



Política de Seguridad – GreenOnline B.V.

Versión 1.5 – 4 de junio de 2025

Este documento describe la política de seguridad de la información de GreenOnline B.V. y se aplica a todos nuestros sitios web, incluyendo: moneytoring.com, opzeggen.nl y opzeggen.be.

GreenOnline B.V. tiene su sede en Tommaso Albinonistraat 7, 1083 HM Ámsterdam, y está registrada en la Cámara de Comercio de los Países Bajos con el número 34202424.

1. Seguridad de la información como principio básico

En GreenOnline, la seguridad de los datos y sistemas es una prioridad fundamental. Aunque la seguridad absoluta no existe, tomamos todas las medidas razonables y necesarias para proteger nuestra infraestructura, datos y software contra accesos no autorizados, pérdidas y usos indebidos. Nuestros empleados son conscientes de su papel en la protección de la información y reciben formación continua sobre riesgos y procedimientos de seguridad.

2. Alojamiento e infraestructura

Nuestras aplicaciones se ejecutan en servidores ubicados dentro de la Unión Europea. Actualmente utilizamos Amazon Web Services (AWS), cuyos centros de datos cumplen con normas y certificaciones internacionales, como:

- ISO/IEC 27001 – Seguridad de la información
- ISO/IEC 27017 – Seguridad en la nube
- ISO/IEC 27018 – Protección de datos personales en la nube

Además, hemos iniciado la transición hacia LICO Innovations como socio de alojamiento adicional. LICO cuenta con la certificación ISO/IEC 27001 y se distingue como un socio fiable para el desarrollo seguro de software y



alojamiento dentro de la UE. Esta decisión se alinea con nuestra ambición de ofrecer una infraestructura transparente, escalable e independiente de las grandes plataformas en la nube.

El acceso a los servidores está limitado a empleados autorizados mediante un cortafuegos gestionado. Todos los accesos son registrados y la infraestructura se monitoriza de forma continua para detectar anomalías. Las actualizaciones de seguridad (parches) se aplican activamente y de forma oportuna. En el entorno de LICO, el acceso está aún más restringido mediante autenticación SSH.

3. Cifrado y protección de datos

- Los datos sensibles se almacenan cifrados en reposo (“at rest”) usando cifrado AES-256.
- La transferencia de datos entre usuarios y nuestros servidores se realiza mediante HTTPS con cifrado TLS.
- Se realizan copias de seguridad diarias de forma automática. Estas no están cifradas, pero se almacenan en un entorno de respaldo seguro.
- Los datos solo son accesibles por personal con un rol autorizado.
- Los datos personales se almacenan exclusivamente dentro del Espacio Económico Europeo (EEE).

4. Seguridad de las aplicaciones

Nuestros sistemas se desarrollan siguiendo el principio de “secure-by-design” y utilizan un framework web moderno que protege contra vulnerabilidades comunes, como:

- Inyecciones SQL
- Cross-site scripting (XSS)



- Cross-site request forgery (CSRF)

Las contraseñas y credenciales de autenticación nunca se almacenan en el código fuente; se gestionan a través de parámetros de configuración externos. No registramos datos sensibles como contraseñas o tokens en nuestros registros de aplicaciones.

5. Entorno de pruebas y desarrollo

El desarrollo y las pruebas se realizan en un entorno separado, debidamente aislado:

- No se utilizan datos personales del entorno de producción.
 - El acceso está limitado al personal autorizado.
 - Toda nueva funcionalidad se prueba primero en este entorno antes de implementarse en producción.
-

6. Comentarios finales

Revisamos y mejoramos continuamente nuestra política de seguridad. Los socios o clientes que tengan preguntas específicas o deseen garantías adicionales pueden ponerse en contacto con nosotros en:

info@greenonline.nl.