

Tietosuojaseloste (GDPR)

Voimassa alkaen: 07.09.2025

Tämä tietosuojaseloste on laadittu EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ("GDPR") 12–14 artiklojen mukaisesti.

1. Rekisterinpitäjä

Everia Oy / Abilvi-palvelu

Y-tunnus: 3487928-7

Sähköposti: tuki@abilvi.fi

Puhelin: 020 755 9060

Postiosoite: Kukkolinankatu 5, 55120 Imatra

2. Yhteyshenkilö tietosuoja-asioissa

Vastuuhenkilö: Niklas Mäkelä, niklas.makela@everia.fi, p. 020 755 9060

3. Henkilötietojen käsittelyn tarkoitukset

- Käyttäjätilien hallinta ja todennus (kirjautuminen, SSO / OIDC / SAML)
- Kokeiden ("kokeet") luonti, hallinta ja ajastus
- Lokitus ja tietoturvan varmistaminen (häiriötilanteiden selvitys, väärinkäytösten estäminen)
- Järjestelmän tekninen analytiikka ja suorituskyvyn seuranta (Matomo, itse isännöity)
- Tukipyyntöihin vastaaminen
- Varaus- ja kapasiteettipalvelinten provisiointi ja hallittu alasajo

4. Käsittelyn oikeusperusteet (GDPR 6 art.)

Tarkoitus	Oikeusperuste
Peruskäyttö / kirjautuminen	Sopimus (GDPR 6(1)(b))
Palvelun tietoturva ja lokitus	Oikeutettu etu (GDPR 6(1)(f))
Analytiikka (rajattu, ei profilointia)	Oikeutettu etu (GDPR 6(1)(f))
Virhe- ja kapasiteettiseuranta	Oikeutettu etu
Lainsäädännöllisten velvoitteiden täyttäminen (esim. tietoturvaloukkaukset)	Lakisääteinen velvoite (GDPR 6(1)(c))

Oikeutettua etua arvioitaessa on huolehdittu minimoinnista, pseudonymisoinnista ja rajoitetuista säilytysajoista.

5. Käsiteltävät henkilötietoryhmät

- Perustiedot: nimi (etunimi, sukunimi), sähköpostiosoite
- Tunnistetiedot: käyttäjätunnus / sisäinen ID, kirjautumislähde

- Lokitiedot: IP-osoite, ajankohdat, tekniset pyyntöparametrit (rajattu), virhelogit
- Kokeisiin liittyvät hallinnolliset metatiedot (kokeen nimi, ajastus)
- Pilvipalvelinresurssien tekniset tunnisteet (ei sisällä sisältöaineistoa)

Ei käsitellä arkaluonteisia erityisiä henkilötietoryhmiä (GDPR 9 art.). Palvelu ei tee profilointia tai automatisoituja päätöksiä, joilla olisi oikeusvaikutuksia.

6. Tietolähteet

- Käyttäjä itse rekisteröitymisen / kirjautumisen yhteydessä
- SSO-palveluntarjoajat (OIDC / SAML) välittävät vahvistetut attribuutit (esim. nimi, sähköposti)
- Järjestelmän tekniset lokit (automaattisesti muodostuvat)

7. Vastaanottajat ja luovutukset

Henkilötietoja ei myydä eteenpäin.

Tekniset alihankkijat / infrastruktuuritoimittajat:

- Hetzner / UpCloud (palvelininfrastrukturi)
- PowerDNS (DNS-hallinta) - Sähköpostipalvelimen välittäjä (SMTP)

Sopimuksilla varmistetaan tietosuojan toteutuminen (GDPR 28 art.).

8. Siirrot EU/ETA:n ulkopuolelle

Tavoite on käsitellä tiedot EU/ETA-alueella. Mikäli yksittäinen siirto tapahtuisi (esim. varmistuspalvelu), käytetään GDPR:n luvun V mukaista suojamekanismia (esim. vakiolausekkeet). Ilmoitamme rekisteröidyille olennaisista muutoksista.

9. Säilytysajat

Tietoryhmä	Säilytysaika
Käyttäjätili	Aktiivisuuden päättymisen jälkeen enintään 24 kk tai pyyntö poistosta (ellei lakisääteinen velvoite estä)
Lokit (tietoturva)	90 vrk, vakavien häiriöiden selvityspoikkeus max 12 kk
Kokeiden metatiedot	Kokeen päättymisestä 12 kk (anonymisoidaan / poistetaan tämän jälkeen)
Palvelininfrastruktuurin provisiointitiedot	Automaattinen poisto viimeistään 30 vrk tuhoutumisesta
Tukipyynnöt	12 kk käsittelyn päättymisestä

Tietoja voidaan anonymisoida ennen poistoa tilastollisiin tarkoituksiin.

10. Suojauksen periaatteet

Tekniset toimet:

- Salaus siirrossa (HTTPS / TLS)
- Rajoitettu pääsy (roolipohjaiset käyttöoikeudet)
- Palvelinresurssien eristys ja automatisoitu provisiointi
- Lokien pääsynvalvonta ja minimointi
- Hajautettu varmistus (ilman tarpeetonta henkilötietoa)

Organisatoriset toimet:

- Henkilöstön salassapitositoumukset
- Rajoitettu pääsoikeus vain tarpeellisille
- Prosessit tietoturvaloukkausten havaitsemiseksi ja ilmoittamiseksi

11. Rekisteröidyn oikeudet

Rekisteröidyllä on (GDPR 15–22 art.):

- Oikeus saada pääsy tietoihin (tarkastusoikeus)
- Oikeus oikaista virheelliset tiedot
- Oikeus poistaa tiedot ("oikeus tulla unohdetuksi") edellytysten täytyessä
- Oikeus rajoittaa käsittelyä
- Oikeus vastustaa käsittelyä oikeutetun edun perusteella
- Oikeus siirtää tiedot koneluettavassa muodossa
- Oikeus peruuttaa suostumus (jos käsittely perustuisi suostumukseen; ei pääasiallisesti käytössä) - Oikeus tehdä valitus valvontaviranomaiselle: Tietosuojavaltuutetun toimisto (<https://tietosuoja.fi>)

Oikeuspyynnöt: rekisterin yhteyshenkilölle (Niklas Mäkelä)

Vastaamme ilman aiheutonta viivytystä ja viimeistään 30 päivän kuluessa (tarvittaessa +60 päivää GDPR 12(3) mukaisesti).

12. Evästeet ja vastaavat tekniikat

Palvelu käyttää:

- Välttämättömiä istuntoevästeitä (kirjautumisen ylläpito)
- CSRF-suojaeväste / token Ei kolmannen osapuolen markkinointievästeitä.

Selainasetuksilla voi estää evästeet, mutta välttämättömät evästeet ovat toiminnan kannalta pakollisia.

13. Analytiikka

Itse isännöity Matomo:

- IP-osoite lyhennetään/anonymisoidaan ennen tallennusta
- Ei kolmannen osapuolen jakelua
- Tietoja käytetään palvelun laadun ja suorituskyvyn seurantaan

14. Lokit

Lokit voivat sisältää IP-osoitteen, aikaleiman, resurssipolun ja virhekoodit.

Lokeja käytetään vain:

- Tietoturva (tunkeutumisten torjunta)
- Virhetilanteiden diagnostiikka
- Kapasiteetin suunnittelu

15. Automaattinen päätöksenteko / profilointi

Ei suoriteta automatisoitua päätöksentekoa tai profilointia, jolla olisi oikeusvaikutuksia.

16. Tietoturvaloukkaukset

Mahdollisista henkilötietojen tietoturvaloukkauksista ilmoitetaan: - Tietosuojaviranomaiselle 72 h kuluessa, jos vaadittu (GDPR 33) - Rekisteröidyille, jos korkea riski oikeuksille/vapauksille (GDPR 34)

17. Muutokset selosteeseen

Päivitetty versio julkaistaan tässä tiedostossa. Olennaisista muutoksista voidaan ilmoittaa sähköpostitse tai palvelun sisäisesti.

18. Yhteydenotot

Tietosuoja- ja oikeuspyynnöt: rekisterin yhteyshenkilölle (Niklas Mäkelä)

Pyynnön nopeuttamiseksi kuvaa:

- Mitä oikeutta käytät
- Riittävä yksilöinti henkilöllisyyden varmentamiseksi

19. Versiohistoria

- 1.0 (07.09.2025): Ensiversio

Tämä dokumentti on informatiivinen. Tarvittaessa hanki erillinen juridinen arvio.