Security Policy – GreenOnline B.V.

Version 1.5 – June 4, 2025

This document outlines the information security policy of GreenOnline B.V. and applies to all our websites, including: moneytoring.com, opzeggen.nl, and opzeggen.be.

GreenOnline B.V. is located at Tommaso Albinonistraat 7, 1083 HM Amsterdam, The Netherlands, and is registered with the Dutch Chamber of Commerce under number 34202424.

1. Information Security as a Core Principle

At GreenOnline, the security of data and systems is a top priority. While absolute security does not exist, we take all reasonable and necessary measures to protect our infrastructure, data, and software from unauthorized access, loss, and misuse.

Our employees are aware of their role in protecting information and are regularly informed about security risks and procedures.

---

2. Hosting & infrastructure

Our applications run on servers located within the European Union. We currently use Amazon Web Services (AWS), with data centers that comply with international standards and certifications, including:

ISO/IEC 27001 – Information Security

ISO/IEC 27017 – Cloud Security

ISO/IEC 27018 – Protection of Personal Data in the Cloud

In addition, we have begun transitioning to LICO Innovations as an additional hosting partner. LICO is ISO/IEC 27001 certified and is recognized as a reliable provider of secure software development and hosting within the EU. This move aligns with our ambition to organize our infrastructure transparently, scalably, and independently of large cloud platforms.

Server access is restricted to authorized personnel through a managed firewall. All access is logged, and the infrastructure is continuously monitored for anomalies. Security updates (patches) are applied actively and promptly. Within the LICO environment, access is further restricted to SSH authentication only.

3. Encryption and Data Security

- Sensitive data is stored encrypted (“at rest”) using AES-256 encryption.
- Data transmission between users and our servers is secured via HTTPS with TLS encryption.
- Daily backups are created automatically. These backups are not encrypted but are stored in a secure backup environment.
- Data is only accessible to employees with authorized roles.
- Personal data always remains within the European Economic Area (EEA).

4. Application Security

Our software is developed according to secure-by-design principles and uses a modern web framework that protects against common vulnerabilities such as:

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

Passwords and authentication credentials are never stored in the source code but are provided through external configuration parameters. We do not log sensitive data such as passwords or tokens in our application logs.

5. Test and Development Environment

We use a separate, strictly isolated environment for development and testing:

- No production personal data is used in this environment.
- Access is limited to authorized personnel.
- New functionality is thoroughly tested in this environment before being released to production.

6. Final Remarks

We continuously evaluate and improve our security policy. Partners or clients with specific questions or who require additional assurances are encouraged to contact us at: **info@greenonline.nl.**