# Politica di Sicurezza – GreenOnline B.V.

Versione 1.5 – 4 giugno 2025

Questo documento descrive la politica di sicurezza delle informazioni di GreenOnline B.V. ed è applicabile a tutti i nostri siti web, inclusi: moneytoring.com, opzeggen.nl e opzeggen.be.

GreenOnline B.V. ha sede in Tommaso Albinonistraat 7, 1083 HM Amsterdam, ed è registrata presso la Camera di Commercio dei Paesi Bassi con il numero 34202424.

## 1. Sicurezza delle informazioni come principio fondamentale

Per GreenOnline, la sicurezza dei dati e dei sistemi è una priorità assoluta. Pur riconoscendo che la sicurezza assoluta non esiste, adottiamo tutte le misure ragionevoli e necessarie per proteggere la nostra infrastruttura, i dati e i software da accessi non autorizzati, perdite e abusi.

I nostri dipendenti sono consapevoli del loro ruolo nella protezione dei dati e vengono costantemente informati sui rischi e sulle procedure di sicurezza.

---

## 2. Hosting e infrastruttura

Le nostre applicazioni sono ospitate su server situati all'interno dell'Unione Europea. Attualmente utilizziamo Amazon Web Services (AWS), i cui data center sono certificati secondo standard internazionali tra cui:

- ISO/IEC 27001 – Sicurezza delle informazioni
- ISO/IEC 27017 – Sicurezza nel cloud
- ISO/IEC 27018 – Protezione dei dati personali nel cloud

Abbiamo inoltre avviato la transizione verso LICO Innovations come partner di hosting supplementare. LICO è certificata ISO/IEC 27001 e si distingue come partner affidabile per lo sviluppo e l’hosting sicuro di software all’interno dell’UE. Questa scelta riflette la nostra ambizione di

costruire un’infrastruttura trasparente, scalabile e indipendente dalle grandi piattaforme cloud.

L’accesso ai server è limitato ai dipendenti autorizzati tramite un firewall gestito. Gli accessi vengono registrati e l'infrastruttura è costantemente monitorata per rilevare eventuali anomalie. Gli aggiornamenti di sicurezza (patch) vengono applicati attivamente e tempestivamente. Nell’ambiente LICO, l’accesso è ulteriormente limitato all’autenticazione SSH.

---

### 3. Crittografia e protezione dei dati

- I dati sensibili vengono archiviati in forma crittografata (“at rest”) utilizzando la crittografia AES-256.
- I trasferimenti di dati tra gli utenti e i nostri server avvengono tramite HTTPS con crittografia TLS.
- I backup giornalieri vengono creati automaticamente. Non sono crittografati, ma sono accessibili solo in un ambiente di backup sicuro.
- L'accesso ai dati è riservato esclusivamente a personale autorizzato.
- I dati personali rimangono sempre all'interno dello Spazio Economico Europeo (SEE).

---

### 4. Sicurezza delle applicazioni

I nostri software sono sviluppati secondo il principio del "secure-by-design" e utilizzano un moderno framework web che protegge dalle vulnerabilità più comuni, tra cui:

- Iniezioni SQL
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)

Le password e le credenziali di autenticazione non vengono mai memorizzate nel codice sorgente, ma fornite tramite parametri di configurazione esterni. Non registriamo mai informazioni sensibili come password o token nei log delle applicazioni.

---

**5. Ambiente di test e sviluppo**

Per lo sviluppo e i test utilizziamo un ambiente separato e rigorosamente isolato:

- I dati personali provenienti dall'ambiente di produzione non vengono utilizzati.
- L'accesso è limitato al solo personale autorizzato.
- Le nuove funzionalità vengono sempre testate prima in quest'ambiente, prima di essere rilasciate in produzione.

---

**6. Note finali**

Continuiamo a migliorare ed aggiornare la nostra politica di sicurezza in modo continuo. Partner e clienti che hanno domande specifiche o richiedono garanzie aggiuntive possono contattarci via email: info@greenonline.nl.