuksellisuuden säilyttäminen
- Eheyden säilyttäminen
- Henkilötietojen minimoiminen
- Vastuiden eriyttäminen
- Säännöllinen valvonta
- Lokien systemaattinen käyttö ja seuranta
- Säilytysaikojen noudattaminen

3.2 Yleiset vaatimukset

Lokitiedon tulee olla eheää ja kiistämätöntä. Tämä tarkoittaa sitä, että kertyneitä lokitietoja ei saa pystyä muuttamaan ja niiden muuttumattomuus on tarvittaessa pystyttävä todistamaan.

Lokitieto sisältää katkeamattomasti vähintään seuraavat tiedot:

- Aikaleima (milloin tapahtuma oli?)
- Tapahtuma (mitä tehtiin tai yritettiin tehdä?)
- Toimija (kuka tai mikä teki?)
- Tapahtuman lähde (mistä tehtiin, mistä muutostieto on peräisin?)
- Tapahtuman kohde (mihin tietoon tai järjestelmään toiminta kohdistui?)
- Tapahtuman tila (onnistui / ei onnistunut / epäonnistumisen syy)

Lokien muodostamisessa tulee mahdollisuuksien mukaan hyödyntää järjestelmien oletus (default) lokeja.

Lokitieto tulee olla koko elinkaarensa ajan muutettavissa yleisesti hyväksyttyyn koneluettavaan muotoon.

Lokitiedon muodostumisesta vastaa sovelluksen tai tietojärjestelmän omistaja. Jos lokitieto sisältää henkilötietoja muodostuu siitä henkilörekisteri.

Rekisterinpitäjä vastaa ja päättää kunkin henkilörekisterin osalta henkilötietojen käytön seurannan tarpeesta, asianmukaisesta henkilötietojen käytön valvonnan toteuttamisesta sekä valvonnan periaatteiden ja käytäntöjen dokumentoinnista.

Rekisteröidyillä on oikeus saada lokien perusteella selvitys siitä, onko henkilötietojen käsittely ollut asianmukaista. 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.

4. Kerättävät lokityypit

4.1 Käyttöloki eli tapahtumaloki (sovellusloki)

Käyttö- eli tapahtumaloki rekisteröi tapahtumia käyttäjien sisään- ja uloskirjautumisista ja muista normaaleista järjestelmän suorittamista prosesseista.

Järjestelmän moduulit jättävät jäljen käyttölokiin kutsuessaan toisia moduuleita. Tulostustapahtumista ja tietosisällön lukemisesta tietokannasta kirjataan myös merkintä käyttölokiin.
Operatiivisissa järjestelmissä ja henkilötietojen käsittelyssä käyttölokitietoa täytyy muodostua myös seuraavista tapahtumista:

- Käyttäjän toimenpiteet
    - Aikaleima
    - Sisään- ja uloskirjautumiset (myös epäonnistuneet)
    - Henkilötietojen katselu, lisääminen ja poistaminen
    - Henkilötietojen luovutus eri rekisterien tai rekisterinpitäjien välillä (yleisemmin luovutusloki)
- Pääkäyttäjän toimenpiteet
    - Aikaleima
    - Sisään- ja uloskirjautumiset
    - Suoritetut komennot
    - Haut henkilötietoja sisältäviin tietueisiin
    - Henkilötietojen luovutus eri rekisterien tai rekisterinpitäjien välillä (yleisemmin luovutusloki)
- Integraatiorajapintojen toiminta
    - Aikaleima
    - Henkilötietojen viennit ja tuonnit
    - Henkilötietojen luovutus eri rekisterien tai rekisterinpitäjien välillä (yleisemmin luovutusloki)

Käyttölokitietoja hyödynnetään järjestelmän sidosryhmien – omistajaorganisaation, käyttäjien sekä henkilötietojen osalta rekisteröityjen – oikeuksien turvaamiseen sekä mahdollisten väärinkäytösten selvittämiseen ja ennalta ehkäisyyn.
Täysin ulkoistetuissa palveluissa, kuten SaaS-palvelut, henkilötietojen käyttölokitieto on käytännössä ainoa asiakasorganisaation tarvitsema lokitieto, jos sovellus tai tietojärjestelmä on muuten teknisesti täysin toimittajaorganisaation vastuulla.

4.2 Virheloki

Virheloki sisältää tietoja järjestelmässä, sovelluksessa tai tapahtumassa havaituista virheistä. Se on erityisen tarpeellinen ongelmatilanteiden selvittämisessä. Kun virheen syy kirjataan lokiin mahdollisimman tarkasti, sen aiheuttaja on myös helpompi korjata.

4.3 Viestintäloki

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

4.4 Ylläpitoloki

Ylläpitolokilla ylläpidetään tietoa järjestelmän toimintaan tehdyistä muutoksista ja järjestelmän käyttöoikeuksien muutoksista sekä tietoja esimerkiksi tallennettuihin lokitietoihin kohdistuvista toimenpiteistä. Sillä hallitaan myös virhetilanteita versionhallinnassa.

4.5 Tietoturvaloki

Tietoturvalokilla valvotaan käyttöoikeuskohteen kuten esim. verkon estettyä tai sallittua toimintaa tunkeutumisten ja poikkeamatilanteiden havaitsemiseksi. IT-infrastruktuurijärjestelmien osalta tietoturvalokitietoa tulee muodostua vähintäänkin alla mainituista tietoturvapoikkeamiksi luokitelluista tapahtumista:

- Ulkoiset DNS-lokit sekä kyselyiden tietosisältö
- DHCP-lokit
- Palomuurin tapahtumat
- IDS/IPS
- VPN-lokit
- Virustorjuntalokit
- Domain controllerin tapahtumat
- Autentikointipisteiden tunnistautumistapahtumat (myös. MFA)

5. Lokitietojen säilytys

Säilytysaika johdetaan aina lokien käyttötarkoituksesta, eli siitä, miksi lokia ja sen tietoja kerätään. Tällöin tulee ottaa huomioon:

- Tietoaineiston alkuperäisen käyttötarkoituksen mukainen tarpeellisuus viranomaisen toiminnassa;
- Luonnollisen henkilön tai oikeushenkilön etujen, oikeuksien, velvollisuuksien ja oikeusturvan toteuttaminen ja todentaminen;
- Sopimuksen tai muun yksityisoikeudellisen oikeustoimen vaikutus;
- Vahingonkorvausoikeudelliset vanhentumisajat
- Rikosoikeudelliset vanhentumisajat
- Henkilötietojärjestelmien lokivaatimukset

Seuraavien törkeiden rikosten syyteoikeuden vanhenemisaika on 10 vuotta:

- törkeä viestintäsalaisuuden loukkaus
- törkeä tietoliikenteen häirintä
- törkeä tietojärjestelmän häirintä
- törkeä tietomurto
- törkeä virka-aseman väärinkäyttäminen

Henkilötietojärjestelmien käyttölokien 10 vuotta.

Jos edellä kuvatut säilytysaikaperiaatteet ja -vaatimukset eivät rajaa säilytysaikaa, käytetään seuraavia:

Lokityyppi	**Säilytysaika**
Käyttöloki	10 v
Virheloki	3 kk
Viestintäloki	10 v
Ylläpitoloki	10 v
Tietoturvaloki	3kk (kaikki) ja 10 v (tietoturvapoikkeamat)

6. Lokitietojen poisto

On tärkeää varmistaa, että lokitiedot säilyvät ja ovat käytettävissä koko määritellyn säilytysajan, jonka jälkeen ne on poistettava, koska niiden säilyttämiselle ei enää ole perustetta. Lokitietojen poistamista suositellaan hoidettavaksi automaattisella menettelyllä ennalta sovitun määrittelyn mukaisesti. Mikäli automaattinen poistaminen ei ole mahdollista, voi poiston tehdä rekisterinpitäjän luvalla ja pyynnöstä dokumentoidusti.

7. Lokienhallinnan toteuttaminen

Lokitiedot tulee tallentaa vähintään kuukausittain, mieluiten päivittäin tai online-tyyppisesti, valvottavan järjestelmän ulkopuolelle erilliseen järjestelmään tai paikkaan, joka on suojattu riittävillä tietoturvakäytännöillä ja -teknologioilla. Näillä toimilla voidaan taata katkeamattoman lokitiedon eheys, luottamuksellisuus ja saatavuus. Menetelmät niiden säilytysaikojen umpeutumisen yhteydessä on dokumentoitava erikseen, esimerkiksi sovellusten tai henkilörekisterien omissa kuvauksissa.

Lokien käytön ja niiden hallinnan kannalta on Turun kaupungin Tietohallinnon ohjausryhmä linjannut, että toimittaja ylläpitää lokitusta tämän politiikan mukaisesti. Toimittajan ylläpitämää lokitusta voidaan täydentää, esimerkiksi seuraavilla tarkennuksilla: mitä lokitetaan, kuinka kauan lokeja säilytetään, missä lokit sijaitsevat, lokien poistoprosessi, käyttöoikeudet, lokitusten luovutus, lokitietojen tarkastelu ja analysointi.

Käyttölokien seuranta tulee olla aktiivista ja siinä voidaan tukeutua mm. automaattihälytyksiin. Mikäli lokienhallintaan ja analysointiin käytetään erityistä havainnointijärjestelmää, voidaan hälytykset muodostaa lokienhallintajärjestelmään sisältämän kerätyn lokitiedon pohjalta. Tarkempi määrittely, jossa tunnistetaan hälytyksen muodostavat tapahtumat, sekä havainnoinnin kohteena olevat järjestelmät, tehdään erikseen. Automaattista havainnointia voi toteuttaa kolmas osapuoli.

7.1 Lokitietojen käyttöoikeudet

Lokitietoa saa käsitellä vain ajantasaisen tietosuojalainsäädännön mukaisesti ja käyttöoikeudet tulee luovuttaa vain niille henkilöille, jotka niitä työtehtävissään välttämättä tarvitsevat. Oikeus myönnetään tapauskohtaisen harkinnan perusteella. Hyväksynnän voi antaa sovelluksen tai tietojärjestelmän omistaja, tai henkilörekisterin tapauksessa rekisterivastuuhenkilö. Myönnetyt oikeudet on dokumentoitava prosessein käyttövaltuushallintapolitiikan mukaisesti.

Sähköisten viestien ja välitystietojen (viestintälokit) käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa, eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Työntekijän sähköpostin avaamiseen pakottavissa tapauksista työnantajan toimesta on olemassa erilliset ohjeet.

Lokienhallinnan työtehtäviä suunnitellessa on vältettävä vaarallisten työyhdistelmien syntyä. Esimerkiksi henkilö ei voi käsitellä tai poistaa omia lokitietojaan.

8. Poikkeukset lokienhallintapolitiikkaan

Rekisterivastuuhenkilö tai sovelluksen omistaja voivat poiketa tapauskohtaisen harkinnan perusteella tämän politiikan linjauksista, kuten määritellystä tallennusajasta erityisen painavien teknisten tai muiden syiden vuoksi. Ennen hyväksyntää on pyydettävä asiaan tietosuojavastaavan kommentti. Poikkeukset määritellyistä tallennusajoista on hyväksytettävä konsernihallinnon asianhallinnan vastuuhenkilöllä ennen menettelyn aloittamista. Mahdollisesti syntyvä riski on hyväksytettävä sovelluksen tai tietojärjestelmän omistajalla ja siitä on informoitava tietoturvapäällikköä ja tietosuojavastaavaa.

9. Dokumentin muutoshistoria

Versio	PVM	Nimi	Muutoskuvaus
1.0	7.1.2019	Janne Mutanen	Ensimmäinen hyväksytty versio
1.1	4.10.2021	Pasi Kalevo	Päivitetty versio uudella dokumenttipohjalla
1.2	5.10.2021	Pasi Kalevo	Päivitetty versio uudella sisältörakenteella
1.3	8.10.2021	Pasi Kalevo	Pääsynvalvontaloki poistettu (sis. käyttölokiin)
1.4	8.10.2021	Pasi Kalevo	Kohta 8. muutettu
1.5	10.11.2021	Pasi Kalevo	Päivitetty kohtaa 7.1
1.6	23.11.2021	Pasi Kalevo	Päivitetty kohdat: 2 ja 7
1.7	7.12.2021	Pasi Kalevo	Päivitetty yleisiä säilytysaikoja 3kk/10v
1.8	8.2.2022	Pasi Kalevo	Säilytysajat vahvistettu lokienhallintajärjestelmä-projektille
1.9	21.2.2022	Pasi Kalevo	Muutoksia kommenttien pohjalta kohtiin 2. / 3.2 / 8.
1.10	22.2.2022	Pasi Kalevo	Muutoksia kommenttien pohjalta kohtiin 1. / 7.2
1.11	28.2.2022	Pasi Kalevo	Muutoksia 7.1
1.12	18.3.2022	Pasi Kalevo	Korjauksia saatujen kommenttien pohjalta
1.13	8.12.2022	Pasi Kalevo	3.2 ja 7: Lokitieto oltava katkeamatonta 4.1: SaaS-palveluissa vain käyttöloki 7: vähintään kuukausittain, mieluiten päivittäin tai online-tyyppisesti
2.0	1.2.2023	Pasi Kalevo	Läpikäynti tietosuojan kanssa ennen lopullista hyväksyntää.
2.1	27.11.2024	Sami Kokkala	Poistettu sosiaali- terveydenhuoltoon viittaavat kohdat.
2.2	9.1.2025	Sami Kokkala	Kappale numerointi lisätty. Kpl 7 muokattu Tiha Ohry:n linjauksen mukaiseksi. Tekstiä selkey-tetty.