Sicherheitsrichtlinie – GreenOnline B.V.

Version 1.5 – 4. Juni 2025

Dieses Dokument beschreibt die Informationssicherheitsrichtlinie von GreenOnline B.V. und gilt für alle unsere Websites, darunter: moneytoring.com, opzeggen.nl und opzeggen.be.

GreenOnline B.V. hat seinen Sitz in der Tommaso Albinonistraat 7, 1083 HM Amsterdam, und ist bei der niederländischen Handelskammer unter der Nummer 34202424 registriert.

1. Informationssicherheit als Grundprinzip

Bei GreenOnline steht die Sicherheit von Daten und Systemen im Mittelpunkt. Auch wenn absolute Sicherheit nicht existiert, treffen wir alle angemessenen und notwendigen Maßnahmen, um unsere Infrastruktur, Daten und Software vor unbefugtem Zugriff, Verlust und Missbrauch zu schützen.

Unsere Mitarbeitenden sind sich ihrer Verantwortung beim Schutz von Daten bewusst und werden regelmäßig über Sicherheitsrisiken und -verfahren informiert.

---

2. Hosting & Infrastruktur

Unsere Anwendungen laufen auf Servern innerhalb der Europäischen Union. Derzeit nutzen wir Amazon Web Services (AWS), mit Rechenzentren, die internationalen Standards und Zertifizierungen entsprechen, unter anderem:

- ISO/IEC 27001 – Informationssicherheit
- ISO/IEC 27017 – Cloud-Sicherheit
- ISO/IEC 27018 – Schutz personenbezogener Daten in der Cloud

Zusätzlich haben wir mit dem Wechsel zu LICO Innovations als ergänzendem Hosting-Partner begonnen. LICO ist nach ISO/IEC 27001

zertifiziert und gilt als zuverlässiger Partner für sichere Softwareentwicklung und Hosting innerhalb der EU. Dieser Schritt passt zu unserem Ziel, unsere Infrastruktur transparent, skalierbar und unabhängig von großen Cloud-Plattformen zu gestalten.

Der Zugriff auf Server ist auf autorisierte Mitarbeiter über eine verwaltete Firewall beschränkt. Alle Zugriffe werden protokolliert, und die Infrastruktur wird kontinuierlich auf Auffälligkeiten überwacht. Sicherheitsupdates (Patches) werden aktiv und zeitnah implementiert. Im LICO-Umfeld ist der Zugang zudem ausschließlich über SSH-Authentifizierung möglich.

---

3. Verschlüsselung und Datenschutz

- Sensible Daten werden im Ruhezustand („at rest“) mit AES-256-Verschlüsselung gespeichert.
- Die Datenübertragung zwischen Nutzern und unseren Servern erfolgt verschlüsselt über HTTPS mit TLS.
- Tägliche Backups werden automatisch erstellt. Diese sind nicht verschlüsselt, jedoch ausschließlich innerhalb einer gesicherten Backup-Umgebung zugänglich.
- Der Zugriff auf Daten ist ausschließlich autorisiertem Personal vorbehalten.
- Personenbezogene Daten verbleiben jederzeit innerhalb des Europäischen Wirtschaftsraums (EWR).

---

4. Anwendungssicherheit

Unsere Software wird nach dem „secure-by-design“-Prinzip entwickelt und verwendet ein modernes Web-Framework, das gegen gängige Sicherheitslücken schützt, darunter:

- SQL-Injection

- Cross-Site-Scripting (XSS)
- Cross-Site-Request-Forgery (CSRF)

Passwörter und Authentifizierungsdaten werden niemals im Quellcode gespeichert, sondern über externe Konfigurationsparameter bereitgestellt. Wir protokollieren keine sensiblen Informationen wie Passwörter oder Tokens in unseren Anwendungslogs.

---

5. Test- und Entwicklungsumgebung

Für Entwicklung und Tests verwenden wir eine strikt abgeschottete Umgebung:

- Es werden keine produktiven personenbezogenen Daten verwendet.
- Der Zugriff ist auf autorisiertes Personal beschränkt.
- Neue Funktionen werden zunächst in dieser Umgebung getestet, bevor sie in die Produktion überführt werden.

---

6. Schlussbemerkungen

Wir überprüfen und verbessern unsere Sicherheitsrichtlinien laufend. Partner oder Kunden mit spezifischen Fragen oder dem Wunsch nach zusätzlichen Garantien können sich gerne an uns wenden: **info@greenonline.nl.**