

FINAS-akkreditointipalvelun luottamuksellisen toiminnan periaatteet

Tiedote 2

04.07.2024



Sisällysluettelo

1	Johdanto	3
2	Tietojen luovuttaminen toiselle viranomaiselle	4
3	Periaatteet	4
3.1	Periaate I	4
3.2	Periaate II	5
3.3	Periaate III	6
3.4	Periaate IV	6
3.5	Periaate V	6
4	Voimaantulo	7
5	Muutokset edelliseen versioon	7

1 Johdanto

Tässä tiedotteessa esitetään FINAS-akkreditointipalvelun (myöhemmin FINAS) luottamuksellisen toiminnan periaatteet. FINAS huomioi toiminnassaan (EU) 2016/679 yleisen tietosuoja-asetuksen (GDPR) sekä lain julkisen hallinnon tiedonhallinnasta (906/2019), joka määrittää julkisen hallinnon organisaatioiden toiminnalta edellytettävät tietoturvallisuusvaatimukset. Lisäksi FINASin toiminnassa ja toimintaohjeissa on otettu huomioon Turvallisuus- ja kemikaalivirasto Tukesin tietoturvapoliittikka, tietoturvaohjeet ja etätyöohjeet sekä soveltuvilta osin nykyisin Digi- ja väestötietoviraston DVV ylläpitämä VAHTI-ohjeistus sekä Kyberturvallisuuskeskuksen ohjeet. Tietoaaineistolla tarkoitetaan tässä yhteydessä sähköisillä, paperisilla ja muilla tietovälineillä olevia asiakirjoja ja tietoja.

Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 765/2008 säädettiin akkreditoinnista ensimmäistä kertaa yhteisön tasolla. Edellä mainitun asetuksen 8.1 artiklan 4 alakohdassa käytännössä toistetaan standardissa SFS-EN ISO/IEC 17011:2017 mainittu periaate siitä, että kansallisella akkreditointiorganisaatiolla on oltava asianmukaiset järjestelyt saamiensa tietojen luottamuksellisuuden turvaamiseen.

FINASin toiminta rinnastetaan viranomaistoimintaan, ja FINASin antamat päätökset ovat hallintopäätöksiä. FINASin tulee toiminnassaan noudattaa hallintolakia (434/2003 ja sen muutokset), jossa muun muassa säädetään, että päätökset on perusteltava. FINASin arviointitoimintaan sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (julkisuuslaki 621/1999 ja sen muutokset). Lähtökohtana on, että viranomaisten asiakirjat ovat julkisia, kuten esimerkiksi FINASin akkreditointipäätökset liitteineen ja salassa pidettävät tiedot määritetään erikseen.

Vaatimustenmukaisuuden arvioinnissa todennetaan toiminnan pätevyyttä ja luotettavuutta sekä toimivuutta ja tuodaan esiin arviointikohteen vahvuuksia ja heikkouksia. Arviointi kattaa muun muassa erilaisten mittauslaitteiden tarkkuuden ja toimintavarmuuden, henkilöstön pätevyyden, työskentelytavat, menettelyt ja laadunvarmistuksen yksityiskohtaiset tulokset. Tällaiset yksityiskohtaiset tiedot voivat olla julkisuuslain 24 §:n 1 momentin 17 ja 20 kohtien perusteella salassa pidettäviä liike- ja ammattisalaisuuksia. Lisäksi tulevat sovellettaviksi tietosuojalainsäädännön edellyttämät henkilötietojen suojaamiseksi tarkoitetut säännökset. Tarkempi määritelmä tietosuojalainsäädännölle on EU:n yleinen tietosuoja-asetus (2016/679), tietosuojalaki (1050/2018) ja muu soveltuva tietosuojalainsäädäntö sekä tietosuojaviranomaisten sitovat määräykset. Luottamuksellisina pidettäviä tietoja on FINASin akkreditointiin ja arviointiin liittyvissä hakemuksissa, arviointiselosteissa ja arviointilausunnoissa.

2 Tietojen luovuttaminen toiselle viranomaiselle

Tietopyynnön saatuaan FINAS voi antaa salassa pidettäviä tietoja toiselle viranomaiselle, jos asiakirjaa pyytävällä viranomaisella on laissa säädetty oikeus saada tällaisia tietoja tai jos arvioinnin kohde on antanut suostumuksensa tietojen luovuttamiseen. Tämä koskee myös henkilötietoja. Ensisijaisesti kuitenkin toivotaan, että valvovat viranomaiset pyytävät tarvitsemansa tiedot suoraan toimijalta osana valvonnan velvoitteita.

3 Periaatteet

FINAS on kansainvälisessä akkreditointiorganisaatioiden yhteistyössä sitoutunut yhdenmukaisiin menettelyihin ja periaatteisiin. Kansainvälisten velvoitteiden taustalla on se, että akkreditointi ja siihen liittyvät arvoinnit perustuvat luottamuksellisuuteen (Euroopan parlamentin ja neuvoston asetusta (EY) N:o 765/2008 8 artiklan 1 kohdan 4 alakohta ja standardi SFS-EN ISO/IEC 17011:2017, kohta 8.1). FINASia koskevat periaatteet luottamuksellisuudesta koskevat myös FINASin ulkopuolisia arvioijia kuten ulkopuolisia pääarvioijia, teknisiä arvioijia ja teknisiä asiantuntijoita.

3.1 Periaate I

Akkreditointipäätökset ja niiden liitteet ovat julkisia.

Asiakkaalta arviointia varten ja arviointiprosessin aikana saadut dokumentit ja tiedot sekä arvioinnista laaditut arviointiselosteet ovat luottamuksellisia.

Akkreditoinnissa on ensiarvoisen tärkeää, että FINAS saa mahdollisimman kattavasti ja avoimesti tietoja arvioidakseen akkreditoinnin edellytysten täytymistä. FINAS täyttää kansainväliset velvoitteensa, kun se säilyttää akkreditointipäätöksiin liittyvien arviointiselosteiden luottamuksellisuuden. FINAS käsittelee jokaisen saamansa tietopyynnön erikseen. Jos FINAS olisi velvollinen antamaan arviointiselosteet aina sellaisenaan niitä pyytävälle, riskinä olisi, että arvioinnin kohteet eivät luovuttaisi avoimesti tietojaan. Tällöin FINAS ei saisi riittävästi tietoja arviointinsa pohjaksi.

Akkreditointipäätöksessä mainitaan FINASin arvioinnissa käyttämät menettelyt ja kriteerit, jotka arvioinnin kohteen katsotaan täyttävän. Päätös perustellaan kokoavassa katsauksessa, joka on yhteenveto tehdyistä arvioinneista. Kokoava katsaus sisältää arviointien julkisiksi katsottavat osiot:

- organisaation perustiedot
- arviointivaatimusten täyttyminen tai täyttymättä jääminen
- esitys akkreditointipäätökseksi

3.2 Periaate II

Asiakkaiden on voitava luottaa siihen, että FINASin henkilökunta ja arviointeihin osallistuvat arvioijat käsittelevät asiakkaiden toimintaan liittyviä tietoja luottamuksellisesti.

Kaikki FINASin arviointeihin osallistuvat ulkopuoliset arvioijat allekirjoittavat vaitiolovakuutuksen. Vaitiolovelvollisuus koskee kirjallista tietoa, mutta myös tallentamatonta tietoa (suullisesti saatu, arvioinnissa nähty). Vaitiolovelvollisuus jatkuu palvelussuhteen tai tehtävän päättymisen jälkeenkin. Asiakkaan tietoja ei luovuteta arviointiin osallistuvalla FINASin ulkopuoliselle arvioijalle ennen kuin tämä on allekirjoittanut vaitiolovakuutuksen ja asiakkaalta on saatu suostumus kyseisen henkilön osallistumisesta arviointiin.

Etäarviointien luottamuksellisuuteen liittyvät asiat on huomioitu FINASin etäarviointien arviointiperiaatteessa.

Luottamuksellinen tietojen käsittely varmistetaan FINASissa laitteiden ja ohjelmistojen tietoturvasta huolehtimisella huomioiden pilvipalvelut sekä omalla huolellisuudella (esim. päivitykset, laitteiden lukitus ja valvonta, salasanasuojaus, ulkoisen kovalevyn tai muistitikun salaus, keskustelujen luottamuksellisuus, sähköisten tallennusvälineiden, paperitulosteiden ym. asianmukainen säilytys). Edellä mainitut asiakohdat koskevat myös arviointiin osallistuvia henkilöitä, joten ulkoisten arvioijien on varmistuttava esimerkiksi pilvipalvelun riskeistä luottamuksellisen tiedon hallinnassa.

Arvioinneissa valokuvien tai kuvakaappauksien ottaminen on kiellettyä. Lisäksi FINASille luovutettuja aineistoja ei saa kääntää verkkosovellusten avulla, esim. Google kääntäjä/Google translate.

FINAS ei pyydä ennakkoaineistossa potilastietoja sisältäviä dokumentteja, eikä arvioinneissa mahdollisesti nähtyjä potilastietoja dokumentoida muistiinpanoihin eikä arvioinnin selosteisiin.

FINASin henkilökunta on saanut koulutusta henkilötietojen asianmukaisesta käsittelystä. Henkilötietojen käsittelystä kerrotaan tarkemmin tietosuojaselosteissa <https://www.finas.fi/Tietoa/Sivut/Tietosuoja.aspx>. FINASin arviointeihin osallistuvia ulkopuolisia arvioijia on tiedotettu FINASin henkilötietojen käsittelyyn liittyvistä periaatteista. FINASissa tietoja käsitellään erilaisissa

tietojärjestelmissä. Järjestelmätoimittajien kanssa on tehty tietojenkäsittelysovimukset ja vaitiolovakuutukset eli toimittajat ovat sitoutuneet noudattamaan muun muassa tietosuojasäädöksiä.

3.3 Periaate III

Aineiston siirto on luottamuksellista.

Luottamuksellisen tietoaineiston siirtoon käytetään suojattua yhteyttä (FINASin Ekstranet tai turvasähköposti). Tämä liittyy ensisijaisesti FINASin ja asiakkaan sekä FINASin ja arvioijien välillä vaihdettavaan luottamukselliseen aineistoon. Arviointiin liittyvää luottamuksellisesta materiaalia ovat esimerkiksi asiakkaan toimittama aineisto ja arvioijien selosteet.

Asiakkaat saavat halutessaan lähettää tietoa suojaamattomana, sillä lähetys on asiakkaan vastuulla (periaate IV) ja asiakas vastaa siitä, miten luottamukselliseksi toimitettava materiaali on luokiteltu. FINASin tulee asiakkaan käytännöistä huolimatta huolehtia aineiston luottamuksellisuuden varmistamisesta aineistoa eteenpäin toimitettaessaan. FINASin vastuulla on tiedottaa asianosaisille luottamukselliseen tietoaineiston siirtoon ja suojaukseen liittyv. Asiakkaan ei tule lähettää FINASiin turvallisuusluokiteltua aineistoa. Tämän osalta asiakkaan tulee olla ensin yhteydessä FINASiin.

3.4 Periaate IV

Kun arviointeihin liittyvä tietoaineisto on luovutettu tietosisältöineen vastaanottajan hallintaan, sen mukana siirtyvät myös käsittely- ja käyttöoikeudet sekä -velvollisuudet.

Toimittamisen luottamuksellisuus on lähettäjän vastuulla. Asiakkaan toimittaessa FINASille aineistoa, sen käsittely on FINASin vastuulla vasta sitten, kun FINAS on sen vastaanottanut. Vastaavasti FINASin toimittaessa aineistoa, esimerkiksi tekniselle arvioijalle, on aineisto teknisen arvioijan vastuulla vasta sitten, kun hän on sen vastaanottanut.

3.5 Periaate V

Luottamuksellisten tietojen hävittäminen.

FINAS-akkreditointipalvelu noudattaa akkreditointiprosessiin liittyvien asiakirjojen arkistoinnissa tiedonohjaussuunnitelmaa. Tiedonohjaussuunnitelman mukaisesti julkiset asiakirjat sekä arviointiprosessissa tuotetut selosteet arkistoidaan. Muu arviointiprosessiin liittyvä aineisto tuhoetaan arviointiprosessin päätyttyä (esimerkiksi ennen arviointia pyydetty arviointimateriaali). Myös arvioijaryhmän tulee tuhota saamansa aineisto. Tuhoaminen on tehtävä niin,

että luottamuksellisuus ei vaarannu. Aineisto tulee poistaa omalta koneelta lopullisesti huomioiden myös palvelimet. Varmin tapa tuhota muistitikulla oleva sähköinen tietoaineisto, on tuhota muistitikku fyysisesti. Luottamuksellisia tapoja tuhota paperinen aineisto on esimerkiksi toimittaa aineisto tietosuojastiaan, silputa silppurilla tai polttaa.

4 Voimaantulo

Tämä tiedote tulee voimaan 04.07.2024 ja on voimassa toistaiseksi.

Tällä tiedotteella kumotaan 13.5.2019 annettu FINAS-akkreditointipalvelun Tiedote 2.

Johtaja

Katriina Luoma

Johtava asiantuntija

Annika Wickström

5 Muutokset edelliseen versioon

04.07.2024

	Kappale	Muutos
1	Johdanto	Huomioitu salassa pidettävät tiedot
2	Tietojen luovuttaminen toiselle viranomaiselle	Huomioitu tietopyynnön menettely
3	Periaatteet	Päivitetty, että valokuvia ja kuvakaappauksia ei saa ottaa eikä potilastietoja dokumentoida muistiinpanoihin tai selosteisiin. Myös verkkosovellusten käyttäminen kääntämiseen on kiellettyä. Periaate turvallisuusluokiteltujen aineistojen kanssa päivitetty.