CSC-Tieteen tietotekniikan keskus Oy

Lausunto

26.06.2020 THL/2492/4.00.00/2020

Asia: THL/2492/4.00.00/2020

MUIDEN PALVELUNTARJOAJIEN TIETOTURVALLISILLE KÄYTTÖYMPÄRISTÖILLE ASETETTAVAT VAATIMUKSET

Määräyskirje

Lausuntonne tästä kohdasta:

CSC – Tieteen tietotekniikan keskus Oy

Lausunto muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettaville vaatimuksille

THL/2492/4.00.00/2020

26.06.2020

CSC – Tieteen tietotekniikan keskus Oy (CSC) kiittää mahdollisuudesta lausua sosiaali- ja terveysalan tietolupaviranomaisen Findatan määräysluonnoksesta koskien tietoturvallisia käyttöympäristöjä. CSC on Suomen valtion ja korkeakoulujen omistama erityistehtäväyhtiö ja ICT-osaamiskeskus. Tarjoamme teknologian ja palvelukehityksen ratkaisuja tutkimuksen, koulutuksen, kulttuurin ja julkishallinnon erityisosaamisalueilla. Ratkaisujemme perustana toimivat ICT-alustat, valtakunnallinen tutkimus- ja koulutusverkko Funet sekä tehokkaat konesalitoiminnot. CSC on yli 40 vuoden ajan tehnyt ICT-ratkaisuja edistyneen ja haastavan tutkimuksen tarpeisiin ja yli 20 vuoden kokemuksella tuottanut genomitiedon käsittelyn ja hallinnan palveluja tutkimukselle. CSC on myös biologisen tiedon hallintaa kehittävän kansainvälisen ELIXIR-infrastruktuurin Suomen osakeskus.

CSC kannattaa sitä, että asetetaan vaatimuksia muiden palveluntarjoajien tietoturvallisille käyttöympäristöille, mutta tutkimuksen näkökulmasta on välttämätöntä, että Findatan tietoturvamäärittelyissä huomioidaan ja tunnistetaan ne tarpeet, joita tutkimus- ja innovaatiotoimijoilla tässä kentässä on, ja huolehditaan siitä, että ne palveluntarjoajat, jotka pystyvät vastaamaan näihin tarpeisiin, voivat olla tukena tietoaineistojen käsittelyssä. Kansallisella

tasolla tulee tunnistaa ne toimijat, joilla on tarvittava kapasiteetti ja osaaminen tietoturvallisesta tietoaineistojen käsittelystä, ja jotka täyttävät vaaditut tietoturvastandardit. Lisäksi tulee varmistaa kansainvälisen tutkimusyhteistyön toimintamahdollisuudet. Näin turvataan sosiaali- ja terveysalan tutkimus- ja innovaatiotoiminnan edellytykset ja varmistetaan hallitusohjelman linjausten toteutuminen.

Suomen hallinnon järjestyneisyys ja kansalaisten kattava terveydenhuolto tuottaa tietoaineistoja, jotka ovat kansainvälisesti tunnistettuja ja arvostettuja tietolähteitä ihmisten terveyden ja hyvinvoinnin edistämiseksi. Sosiaali- ja terveysalan tietoaineistot ovat erityisen arvokkaita niiden rakenteellinen muodon ja aineistojen väestöpohjallisen kattavuuden takia. Yhdessä geneettisen perimän kanssa ne luovat perustan alan tutkimukselle, joka on välttämätöntä mm. lääketieteen kehittämisen näkökulmasta. Lisäksi nämä aineistot muodostavat kasvupohjan terveys- ja hyvinvoinnin asiantuntijoiden uusille yrityksille ja työpaikoille vuosikymmeniksi eteenpäin. Näin ollen sosiaali- ja terveystietojen avaaminen entistä laajemmin tutkimukselle ja tuotekehitykselle tietoturvaa noudattaen ja EU:n tietosuoja-asetuksen mukaisesti on suomalaisen hyvinvointiyhteiskunnan turvaamisen edellytys. Tietoaineistojen hallittu avaaminen tutkimukselle tukee myös kansallisen terveysalan tutkimus- ja innovaatiotoiminnan kasvustrategian tavoitteita sekä hallitusohjelman kirjausta ”Selvitetään sosiaali- ja terveysdatan hyödyntämistä osana terveysalan tutkimus- ja innovaatiotoimintaa huolehtien tietosuojan korkeasta tasosta”.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (”toisiolaki”) asettaa erityisen tiukat raamit sote-toimialan tietoaineistojen käsittelylle. Lain mukaan kaikki tietoaineistot tulee käsitellä lähtökohtaisesti tietolupaviranomaisen käyttöympäristössä eli Findatassa. Tapauskohtaisen harkinnan perusteella on mahdollista käsitellä tietoaineistoja myös muualla kuin Findatassa silloin, kun sen katsotaan olevan välttämätöntä ja edellyttäen, että käyttöympäristö täyttää 20 §:n 2 momentissa ja 21–29 §:ssä säädetyt edellytykset. Tutkimuksen näkökulmasta katsottuna, edellä mainitut, muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetetut vaatimukset välttämättömän käsittelyn kriteerien suhteen on kuitenkin asetettu niin tiukoiksi, että käytännössä tietoaineistojen käsittely muualla kuin Findatassa on vaikeaa, ja tulee yhteiskunnalle kalliiksi. Tämä hankaloittaa tai jopa estää tietoaineistojen tuomisen dataintensiivistä tutkimusta varten suunniteltuihin ympäristöihin. Tämä on huippututkimuksen, sekä yleisemminkin koko sosiaali- ja terveysalan kehityksen kannalta erittäin huolestuttavaa.

Huippututkimukselle tarkoitettuihin tutkimusinfrastruktuureihin tehtyjä mittavia investointeja ja sensitiivisen tiedon käsittelyn vankkaa kansallista osaamista on voitava hyödyntää täysimääräisesti. Esimerkiksi EU:n komission ja jäsenmaiden EuroHPC-yhteisyrityksen investoinnin myötä Suomeen syntyy yksi maailman johtavista datanhallinnan ja laskennan ekosysteemeistä, LUMI, joka lisää merkittävästi kotimaisen tutkimuksen kilpailukykyä sekä työllisyyttä ja talouskasvua. Tämä investointi muodostaa, yhdessä kansallisen laskennan ja datanhallinnan ekosysteemin kanssa, dataintensiiviselle tutkimukselle tärkeän poikkitieteellisen tutkimusinfrastruktuurin, ja näin ollen sen yhteiskunnallinen lisäarvo on merkittävä. Huippututkimukselle suunnatun tehokkaan laskentakapasiteetin ja datankäsittelyn ympäristöjen hyödyntäminen on välttämätöntä silloin, kun kehitetään esimerkiksi uusia lääkeaineita tai hoitoja harvinaisiin sairauksiin. Suomalaisen hyvinvointiyhteiskunnan etu erityisesti nykyisessä taloustilanteessa on se, että toimialan

tietoaineistoja voidaan käsitellä tietoturvallisesti tutkimusta varten niille kulloinkin tarkoituksenmukaisessa ja kustannustehokkaassa ympäristössä, tarvittaessa myös muualla kuin Findata-ympäristössä.

Yleisesti pitäisi selkeästi kertoa mitä toisiolain käyttötapausta tämä vaatimusmäärittely koskee. Käyttöympäristölle asetettujen kriteerien tulee lisäksi olla linjassa tutkimusinfrastruktuurien EU-tason aloitteiden, kuten eurooppalaisen tutkimuksen pilvipalvelualoitteen (European Open Science Cloud) ja EU:n data-avaruuksien (Common European Data Spaces) kanssa. Lisäksi tulee varmistaa, että palveluntarjoajat noudattavat jonkin EU-maan lainsäädäntöä, jotta varmistetaan yhteensopivuus GDPR:n kanssa. Kansainvälinen yhteistyö ja kansainvälisen referenssidatan käyttö on välttämätöntä esimerkiksi lääketieteellisten läpimurtojen saavuttamiseksi. Näin ollen toisiokäyttö ei rajoitu ainoastaan suomalaisten tekemään tutkimukseen, vaan toisiolupakäytännön pitää mahdollistaa kansainvälisten yhteistyökumppaneiden pääsy tutkimusaineistoihin.

CSC haluaa korostaa myös alla esitettyjen kohtien osalta seuraavia huomioita, jotka ovat myös lisätty lukuja koskeviin alakohtiin:

Luku 2.1 Tunnistautuminen

- Ensitunnistuksen ja hyväksyttyjen tunnistelähteiden luotettavuuden arviointikriteeristö tulisi julkaista määräyksen yhteydessä.

- Tunnuksen sulkeminen ja pääsyoikeuksien määrittäminen tulisi eriyttää tunnistelähteiden toimesta.

- Erityisesti tulisi kiinnittää huomioita kansainvälisten käyttäjien tunnistautumiseen.

Luku 2.3 Ympäristön suojaaminen

- Etäkäyttöympäristöön kirjautuminen vain etukäteen määrätyistä IP-osoitteista ei ole realistinen vaatimus modernissa humaanissa maailmassa.

- Kyseenalaista on, voiko vaatimusten perusteella hyödyntää suurteholaskentaa. Riskinä on, että maailmanluokan tietojärjestelmään tehdyt investoinnit jäävät hyödyntämättä.

- Mikä on riittävä eriytystaso ympäristöjen välillä? Riittääkö looginen eriytys vai tarvitaanko erilliset laitteistot Findatan luvittamien aineistojen tallentamiseen ja käsittelemiseen?

- Aineistojen suojaustasot tulisi määritellä riskiperustaisesti, aineistokohtaisesti.

Luku 2.6 Aineistojen poisto ympäristöstä

- Aineisto termi pitäisi määrittä tarkemmin. Tarkoittaako aineisto vain Findatan luovuttamaa aineistoa vai kaikkia aineistoja?

- Millä perustella aikarajat on asetettu? Miten tämä suhtautuu tietosuoja-asetuksen vaatimuksiin?

Luku 3.2.1 Tietolupaviranomaisen asettamat vaatimukset tietosuojaan

- Palveluntarjoajan velvollisuus tulee rajata siten, että palveluntarjoaja vastaa vain itse ympäristöstä sekä mahdollisesti ulos lähtevää verkkoliikenteestä. Tutkimuksessa yleisesti tutkimusryhmä itse luo vähintään osan ohjelmistosta, eikä palveluntarjoajaa voida velvoittaa tällaisen ohjelmiston vastuusta.

- Ohjelmistot -sana tulisi määritellä tarkemmin. Onko kyseessä ns. valmisohjelmistoja tai koskeeko tämä myös tutkimusryhmän kirjoittamaa ohjelmistokoodia?

Espoossa, 26.06.2020

CSC –Tieteen tietotekniikan keskus Oy

Kimmo Koski	Pekka Lehtovuori
Toimitusjohtaja	Johtaja, laskennallisen tutkimuksen palvelut

1.1 Toiminnallinen yleiskuvaus

Toiminnallinen yleiskuvaus on asianmukainen:

-

Lausuntonne tästä kohdasta:

-

1.2 Tekninen arkkitehtuuri

Tekninen arkkitehtuuri on asianmukainen:

-

Lausuntonne tästä kohdasta:

-

1.3 Määritelmät

Lausuntonne tästä kohdasta:

-

1.4 Käyttöympäristöjen palveluntarjoajat

Lausuntonne tästä kohdasta:

-

1.5 Luotetut tunnistefederaatiot

Lausuntonne tästä kohdasta:

-

2.1.2 Tietolupaviranomaisen asettamat vaatimukset:

Tunnistautumiseen liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

Luku 2.1 Tunnistautuminen:

- Ensitunnistuksen ja hyväksyttyjen tunnistelähteiden luotettavuuden arviointikriteeristö tulisi julkaista määräyksen yhteydessä.

- Tunnuksen sulkeminen ja pääsyoikeuksien määrittäminen tulisi eriyttää tunnistelähteiden toimesta.

- Erityisesti tulisi kiinnittää huomioita kansainvälisten käyttäjien tunnistautumiseen.

2.2.2 Tietolupaviranomaisen asettamat vaatimukset:

Käyttäjien ja käyttöoikeuksien hallintaan liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

2.3.2 Tietolupaviranomaisen asettamat vaatimukset:

Ympäristön suojaamiseen liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

Luku 2.3 Ympäristön suojaaminen:

- Etäkäyttöympäristöön kirjautuminen vain etukäteen määrätyistä IP-osoitteista ei ole realistinen vaatimus modernissa humaanissa maailmassa.

- Kyseenalaista on, voiko vaatimusten perusteella hyödyntää suurteholaskentaa. Riskinä on, että maailmanluokan tietojärjestelmään tehdyt investoinnit jäävät hyödyntämättä.

- Mikä on riittävä eriytystaso ympäristöjen välillä? Riittääkö looginen eriytys vai tarvitaanko erilliset laitteistot Findatan luvittamien aineistojen tallentamiseen ja käsittelemiseen?

- Aineistojen suojaustasot tulisi määritellä riskiperustaisesti, aineistokohtaisesti.

2.4.2 Tietolupaviranomaisen asettamat vaatimukset:

Lokitukseen liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

2.5.1 Tietolupaviranomaisen asettamat vaatimukset:

Valvontaan liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

2.6.1 Tietolupaviranomaisen asettamat vaatimukset:

Aineistojen poistoon liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

Luku 2.6 Aineistojen poisto ympäristöstä:

- Aineisto termi pitäisi määrittä tarkemmin. Tarkoittaako aineisto vain Findatan luovuttamaa aineistoa vai kaikkia aineistoja?

- Millä perustella aikarajat on asetettu? Miten tämä suhtautuu tietosuoja-asetuksen vaatimuksiin?

2.7.1 Tietolupaviranomaisen asettamat vaatimukset:

Ympäristön hallintaan ja valvontaan liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

3.1.2 Tietolupaviranomaisen asettamat vaatimukset:

Toimijan luotettavuuteen liittyvät yleiset vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

3.2.1 Tietolupaviranomaisen asettamat vaatimukset:

Tietosuojaan liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

Luku 3.2.1 Tietolupaviranomaisen asettamat vaatimukset tietosuojaan:

- Palveluntarjoajan velvollisuus tulee rajata siten, että palveluntarjoaja vastaa vain itse ympäristöstä sekä mahdollisesti ulos lähtevää verkkoliikenteestä. Tutkimuksessa yleisesti tutkimusryhmä itse luo vähintään osan ohjelmistosta, eikä palveluntarjoajaa voida velvoittaa tällaisen ohjelmiston vastuusta.

- Ohjelmistot -sana tulisi määritellä tarkemmin. Onko kyseessä ns. valmisohjelmistoja tai koskeeko tämä myös tutkimusryhmän kirjoittamaa ohjelmistokoodia?

3.3.1 Tietolupaviranomaisen asettamat vaatimukset:

Toimitiloihin liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

3.4.1 Tietolupaviranomaisen asettamat vaatimukset:

Henkilöstöön liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

4 Tietoturvallisen käyttöympäristön keskeiset prosessivaiheet

Keskeisiin prosessivaiheisiin liittyvät vaatimukset ovat asianmukaisia:

-

Lausuntonne tästä kohdasta:

-

Lindell Miia
CSC-Tieteen tietotekniikan keskus Oy