



TIETOSUOJAVALTUUTETUN TOIMISTO

KÄYTTÄJÄLOKIN TIETOJEN KÄSITTELY HENKILÖTIETOLAIN MUKAAN

Päivitetty 27.07.2010

www.tietosuoja.fi

KÄYTTÄJÄLOKIN TIETOJEN KÄSITTELY HENKILÖTIETOLAIN MUKAAN

Henkilörekisteri muodostuu myös lokitietojen osalta, jos ne sisältävät tunnistettavaa henkilöä koskevia merkintöjä. Lokijärjestelmällä tarkoitetaan tässä ohjeessa tietojärjestelmää, jonka tarkoituksena on suojata rekisteröityjä tietoja ja siten rekisteröidyn yksityisyyttä. Lokijärjestelmän avulla rekisterinpitäjä vastaa henkilötietojen käsittelyn lainmukaisuudesta. Näin ollen lokeihin sovelletaan ainakin henkilötietolaki (523/1999) ja muita henkilötietojen ja yksityisyyden suojasta mahdollisesti annettuja lakeja.

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

1. Oikeusperuste

Henkilötietolain tarkoituksena on toteuttaa perustuslain turvaamaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Tämän tarkoituksen toteuttamiseksi laissa edellytetään, että rekisterinpitäjä toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen **suojaamiseksi** asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Sama velvollisuus on sillä, joka itsenäisenä elinkeinonharjoittajana toimii rekisterinpitäjän lukuun.¹

Tässä ohjeessa tarkoitettu lokitietojen käsittely tapahtuu siis sekä rekisteröidyn yksityisyyden ja siihen liittyvien oikeuksien että rekisterinpitäjän intressien² toteuttamiseksi.

On huomattava, että pelkkä lokitietojärjestelmä ei yksin vastaa edellä esitettyä, vaan sen ohella rekisterinpitäjän on syytä ryhtyä muihinkin tietoturvallisuuden toteutumisen varmistaviin toimenpiteisiin, kuten³

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

¹ Henkilötietolaki 32 §

² kts. henkilötietolaki 12 §:n 1 momentin 4-kohta

³ Kts. valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeistus

- vaitiolositoumukset

On huomattava, että tietomurto eli tunkeutuminen luvatta tietojärjestelmään on kriminalisoitu.

2. Käsittelyn tarkoituksen määrittely

Lokin avulla tapahtuvan henkilötietojen käsittelyn tarkoitus on *valvoa ja tarvittaessa reagoida rekisteröidyn turvaksi, että rekisteröityjä koskevia henkilötietoja käsitellään annettujen ehtojen, määräysten ja lain mukaisesti*. Lokia voidaan käyttää myös *tilastotarkoitusta varten* esimerkiksi tietoliikenteen kapasiteetin 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.⁴

Lokia saavat käyttää vain ne henkilöt, joiden työtehtäviin kuuluu vastata tietoturvan toteutumisesta ja tietojen laadun edellyttämistä toimenpiteistä. Nämä tehtävät ja talletettavat tiedot on määriteltävä siten, että ne perustuvat vain lokin käyttötarkoitukseen, eli rekisteröityjen yksityisyyden toteuttamiseen. Ota tämä vaatimus huomioon sopiessasi henkilötietojen käsittelytehtävien ulkoistamisesta.

Henkilötietolain mukainen rekisterinmäärittelmä perustuu loogisen rekisterin käsitteeseen; samaan rekisteriin kuuluviksi luetaan ne henkilötiedot, joilla on yhteinen käsittelyn tarkoitus. Näin ollen esimerkiksi asiakkaita koskevat tiedot eivät lain tarkoittamassa mielessä sisälly tähän rekisterin suojaamiseksi perustettuun tapahtumalokiin, vaikka ne teknisesti ilmenisivätkin sanotusta lokista. Muuhun tarkoitukseen, kuten asiakassuhteen hoitamiseen yms. Tarkoitettujen henkilötietojen käsittelyyn sovelletaan henkilötietolakia tai sovellettavaksi tulevia erityislakeja.

3. Suunnittelu ja huolellisuus

Kaikki henkilötietojen käsittely tulee suunnitella henkilötietolain 6 §:n mukaisesti. Suunnittelussa on huomioitava lokiin sisältyvien henkilötietojen koko elinkaaren ajalta henkilötietolain velvoitteet.

Myös loki on suojattava ja lokin käyttöä on edellä mainitun tarkoituksen toteuttamiseksi valvottava.

4. Rekisteriseloste

⁴ yksityisyyden suojasta työelämässä annetun lain (477/2001) 9 §:ssä säädetään työntekijöihin kohdistuvasta teknisestä valvonnasta.

Koska lokilla on itsenäinen käyttötarkoitus suhteessa kulloinkin kyseessä olevaan ydintoiminnon henkilötietojen käsittelyn tarkoitukseen, on myös lokista laadittava henkilötietolain tarkoittama rekisteriseloste. Kun suunnittelet lokia, käytä suunnittelussa apuna rekisteriselostetta.

5. Informointi

Huolehdi, että ne henkilöt, joiden tietoja lokiin tallentuu, saavat henkilötietolain ja yksityisyyden suojasta työelämässä annetun lain⁵ tarkoittamalla tavalla tietoonsa lain edellyttämät tiedot;

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

Informoi myös siitä, kenen puoleen henkilö voi kääntyä halutessaan käyttää lakiin perustuvia oikeuksiaan.

Informointi voidaan toteuttaa esimerkiksi tietojärjestelmän käyttökoulutuksen yhteydessä, henkilöstöoppaan avulla tai muulla tehokkaalla tavalla. Muista, että rekisterinpitäjä on velvollinen tarvittaessa osoittamaan, että tiedot on lain edellyttämällä tavalla annettu.

Lokin edellä mainittuun käyttötarkoitukseen ei kuulu tietojen luovuttaminen sivulliselle⁶. Myös tämä on syytä informoida informointiin oikeutetuille henkilötietoja käsitteleville. Lokiin talletettuja tietoja saa luovuttaa vain silloin, kun tiedon pyytäjällä on lakiin perustuva oikeus saada näitä tietoja.

6. Rekisteröityjen oikeudet

Niillä henkilöillä (käsittelijöillä), joita koskevia henkilötietoja lokiin tallentuu, on oikeus tarkastaa tietonsa ja tarvittaessa vaatia virhe oikaistuksi, ellei tarkastusoikeutta ole tapauskohtaisesti rajoitettu henkilötietolain perusteella. Heitä 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 vaitiovelvollinen, eikä hän saa saamiaan tietoja lainvastaisesti ilmaista sivulliselle⁷.

Rekisteröity (esim. asiakas tai potilas), jonka eduksi lokijärjestelmä on luotu, voi olla oikeutettu saamaan tietoonsa sen, kuka häntä koskevia tietoja on käsitellyt julkisuuslain asianosaiselle kuuluvan tiedonsaantioikeuden nojalla.

⁵ Yksityisyyden suojasta työelämässä annetun lain (471/2001) 9 §. Asiaan tulee sovellettavaksi yhteistoiminnasta annetun lain 6 §:n 8 –kohta. (Mikäli asiassa tulisi sovellettavaksi em. lain 8a-kohta, ei käyttötarkoituksia voitaisi pitää yhteensopivina).

⁶ Kts. henkilötietolaki 3 § 6-kohta

⁷ kts. henkilötietolaki 33 § tai asiaa koskevat erityissäännökset

Henkilötietolain mukainen tarkastusoikeus koskee rekisteröityä itseään koskevia henkilötietoja. Rekisterin suojaamiseksi toteutettuun lokiin tallentuu tietoja henkilötietoja käsittelevistä muista henkilöistä. Näin ollen tarkastusoikeus on vain henkilötietoja käsittelevillä henkilöillä itseään koskeviin tietoihin. Rekisteröity voi tilanteessa, jossa on perusteltu syy epäillä rikosta, saattaa asian tietosuojavaltuutetun tai poliisin tutkittavaksi.

7. 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 säilyttämiseksi menettäneen merkityksensä. Hävitä lokitiedot turvallisesti!

8. Viranomaisilmoitukset

Koska lokiin saa tallettaa tietoja vain sellaisista henkilötietoja käsittelevistä, joilla on asiakkuuteen tai palvelussuhteeseen perustuva asiallinen yhteys rekisterinpitäjään, ei lokista tarvitse tehdä ilmoitusta tietosuojavaltuutetulle.

9. Virhetilanteet

Huolehdi, että loki toimii ”audit trail” –periaatteen mukaisesti. Ole valmis tarvittaessa selvittämään virhetilanteet.