Liite 1: Tietoturvallisen käyttöympäristön vaatimukset

Sisällys

1 Yleistä

Tämä dokumentti kuvaa ja tarkentaa tietoturvavaatimukset toisiolain 20 §:n 2 momentissa ja 21 – 29 §:issä edellytetylle tietoturvalliselle käyttöympäristölle. Palveluntarjoajan edellytetään noudattavan toisiolain 18 §:n yleisiä tietoturvavaatimuksia. Tietoturvallisella käyttöympäristöllä varmistetaan toisiolain nojalla luovutettujen tietojen tietoturvallinen, lupaehtojen mukainen käsittely. Viranomainen saa luovuttaa tietoaineistot hakijalle vain, jos käyttöympäristö täyttää 20 §:n 2 momentissa ja 21–29 §:ssä säädetyt edellytykset.

Tietolupa määrittää mitä toisiolain mukaisia tietoaineistoja tietoturvalliseen käyttöympäristöön luovutetaan. Tässä määräyksessä ei aseteta käyttöympäristölle eritasoisia tietoturvavaatimuksia käyttöympäristössä käsiteltävien tietoaineistojen turvallisuusluokitusten perusteella. Jos tietoaineistot ovat turvallisuusluokiteltu tai niille on asetettu suojaustasovaatimuksia, joita käsittely-ympäristön on täytettävä, on niistä johtuvat vaatimukset huomioitava erikseen.

Tietoturvavaatimuksilla pyritään varmistamaan, että tietoturvallisen käyttöympäristön palveluntarjoajalla on riittävät turvallisuusjärjestelyt salassa pidettävien tietojen oikeudettoman paljastumisen ehkäisemiseksi. Tämä määräys ei ota kantaa tekniseen toteutukseen, ja siksi vaatimuksia on tarkasteltava tapauskohtaisesti soveltaen.

Arvioinnin toteuttava ja todistuksen myöntävä tietoturvallisuuden arviointilaitos arvioi omalla ammattitaidollaan, soveltuvatko palveluntarjoajan tietoturvallista käyttöympäristöä koskevat, voimassa olevat tietoturvallisuuteen liittyvät todistukset määräyksessä esitettyjen vaatimustenmukaisuuden osoittamiseen. Arvioitavan kohteen osat, joita olemassa oleva todistus ei kata, tulee erikseen arvioida. Arviointilaitos tarkastaa palveluntarjoajan voimassa olevan todistuksen voimassaoloajan ja asettaa tarvittaessa rajoituksen tämän määräyksen perusteella myönnettävän todistuksen voimassaoloajalle. Tietolupaviranomainen ei tee arviointia eikä tarjoa teknistä neuvontaa tietoturvallisen käyttöympäristön tietoturvallisuuteen liittyen.

Tietoturvavaatimuksissa on viitattu seuraaviin säännöksiin ja kriteeristöihin:

- Toisiolaki eli laki sosiaali- ja terveystietojen toissijaisesta käytöstä, 552/2019
- KATAKRI 2015 - Tietoturvallisuuden auditointityökalu viranomaisille
    - Suojaustasoja tai turvallisuusluokkia ei huomioida arvioinnissa vaan sovellettavat KATAKRI-vaatimukset ovat ilmoitettu arvioitavan kohteen vaatimusten yhteydessä.
- PiTuKri versio 1.1. maaliskuu 2020 - Pilvipalveluiden turvallisuuden arviointikriteeristö
    - Arviointilaitoksella on mahdollisuus perustaa arviointi PiTuKrin vaatimuksiin KATAKRI:n sijaan kohdissa, joissa se arvioitavan kohteen osalta on tarkoituksenmukaista.

- Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

- Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta

- ISO/IEC 27001 –standardi

1.1 Määritelmät

Tässä määräyksessä:

- Aineistolla tarkoitetaan henkilötietoja sisältävää tietoaineistoa.

- Fyysisesti ja teknisesti suojatulla alueella tarkoitetaan ympäristöä, jossa tilat ja tekniset ratkaisut estävät ulkopuolisten kontrolloimattoman pääsyn tietoihin. Tiloihin liittyvät vaatimukset ovat esitetty kohdassa 3.3 Toimitilat.

- Karanteeniympäristöllä tarkoitetaan eriytettyä ja suojattua ratkaisua, missä salattu aineisto muunnetaan selkokieliseksi ja sille tehdään eheys- sekä haittaohjelmatarkastus. Samassa ympäristössä Tietolupaviranomaiselle tarkastettavaksi lähetettävä aineisto salataan toimitusta varten. Ympäristöstä ei saa olla yhteyttä Internetiin.

- Käyttäjäympäristöllä tarkoitetaan tietoturvallisessa käyttöympäristössä sijaitsevaa tietolupakohtaisesti eriytettyä tietojenkäsittely-ympäristöä, jossa asiakas/tutkija tai -ryhmä käsittelee henkilötietoja sisältäviä aineistoja. Ympäristöstä ei saa olla suoraa yhteyttä Internetiin eikä muihin käyttäjäympäristöihin.

- Käyttäjä- ja pääsynhallinnalla tarkoitetaan ratkaisua, joka sijaitsee varsinaisen tutkimusympäristön ja Internetin välissä, ja jolla suoritetaan käyttäjien tunnistaminen ja toteutetaan pääsynhallintaa.

- Lokienhallinnalla tarkoitetaan eriytettyä ja suojattua ratkaisua, jolla toteutetaan käyttöympäristön lokitietojen keräys, valvonta ja raportointi.

- Lokitietoja ovat mm. käyttöloki- ja luovutuslokitiedot sekä tekniset lokitiedot, joita käyttöympäristön laitteet keräävät.

- Palveluntarjoaja on käyttöympäristöstä ja sen vaatimustenmukaisuudesta vastuussa oleva taho, joka voi käyttää myös alihankkijoita.

- Teknisen, organisatorisen ja fyysisen tietoturvan hallinta tarkoittaa käyttöympäristön toteutukseen liittyvien eri osa-alueiden hallinta- ja valvontaratkaisuja.

- Tietolupaviranomaisen järjestelmillä tarkoitetaan Tietolupaviranomaisen hallinnoimia tietojärjestelmiä, joissa suoritetaan mm. lupakäsittelyä, aineistojen siirtoa, kokoamista, esikäsittelyä ja yhdistämistä sekä pseudonymisointia ja anonymisointia.

- Tietoturvallisella käyttöympäristöllä (jatkossa myös pelkkä käyttöympäristö) tarkoitetaan teknistä, organisatorista ja fyysistä tietojen käsittelyn toimintaympäristöä.

- Tietoturvaskannaus tarkoittaa teknisin apuvälinein toteutettua tarkastusta tietojenkäsittely-ympäristölle. Tällä varmistetaan, ettei ympäristössä ole mm. haavoittuvuuksia eikä tietoturvaa vaarantavia virheellisiä konfigurointeja.

- Tunnistuslähde on järjestelmä, jossa sijaitsevat tunnistamisen ja käyttövaltuushallinnan tarvitsemat käyttäjätunnukset.

- Vähimpien oikeuksien periaate (myös pienimmän oikeuden periaate) on tietoturvallisuuteen liittyvä käsite, jonka mukaan tietojärjestelmän käyttöoikeudet tulee rajata suppeimpiin mahdollisiin oikeuksiin, joilla käyttäjä tai prosessi kykenee suoriutumaan sille määrätystä tehtävästä. Käyttöoikeudet tulee rajata myös ajallisesti lyhyimpään mahdolliseen ajanjaksoon, jonka aikana tehtävä voidaan suorittaa.

1.2 Toiminnallinen kuvaus

Tietoturvallisella käyttöympäristöllä tarkoitetaan teknistä, organisatorista ja fyysistä tietojen käsittelyn toimintaympäristöä, jossa tietoturvallisuus on varmistettu asianmukaisin hallinnollisin ja teknisin toimin. Tietoturvallisessa käyttöympäristössä on voitava varmistaa tietojen tietoturvallinen, tietoluvan mukainen käsittely ja ainoastaan tietoluvassa yksilöidyille käyttäjille annetaan pääsy kyseistä hanketta varten perustettavaan käyttäjäympäristöön.

Palveluntarjoaja on se toimija, joka tarjoaa tietoturvallisen käyttöympäristön palveluita asiakkaidensa käyttöön. Palveluntarjoaja voi tarvittaessa käyttää alihankkijoita eri osakokonaisuuksien toimittajina, esimerkiksi prosessoinnin ja tallennuskapasiteetin osalta. Palveluntarjoaja vastaa siitä, että tietoturvallinen käyttöympäristö ja sen tuottamiseen osallistuvat osapuolet noudattavat tässä määräyksessä asetettuja vaatimuksia.

Tärkeimpiä toiminnallisuuksia liittyen tietoturvalliseen käyttöympäristöön:

- Käyttäjäympäristöön kirjaudutaan luotettaviksi arvioitujen tunnistuslähteiden tunnuksilla.

- Käyttäjäympäristöön kirjautumisessa käytetään pääsääntöisesti kaksivaiheista tunnistautumista.

- Käyttäjäympäristössä asiakas saa käyttöönsä vain kyseisen tietoluvan mukaiset aineistot.

- Tietojen siirtäminen käyttäjäympäristöjen välillä on estetty.

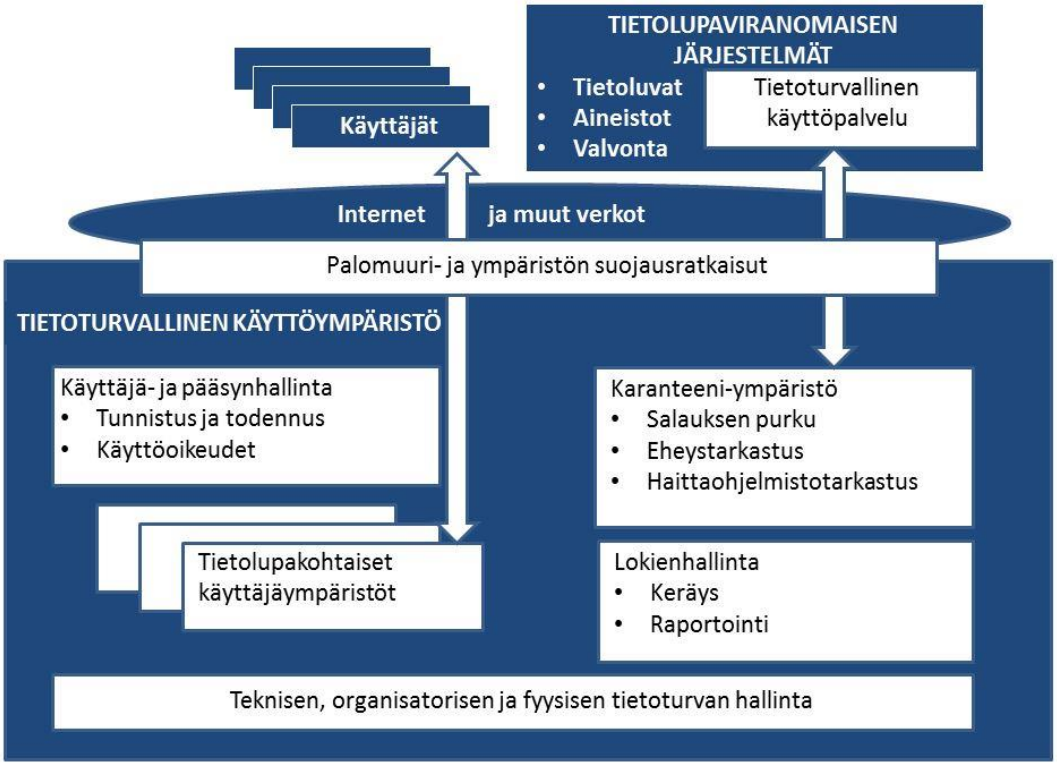
- Henkilötietoaineistojen siirto tietoturvalliseen käyttöympäristöön tapahtuu tietoturvallisesti.

- Käyttäjäympäristöön ei tule olla 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.

Tietoturvallisen käyttöympäristön arkkitehtuuri on kuvattu alla ja keskeiset palveluntarjoajaa koskevat prosessivaiheet kohdassa 4.

1.3 Järjestelmäarkkitehtuuri

Seuraavassa kuvassa on esitetty Tietoturvallisen käyttöympäristön periaatteellinen järjestelmäarkkitehtuuri. Tämän tarkoituksena on selventää, mistä toiminnoista tietoturvallinen käyttöympäristö koostuu ja miten se liittyy muihin keskeisiin toisiolain mukaisiin toimintoihin.



Kuva: Tietoturvallisen käyttöympäristön periaatteellinen järjestelmäarkkitehtuuri

1.4 Palveluntarjoajat

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.

Palveluntarjoajan on myös tunnistettava mahdollinen henkilötietojen kasautumisvaikutus ja huomioitava tämä tarjoamansa käyttöympäristön suojauksessa. Kasautumisvaikutus voi syntyä esimerkiksi tilanteissa, joissa käyttöympäristössä on tarkoitus säilyttää useita henkilötietoaineistoja ja/tai aineistojen koot muodostuvat suuriksi. Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira ylläpitää julkista rekisteriä sille ilmoitetuista vaatimukset täyttävistä käyttöympäristöistä.

1.5 Luotetut tunnistuslähteet

Tietolupaviranomainen ylläpitää ajantasaista listaa luottamistaan tunnistuslähteistä ja julkaisee ne osoitteessa https://findata.fi. Listattujen luotettujen tunnistuslähteiden lisäksi voi käyttää tunnistelähteitä, jotka tunnistautumisen osalta täyttävät tämän määräyksen kohdan 2.1.2 vaatimukset.

2 Tekniset vaatimukset

2.1 Tunnistautuminen

2.1.1 Toisiolain asettamat vaatimukset

21 § Tietoturvallisen käyttöympäristön käyttäjien tunnistaminen
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P21

2.1.2 Tietolupaviranomaisen asettamat vaatimukset

1. Käyttäjän ensitunnistaminen toteutetaan ensisijaisesti vahvalla sähköisellä tunnistamisella, esimerkiksi Suomi.fi-palvelulla. Jos vahvaa sähköistä ensitunnistusta ei ole mahdollista tehdä, on käyttäjän identiteetti varmistettava henkilöllisyyden todentamisasiakirjoja käyttäen käyttäjän läsnä ollessa dokumentoidusti. Jos käyttäjän läsnäolon vaatiminen ei ole kohtuullista esim. matkustamisen takia, voidaan ensitunnistaminen toteuttaa tavalla, jossa käyttäjään työ-, toimeksianto-, sopimus-, tai vastaavassa suhteessa oleva organisaatio vahvistaa käyttäjän identiteetin kirjallisesti ja sitovasti tarvittavine dokumentteineen.

2. Tunnuksien haltijoilla ja tunnistuslähteen välillä pitää olla joko sopimussuhde (esimerkiksi työ- tai tutkimussopimus), affiliaatio (esimerkiksi tutkimushankkeen kautta) tai muu juridisesti sitova suhde. Tunnistuslähteiden ylläpitäjillä on velvollisuus sulkea tunnukset välittömästi sopimussuhteen päätyttyä tai mikäli epäilevät tunnuksien vuotamista tai muuta väärinkäytöstä.

3. Käyttäjätunnistuksen tulee olla vähintään kaksivaiheinen, jossa käytetään kahta eri tunnistusmenetelmää. Käyttäjätunnus-salasanayhdistelmän lisäksi käytetään erillistä tunnistetta, esimerkiksi matkapuhelinsovellusta tai muuta vastaavaa tunnistusmetodia. Kaksivaiheinen tunnistus pitää olla tapahtunut, ennen kuin tietoluvan mukaisten aineistojen käsittely aloitetaan käyttäjän toimesta.

4. Jos palveluntarjoajan käyttäjälle järjestämä ja osoittama, käyttäjäympäristön käyttöön dedikoitu päätelaite sijaitsee käyttäjäympäristön kanssa saman fyysisesti ja teknisesti suojatun alueen sisällä, ei kaksivaiheista tunnistusta edellytetä, mutta käyttäjän henkilöllisyydestä on oltava varmuus ennen dedikoidun päätelaitteen käyttöön luovutusta.

5. Lisäksi arvioinnissa käytetään KATAKRI kohtia I 06 (Toteutusesimerkin kohdat 1-8) ja I 07 (Toteutusesimerkin kohdat 1-7) soveltuvin osin.

2.2 Käyttäjien ja käyttöoikeuksien hallinta

2.2.1 Toisiolain asettamat vaatimukset

22 § Tietoturvallisen käyttöympäristön käyttäjien käyttöoikeudet
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P22

2.2.2 Tietolupaviranomaisen asettamat vaatimukset

1. Ympäristön käyttöoikeudet on rajoitettu siten, että käyttäjät pääsevät käsiksi vain niihin aineistoihin ja resursseihin, joihin heille on myönnetty lupa.

2. Ympäristön käyttöoikeudet on rajoitettu tietolupien mukaan. Jos henkilöllä on useampia tietolupia käyttöympäristössä, on sallittua pitää auki yhteys usean tutkimusluvan aineistoihin, mutta aineiston siirto käyttäjäympäristöjen välillä on kielletty.

3. Ympäristön käyttöoikeudet myönnetään vähimpien oikeuksin periaatteella KATAKRI I 06, vaatimus 1-2 mukaisesti.

4. Ympäristössä käytetään vain kohdan 1.5 mukaisten tunnistuslähteiden tunnuksia.

5. Havaitessaan väärinkäytöksen, on palveluntarjojan viipymättä estettävä lisävahinkojen synty esimerkiksi käyttöoikeuksia rajoittamalla.

6. Käyttöoikeus käyttäjäympäristöön lukittuu automaattisesti tietoluvan voimassaolon päätyttyä.

7. Käyttäjäympäristön aineistot poistetaan automaattisesti viimeistään 6 kk kuluttua käyttöoikeuden päätyttyä, ellei laki määrää muuta.

8. Lisäksi arvioinnissa käytetään KATAKRI kohtaa I 06 (Toteutusesimerkin kohdat 1-8) soveltuvin osin.

2.3 Ympäristön suojaaminen

2.3.1 Toisiolain asettamat vaatimukset

18 § Yleiset tietoturvavaatimukset https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P18

23 § Tietoturvallisen käyttöympäristön suojaaminen https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P23

24 § Tietoturvallisen käyttöympäristön vähimmäisvaatimukset https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P24

2.3.2 Tietolupaviranomaisen asettamat vaatimukset

1. Pääsynhallintaympäristö tulee suojata KATAKRI I 01 Toteutusesimerkin kohdat 1-2 mukaisesti.

2. Käyttäjäympäristön ja Karanteeniympäristön osalta suojaaminen tulee tapahtua KATAKRI I 01 Toteutusesimerkin kohdat 1-2 mukaisesti.

3. Tarkennuksia vaatimuksiin:

    a. Käyttäjäympäristö on eriytetty Internetistä palomuuriratkaisulla.

    b. Jos palveluntarjoajan käyttäjälle järjestämä, käyttäjäympäristön käyttöön dedikoitu päätelaite sijaitsee käyttäjäympäristön kanssa saman fyysisesti ja teknisesti suojatun alueen sisällä, ei kaksivaiheista tunnistusta edellytetä, mutta käyttäjän henkilöllisyydestä on oltava varmuus ennen dedikoidun päätelaitteen käyttöön luovutusta. Päätelaitteelta ei saa olla yhteyttä käyttäjäympäristön ulkopuolelle eikä käyttäjällä saa olla mahdollisuutta tuoda tai viedä tietoja käyttäjäympäristöstä päätelaitetta käyttäen, esim. USB-muistia käyttäen.

    c. Jos päätelaite ei sijaitse käyttäjäympäristön kanssa saman fyysisesti ja teknisesti suojatun alueen sisällä, tulee sisäänkirjautuminen toteuttaa kaksivaiheisella tunnistuksella, jossa jälkimmäinen vaihe on toteutettava ennen aineistoihin pääsyä.

    d. Käyttäjäympäristöön ei sallita suoria yhteyksiä käyttäjän päätelaitteelta. Yhteydellä siirretään esimerkiksi vain näyttökuvaa sekä näppäimistön ja hiiren syötettä.

    e. Eri tietolupien käyttäjäympäristöt pitää olla eriytettyinä toisistaan siten, että vain kyseisessä tietoluvassa mainitut käyttäjät saavat pääsyn lupaa koskevaan tietoaineistoon.

    f. Käyttäjille ei oletusarvoisesti myönnetä ylläpito-oikeuksia käyttöympäristön koneisiin. Käyttöoikeuksien hallinnointi tulee tapahtua KATAKRI I 06 Toteutusesimerkin kohdat 1-8 mukaisesti noudattaen Vähimpien oikeuksien periaatetta. Käyttäjälle voidaan myöntää oikeuksia, jotka ovat peruskäyttäjän oikeuksia suuremmat, jos nämä liittyvät tietoluvan mukaiseen tietojen käsittelyyn, eivätkä ne käyttöympäristön ylläpitäjän riskiarvion mukaan vaaranna tietoturvallisuutta.

    g. Käyttöympäristön verkon rakenteellisen turvallisuuden kohdalla tulee noudattaa KATAKRI I 01 vaatimuksia kohtien 1-2 mukaisesti soveltuvin osin. Kohdan 2 vaatimusta noudatetaan vaikka suojaustasoja ei olisi yhteen liitettäville ympäristöille määritelty. Liikennöitäessä julkisen tai muun heikommin suojatun verkon kautta, on tietoliikenne salattava tunnetulla ja yleisesti luotettavana pidetyllä salausratkaisulla tai ratkaisun luotettavuudesta on varmistuttu jollain muulla luotettavalla menetelmällä. Tietoliikenteen salauksessa käytettävien

salausavainten hallinnassa noudatetaan KATAKRI I 12 Toteutusesimerkin 2 vaatimuksia soveltaen. Pilvipalvelutarjoajan tarjoamaa avaintenhallintaa voidaan hyödyntää, mikäli salaisten avainten luottamuksellisuudesta voidaan riittävällä tasolla varmistua.

4. Järjestelmän suojaamisessa noudatetaan soveltuvin osin Vähimmäistoimintojen ja vähimpien oikeuksien periaatetta KATAKRI I 08 mukaisesti (Toteutusesimerkin kohdat 1-17).

5. Järjestelmän suojaamisessa noudatetaan soveltuvin osin Monitasoisen suojaamisen periaatetta KATAKRI I 09 Toteutusesimerkin kohdat 1-7 sekä I 13 Toteutusesimerkin kohdat 1-3 mukaisesti. Haittaohjelmatunnisteiden säännöllinen päivittyminen voidaan järjestää rajaamalla sen tarvitsema liikennöinti tarkasti esimerkiksi palomuurisäännöstöjen avulla.

6. 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. Tässä noudatetaan KATAKRI:n kohtaa I 15 (Toteutusesimerkki 2) soveltuvasti.

7. Ohjelmistohaavoittuvuuksien hallinnassa noudatetaan KATAKRI:n kohtaa I 23 (Toteutusesimerkin kohdat 1-2) soveltuvin osin.

8. Käyttöympäristölle tulee suorittaa säännöllisiä tietoturvaskannauksia.

2.4 Lokitus

2.4.1 Toisiolain asettamat vaatimukset

19 § Lokitiedot https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P19

2.4.2 Tietolupaviranomaisen asettamat vaatimukset

1. Lokitietoja tulee käsitellä samalla tietoturvallisella tavalla kuin erityisiin henkilötietoryhmiin kuuluvia henkilötietoja.

2. Käyttölokeihin on tallennettava tieto tietoluvan saaneesta rekisterinpitäjästä, toisiolain mukaisesta käyttötarkoituksesta, käsittelyyn oikeuttavasta tietoluvasta, tietojen käsittelyyn tietoluvan mukaan oikeutetusta käyttäjästä, käsitellyistä tiedoista ja tietoryhmistä sekä käyttöajankohdasta.

3. Teknisiä lokitietoja tulee kerätä kattavasti, jotta mahdolliset virhetoiminnot tai tietomurrot voidaan selvittää riittävän kattavasti. Näitä teknisiä lokeja tulee säilyttää vähintään 5 vuotta.

4. Muilta osin lokitus toteutetaan KATAKRI I 10 Toteutusesimerkin kohdat 1-7 mukaisesti.

5. Hallintayhteydet ja käyttö tulee suojata soveltaen KATAKRI:n I 04 vaatimuksia. Jos toteutus edellyttää liikenteen salausta, salaustuotteen ei tarvitse olla viranomaisen hyväksymä. Turvallisuuden arvioinnissa huomioidaan myös kompensoivat kontrollit.

6. Lokeja on seurattava ja analysoitava suunnitelmallisesti ja säännöllisesti.

7. Lokitietojen käyttö tulee olla toteutettu siten, että myös katselusta jää tieto järjestelmään.

8. Lupakohtaiset aineistojen käyttölokitiedot ja käyttäjärekisterit on toimitettava Tietolupaviranomaiselle sen pyynnöstä ilman aiheetonta viivytystä.

2.5 Ympäristön hallinta ja valvonta

2.5.1 Tietolupaviranomaisen asettamat vaatimukset

1. Käyttöympäristö on dokumentoitu ja dokumentointia tulee voida käyttää arviointilaitoksen suorittamassa arvioinnissa sekä muissa tarkastuksissa.

2. Käyttöympäristöä tulee valvoa automaattisesti ympärivuorokautisesti ja poikkeamiin reagointi on vastuutettu ja ohjeistettu.

3. Käyttöympäristön valvonnassa tulee kiinnittää erityistä huomioita tietoturvan valvontaan.

4. Käyttöympäristön poikkeuksien havainnoinnissa tulee hyödyntää KATAKRI I 11 Toteutusesimerkin kohdat 1-4 kriteerejä soveltuvilta osin. Verkkoliikennetason havainnointikyvyn tulisi kattaa erityisesti verkon/kohteen ulkorajan liikennöinnin.

5. Käyttöympäristön tietoturvan ajantasaisuutta tulee valvoa ja katselmoida säännöllisesti.

6. Käyttöympäristön hallinta tulee tehdä tietoturvan osalta kovennetulta työasemalta salatulla tietoliikenneyhteydellä.

7. Käyttöympäristön ylläpito tulee tehdä siihen soveltuvista tiloista. Etähallinta on mahdollista edellyttäen, että ylläpitohenkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.

8. Käyttöympäristön palvelimien tulee sijaita suojatuissa tiloissa, jotka täyttävät tämän määräyksen toimitiloille asetetut vaatimukset.

9. Käyttöympäristön ylläpitokäyttöoikeuksien tulee olla henkilökohtaisia, erikseen työtehtävien mukaan määriteltyjä käyttöoikeuksia.

10. Käyttöympäristön ylläpitokäyttöoikeudet tulee tarvittaessa jakaa eri tason ylläpitokäyttöoikeuksiin (Adminitration Tier Model)

11. Käyttöympäristön ylläpitokäyttöoikeuksissa tulee noudattaa vähimpien oikeuksien periaatetta KATAKRI I 06 Toteutusesimerkin kohdat 1-8 mukaisesti sekä monitasoisen suojaamisen periaatetta KATAKRI I 07 Toteutusesimerkin kohdat 1-7 mukaisesti.

12. Käyttöympäristön hallinnassa ja valvonnassa noudatetaan KATAKRI I 03 ja I 04 -osiota soveltuvin osin.

13. Käyttöympäristön muutoshallinnassa noudatetaan KATAKRI I 20 (Toteutusesimerkin kohdat 1-3) osiota soveltuvin osin.

14. Myös tietoturvallisen käyttöympäristön ylläpitäjien toimet on sisällytettävä lokienhallintaan.

15. Jos epäillään, että tietojen käsittely on lain tai myönnetyn tietoluvan ehtojen vastaista, on palveluntarjoajalla oltava kyky viivyttelemättä ilmoittaa asiasta tietolupaviranomaiselle ja toimittaa asiasta yksityiskohtainen selvitys. Tämä ei poissulje muita lainsäädännön asettamia velvoitteita.

2.6 Aineistojen poisto käyttöympäristöstä

2.6.1 Tietolupaviranomaisen asettamat vaatimukset

1. Aineistot tulee poistaa käyttöympäristöstä 6 kk tietoluvan päättymisen jälkeen, ellei tietoluvassa ole toisin määrätty.

2. Aineiston poistossa tulee noudattaa KATAKRI I 19 kohtien 2 ja 3 vaatimuksia soveltaen.

3. Aineistojen säilytyksessä on huomioitava mahdolliset tietoluvassa asetetut ehdot.

3 Toimijan luotettavuus

3.1 Yleistä

3.1.1 Toisiolain asettamat vaatimukset

20 § Tietoturvallinen käyttöympäristö https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P20

25 § Tietoturvallisen käyttöympäristön tietoturvallisuuden osoittaminen
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P25

26 § Tietoturvallisuuden arviointi https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P26

27 § Arviointilaitoksen myöntämän todistuksen peruuttaminen
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P27

28 § Tietoturvallisuuden arviointilaitoksen ilmoittamisvelvollisuus
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P28

29 § Tietoturvallisen käyttöympäristön käyttöönoton jälkeinen seuranta
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P29

30 § Tietojärjestelmien valvonta ja tarkastukset
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P30

31 § Sosiaali- ja terveysalan lupa- ja valvontaviraston oikeus ulkopuolisen asiantuntijan käyttöön
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P31

32 § Sosiaali- ja terveysalan lupa- ja valvontaviraston tiedonsaantioikeus
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P32

33 § Sosiaali- ja terveysalan lupa- ja valvontaviraston määräys puutteiden korjaamiseksi ja uhkasakko
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P33

34 § Määräys velvollisuuksien täyttämiseksi
https://www.finlex.fi/fi/laki/ajantasa/2019/20190552#L3P34

3.1.2 Tietolupaviranomaisen asettamat vaatimukset

1. Tietoturvallisen käyttöympäristön on fyysisesti sijaittava EU/ETA-alueella.

2. Tietoturvallisen käyttöympäristön palveluntarjoajan on oltava EU/ETA-alueella rekisteröity organisaatio.

3. Palveluntarjoajan ja käyttöympäristön tuottamiseen osallistuvien organisaatioiden yleinen luotettavuus arvioidaan suhteessa kykyyn toimia tämän määräyksen vaatimusten mukaisesti. Arvioinnissa voidaan käyttää Katakria soveltuvin osin. Pilvipalveluita käytettäessä voidaan arvioinnissa hyödyntää PiTuKrin lukua ”Palvelun tuottaminen” Katakrin sijaan. Arviointi voi tapahtua palveluntarjoajan esittämän asiakirjanäytön perusteella.

4. Palveluntarjoaja vastaa alihankkijan toiminnasta kuin omastaan ja tämän määräyksen velvoitteista on sitovasti sovittu palveluntarjojan ja alihankkijan välillä. Alihankkijalla tarkoitetaan esimerkiksi käyttöpalvelutoimittajaa tai pilvipalvelun tarjoajaa. Palveluntarjoajan on osoitettava luotettavuus tietoturvallisuuden hallintajärjestelmällä, esimerkiksi ISO/IEC 27001 -standardin mukaisesti.

5. Sosiaali- ja terveysalan lupa- ja valvontavirastolla (Valvira) tai sen osoittamalla ulkopuolisella asiantuntijalla (esimerkiksi tietoturvallisuuden arviointilaitoksella) on oikeus tehdä valvonnan edellytyksenä olevia tarkastuksia. Tarkastuksen suorittamiseksi tarkastajalla on oikeus päästä kaikkiin tiloihin, joissa harjoitetaan tässä laissa tarkoitettua toimintaa tai säilytetään tämän lain noudattamisen valvonnan kannalta merkityksellisiä tietoja. Vaatimus koskee myös palveluntarjoajan käyttämiä alihankkijoita.

3.2 Tietosuoja

3.2.1 Tietolupaviranomaisen asettamat vaatimukset

1. Käyttöympäristöstä on oltava laadittuna EU:n yleisen tietosuoja-asetuksen (GDPR) 35 artiklan mukainen tietosuojaa koskeva vaikutustenarviointi (DPIA).

2. Rekisterinpitäjää ja henkilötietojen käsittelijää koskevat velvoitteet ja sopimukset ovat huomioitu tietosuoja-asetuksen voimassa olevien ohjeiden mukaisesti. Asetus ei sisällä ohjeita vaan se velvoittaa suoraan.

3. Palveluntarjoaja vastaa siitä, että palveluntarjoajan toimin 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. Käyttäjälle voidaan sallia aineistojen käsittelyssä tarvittavien komentosarjojen tai muiden vastaavien koodien siirto esimerkiksi leikepöytää käyttäen, mutta tiedostojen siirto käyttäjän toimin tulee olla estetty.

3.3 Toimitilat

3.3.1 Tietolupaviranomaisen asettamat vaatimukset

1. Käyttöympäristön hallintaoikeuksia edellyttävä ylläpito tulee tehdä ylläpitoon soveltuvista tiloista. Arviointilaitos arvioi tilojen turvallisuuden tämän määräyksen pohjalta. Arviointia ei tarvitse tehdä paikan päällä, jos muu näyttö on riittävää. Etähallinta on mahdollista edellyttäen, että ylläpitohenkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.

2. Ympäristön palvelimet tulee sijaita soveltuvissa tiloissa. Arviointilaitos arvioi tilojen turvallisuuden tämän määräyksen pohjalta. Arviointia ei tarvitse tehdä paikanpäällä, jos muu näyttö on riittävää.

3. Toimitilaturvallisuuden osalta noudatetaan KATAKRI:n fyysisen turvallisuuden arviointikriteeristöä F 01-08 Hallinnollista aluetta koskevan kriteeristön osalta soveltuvin osin.

3.4 Henkilöstö

3.4.1 Tietolupaviranomaisen asettamat vaatimukset

1. Henkilöstö, jolla on pääsy henkilötietoaineistoihin, tulee olla perehdytetty aineistoja koskeviin käsittelyohjeisiin.

2. Käyttöympäristön ylläpitotehtävissä toimiville henkilöille, joilla on pääsy henkilötietoaineistoihin, tulee olla tehtynä perusmuotoinen turvallisuusselvitys tai muu vastaava viranomaisselvitys ellei lainsäädäntö aseta sille estettä. Käyttöympäristön ratkaisu, joilla rajoitetaan ylläpitohenkilöstön pääsyä henkilötietoaineistoon voidaan hyväksyä riittävän luotettavaksi, mikäli esitetty näyttö tukee tätä. Tällöin ylläpitohenkilöstöltä ei edellytetä viranomaisen tekemää selvitystä henkilön luotettavuudesta. Lisäksi voidaan Henkilöstöturvallisuuden arvioinnissa hyödyntää KATAKRI T 08-12 -osioita sekä PiTuKri HT-02 kohtaa 1 soveltuvin osin.

4 Tietoturvalliseen käyttöympäristöön liittyvät keskeiset prosessivaiheet

Prosessin vaihe	**Tehtävät**	**Huomioitavaa**
Vaatimusten-mukaisuuden varmistaminen	Palveluntarjoaja huolehtii, että omaa voimassa olevan tietoturvallisuuden arviointilaitoksen antaman todistuksen käyttöympäristön tietoturvallisuudesta.	(Vrt. 552/2019 25 §) Todistuksen on katettava kaikki tietoturvallisen käyttöympäristön osa-alueet, joissa käsitellään henkilötietoja ja osa-alueet, joilla on vaikutusta henkilötietojen tietosuojan toteutumiseen.
	Tietolupaviranomainen tarkastaa Sosiaali- ja terveysalan lupa- ja valvontaviraston julkisesta rekisteristä, että palveluntarjoajalla on voimassa oleva todistus.	(Vrt. 552/2019 28 §, 30 §)
	Palveluntarjoaja tarjoaa valvovalle viranomaiselle tai sen osoittamalle taholle mahdollisuuden valvoa, että tietosuojaa ja tietoturvaa koskevat vaatimukset täyttyvät.	(Vrt. 552/2019 30 §)
	Palveluntarjoajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellytyksenä olevat tiedot vähintään viisi vuotta tietoturvallisen käyttöympäristön tuotantokäytön päättymisestä. Käyttö- ja luovutuslokitiedot on hävitettävä tai arkistoitava 12 vuoden kuluttua tietoluvan päättymisestä.	(Vrt. 552/2019 29 §, 19 §)
Tietoturvallisen käyttöympäristön käytön seuranta ja arviointi	Palveluntarjoajan seuraa ja arvioi ajantasaisella järjestelmällisellä menettelyllä tietoturvallisesta käyttöympäristöstä sen tuotantokäytön aikana saatavia kokemuksia. Palveluntarjoaja seuraa lain muutoksia ja tekee käyttöympäristöön muutosten edellytyksenä olevat korjaukset.	(Vrt. 552/2019 29 §)
Neuvonta	Palveluntarjoaja tarjoaa tietoturvallisen käyttöympäristön palvelukuvauksen, hinnaston sekä asiaan liittyvää neuvontaa.	Tietolupaviranomainen tarjoaa neuvontapalvelua vain itse järjestämänsä tietoturvallisen käyttöympäristön osalta.

Prosessin vaihe	**Tehtävät**	**Huomioitavaa**
Käyttäjäympäristön tilaaminen	Asiakas tekee tilauksen palveluntarjoajan järjestämällä menettelyllä tietoluvassa mainitusta käyttäjäympäristöstä ja liittää virallisen tietolupapäätöksen tarvittavine liitteineen osaksi tilausta.	Palveluntarjoaja tarjoaa asiakkaalle mahdollisuuden sähköisesti tapahtuvaan asiointiin. Asiakkaalta pyydettäviä keskeisiä tietoja luvassa esiintyvien tietojen lisäksi ovat esim. • tutkimusryhmän jäsenten tunnisteet (yksilöivät sähköiset tunnisteet ja tunnistefederaatiot) • tutkimusryhmän jäsenten yhteystiedot • käyttäjäympäristön tarvittava kapasiteetti • tarvittavat ohjelmistot • laskutustiedot
	Palveluntarjoaja tarkastaa sähköisesti allekirjoitetun tietoluvan aitouden.	Tietolupa on toimitettu asiakkaalle pdf-muodossa sähköisesti allekirjoitettuna.
	Palveluntarjoaja vahvistaa tilauksen vastaanotetuksi.	–
	Palveluntarjoaja käsittelee tilauksen.	Tilauksen pitää perustua voimassa olevaan tietolupaan ja tietoturvallinen käyttöympäristö on osoitettu tietoluvassa. Palveluntarjoaja pyytää asiakkaalta tarvittaessa lisätietoja tilaukseen liittyen.
	Palveluntarjoaja vahvistaa tilauksen käsitellyksi.	–
Käyttäjäympäristön perustaminen	Palveluntarjoaja perustaa asiakkaan tilauksen perusteella tietolupakohtaisen käyttäjäympäristön	–
	Palveluntarjoaja luo käyttäjätilit ja käyttöoikeudet luvassa mainituille käyttäjille	Pääsy- ja käyttöoikeudet voidaan antaa ainoastaan luvan voimassaolon ajaksi siinä mainituille käyttäjille. Käyttöympäristön palveluntarjoajan on varmistettava ennen yhteyden avaamista luvansaajalle, että luvansaaja täyttää tietoluvassa asetetut vaatimukset (Vrt. 552/2019 51 §). Palveluntarjoajan on pidettävä rekisteriä tietoturvallisen käyttöympäristön käyttäjistä sekä näiden käyttöoikeuksista. Käyttöympäristön käyttäjien

Prosessin vaihe	Tehtävät	Huomioitavaa
		käyttöoikeustiedot on hävitettävä tai arkistoitava 12 vuoden kuluttua käyttöoikeuden päättymisestä.
Käyttäjien tunnistus	Käyttäjien tunnistuksessa noudatetaan tässä määräyksessä esitettyjä vaatimuksia.	(Vrt. 552/2019 21 §) Tietoturvallisen käyttöympäristön käyttäjät on tunnistettava luotettavasti sekä todennettava. Luotettava tunnistautuminen voi tapahtua esim. Suomi.fi -palvelun tai luotetun federoidun tunnistuslähteen kautta.
Kirjautumistietojen toimitus käyttäjille	Palveluntarjoaja toimittaa tietoluvassa mainituille henkilöille rekisteröitymis- ja kirjautumisohjeet sekä ohjeet kaksivaiheisen tunnistuksen aktivoimiseksi.	Mahdolliset käyttäjätunnuksiin liittyvät tiedot toimitetaan käyttäjälle tietoturvallisella tavalla.
Käyttöoikeuksien määritys	Tietoluvassa mainituille henkilöille myönnetään käyttöoikeudet luvanmukaisiin aineistoihin. Palveluntarjoaja määrittelee luvansaajan ja muun henkilötietoja käyttöympäristössä käsittelevän henkilön käyttöoikeudet henkilötietoihin.	Kaikkien käyttöympäristön käyttäjien tulee olla mainittuna Tietolupaviranomaisen myöntämässä tietoluvassa. Käyttöoikeudet saavat olla voimassa vain luvan voimassaolon ajan. Palveluntarjoajan on pidettävä rekisteriä tietoturvallisen käyttöympäristön käyttäjistä sekä näiden käyttöoikeuksista. Käyttöympäristön käyttäjien käyttöoikeustiedot on hävitettävä tai arkistoitava 12 vuoden kuluttua käyttöoikeuden päättymisestä.
Aineistojen toimitus tietoturvalliseen käyttöympäristöön	Aineistot siirretään palveluntarjoajalle pääsääntöisesti tietoturvallisen käyttöpalvelun 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.
	Palveluntarjoaja varmistaa vastaanottamiensa aineistojen eheyden ja virheettömyyden sekä tietoturvallisuuden.	–
	Palveluntarjoaja järjestää aineistot käyttäjäympäristöön luvassa mainittujen käyttäjien saataville.	–

Prosessin vaihe	**Tehtävät**	**Huomioitavaa**
Valmiiden tuotosten siirto ulos tietoturvallisesta käyttöympäristöstä	Palveluntarjoaja siirtää asiakkaan valmiit tuotokset tietoturvallisen käyttöpalvelun välityksellä anonymisoinnin osalta Tietolupaviranomaisen tarkastettavaksi.	Tietolupaviranomainen voi kuitenkin perustellusta syystä lupapäätöksessään myöntää luvansaajalle oikeuden toteuttaa itse julkaistavien edellä mainittujen tietojen anonymisoinnin ehdolla, että ne toimitetaan jälkikäteen Tietolupaviranomaisille.
Muutostilausten käsittely ja toteutus	Palveluntarjoaja ottaa vastaan käyttäjäympäristöön liittyvät muutospyynnöt ja lisätilaukset oman palvelukuvauksen mukaisesti ja toteuttaa ne tietoluvan puitteissa dokumentoidusti.	Jos asiakkaan tilaamat muutokset ovat ristiriidassa lain tai voimassa olevan tietoluvan kanssa, ei niitä saa toteuttaa.
Käyttäjäympäristön käytön lopetus	Palveluntarjoaja sulkee käyttäjiltä pääsyn käyttäjäympäristöön tietoluvan voimassaolon loputtua, sopimuksen päätyttyä, asiakkaan pyynnöstä tai viranomaisen niin määrätessä.	–
	Palveluntarjoaja poistaa henkilötietoaineistot tietoturvallisesti asiakkaan kanssa yhdessä ajanhetkestä sopien kuitenkin viimeistään 6 kk kuluttua tietoluvan päättymisestä ellei tästä ole muuta säädetty.	–