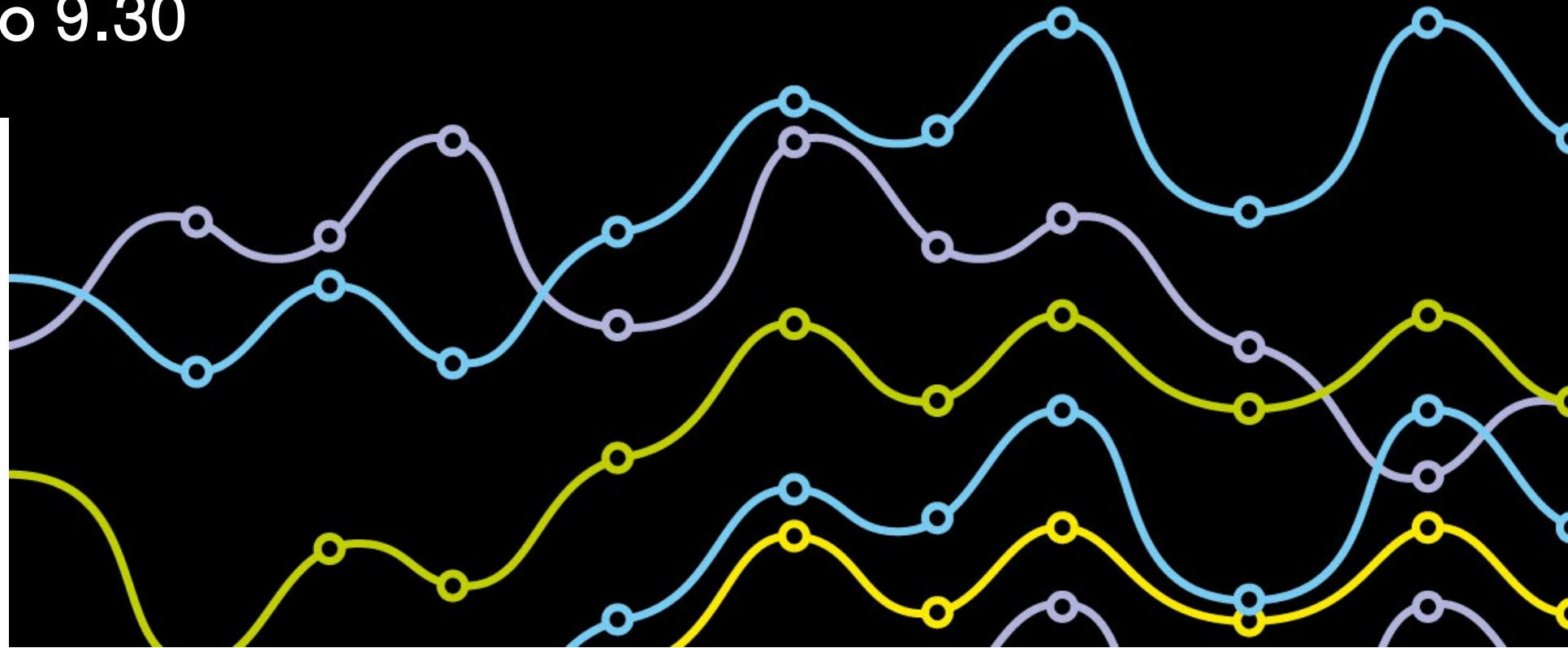
FINDATA

# Tervetuloa!

Infotilaisuus tietoturvallisten käyttöympäristöjen vaatimuksista alkaa klo 9.30



FINDATA

## Ohjelma

| | |
|---|---|
| 9.30–9.35 | Tilaisuuden avaus<br>*Antti Piirainen, Findata* |
| 9.35–10.30 | Määräyksen esittely<br>*Heikki Lanu, ICT-päällikkö* |
| 9.35–9.45 | Määräyksen rakenne ja tarkoitus |
| 9.45–10.00 | Yleistä tietoturvallisen käyttöympäristön vaatimuksista |
| 10.00–10.15 | Tekniset vaatimukset ja toimijan luotettavuus |
| 10.15–10.30 | Tietoturvalliseen käyttöympäristöön liittyvät keskeiset prosessivaiheet |
| 10.30–11.00 | Osallistujilta tulleiden kysymysten käsittelyä<br>*Heikki Lanu, ICT-päällikkö*<br>*Kirsi Talonen, lakimies* |

FINDATA TERVEYS & HYVINVOINTI

# Infotilaisuus tietoturvallisten käyttöympäristöjen vaatimuksista 7.10.2020

**HEIKKI LANU, ICT-PÄÄLLIKKÖ**

FINDATA

# TIETOTURVALLINEN KÄYTTÖYMPÄRISTÖ

Määräyksen rakenne ja tarkoitus

- Tekninen, organisatorinen ja fyysinen tietojen käsittelyn toimintaympäristö
- Tietoturvallisuus varmistettu asianmukaisin hallinnollisin ja teknisin toimin
- Osa toisiolain määrittämää ICT-kokonaisuutta. Muita teknisiä ratkaisuja edellyttäviä palveluita ovat
  - Neuvontapalvelu
  - Tietopyyntöjen hallintajärjestelmä
  - Tietoturvallinen käyttöpalvelu
  - Tietojen kokoamis-, yhdistämis- ja esikäsittelypalvelu
  - Tunnisteiden hallinnointipalvelu
  - Aineistoeditori ja -katalogi
  - ICT-infrastruktuuri (sis. tunnistusratkaisut, lokienhallinta jne.)

FINDATA

# Määräyksen rakenne ja tarkoitus

## MÄÄRÄYKSEN RAKENNE

Määräys

- Tausta, soveltamisala, voimassaolo ja muutokset, sovelletut oikeusohjeet

Liite 1

1. Yleistä
2. Tekniset vaatimukset
3. Toimijan luotettavuus
4. Tietoturvalliseen käyttöympäristöön liittyvät keskeiset prosessivaiheet

FINDATA

Määräyksen rakenne ja tarkoitus

## SOVELTAMISALA

- Kaikki toisiolaissa säädetyt käyttötarkoitukset, joihin tarvitaan tietolupa:
  - Tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä
  - Opetuksen osalta määräys koskee opetusaineiston valmistamista, ei varsinaista opetusta.
- Määräyksen vaatimusten toteuttaminen edellytyksenä, että tietoaineistoja voi luovuttaa luvansaajan käsiteltäväksi muussa kuin Findatan käyttöympäristössä 1.5.2021 alkaen.
- Vaatimusten toteutuminen todennetaan tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Arvioinnista säädetään toisiolain 26 §:ssä.

FINDATA

Määräyksen rakenne ja tarkoitus

## MIKSI MÄÄRÄYS ON ANNETTU?

- Määräyksen ensisijainen tarkoitus on antaa kriteerit tietoturva-auditoinnille.
  - Palveluntarjoajilla on nyt mahdollisuus ryhtyä valmistelemaan omia toisiokäyttöön suunnittelemiaan käyttöympäristöjä vaatimusten mukaisiksi.
- Tietoturvavaatimuksilla pyritään varmistamaan, ettei salassa pidettäviä tietoja paljastu oikeudettomasti.
  - Edellyttää palveluntarjoajalta riittäviä turvallisuusjärjestelyitä.
- Toisiolaki velvoittaa antamaan määräyksen.

FINDATA

Yleistä tietoturvallisen käyttöympäristön vaatimuksista

## TODISTUS SIIS VAADITAAN

- Tietoturvallisella käyttöympäristöllä varmistetaan toisiolain nojalla luovutettujen tietojen tietoturvallinen, luvan mukainen käsittely.
- Viranomainen saa luovuttaa tietoaineistot hakijalle vain, jos käyttöympäristö täyttää 20 §:n 2 momentissa ja 21–29 §:ssä säädetyt edellytykset.
- Arvioinnin toteuttava ja todistuksen myöntävä tietoturvallisuuden arviointilaitos arvioi omalla ammattitaidollaan, soveltuvatko tietoturvallista käyttöympäristöä koskevat, voimassa olevat tietoturvallisuuteen liittyvät sertifikaatit määräyksessä esitettyjen vaatimusten täyttämisessä.

FINDATA

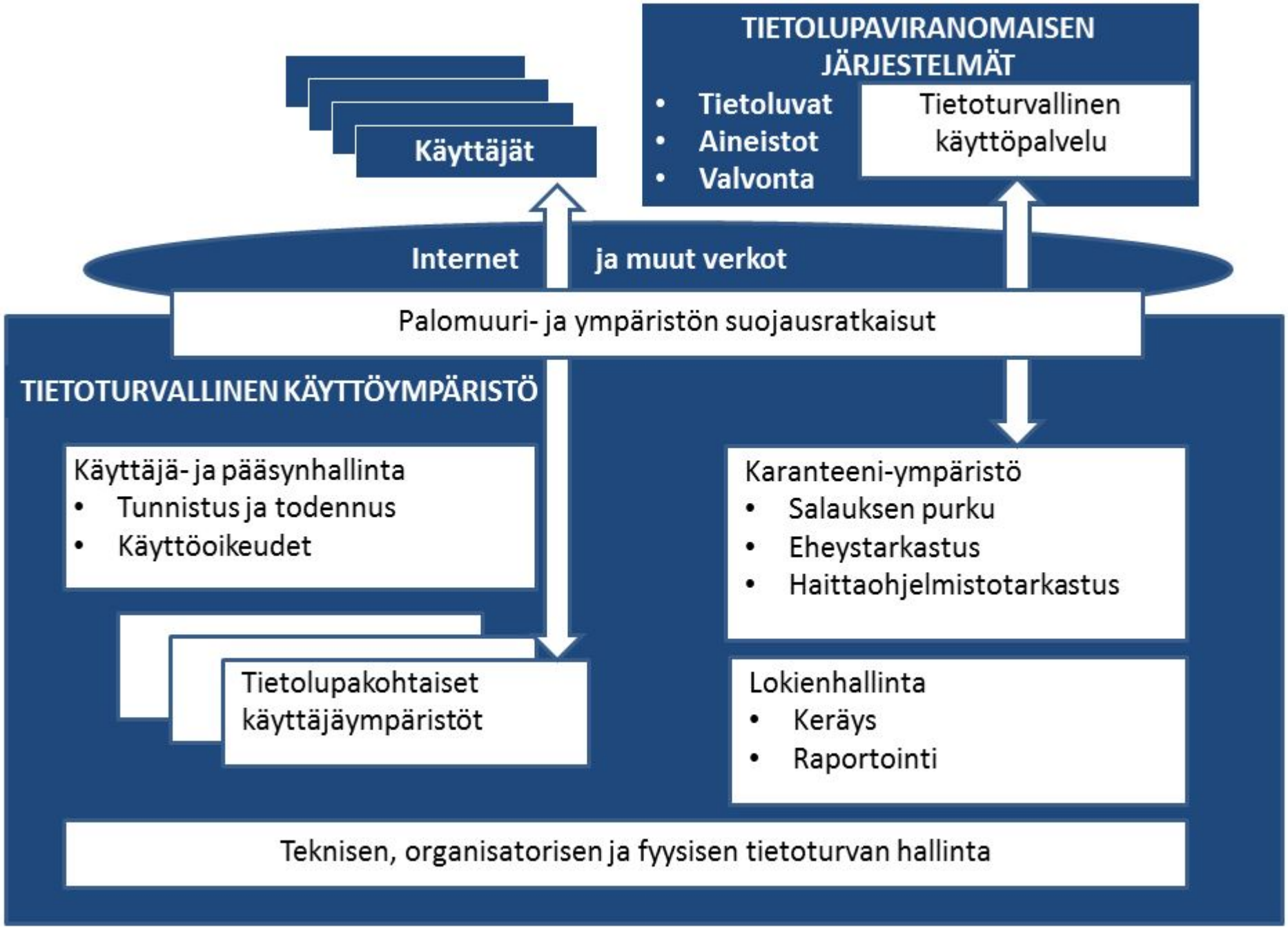
Yleistä tietoturvallisen käyttöympäristön vaatimuksista

## TÄRKEIMPIÄ TOIMINNALLISUUKSIA

- Käyttäjäympäristöön kirjaudutaan luotettaviksi arvioitujen tunnistuslähteiden tunnuksilla.
- Käyttäjäympäristöön kirjautumisessa käytetään pääsääntöisesti kaksivaiheista tunnistautumista.
- Käyttäjäympäristössä asiakas saa käyttöönsä vain kyseisen tietoluvan mukaiset aineistot.
- Mikäli asiakkaalla on useampia tietolupia, mahdollisuus käsitellä käyttäjäympäristössä vain yhden tietoluvan aineistoja kerrallaan
- Henkilötietoaineistojen siirto tietoturvalliseen käyttöympäristöön tapahtuu tietoturvallisesti.
- Käyttäjäympäristöön ei ole mahdollista muodostaa suoria Internet-yhteyksiä.
- Tunnisteellisten henkilötietoaineistojen käsittely on pystyttävä suojaamaan erityisen huolellisesti kaikissa käsittelyn vaiheissa.
- Lokienhallinta tulee tapahtua suojatussa ympäristössä, johon ei ole mahdollista muodostaa suoria Internet-yhteyksiä.

FINDATA

# Periaatteellinen järjestelmä-arkkitehtuuri



FINDATA

Yleistä tietoturvallisen käyttöympäristön vaatimuksista

## MITEN VAATIMUKSET VOI ESIMERKIKSI TÄYTTÄÄ

- Yksinkertaisimmillaan fyysisesti ja teknisesti suojattu tila, jossa on Internetistä ja muista laitteista eristetty päätelaite tietojen analysointiin.
- Myös pilvipalveluihin perustuvat tekniset ratkaisut ovat mahdollisia, kunhan palveluntarjoaja huolehtii vaatimusten mukaisesta tietoturvasta.
- Ensisijaisen käytön ympäristö harvoin sellaisenaan täyttää toisiokäytölle asetettuja vaatimuksia, koska fyysiset, organisatoriset ja tekniset ratkaisut ovat suunniteltu erilaisille käyttötapauksille.

Palveluntarjoaja vastaa siitä, että tietoturvallinen käyttöympäristö ja tuottamiseen osallistuvat osapuolet noudattavat vaatimuksia.

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## TUNNISTAUTUMINEN

- Käyttäjän ensitunnistaminen ensisijaisesti vahvalla sähköisellä tunnistamisella, henkilöllisyydestä varmistuttava
- Tunnuksien haltijoilla ja tunnistuslähteen välillä oltava sopimussuhde
- Jos yhteys muodostetaan fyysisesti ja teknisesti suojatun alueen ulkopuolelta, on käyttäjätunnistuksen oltava vähintään kaksivaiheinen
- Sovelletaan KATAKRI:n kohtia I 06 ja I 07 (mainitut toteutusesimerkit)

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## KÄYTTÄJIEN JA KÄYTTÖOIKEUKSIEN HALLINTA

- Pääsy vain yhteen tietoluvan mukaiseen aineistoon samanaikaisesti
- Käyttöoikeudet myönnetään vähimpien oikeuksin periaatteella
- Tunnistuslähteeseen on voitava luottaa
- Käyttöoikeudet käyttäjäympäristöön voimassa vain tietoluvan määrittämän ajan
- Aineistot poistettava käyttöympäristöstä viimeistään 6 kk kuluttua ellei muuta määrätä
- Sovelletaan KATAKRI:n kohtaa I 06 (mainitut toteutusesimerkit)

FINDATA

# Tekniset vaatimukset ja toimijan luotettavuus

## YMPÄRISTÖN SUOJAAMINEN

- Pääsynhallintaympäristö, karanteeniympäristö ja käyttäjäympäristö tulee suojata KATAKRI I 01 Suojaustaso IV mukaisesti
- Tarkennuksia
  - Käyttäjäympäristö on eriytetty Internetistä palomuuriratkaisulla
  - Ulkoa tulevat yhteydet varmistetaan 2-vaiheisella kirjautumisella
  - Käyttäjäympäristöön ei sallita suoria yhteyksiä käyttäjän päätelaitteelta
  - Eri tietolupien käyttäjäympäristöt pitää olla eriytettyinä toisistaan
  - Käyttäjille ei myönnetä ylläpito-oikeuksia käyttöympäristön koneisiin
- Suojaamisessa sovelletaan Vähimmäistoimintojen ja vähimpien oikeuksien sekä Monitasoisen suojaamisen periaatetta (KATAKRI useita)
- Aineistojen siirto rekisterinpitäjän oman ympäristön sisällä on mahdollista
- Ohjelmistohaavoittuvuudet ja skannaukset (KATAKRI I 23, esimerkit 1-2)

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## LOKITUS

- Lokitietoja tulee käsitellä samalla tietoturvallisella tavalla kuin erityisiin henkilötietoryhmiin kuuluvia henkilötietoja
- Käyttölokeihin on tallennettava tieto
  - tietoluvan saaneesta rekisterinpitäjästä
  - toisiolain mukaisesta käyttötarkoituksesta
  - käsittelyyn oikeuttavasta tietoluvasta
  - tietojen käsittelyyn tietoluvan mukaan oikeutetusta käyttäjästä
  - käsitellyistä tiedoista ja tietoryhmistä
  - käyttöajankohdasta
- Teknisiä lokitietoja tulee kerätä kattavasti, ratkaisu on suojattu ja seurannassa
- Sovelletaan KATAKRI I 10 -ohjeistusta (Toteutusesimerkit 1-7)
- Lupakohtaiset aineistojen käyttölokitiedot ja käyttäjärekisterit on toimitettava Tietolupaviranomaiselle sen pyynnöstä

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

# YMPÄRISTÖN HALLINTA JA VALVONTA (1/2)

- Käyttöympäristö on dokumentoitu ja automaattisessa valvonnassa
- Erityinen huomio tietoturvan valvontaan ja varmistamiseen KATAKRI I 11 soveltaen
- Käyttöympäristön hallinta tulee tehdä tietoturvan osalta kovennetulta työasemalta salatulla tietoliikenneyhteydellä siihen soveltuvista tiloista
- Käyttöympäristön palvelimien tulee sijaita suojatuissa tiloissa, noudattaen KATAKRI F 01 ohjeita
- Käyttöympäristön ylläpitokäyttöoikeuksien tulee olla henkilökohtaisia, erikseen työtehtävien mukaan määriteltyjä käyttöoikeuksia
- Käyttöympäristön ylläpitokäyttöoikeuksissa noudatetaan vähimpien oikeuksien periaatetta KATAKRI I 06 (esimerkit 1-10) sekä monitasoisen suojaamisen periaatetta KATAKRI I 07 (esimerkit 1-7)

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

# YMPÄRISTÖN HALLINTA JA VALVONTA (2/2)

- Käyttöympäristön hallinnassa ja valvonnassa noudatetaan KATAKRI I 03 ja I 04 -osiota soveltuvilta osin
- Käyttöympäristön muutoshallinnassa sovelletaan KATAKRI I 20 (Toteutusesimerkin kohdat 1-3) osiota soveltuvilta osin
- Myös tietoturvallisen käyttöympäristön ylläpitäjien toimet on sisällytettävä lokienhallintaan
- Jos epäillään, että tietojen käsittely on lain tai myönnetyn tietoluvan ehtojen vastaista, on palveluntarjoajalla oltava kyky viivyttelemättä ilmoittaa asiasta

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## AINEISTOJEN POISTO KÄYTTÖYMPÄRISTÖSTÄ

- Aineistot tulee poistaa käyttöympäristöstä 6 kk tietoluvan päättymisen jälkeen, ellei tietoluvassa ole toisin määrätty
- Aineiston poistossa tulee noudattaa KATAKRI I 19 -ohjeistusta (Toteutusesimerkin kohdat 2 ja 3)
- Aineistojen säilytyksessä on huomioitava mahdolliset tietoluvassa asetetut ehdot

FINDATA

# Tekniset vaatimukset ja toimijan luotettavuus

## TOIMIJAN LUOTETTAVUUS

- Tietoturvallisen käyttöympäristön on fyysisesti sijaittava EU/ETA-alueella
- Tietoturvallisen käyttöympäristön palveluntarjoajan on oltava EU/ETA-alueella rekisteröity organisaatio
- Palveluntarjoajan luotettavuus tulee voida arvioida PiTuKri Luku "Palvelun tuottaminen" (s. 12) soveltaen
- Palveluntarjoajan on osoitettava luotettavuus turvallisuuden hallintajärjestelmällä, esimerkiksi ISO/IEC 27001 -standardin mukaisesti
- Tarkastuksen suorittamiseksi tarkastajalla on oikeus päästä kaikkiin tiloihin. Vaatimus koskee myös palveluntarjoajan käyttämiä alihankkijoita

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## TIETOSUOJA

- Käyttöympäristöstä on oltava laadittuna EU:n yleisen tietosuoja-asetuksen (GDPR) 35 artiklan mukainen tietosuojaa koskeva vaikutustenarviointi (DPIA).
- Rekisterinpitäjää ja henkilötietojen käsittelijää koskevat velvoitteet ja sopimukset ovat huomioitu tietosuoja-asetuksen voimassa olevien ohjeiden mukaisesti. Asetus ei sisällä ohjeita vaan se velvoittaa suoraan.
- Palveluntarjoaja vastaa siitä, että käyttöympäristöön sekä käyttäjäympäristöön siirrettävät ja siellä käytettävät ohjelmistot, koodit tai muut sellaiset eivät vaaranna henkilötietojen käsittelyn tietoturvallisuutta.
  - Erityisesti on varmistettava ettei käyttäjäympäristöstä siirry ulos henkilötietoja muulla tavoin kuin mitä aineistojen siirrosta on määrätty.

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## TOIMITILAT

- Ympäristön ylläpito tulee tehdä tiloista, jotka ovat tietoturvallisuuden arviointilaitoksen hyväksymät
- Ympäristön palvelimet tulee olla tiloissa, jotka ovat tietoturvallisuuden arviointilaitoksen hyväksymät
- Toimitilaturvallisuuden osalta noudatetaan KATAKRI:n fyysisen turvallisuuden arviointikriteeristöä F 01-08 soveltuvin osin

FINDATA

Tekniset vaatimukset ja toimijan luotettavuus

## HENKILÖSTÖ

- Käyttöympäristön ylläpitotehtävissä toimiville henkilöille, joilla on pääsy henkilötietoaineistoihin, tulee olla tehtynä perusmuotoinen turvallisuusselvitys tai muu vastaava viranomaisselvitys
- Henkilöstö, jolla on pääsy henkilötietoaineistoihin, tulee olla perehdytetty aineistoja koskeviin käsittelyohjeisiin
- Henkilöstöturvallisuuden osalta noudatetaan KATAKRI T 08-12 -osioita soveltaen

FINDATA

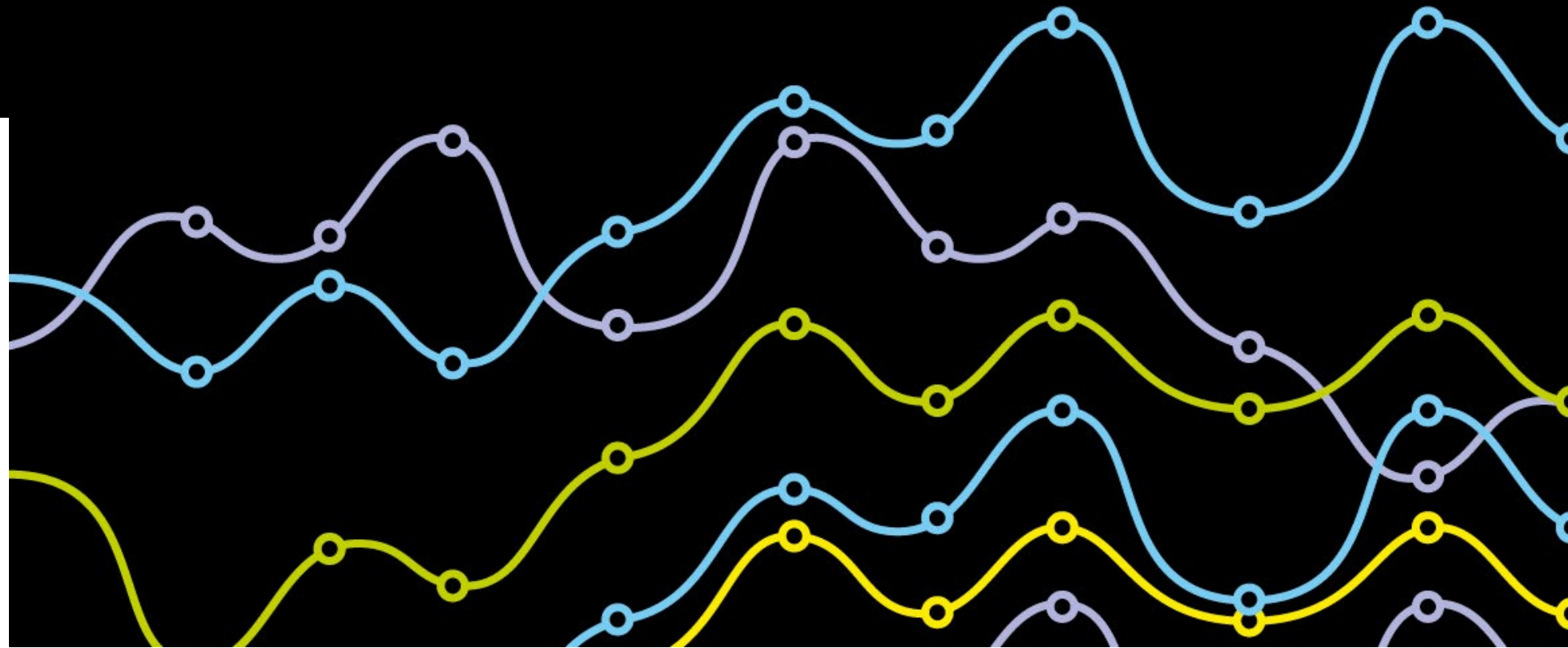
Tietoturvalliseen käyttöympäristöön liittyvät keskeiset prosessivaiheet

## PALVELUNTARJOAJAN TEHTÄVIÄ TIIVISTETTYNÄ

- Vaatimustenmukaisuuden varmistaminen
- Tietoturvallisen käyttöympäristön käytön seuranta ja arviointi
- Neuvonta, käyttäjäympäristön tilaus/toimitus
- Käyttäjä- ja käyttöoikeushallinnan toimet
- Aineistojen ja tuotosten siirrot
- Muutostilaukset
- Käyttäjäympäristön käytön lopetus

FINDATA

# Keskustelu



FINDATA

# Esityksen aikana tulleet kysymykset ja vastaukset

1) Miksi puhutaan tietopyyntöjen hallintajärjestelmästä, vaikka toisiolaissa tietopyynnöillä tarkoitetaan aggregaattiaineistoja?

- Hyvä huomio! Termi tulee suoraan toisiolaista, sillä tarkoitetaan siinä "järjestelmää, jonka välityksellä tietoluvan hakija tai tietoja tämän lain perusteella muutoin pyytävä toimittaa tietolupahakemuksen tai tämän lain mukaisen tietopyynnön ja sen liitteet viranomaiselle ja jossa tietolupaa tai tietopyyntöä koskeva päätös annetaan tiedoksi luvan hakijalle".

2) 1.1. kohta 4: Saako tietoturvallisesta käyttöympäristöstä päästä rajoitetusti Internetiin esim. proxy-palvelimen kautta? Use caseina siis käyttöympäristön käyttöjärjestelmän ohjelmistopäivitykset ja tutkijan analyysityökalujen uusien versioiden asennus.

- Kyllä, mutta suoraa yhteyttä ei saa olla. Tällä pyritään estämään se, ettei esim. ympäristön asetuksia pääse konfiguroimaan taho, jolla siihen ei ole oikeutta. Aineistojen ja ohjelmistojen yms. siirroissa on huomioitava, mitä käyttöympäristön hallinnasta on määrätty.

3) Oletteko ajatelleet fyysisen tilan suojauksien lisäksi virtuaalisen tilan suojauksia?

- Jos kysymys tarkoittaa virtualisointiteknologialla toteutettua tietoteknistä ympäristöä, niin määräys ei ota suoraan kantaa asiaan, mutta määräyksen vaatimukset ovat sovellettavissa myös tuon kaltaiseen toteutukseen, vrt. pilvialustat.

4) 1.1. kohta 3: Miten karanteeniympäristön vaatimus "ei saa olla yhteyttä Internetiin" toimii yhdessä haittaohjelmatarkastuksen kanssa? Onko signature-based-haittaohjelmantunnistus kokonaan poissa laskuista, koska sehän vaatii luotettavasti toimiakseen yhteyden Internetiin haittaohjelmakuvausten päivittämistä varten.

- Haittaohjelmatorjunta pitää olla tietysti ajan tasalla, mutta se ei voi olla suorassa yhteydessä internetiin, vaan päivitykset ynnä muut pitää tapahtua muulla tavoin.

5) 2.3.2. kohta 3d. Mitä tällä tarkalleen tarkoitetaan? Onko SSH-yhteys sallittu? Entä etätyöpöytäyhteyden leikepöytätoiminto?

- Tähän vaatimukseen on olemassa monta ratkaisua. Asiaa on käsitelty Katakri I 01 kohdassa.

6) 3.4.1. johdanto: Mitkä ovat juridiset perusteet perusmuotoisen turvallisuusselvityksen vaatimukselle? Siis mihin turvallisuusselvityslain 19 § kuudesta vaihtoehdosta tämä vaatimus perustuu ja miksi? Kysyn tätä sen vuoksi, että perusmuotoinen turvallisuusselvitys puuttuu merkittävästi palveluntarjoajan työntekijän yksityisyydensuojaan ja siksi sen vaatimiselle pitää olla painavat perusteet.

- Edellytykset perusmuotoisen turvallisuusselvityksen laatimiselle on toki asetettu varsin korkealle turvallisuusselvityslaissa. Säännöksen (19 §) kohta 1 toimii tässä lähimmin perustana. Findata voi tähän asiaan vielä palata

- tarkemmin. On hyvä huomata se, että toisiolaissa säädetään, että muun käyttöympäristön vaatimukset tulee asettaa/niiden tulee täyttää sama turvataso kuin mikä on Findatan käyttöympäristössä. Kuten Heikki Lanu totesi, kyse on muustakin kuin ympäristön teknisestä toteutuksesta. Findatan koko henkilöstö on perusmuotoisesti turvallisuusselvitetty. Turvallisuusselvityslaki antaa Supolle toki mahdollisuuden toteuttaa perusmuotoisena haettu turvallisuusselvitys myös suppeana.

7) Jos tietoluvassa mainitaan käyttäjähenkilöt, niin kuinka toimitaan silloin kun tapahtuu henkilövaihdoksia? Esim. uudet ihmiset projektissa

- Uusille käyttäjille myönnetään lupa käsitellä aineistoa tietoluvan muutospäätöksellä.

8) Esitetystä poiketen Valvira ei akkreditoi tietoturvallisuuden arviointilaitoksia. Tämä tapahtuu Traficomin Kyberturvallisuuskeskuksessa.

- Ok, kiitos tarkennuksesta! Valvira tosiaan ylläpitää julkista rekisteriä sille ilmoitetuista vaatimukset täyttävistä käyttöympäristöistä, ja Valviralla tai sen osoittamalla ulkopuolisella asiantuntijalla on oikeus tehdä valvonnan edellytyksenä olevia tarkastuksia.

9) Ei suoria nettiyhteyksiä = Käyttäjä ei voi päivittää paketteja/asentaa uusia a priori speksattuun ympäristöön? Tai voi, mutta pitää kikkailla manuaalisesti?

- Asennukset vaativat ylläpitäjän oikeuksia ja siihen liittyen on esitetty omat vaatimukset. Käyttäjällä ei saa olla ylläpitäjän oikeuksia.

10) Lokienhallinnan tulee määräyksen mukaan tapahtua ympäristössä, johon ei ole mahdollista muodosta suoria Internet-yhteyksiä. Sulkeeko tämä pois julkiset pilvipalvelut, joiden kattavat lokipalvelut ovat autentikoitujen ylläpitäjien käytettävissä suoraan?

- Lokienhallinnan ratkaisu täytyy olla toteutettu tietoturvallisessa ympäristössä. Lokitietoihin pääsy pitää olla rajattu vain ylläpitäjätasoisille henkilöille noudattaen vaatimuksia.

11) Kuinka toimitaan 1.5.2021 alkaen niiden valmiiksi koottujen aineistojen suhteen, jotka jo ovat toimijoiden omilla palvelimilla analysoitavana? Saako ko. datoja edelleen analysoida voimassa olevan käyttöluvan puitteissa omissa ympäristöissä?

- V. Vaatimus ei tule takautuvasti voimaan. Eli jo luvan saaneiden hankkeiden osalta voidaan jatkaa ko. ympäristössä, auditointivaatimus ei tule takautuvasti voimaan. Ajankohtainen tieto muutoshakemuksista löytyy Findatan verkkosivuilta.

12) Määräyksessä viitataan Katakri I 01 kohtaan. Toteutusesimerkin kohdassa 3 mainitaan, että liikenneyhteydet salataan viranomaishyväksytyllä salausratkaisulla. Tarkoitetaanko tällä NCSA.FI:n salausratkaisut-dokumentin taulukkoa 3.3.? Ensisilmäyksellä ei vaikuta siltä, että hyväksytyissä salausratkaisuissa olisi yleisen pilvipalveluntarjoajan pilveen sopivaa hyväksyttyä salausratkaisua. Olenko tässä väärässä vai miten tämä kohta saadaan määräyksen täyttävä ratkaisu rakennettua?

- Tässä kannattaa kääntyä viranomaistoiminnan salausratkaisuja tuntevan asiantuntijan puoleen.

13) Olisiko mahdollista saada jonkinlainen, esimerkinomainen speksi/arkkitehtuurikuva riittävän hyvästä analyysiympäristöstä toteutettuna AWS:ssä tai GCP:ssä? Käyttötapauksena vaikka rintasyöpäpotilaiden survivalin laskeminen siten, että yhdistetään kahden sairaalan dataa tilastokeskuksen kuolinsyydataan? Tällainen auttaisi hahmottamaan kokonaiskuvaa

- Teknisissä ja tuotteisiin/palveluihin liittyvissä ratkaisuissa on syytä kääntyä niihin perehtyneiden asiantuntijoiden puoleen.

14) Onko tietoa kuinka moni taho on rakentamassa omaa tietoturvallista ympäristöä? Onko ympäristöjen akkreditointia tekevällä taholla kapasiteettia suoriutua kaikkien eri ympäristöjen läpivalaisusta 1.5.2021 mennessä? Kauanko yhden ympäristön läpikäynti kestää ja paljonko se maksaa?

- Meillä ei ole tietoa, arviointilaitokset ovat parhaita vastaamaan tähän.

15) Käytäntö on osoittanut, että 6kk on lyhyt aika yksinkertaisellekin tutkimusprojektille. Pelkkä  vertaisarviointivaihe julkaisuun voi kestää noin kauan. Millainen prosessi käytännössä on pidentää ko. aikaa?

- Vertaisarviointivaihe on syytä ottaa huomioon jo lupaa hakiessa / luvan pituudessa. 6 kk rajan tarkoituksena on, ettei arkaluontoisia aineistoja jää lojumaan käyttöympäristöihin.

16) Onko tarkoituksellista, että määritelmä ("Käyttäjä- ja pääsynhallinnalla tarkoitetaan ratkaisua, joka sijaitsee varsinaisen tutkimusympäristön ja Internetin välissä, ja jolla suoritetaan käyttäjien tunnistaminen ja toteutetaan pääsynhallintaa.") rajaa IAM järjestelmän sijainnin tarkkaan? Lisäksi määritelmä ei kata käyttövlatuushallinnan hallinnollista prosessia.

- Asia on kerrottu toiminnallisuuden näkökulmasta ottamatta kantaa IAM-ratkaisun tekniseen ja fyysiseen toteutukseen. Käyttäjien tunnistus sekä mihin ja mitä oikeuksia käyttäjillä on kuuluu käyttöympäristön oleellisiin toiminnallisuuksiin. Järjestelmäarkkitehtuuri on esitetty periaatteellisella tasolla, jonka tarkoituksena on havainnollistaa keskeisiä käyttöympäristöön liittyviä komponentteja.

17) 'Aineisto on poistettava 6kk sisällä'. Tarkoitetaanko vain alkuperäistä aineistoa, vai myös alkuperäisestä koottuja tietoja. Esim. Frekvenssejä tiettyjen ehtojen perusteella?

- 6 kk sääntö koskee  käyttäjäympäristöön siirrettyä aineistoa tietoluvan päätyttyä.

18) Vaaditaanko virustarkastuksia kaikissa ympäristöissä? Esim. jos käytössä on unix/linux-pohjaisia palvelimia?

- Kyllä. Kaikissa käyttöjärjestelmissä on haavoittuvuutensa.

19) Pitääkä myös tällä hetkellä ja ennen 1.5. käytössä olevat, aineistoja sisältävät tietoluvan omaavat käyttöympäristöt auditoida 1.5. mennessä? Entä jos ei läpäise auditointia?

- Ei pidä, ellei tätä halua, eli vaatimus ei tule takautuvasti voimaan. 1.5.2020 lähtien myönnetyillä tietoluvilla ei saa aineistoja siirtää muihin kuin todistuksen omaaviin käyttöympäristöihin.

20) Eli vaaditaanko ISO/IEC 27001 standardi palveluntarjoajalta vai ei?

- Ei. Määräyksessä edellytetään palveluntarjoajalta sellaista tietoturvallisuuden hallintajärjestelmää, jolla pystyy osoittamaan auditoijalle luotettavuutensa.

21) Edellytetäänkö ISO 27001 -sertifiointia 1.5.2021? Tai muuta todistetta hallintajärjestelmästä?

- Sertifiointia ei edellytetä. Määräyksessä edellytetään palveluntarjoajalta tietoturvallisuuden hallintajärjestelmää, jolla pystyy osoittamaan auditoijalle luotettavuutensa.

22) Yleisenä kommenttina on ikävää, kun laaditaan lakeja, joita ei voi noudattaa (liittyen esim. tähän pilvipalvelun "tilojen tarkastukseen")

- Palveluntarjoaja voi käyttää alihankkijoita esimerkiksi tietoteknisten palveluiden tuottamiseksi, mutta palveluntarjoaja vastaa aina tietoturvallisen käyttöympäristön vaatimustenmukaisuudesta. Käytännössä palveluntarjoajan ja käytettävän alihankkijan välillä on oltava sitova sopimussuhde. Arvioinnin toteuttava ja todistuksen myöntävä tietoturvallisuuden arviointilaitos arvioi omalla ammattitaidollaan, soveltuvatko tietoturvallista käyttöympäristöä koskevat, voimassa olevat tietoturvallisuuteen liittyvät sertifikaatit määräyksessä esitettyjen vaatimusten täyttämisessä.

23) Eikö ylläpito ole mahdollista etätyönä?

- Käyttöympäristön ylläpito tulee tehdä siihen soveltuvista tiloista ja jotka ovat tietoturvallisuuden arviointilaitoksen hyväksymät. Lisäksi hallinta tulee tehdä tietoturvan osalta kovennetulta työasemalta salatulla tietoliikenneyhteydellä. Asiaa on käsitelty Katakri I 04 kohdassa.

24) Siis mahdollistaako tämä koko homma nyt esim. Googlen tai Amazonin pilven käytön? kyllä [ ] ei [ ]

- Kyllä, mikäli sopimuksissa ja toteutuksessa on huolehdittu, että määräyksen vaatimukset toteutuvat. On tärkeää huomata, että palveluntarjoajan roolissa toimivalla taholla on huolehdittavana useita tehtäviä, joita pilvipalveluntarjoaja ei todennäköisesti pysty/halua toteuttaa.

25) Viitataanko toimitilaturvallisuudella käyttöympäristöön vai myös loppukäyttäjien ympäristöihin ja tiloihin?

- Käyttöympäristön toimitilaturvallisuuteen.

26) Mitä tulee Valviran valvontaoikeuksiin: toisiolaissa ei aseteta käyttöympäristön "ylläpitäjälle" mitään velvollisuutta sisällyttää palveluntarjoajan kanssa tehtyyn sopimukseen velvoitetta Valviran valvonta- ja tarkastusoikeuksista. Toisiolaissa todetaan ainoastaan, että Valviralla on tämä oikeus. Jos palveluntarjoaja on toisessa ETA-maassa, toisiolaissa Valviralle annettu tarkastusoikeus on itsessään merkityksetön, ellei esim. EU-oikeuden kautta tule lisätukea.

- Tietoturvallisella käyttöympäristöllä on oltava nimetty palveluntarjoaja, joka on vastuussa tämän määräyksen vaatimusten toteuttamisesta. Palveluntarjoaja voi käyttää alihankkijoita esimerkiksi tietoteknisten palveluiden tuottamiseksi, mutta palveluntarjoaja vastaa aina tietoturvallisen käyttöympäristön vaatimustenmukaisuudesta. Käytännössä palveluntarjoajan ja käytettävän alihankkijan välillä on oltava sitova sopimussuhde.

27) Estääkö määräys kokonaan esimerkiksi Googlen pilvipalvelun käytön?

- Ei, mutta sopimuksissa ja toteutuksessa tulee huolehtia, että määräyksen vaatimukset toteutuvat. Erityistä huomiota kannattaa kiinnittää palveluntarjoajan vastuisiin.

28) Kohdassa 3.3 mainitaan että ympäristön ylläpito tulee tehdä arviointilaitoksen hyväksymistä tiloista. Kuinka tämä suhteutuu aiemmin kohdassa 2.5.1 mainittuun, että käyttöympäristön ylläpito tehdään siihen soveltuvista tiloista? Ylläpitäjien etätyöskentely on siis mahdollista vain tällaisista hyväksytyistä tiloista?

- Ylläpitotoimet edellyttävät erityistä huomiointia. Taustalla on olettamus, että hallintayhteydellä on mm. mahdollisuus pääsyyn käyttöympäristössä sijaitseviin kaikkiin henkilötietoaineistoihin. Auditoija arvioi tilojen soveltuvuuden vaatimuksiin nähden. Tässä noudatetaan KATAKRI:n fyysisen turvallisuuden arviointikriteeristöä F 01-08 soveltuvin osin. Vaatimukset ovat varsin konkreettisia ja selkeitä, kuten esimerkiksi ‘‘salassa pidettävää tietoa käsitellään siten, ettei tieto näy asiattomille’’.

29) Miten etätyö ja tutkimus on tarkoitus hoitaa tämän määräyksen osalta. Tämä tehokkaasti lopettaa kaiken tutkimuksen näin korona aikana.

- Määräys ei aseta käyttäjän sijainnille rajoituksia. Ylläpito- ja hallintatoimiin tulee kiinnittää erityistä huomiota.

30) Tulkinnan mukaan jokainen SHP luokitellaan määräyksessä palveluntarjoajaksi. Onko arvioitu vaatimusten toteuttamisen kustannuksia ja toteuttamis mahdollisuuksia ylipäätään?

- Laki edellyttää toisiokäytössä noudatettavan varsin tiukkoja tietoturvavaatimuksia. Määräys ei koske ensisijaisen käytön ympäristöjä. Toisiokäytön käyttöympäristön voi toteuttaa monella tavalla ja kustannukset riippuvat paljolti siitä minkälaista ratkaisua palveluntarjoaja tavoittelee.

31) Millaiset vaatimukset on kansainväliselle toimijalle, jos suomalaisten potilaiden dataa luovutetaan ulkomaille tutkimusyhteistyöhön?

- Määräys koskee myös ulkomaisia toimijoita. Mikäli suomalaista dataa on välttämätöntä siirtää ulkomaiseen, tietoturvalliseen käyttöympäristöön, sen tulee toteuttaa vaatimukset ja siitä pitää olla todistus.

32) Aws:stä ja GPC:stä kysyttiinkin jo. Samat kysymykset myös Azureen liittyen. Olisi ikävää rakentaa pilvipohjainen ratkaisu ja kuulla 30.4.2021, että ei kelpaa.

- Tietoturvallisuuden arviointilaitos on oikea taho kertomaan, onko jokin tekninen suunniteltu tai toteutettu ratkaisu mahdollinen. Määräys ei ota kantaa tekniseen ratkaisuun, vaan tarjoaa kriteerit auditointiin. Auditointiin kannattaa varautua suunnitelmallisesti ja tarvittaessa käyttää asiantuntija-apua.

33) Leikepöydästä vielä. Tietoa ei saa siirtää ulos järjestelmästä käyttäjän toimesta, mutta saako käyttäjä tuoda tietoa järjestelmään (esimerkiksi analysointiin käytettäviä koodipätkiä yksisuuntaisen leikepöydän kautta)

- Määräyksellä ei ole tarkoitus rajoittaa käyttötapauksia vaan kertoa vaatimukset sillä tasolla, että erilaiset toteutusratkaisut ovat mahdollisia. Perusperiaate on, että palveluntarjoaja vastaa siitä, että käyttöympäristöön sekä käyttäjäympäristöön siirrettävät ja siellä käytettävät ohjelmistot, koodit tai muut sellaiset eivät vaaranna henkilötietojen käsittelyn tietoturvallisuutta. Viimekädessä auditoija arvioi käytettävän ratkaisun.

34) Jos on omilla palvelimila vanhoja jo koottuja aineistoja, joiden käyttölupaa haluaisi päivittää 1.5.2021 jälkeen, voiko käsittelyä edelleen jatkaa omissa ei-auditoiduissa vanhoissa ympäristöissä? Esim. jos lisätään uusia tutkijoita tai pidennetään käyttölupia. Vai täytyykö tässä vaiheessa koko data siirtää auditoituun ympäristöön? Uutta dataa ei siis kerättäisi.

- Voi jatkaa, ellei halua siirtää aineistoja auditoituun ympäristöön. Vaatimus ei tule takautuvasti voimaan.

35) Onko mahdollista saada chatissa esitetyt kysymykset ja vastaukset niihin kirjallisesti?

- Kyllä, lisäämme ne esitysmateriaalien loppuun.

36) Onko diat mahdollista saada?

- Kyllä (kts. edellinen kommentti)

37) Ovatkohan esimerkiksi kaikki 310 kuntaa ja kaikki yksityiset sote-palveluntuottajat nyt kartalla siitä, että eivät voi luovuttaa aineistoja muualle kuin tietoturvallisiin käyttöympäristöihin 1.5.2021 alkaen.

- Hankala sanoa. Toisiolaki on ollut voimassa 1.5.2019 asti ja toimijoiden tulisi toki olla tietoisia omista lakisääteistä velvoitteistaan. Findata välittää omalta osaltaan tietoa päivittäin eteenpäin ollessaan yhteydessä rekisterinpitäjiin ja asiakkaisiin.

38) Aineiston säilyttämisestä: Kirsin mainitsemien lakisääteisten velvollisuuksien lisäksi tutkimuksien julkaisu täysin säännönmukaisesti edellyttää, että tutkimusaineisto on olemassa mahdollista muiden tahojen suorittamia varmistustutkimusta varten. Käytännössä tutkimusaineistojen poistaminen johtaa siihen, että suomalaista tutkimusta ei enää voi julkaista tiedejulkaisuissa. Olisiko kuitenkin järkevämpää luoda jokin tietoturvallinen arkistointijärjestelmä näitä tilanteita varten? Siksi toisekseen, on älytöntä resurssien haaskausta jos Hanke A on käyttänyt paljon aikaa ja resursseja jonkin rekisteriaineiston jalostamiseen ja jos Hanke B haluaa käyttää samaa aineistoa, Hankkeen B pitää tehdä sama työ kokonaan uudelleen.

- Tutkimusta varten toimitettujen aineistojen käsittelyaika ja käsittelijät määräytyy tietoluvan voimassaoloajan ja siinä mainittujen henkilöiden mukaan. Asia on siis syytä huomioida haettaessa tietolupaa. Tietolupaan on mahdollista hakea tarvittaessa jatkoaikaa tai tehdä henkilömuutoksia muutoshakemuksella. Varsinainen tutkimusaineisto on tietysti aina tallessa rekisterinpitäjillä ja Findatalla tarkat poimintatiedot. Eli tutkimus on aina toistettavissa samanlaisena.

39) Aineistojen käsittely Findatan omassa suljetussa verkkoympäristössä oli yksi keskeinen toisiolain läpimenon edellytyksistä: Aineiston antaminen sen ulkopuolelle on poikkeuksellista ja täytyy erikseen perustella. Millä perusteella aineistoja nyt käytännössä annetaan ulos?

- Toisiolain mukaisilla perusteilla: mikäli aineiston analysoiminen muualla on välttämätöntä. Käytännön esimerkkinä kuvantamisaineistot, jotka ovat suurikokoisia ja joiden pseudonymisointi on käytännössä mahdotonta ilman, että itse tutkimuskohde vääristyy. Myös tutkimukset, jotka ovat välttämättömiä suorittaa yhteydessä tosiaikaisesti päivittyvään suureen aineistoon ovat tapauksia, joissa tarve on ilmeinen.

40) AWS ja Google ovat USAlaisia yrityksiä, joita koskee SCHREMSII päätös. Millä perusteilla annatte käyttää niitä ilman lisätoimia käyttää edellen?

- Käytettäessä pilvipalveluita tai muita alustaratkaisuja osana tietoturvallista käyttöympäristöä, on niiden ja aineistojen sijaittava fyysisesti EU/ETA-alueella ja käyttöympäristöstä vastaavan palveluntarjoajan on varmistettava määräyksen mukaisten velvoitteiden toteutuminen käyttämiensä alihankkijoiden kohdalla. Tietoturvallisen käyttöympäristön palveluntarjoajan on oltava EU/ETA-alueella rekisteröity organisaatio.

41) Kun aineisto siirretään määräysten mukaan käyttöympäristöstä ulos, mikä on suositeltu käytännön tapa tämän siirtämiseksi tutkijan käytössä esim. etätöissä olevalle koneelle? Eli virus- ja verkkomääräykset huomioiden, muistitikku / ulkoinen kovalevy / pilvipalvelu / tms?

- Valmiit tuotokset luovutetaan anonymisoituna. Palveluntarjoaja siirtää asiakkaan valmiit tuotokset tietoturvallisen käyttöpalvelun välityksellä anonymisoinnin osalta Findatan tarkastettavaksi. Findata voi kuitenkin perustellusta syystä lupapäätöksessään myöntää luvansaajalle oikeuden toteuttaa itse julkaistavien edellä mainittujen tietojen anonymisoinnin ehdolla, että ne toimitetaan jälkikäteen Findatalle. Tähän on tulossa tarkentavaa käytännön ohjeistusta.

42) Määräyksen mukaan: Tietolupaviranomainen ylläpitää ajantasaista listaa luottamistaan tunnistuslähteistä ja julkaisee ne osoitteessa www.findata.fi. Milloin lista julkaistaan?

- Findatan luottamat tunnistelähteet julkaistaan viikon 43 aikana.

43) Miten suhtaudutaan esimerkiksi SHP.n tai yliopistosairaaloiden omaan tutkimukseen. Jos ei yhdistetä datoja minnekään vaan tehdään oman organisaation luvalla tutkimusta, pitääkö näissäkin tapauksissa data ensin siirtää auditoituun käyttöympäristöön?

- Tietolupaa edellyttävän toisiolain alaisen aineistojen käsittelyn tulee tapahtua määräyksen mukaisessa käyttöympäristössä.

44) Anonyymille: Jos esim. HUS-tutkija tekee rekisteritutkimuksen pelkästään kohdistuen HUS-rekisteriin ilman, että Findata on millään tavalla mukana, sama määräys ja vaatimuksen on voimassa.

- Tietolupaa edellyttävän toisiolain alaisen aineistojen käsittelyn tulee tapahtua määräyksen mukaisessa käyttöympäristössä.

45) Jos haluaisi tehdä tutkimusta vain yhden rekisterinpitäjän aineistossa ja tekisi tämän kyseisen rekisterinpitäjän tietoturvallisessa käyttöympäristässö tarvisiko tieto kierrättää Findatan kautta?

- Jos rekisterinpitäjällä on tarve siirtää omassa ympäristössään sijaitsevaa luvitettua aineistoa omaan, saman fyysisesti ja teknisesti suojatun alueen sisällä sijaitsevaan tietoturvalliseen käyttöympäristöön, voi siirron suorittaa myös ilman tietoturvallista käyttöpalvelua.

46) Selvyyden vuoksi: jos palvelunantaja käsittelee tietoja tietojohtamistarkoituksessa, koskeeko vaatimus  tietoturvallisesta käyttöympäristöstä myös sitä tilannetta?

- Ei. Kuten määräyksessä todetaan: määräystä sovelletaan kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin toisiolain mukaan tarvitaan tietolupa. Näitä käyttötarkoituksia ovat tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä. Opetuksen osalta määräys koskee opetusaineiston valmistamista, ei varsinaista opetusta. Tietojohtamiseen ei tarvita tietolupaa.

FINDATA

# Kiitos osallistumisesta!

Anna palautetta:
https://webropol.com/s/findata-infotilaisuus

Tallenne katsottavissa 21.10. asti