Security Policy – GreenOnline B.V.

Versie 1.5 – 4 juni 2025

Dit document beschrijft het informatiebeveiligingsbeleid van GreenOnline B.V. en is van toepassing op al onze websites, waaronder: moneytoring.com, opzeggen.nl en opzeggen.be.

GreenOnline B.V. is gevestigd aan de Tommaso Albinonistraat 7, 1083 HM Amsterdam en geregistreerd bij de Kamer van Koophandel onder nummer 34202424.

1. Informatiebeveiliging als uitgangspunt

Bij GreenOnline staat de veiligheid van gegevens en systemen centraal. Hoewel absolute veiligheid niet bestaat, nemen wij alle redelijke en noodzakelijke maatregelen om onze infrastructuur, data en software te beschermen tegen ongeautoriseerde toegang, verlies en misbruik.

Onze medewerkers zijn zich bewust van hun rol in het beschermen van gegevens en worden actief geïnformeerd over beveiligingsrisico's en -procedures.

---

2. Hosting & infrastructuur

Onze applicaties draaien op servers binnen de Europese Unie. Momenteel maken wij gebruik van Amazon Web Services (AWS), met datacenters die voldoen aan internationale standaarden en certificeringen, waaronder:

- **ISO/IEC 27001** – Informatiebeveiliging
- **ISO/IEC 27017** – Cloudbeveiliging
- **ISO/IEC 27018** – Bescherming van persoonsgegevens in de cloud

Daarnaast zijn wij gestart met de overstap naar **LICO Innovations** als aanvullende hostingpartner. LICO is **ISO/IEC 27001-gecertificeerd** en onderscheidt zich als betrouwbare partij voor veilige softwareontwikkeling en hosting binnen de EU. Deze stap past bij onze ambitie om onze

beveiliging transparant, schaalbaar en onafhankelijk van grote cloudplatformen in te richten.

Toegang tot servers is beperkt tot geautoriseerde medewerkers via een beheerde firewall. Toegang wordt gelogd en de infrastructuur wordt continu gemonitord op afwijkingen. Beveiligingsupdates (patches) worden actief en tijdig toegepast. Binnen de LICO-omgeving is toegang bovendien uitsluitend mogelijk via SSH-authenticatie voor extra beperking.

---

3. Versleuteling en databeveiliging

- Alle data wordt **versleuteld opgeslagen (“at rest”)** met AES-256 encryptie.
- Gegevensoverdracht tussen gebruikers en onze servers vindt plaats via **HTTPS met TLS-encryptie**.
- Dagelijkse back-ups worden automatisch gemaakt. Deze worden niet versleuteld opgeslagen, maar zijn enkel toegankelijk binnen een beveiligde back-upomgeving.
- Gegevens zijn alleen toegankelijk voor medewerkers met een geautoriseerde rol.
- Persoonsgegevens blijven te allen tijde binnen de Europese Economische Ruimte (EER).

---

4. Applicatiebeveiliging

Onze software wordt ontwikkeld volgens de principes van **secure-by-design** en maakt gebruik van een modern webframework dat beschermt tegen veelvoorkomende kwetsbaarheden zoals:

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

Wachtwoorden en authenticatiegegevens worden nooit in de broncode opgeslagen, maar via externe configuratieparameters aangeleverd. We

loggen geen gevoelige gegevens zoals wachtwoorden of tokens in onze applicatielogs.

---

5. Test- en ontwikkelomgeving

Voor ontwikkeling en testen gebruiken wij een gescheiden omgeving die strikt is afgeschermd.

- Persoonsgegevens uit productie worden hier **niet** gebruikt.
- Toegang is beperkt tot geautoriseerd personeel.
- Nieuwe functionaliteit wordt eerst hier getest voordat deze naar productie gaat.

---

6. Slotopmerkingen

Wij blijven ons beveiligingsbeleid continu verbeteren en evalueren. Partners of klanten die specifieke vragen hebben over ons beleid of aanvullende garanties wensen, kunnen contact opnemen via **info@greenonline.nl**.