Politique de sécurité – GreenOnline B.V.

Version 1.5 – 4 juin 2025

Ce document décrit la politique de sécurité de l'information de GreenOnline B.V. et s'applique à l’ensemble de nos sites web, y compris : moneytoring.com, opzeggen.nl et opzeggen.be.

GreenOnline B.V. est établi à Tommaso Albinonistraat 7, 1083 HM Amsterdam, et est enregistré auprès de la Chambre de commerce néerlandaise sous le numéro 34202424.

1. Sécurité de l’information comme principe fondamental

Chez GreenOnline, la sécurité des données et des systèmes est une priorité absolue. Bien que la sécurité absolue n'existe pas, nous mettons en œuvre toutes les mesures raisonnables et nécessaires pour protéger notre infrastructure, nos données et nos logiciels contre les accès non autorisés, les pertes et les abus.

Nos collaborateurs sont conscients de leur rôle dans la protection des données et sont régulièrement informés des risques de sécurité et des procédures applicables.

---

2. Hébergement & infrastructure

Nos applications sont hébergées sur des serveurs situés dans l’Union européenne. Nous utilisons actuellement Amazon Web Services (AWS), dont les centres de données respectent les normes et certifications internationales, notamment :

- ISO/IEC 27001 – Sécurité de l'information
- ISO/IEC 27017 – Sécurité du cloud
- ISO/IEC 27018 – Protection des données personnelles dans le cloud

Nous avons également entamé la migration vers LICO Innovations comme partenaire d’hébergement complémentaire. LICO est certifié ISO/IEC

27001 et se distingue comme un partenaire fiable pour le développement de logiciels sécurisés et l'hébergement au sein de l'UE. Cette décision reflète notre ambition d'organiser notre infrastructure de manière transparente, évolutive et indépendante des grandes plateformes cloud.

L'accès aux serveurs est limité aux employés autorisés via un pare-feu géré. Tous les accès sont enregistrés, et l'infrastructure est surveillée en continu pour détecter les anomalies. Les mises à jour de sécurité (patches) sont appliquées activement et sans délai. Dans l'environnement LICO, l'accès est en outre uniquement possible via une authentification SSH.

---

3. Chiffrement et sécurité des données

- Les données sensibles sont stockées de manière chiffrée (« au repos ») à l'aide du chiffrement AES-256.
- Les échanges de données entre les utilisateurs et nos serveurs sont sécurisés via HTTPS avec chiffrement TLS.
- Des sauvegardes quotidiennes sont effectuées automatiquement. Celles-ci ne sont pas chiffrées, mais sont conservées dans un environnement de sauvegarde sécurisé.
- Les données ne sont accessibles qu'aux employés disposant d'un rôle autorisé.
- Les données personnelles sont conservées exclusivement dans l'Espace économique européen (EEE).

---

4. Sécurité des applications

Nos logiciels sont développés selon les principes du "secure-by-design" et s'appuient sur un framework web moderne qui protège contre les vulnérabilités courantes, telles que :

- Injections SQL

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

Les mots de passe et identifiants d'authentification ne sont jamais stockés dans le code source, mais sont fournis via des paramètres de configuration externes. Nous n'enregistrons jamais d'informations sensibles telles que les mots de passe ou les jetons dans les journaux applicatifs.

---

5. Environnement de test et de développement

Le développement et les tests se font dans un environnement distinct et strictement isolé :

- Aucune donnée personnelle issue de la production n'y est utilisée.
- L'accès est limité au personnel autorisé.
- Toute nouvelle fonctionnalité y est testée avant d'être déployée en production.

---

6. Remarques finales

Nous évaluons et améliorons en permanence notre politique de sécurité. Les partenaires ou clients ayant des questions spécifiques ou souhaitant des garanties supplémentaires peuvent nous contacter à l'adresse suivante : **info@greenonline.nl.**