Sosiaali- ja terveysalan tietolupaviranomainen ver. 01.05.2026

LOMAKE B – Käyttöympäristön tietoturvan ja tietosuojan arviointi

Ohje

Tämän lomakkeen vaatimukset koskevat muun turvallisen käyttöympäristön tietoturvaa ja riskienhallintaa EU:n yleisen tietosuoja-asetuksen ja toisiolain 18 §:n mukaisesti. Lomakkeen arviointi kohdistuu käyttöympäristön teknisiin ja organisatorisiin rakenteisiin, joilla varmistetaan henkilötietojen käsittelyn turvallinen ja hallittu tietolupapäätöksen mukainen toteutus.

Tämä lomake liittyy toisiolain 51 c §:n mukaiseen käyttöympäristöarviointiin silloin, kun Lomake A:ssa tehdyn esiarvion perusteella on todettu edellytykset arvioida muuta turvallista käyttöympäristöä.

Vastaa joka kohtaan ”Kyllä” tai ”Ei”. “Lisätiedot” täytetään **vain tarvittaessa**, esim. jos vastaus on ”Ei” tai toteutus poikkeaa tavanomaisesta. Jokaisessa kohdassa on erikseen mainittu vaadittu liite, joka tulee toimittaa lomakkeen ohessa erillisenä liitteenä. Liitteet on listattu alla.

- **Liite 1:** Arkkitehtuuri, käsittely-ympäristön eriytys ja verkkorajoitukset
- **Liite 2:** Käyttövaltuushallinnan kuvaus (ensitunnistus, MFA, oikeuksien myöntö/päättyminen)
- **Liite 3:** Ulosvientiestot (kopiointi)
- **Liite 4:** Lokitus (sisältö, suojaus, seuranta)
- **Liite 5:** Tietoturvallisuuden hallinta (roolit, riskit, valvonta, reagointi, aineiston poisto)
- **Liite 6:** DPIA-tiivistelmä riskeistä käyttöympäristöä koskien

Toimita liitteessä vain pyydetyt tiedot ja merkitse tämän lomakkeen lopussa, mitkä liitteet toimitat.

Jos käyttöympäristö sijaitsee **EU/ETA:n ulkopuolella**, täytä lisäksi lomakkeen lopussa oleva ”**Lisäosa C – Kolmas maa**”.

1 Tulevan aineiston rekisterinpitäjän tiedot

Organisaatio: _____
Y-tunnus / tunniste: _____
Yhteyshenkilö (johto / vastuullinen): _____
Sähköposti: _____
Puhelin: _____
Tietosuojavastaava / yhteyspiste: _____
Tietoturvavastaa / CISO / vastaava: _____

2 Kohdekäyttöympäristön perustiedot

Käyttöympäristön nimi: _____
Sijainti: ☐ Suomi ☐ EU/ETA (maa: _____) ☐ EU/ETA:n ulkopuoli (maa: _____)
Ylläpitäjä / palveluntarjoaja: _____
Yhteystiedot: _____

3 Itsearvio (vaihe B) – Kyllä / Ei + liiteviite

B1 Tietoturvan hallinta (GDPR 5(2), 24 ja 32 artiklat; toisiolaki 18 §)

Toisiolain 18 § edellyttää, että henkilötietojen käsittelyssä varmistetaan riittävä tietoturvallisuus riskienhallinnan avulla sekä noudattamalla tietoturvallisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita.

Yleinen tietosuoja-asetus edellyttää lisäksi, että rekisterinpitäjä toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet ja pystyy osoittamaan henkilötietojen käsittelyn asetuksen mukaisuuden. Tietoturvan hallinnan avulla varmistetaan näiden edellytysten järjestelmällinen ja jatkuva toteutuminen.

B1.1 Omistajuus ja vastuut (johto + operatiivinen)

Vaadittu liite: Liite 5
Edellytys: Käyttöympäristöllä on nimetty omistaja ja tietoturvavastuut.

☐ Kyllä ☐ Ei

Lisätiedot:

B1.2 Tietoturvan hallintajärjestelmä / riskienhallintamalli

Vaadittu liite: Liite 5
Edellytys: Käyttöympäristöstä vastaavalla organisaatiolla/palveluntarjoajalla on käytössä tietoturvallisuuden hallintajärjestelmä (ISMS) tai vastaava riskiperusteinen malli.

☐ Kyllä ☐ Ei

Lisätiedot:

B1.3 Poikkeamien hallinta ja ilmoittaminen

Vaadittu liite: Liite 5
Edellytys: Poikkeamien havainnointi, reagointi ja ilmoittaminen on ohjeistettu ja vastuutettu sekä käyttöympäristön ylläpitäjällä on kyky ilmoittaa viivytyksettä epäillystä tietolupaehtojen vastaisesta käsittelystä rekisterinpitäjälle.

☐ Kyllä ☐ Ei

Lisätiedot:

B1.4 Haavoittuvuuksien hallinta

Vaadittu liite: Liite 5
Edellytys: Käyttöympäristö on suojattu haittaohjelmistoilta ja haavoittuvuuksien hallinta on järjestetty.

☐ Kyllä ☐ Ei

Lisätiedot:

B2 Pääsyn rajaus tietoluvan mukaisesti (GDPR 5(1)(c) ja 32 artikla; toisiolaki 18 §)

Toisiolain 18 § edellyttää, että henkilötietojen käsittelyssä toteutetaan asianmukainen pääsynhallinta ja että erityistä huomiota kiinnitetään käyttörajoitusten toteuttamiseen.

Yleisen tietosuoja-asetuksen mukaan henkilötietojen käsittely on rajattava siihen, mikä on välttämätöntä käsittelyn tarkoitusten kannalta, ja henkilötietoihin kohdistuva pääsy on estettävä siltä osin kuin se ei ole perusteltua.

Pääsynhallinnan avulla varmistetaan, että henkilötietoja käsitellään vain niiltä osin ja niiden henkilöiden toimesta kuin on käsittelyn kannalta tarpeellista.

B2.1 Luotettava ensitunnistaminen

Vaadittu liite: Liite 2
Edellytys: Käyttäjien henkilöllisyys varmistetaan luotettavasti ennen pääsyn avaamista aineistoon.

☐ Kyllä ☐ Ei

Lisätiedot:

B2.2 Monivaiheinen tunnistautuminen (MFA) ennen aineistoihin pääsyä

Vaadittu liite: Liite 2
Edellytys: Henkilökohtainen käyttäjätunnus ja MFA ennen aineistoihin pääsyä (perusteltu poikkeus suojatun alueen mallissa mahdollinen).

☐ Kyllä ☐ Ei

Lisätiedot:

B2.3 Käyttöoikeudet vain tietoluvan mukaisesti

Vaadittu liite: Liite 2
Edellytys: Käyttöoikeudet aineistoon myönnetään vain tietoluvassa mainituille henkilöille ja vähimpien oikeuksien periaatteella.

☐ Kyllä ☐ Ei

Lisätiedot:

B3 Datan suojaus: eristys ja ulosviennin estäminen (GDPR 5(1)(f) ja 32 artikla; toisiolaki 18 §)

Toisiolain 18 § edellyttää, että henkilötietojen käsittelyssä varmistetaan riittävä tietoturvallisuus siten, ettei tietoja käytetä tai luovuteta käyttötarkoituksen vastaisesti, ja että salassapitovelvoite toteutuu.

Yleinen tietosuoja-asetus edellyttää vastaavasti henkilötietojen suojaamista luvattomalta tai lainvastaiselta käsittelyltä.

Näiden vaatimusten täyttämiseksi henkilötietoja sisältävä käsittely-ympäristö on teknisesti eristettävä ja henkilötietojen luvaton ulosvienti tai siirtäminen estettävä.

B3.1 Verkkoyhteyksien suojaus

Vaadittu liite: Liite 1
Edellytys: Aineiston käsittely-ympäristö on erotettu muista verkoista siten, ettei aineistoon kohdistu uhkia verkkoyhteyksien välityksellä.

☐ Kyllä ☐ Ei

Lisätiedot:

B3.2 Ulosviennin estot (kopiointi)

Vaadittu liite: Liite 3
Edellytys: Käyttäjältä estetty mahdollisuus viedä henkilötietoja ulos ympäristöstä tietoluvan vastaisesti.

☐ Kyllä ☐ Ei

Lisätiedot:

B3.3 Salaus siirrossa ja avainten hallinta (tarvittaessa)

Vaadittu liite: Liite 1
Edellytys: Julkisen/heikommin suojatun verkon yli liikenne on salattu ja avaintenhallinta järjestetty.

❒ Kyllä ❒ Ei

Lisätiedot:

B4 Lokitus ja jäljitettävyys (GDPR 5(2), 24 ja 32 artikla; toisiolaki 18 §)

Toisiolain 18 § edellyttää aktiivista valvontaa henkilötietojen käsittelyssä. Yleinen tietosuoja-asetus puolestaan edellyttää rekisterinpitäjältä osoitusvelvollisuutta eli kykyä osoittaa henkilötietojen käsittelyn lainmukaisuus.

Lokituksen ja jäljitettävyyden avulla mahdollistetaan käsittelyn valvonta, luvan mukaisten käyttörajoitusten noudattamisen todennettavuus sekä poikkeamien ja väärinkäytösten havaitseminen ja selvittäminen.

B4.1 Käyttölokien vähimmäissisältö

Vaadittu liite: Liite 4
Edellytys: Lokit mahdollistavat vähintään käyttäjäkohtaisen käsittely-ympäristön sisään- ja ulos-kirjautumisten jäljitettävyyden.

❒ Kyllä ❒ Ei

Lisätiedot:

B4.2 Lokien suojaus ja säännöllinen seuranta

Vaadittu liite: Liite 4
Edellytys: Lokit suojataan kuten arkaluonteinen data ja niitä seurataan säännöllisesti.

❒ Kyllä ❒ Ei

Lisätiedot:

B4.3 Lokit toimitettavissa pyynnöstä

Vaadittu liite: Liite 4
Edellytys: Lokit ovat toimitettavissa tietolupaviranomaiselle pyynnöstä ilman aiheetonta viivytystä.

❒ Kyllä ❒ Ei
Lisätiedot:

B5 Tietoluvan päättyminen: pääsyn katkaisu ja aineiston poisto (GDPR 32 artikla)

Yleisen tietosuoja-asetuksen mukaan henkilötietoja saa säilyttää ja käsitellä tunnistettavassa muodossa vain niin kauan kuin käsittelyn tarkoitukset sitä edellyttävät. Näiden vaatimusten toteuttaminen edellyttää, että pääsy henkilötietoihin katkeaa ja tiedot poistetaan tai muutoin saatetaan käsittelykelvottomiksi käsittelyn päättyessä.

B5.1 Pääsyn automaattinen päättyminen tietoluvan päättyessä

Vaadittu liite: Liite 2
Edellytys: Pääsy aineistoon katkaistaan tietoluvan päättyessä.

❒ Kyllä ❒ Ei

Lisätiedot:

B5.2 Aineiston poisto määräajassa + todennettavuus

Vaadittu liite: Liite 5
Edellytys: Aineistot poistetaan tietoturvallisesti määräajassa ja poistosta syntyy todennettava raportti/merkintä.

❒ Kyllä ❒ Ei

Lisätiedot:

B6 Tietosuojan vaikutustenarviointi (DPIA) (GDPR 35 ja 89 artikla; toisiolaki 18 §)

Toisiolain 18 § edellyttää riskienhallintaa osana henkilötietojen käsittelyn riittävää tietoturvallisuutta. Yleinen tietosuoja-asetus edellyttää tietosuojaa koskevan vaikutustenarvioinnin laatimista, kun käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille.

Vaikutustenarvioinnin avulla tunnistetaan ja arvioidaan käsittelyyn liittyvät riskit sekä määritetään toimenpiteet, joilla käyttörajoitukset, salassapitovelvoite ja rekisteröidyn suoja toteutuvat käytännössä.

B6.1 DPIA käyttöympäristöstä

Vaadittu liite: Liite 6
Edellytys: Käyttöympäristöstä on laadittu GDPR 35 artiklan mukainen DPIA.

❒ Kyllä ❒ Ei

Lisätiedot:

4 Liitteet

Valitse toimitettavat liitteet. **Huom! Toimita vain kuvauksen kannalta olennainen tieto.**

❒ **Liite 1:** Arkkitehtuuri, käsittely-ympäristön eriytys ja verkkorajoitukset
❒ **Liite 2:** Käyttövaltuushallinnan kuvaus (ensitunnistus, MFA, oikeuksien myöntö/päättyminen)
❒ **Liite 3:** Ulosvientiestot (kopiointi)
❒ **Liite 4:** Lokitus (sisältö, suojaus, seuranta)
❒ **Liite 5:** Tietoturvallisuuden hallinta (roolit, riskit, valvonta, reagointi, aineiston poisto)
❒ **Liite 6:** DPIA-tiivistelmä riskeistä käyttöympäristöä koskien

5 Tulevan rekisterinpitäjän vakuutus

Päätöksen saaja (tietoluvan mukainen rekisterinpitäjä) sitoutuu noudattamaan tämän Lomake B:n ja sen liitteiden mukaisia käyttöympäristöä koskevia teknisiä ja organisatorisia järjestelyjä koko tietoluvan voimassaolon ajan siltä osin kuin Findata on hyväksynyt ne tietolupapäätöksessä.

Päätöksen saaja sitoutuu varmistamaan, että henkilötietojen käsittely tapahtuu ainoastaan tietolupapäätöksessä hyväksytyssä käyttöympäristössä ja että käyttöympäristö täyttää jatkuvasti tässä Lomake B:ssä kuvatun suojaustason.

Päätöksen saaja sitoutuu ilmoittamaan Findatalle etukäteen kaikista olennaisista tietoturvaa heikentävistä muutoksista käyttöympäristöön tai sen hallintaan, mukaan lukien muutokset, joilla voi olla vaikutusta riskienhallintaan, pääsynhallintaan, aktiiviseen valvontaan, lokitukseen, tietojen ulosvientiin, alihankkijoihin tai käyttöympäristön sijaintiin. Olennaiset muutokset voidaan toteuttaa vasta Findatan hyväksynnän jälkeen. Jos Findata ei hyväksy muutoksia, se voi peruuttaa tietoluvan.

Vakuutamme, että tämän lomakkeen tiedot ovat oikeita ja ajantasaisia. Sitoudumme noudattamaan tietoluvan käyttörajoja (pääsy vain tietoluvassa mainituille henkilöille), suojaamaan aineiston ja estämään ulosviennin luvan vastaisesti sekä katkaisemaan pääsyn ja poistamaan aineiston tietoluvan päättyessä.

Paikka ja päiväys: _____
Nimi, tehtävä (johto): _____
Allekirjoitus / sähköinen vahvistus: _____

LISÄOSA C – KOLMAS MAA (täytetään vain tarvittaessa)

Täytä tämä osa, jos käyttöympäristö sijaitsee EU/ETA:n ulkopuolella. ETA:n ulkopuolelle siirto edellyttää GDPR:n mukaista siirtoperustetta ja tapauskohtaista arviointia sekä tarvittaessa täydentäviä suojatoimia.

C1 TIA ja täydentävät suojatoimet

Edellytys: Siirtoperusteen toimivuus arvioitu tapauskohtaisesti rekisterinpitäjän toimesta ja täydentävät suojatoimet tunnistettu/toteutettu tarvittaessa.

☐ Kyllä ☐ Ei

Lisätiedot:

C2 Alihankkijat ja edelleen luovutus

Edellytys: Alihankkijat/edelleen luovutukset kartoitettu ja hallittu rekisterinpitäjän toimesta (sijainnit ja sopimukset).

☐ Kyllä ☐ Ei

Lisätiedot: