# Tietosuojaseloste ja evästekäytäntö

Lapuro Platform - EU:n yleisen tietosuoja-asetuksen (GDPR) mukainen rekisteri- ja evästeseloste

**Keskeiset muutokset versiossa 1:**

Tietosuojaseloste ja evästekäytäntö julkaistu.

## 1. Rekisterinpitäjä, palvelun toimittaja ja yhteystiedot

**Ohjelman ja SaaS-palvelun toimittaja:** BuildComet Oy (info@buildcomet.fi)

**Rekisterinpitäjä (alustan käyttäjätilit, asiakkuudet ja laskutus):** BuildComet Oy

**Asiakaskohtaisen datan osalta (Käsittelijä / Data Processor):** Kukin asiakasyritys toimii rekisterinpitäjänä oman henkilöstönsä, asiakkaidensa ja liiketoimintatietojensa osalta, ja BuildComet Oy toimii EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisena henkilötietojen käsittelijänä.

**Tietosuojayhteydenotot:** info@buildcomet.fi

## 2. Rekisterin nimi ja kohderyhmä

Lapuro Platform -palvelun käyttäjä-, asiakkuus- ja järjestelmälokirekisteri. Rekisteröityjä ovat Palvelun käyttäjät, asiakasyritysten yhteyshenkilöt sekä järjestelmään kirjatut työntekijät.

## 3. Henkilötietojen käsittelyn tarkoitus ja oikeusperuste

Henkilötietoja käsitellään seuraaviin tarkoituksiin:

1. **SaaS-palvelun tarjoaminen ja sopimuksen täyttäminen (GDPR 6.1 b):** Käyttäjätilien luominen, todennus, istuntojen hallinta, toiminnanohjaus ja asiakkuuksien hallinta.
2. **Lakisääteiset velvoitteet (GDPR 6.1 c):** Kirjanpito- ja laskutustietojen säilytys sekä työaikalain mukaisten tietojen ylläpito.
3. **Oikeutettu etu (GDPR 6.1 f):** Järjestelmän tietoturvan varmistaminen, virheiden selvitys ja audit-lokien kerääminen väärinkäytösten estämiseksi.

## 4. Käsiteltävät henkilötietoryhmät

- **Perustiedot:** Etu- ja sukunimi, sähköpostiosoite, käyttäjätunnus, puhelinnumero, yrityksen nimi ja Y-tunnus.
- **Rooli- ja käyttöoikeustiedot:** Organisaatiorooli (Admin, Manager, Accountant, Employee) ja järjestelmäoikeudet.
- **Palvelun käyttötiedot:** Työaikakirjaukset, projektitehtävät, asiakas- ja sopimustiedot, laskutusmerkinnät.
- **Tietoturva- ja lokitiedot:** Kirjautumisajankohdat, IP-osoitteet tietoturvalokeissa ja audit-lokimerkinnät kriittisistä toimenpiteistä.
- **Whistleblowing-tiedot:** Anonyymit ilmoitukset ja vastaukset tallennetaan tietokantaan omalla erillisellä sovellustason AES-256 -salauksella ilman käyttäjän tunnistetietoja tai IP-osoitetta.

### 5. Evästeet (Cookies)

Palvelussa noudatetaan tiukkaa tietosuojaperiaatetta evästeiden suhteen:

- **Ei seuranta- tai markkinointievästeitä:** Emme käytä kolmannen osapuolen mainosverkostoja, kävijäseurantaa tai profilointievästeitä.
- **Vain välttämättömät evästeet:** Käytämme ainoastaan teknisesti pakollisia evästeitä ja selaimen paikallista tallennustilaa:
- **Istuntoeväste:** Ylläpitää käyttäjän kirjautumisistuntoa turvallisesti istunnon ajan (poistuu selaimen sulkeutuessa tai uloskirjautumisen yhteydessä).
- **Tietoturvaeväste:** Suojaa käyttäjää ja palvelua sivustojen väliseltä pyynnön väärentämiseltä (CSRF-suojaus).
- **Evästeasetus:** Tallentaa kuittauksen evästeilmoituksen näyttämisestä selaimen paikalliseen muistiin (localStorage).

### 6. Tietojen luovutukset ja siirrot EU/ETA-alueen ulkopuolelle

Tietoja säilytetään ja käsitellään Euroopan unionin (EU) ja Euroopan talousalueen (ETA) alueella sijaitsevissa suojatuissa konesaleissa (Google Cloud Platform Finland/EU, konesalialue `europe-north1` Hamina, Suomi). Tietoja ei siirretä EU/ETA-alueen ulkopuolelle. Tietoja luovutetaan viranomaisille vain pakottavan lainsäädännön niin vaatiessa.

### 7. Tietojen säilytysaika ja monitasoinen suojaus (Pilvi & Tietokanta)

- **Säilytysaika:** Käyttäjätiedot säilytetään aktiivisen asiakkuussuhteen ajan ja poistetaan tai anonymisoidaan asiakkuuden päätyttyä, ottaen huomioon lakisääteiset säilytysajat (esim. kirjanpitoaineisto 6–10 vuotta).
- **Tiedonsiirron salaus (In transit):** Kaikki tiedonsiirto käyttäjän selaimen ja palvelimen välillä on aina suojattu vahvalla TLS-salauksella (HTTPS).
- **Pilvitallennuksen salaus omalla avaimella (Google Cloud Storage):** Kaikki pilveen tallennetut dokumentit, tiedostot ja KYC-aineistot salataan pilvessä omalla erillisellä Customer-Managed Encryption Key (CMEK / Cloud KMS AES-256) -avaimella.
- **Tietokannan salaus omalla itsenäisellä avaimella (Database):** Arkaluonteiset tiedot (kuten palkkatiedot, pankkitilitiedot IBAN, veroprosentit sekä anonyymit whistleblowing-ilmoitukset) salataan tietokantaan kenttäkohtaisesti omalla, erillisellä ja riippumattomalla sovellustason AES-256 -salausavaimella. Pilven ja tietokannan salausavaimet ovat toisistaan täysin erilliset, mikä muodostaa kaksitasoisen suojauksen.

### 8. Rekisteröidyn oikeudet

Rekisteröidyllä on GDPR:n mukainen oikeus:

- Saada pääsy omiin tietoihinsa ja tarkastaa ne.
- Vaatia virheellisten tai puutteellisten tietojen oikaisemista.
- Vaatia tietojen poistamista ("oikeus tulla unohdetuksi") siltä osin kuin lakisääteinen velvoite ei edellytä tietojen säilyttämistä.
- Tehdä valitus toimivaltaiselle valvontaviranomaiselle (Tietosuojavaltuutetun toimisto, www.tietosuoja.fi).