



TIETOSUOJAVALTUUTETUN TOIMISTO

## LOKITIEDOT HENKILÖTIETOJEN SUOJAAMISEN VÄLINEINÄ

12.11.2012, päivitetty 10.06.2014

### Sisällys

1. Johdanto
2. Henkilötietojen suojaamisen perusteet
3. Käytönvalvonnassa käsiteltävien henkilötietojen käsittelyn perusteet
4. Käyttäjän tiedolliset oikeudet
5. Käytönvalvontajärjestelmän käsittely ja suojaus
6. Asiakkaan oikeus lokitietoihin ja luvattoman käsittelyn selvittäminen
7. Lokitietojen säilyttämisaika

[www.tietosuoja.fi](http://www.tietosuoja.fi)

## 1. Johdanto

Tieto- ja viestintäjärjestelmät tallentavat toiminnastaan tietoja. Yleisesti näitä tietoja kutsutaan lokitiedoiksi ja niiden avulla pyritään selvittämään ja ratkaisemaan tieto- ja viestintäjärjestelmien toiminnan häiriöitä tai virheitä.<sup>1)</sup> Tapahtumien kirjaamista voidaan käyttää myös tietojärjestelmän käytönvalvontaan. Oikeudellinen intressi käytönvalvontaan voi liittyä muun muassa varallisuuden siirtoon, maksullisten palvelujen käyttöön, yrityssalaisuuksiin tai henkilötietojen käsittelyyn. Tässä ohjeessa lokitiedolla tarkoitetaan henkilötietojen suojaamiseksi ylläpidetyn käyttövalvontajärjestelmän tuottamia lokitietoja.

Ohjeessa käytetyt käsitteet ovat:

**Lokitiedot** = suojattavan henkilötiedollisen tietojärjestelmän käsittelystä kerättävät käyttäjäkohtaiset merkinnät

**Käyttöoikeusjärjestelmä** = tiedot luvallisista käyttäjistä, heidän käyttöoikeuksistaan ja tunnisteistaan

**Käytönvalvontajärjestelmä** = käyttöoikeusjärjestelmän ja lokitietojen muodostama looginen kokonaisuus

**Asiakas** = suojattavan tietojärjestelmän rekisteröity

**Käyttäjä** = käytönvalvontajärjestelmän rekisteröity

Tämä ohje kumoaa Tietosuojavaltuutetun toimiston aikaisemman lokiohjeen "Käyttäjälökin tietojen käsittely henkilötietolain mukaan".

## 2. Henkilötietojen suojaamisen perusteet

Henkilötietolain 32 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämislä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Säännökseen sisältyvän suhteellisuusperiaatteen mukaan toimenpiteiden toteuttamisessa voidaan ottaa huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Säännöksen tarkoittamia organisatorisia suojauskeinoja ovat käyttäjille/työntekijöille annetut ohjeet ja määräykset henkilötietojen käsittelystä ja sitoumukset henkilötietojen suojasta (käyttäjäsitoumus). Tekniset keinot liittyvät muun muassa käyttäjien yksilöintiin ja tunnistamiseen, käyttöoikeuksien määrittelyyn tehtävien mukaan, käsittelyaikaisiin tarkisteisiin (esim. perustekysely) sekä viime kädessä käytön jälkikäteiseen selvittämiseen lokitietojen avulla.

## 3. Käytönvalvonnassa käsiteltävien henkilötietojen käsittelyn perusteet

Lokitietojen avulla tapahtuva henkilötietojen käsittelyn valvonta edellyttää käyttäjien yksilöimistä ja tunnistamista. Tässä tarkoituksessa ylläpidetään luvallisista käyttäjistä, heidän tunnisteistaan ja käyttöoikeuksistaan käyttöoikeusjär-

---

1) Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) julkaisemassa Lokiohjeessa (3/2009) s.13 lokitieto määritellään dokumentiksi jonkin tapahtuman toteuttamisesta jonakin tiettyinä hetkenä ks. [tästä](#).

jestelmää. Käyttöoikeusjärjestelmä yhdessä lokitietojen kanssa muodostavat käytönvalvontajärjestelmän.

Henkilötietolain perusvaatimus käytönvalvontajärjestelmälle on ns. asiallisen yhteyden vaatimus, mikä usein täyttyy sillä, että käyttäjä on työsuhteessa suojattavan tietojärjestelmän rekisterinpitäjään.

Henkilötietolain 6 §:n mukaan käytönvalvonnan tietojärjestelmän tulee olla asiallisesti perusteltu rekisterinpitäjän toiminnan kannalta. Vaikka käyttöoikeuksien rajaamisella voidaan rajoittaa pääsyä suojattaviin henkilötietoihin, perustuu henkilötietojen käsittely yksittäisissä tapahtumissa käyttäjien omaan harkintaan ja viime kädessä käyttäjään kohdistuvaan luottamukseen sääntöjen ja määräysten noudattamisessa. Tällöin viime kätinen keino käsittelyn lainmukaisuuden varmistamiseksi on käsittelyn jälkikäteinen selvittäminen lokitietojen avulla. Tämän perusteella voidaan katsoa, että lokitietojen käsittely käytönvalvontatarkoituksessa on asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta.

Henkilötietolain 7 §:n mukaisena käsittelytarkoituksena voidaan pitää suojattavien henkilötietojen käytönvalvontaa, joka voi olla rekisterinpitäjän oma-aloitteista ja asiakasaloitteista valvontaa (ks. ohje Asiakasaloitteisesta käytönvalvonnasta) ja käytönvalvonnan perusteella tehtävien oikeudellisten vaatimusten käsittelyä.

Henkilötietolain 9 §:n 1 momentissa tarkoitettu tarpeellisuusvaatimus määräytyy käytönvalvonnan käytännössä ja viime kädessä oikeudellisessa näytönarvioinnissa esiin tulleiden tietotarpeiden mukaan.

Henkilötietolain 9 §:n 2 momentissa on säädetty velvollisuudesta huolehtia tietojen virheettömydestä. Tämä tarkoittaa muun muassa sitä, että käyttäjien tunnukset ovat henkilökohtaisia eikä tietojärjestelmää saa käyttää muuta kuin omilla tunnuksilla.

#### 4. Käyttäjän tiedolliset oikeudet

Käytönvalvontajärjestelmän henkilötietolaissa tarkoitettu rekisteröity on yksittäinen käyttäjä. Käyttäjällä on omien käyttöoikeusjärjestelmään tallennettujen tietojen ja hänelle annettujen tunnusten käytöstä syntyneisiin lokitietoihin henkilötietolain 26 §:ssä tarkoitettu tarkastusoikeus. Lisäksi käyttäjä voi esittää tietojen korjaamista henkilötietolain 29 §:n perusteella. Koska näiltä osin ei ole oikeuskäytäntöä, ei menestyviä korjausvaatimusten perusteita voida tässä yhteydessä tarkemmin yksilöidä.

Henkilötietolain 24 §:n mukaan rekisterinpitäjän on huolehdittava siitä, että käyttäjä voi rekisteröitynä saada tiedon rekisterinpitäjästä, tämän edustajasta, käsittelytarkoituksesta, säännönmukaisesta luovutuksesta sekä tiedot, jotka tarpeen rekisteröidyn oikeuksien käyttämiseksi. Tämä voidaan toteuttaa pitämällä rekisteriselostetta käytönvalvontajärjestelmästä yleisesti saatavilla ja täydentämällä henkilötietolain 10 §:ssä tarkoitettua rekisteriselostetta viimeksi mainituilla tiedoilla. Katso "Tietosuojaseloste"-lomake ja opas "Laadi tietosuojaseloste" tietosuojavaltuutetun toimiston kotisivuilta.

Kun käyttäjä on työ- tai virkasuhteessa, on yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:n mukaan teknisin menetelmin toteutettava valvonta käytävä läpi yhteistoimintamenettelyssä.

## 5. Käytönvalvontajärjestelmän käsittely ja suojaus

Käytönvalvontajärjestelmän käsittelystä luvattoman henkilötietojen käsittelyn selvittämiseksi on annettu erikseen Ohje asiakasaloitteisesta käytönvalvonnasta.

Tunnistautumisjärjestelmä on myös suojattava asiatonta käsittelyä vastaan. Tässä tarkoituksessa on kiinnitettävä huomiota tunnusten luomiseen, uusimiseen sekä päivittämiseen käyttöoikeuksien päättymisen jälkeen. Lisäksi käytönvalvontajärjestelmää on suojattava ulkopuolista käsittelyä tai muuttamista vastaan.

Virheellisten tietojen estämiseksi olisi syytä harkita käyttäjille annettavaa ohjetta/määräystä siitä, että suojattavaa tietojärjestelmää saa käyttää vain omilla tunnuksilla eikä tunnuksia saa luovuttaa muille.

Lisäksi lokitietoja voidaan pitää julkisuuslain 24 §:n 1 momentin 7 kohdassa tarkoitettuina tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevin ja ainakin niiden toteuttamiseen vaikuttavina asiakirjoina. Tämän perusteella lokitiedot sellaisenaan kuten asiakas- ja käyttäjäkohtaiset lokitulosteet voivat olla tämän perusteella salassa pidettäviä.

## 6. Asiakkaan oikeus lokitietoihin ja luvattoman käsittelyn selvittäminen

Asiakkaan oikeudesta lokitietoihin on erityisesti säädetty sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) annetussa laissa. Yleisemmin on sovellettu julkisuuslain 11 §:n asianosaisten tiedonsaantisäännöstä, joka mahdollistaa myös salassa pidettävän tiedon saamisen.

Henkilötietolaissa säädetty tarkastusoikeus ei tule kyseeseen, koska lokitietojen rekisteröity on käyttäjä, ei asiakas.

Edellä mainitussa Ohjeessa asiakasaloitteisesta käytönvalvonnasta lokitietoja käytetään yhdessä asiakkaan kanssa selvityksen kohdentamiseksi.

## 7. Lokitietojen säilyttämisaika

Henkilötietolain 34 §:n mukaan henkilötiedot tulee hävittää sen jälkeen kun tiedot eivät ole rekisterinpitäjän kannalta enää tarpeellisia. Rekisterinpitäjän intressi lokirekisteritietojen säilyttämiseen kestää niin kauan kuin suojattavan oikeushyvän haltijalla on mahdollisuus esittää oikeudellisia vaatimuksia luvattoman henkilötietojen käsittelyn johdosta.

Vaatimukset ovat rikos- ja/tai vahingonkorvausoikeudellisia ja henkilörekisteririkos vanhenee 2 vuodessa ja virkarikoksena 5 vuodessa (virkavelvollisuuden rikkominen).