GreenOnline

# Politique de sécurité

Version 1.4 – 14/03/2023

Ce document s'applique aux sites Web : moneytoring.com, opzeggen.nl, opzeggen.be, kündigen.de, cancelar.es, resilieronline.fr, disdetteonline.it, kuendigen.ch, comment-resilier.be, contractterminator.pl qui sont une initiative de GreenOnline BV (www.greenonline.nl) enregistrée auprès de la Chambre de commerce néerlandaise sous le numéro 34202424 et le numéro de TVA NL8129.38.124.B01.

Lorsque vous utilisez nos services sur l'un de vos domaines alternatifs, nous devons, bien sûr, nous assurer que vous le faites en toute sécurité. Nous savons tous que la sécurité à 100% ne peut jamais être garantie, mais chez GreenOnline B.V., nous faisons tout notre possible pour rendre notre plate-forme aussi sûre que possible.

Les applications s'exécutent sur des serveurs dans des centres de données au sein de l'Union européenne. Nous avons acheté ces serveurs auprès d'Amazon Cloud Services (AWS) pour leur expertise et leurs certifications, notamment ISO 27001, ISO 27017 (Cloud Security) et ISO 27018 (Cloud Privacy). Les serveurs fonctionnent sur leur propre réseau interne, auquel seuls les employés autorisés peuvent accéder via un pare-feu géré. Nous surveillons également en permanence les applications et informons les employés de toute activité suspecte. Nous nous assurons également que notre infrastructure est à jour en appliquant des correctifs de sécurité.

Toutes les données sont stockées « à l'état d'inactivité » cryptées (AES-256) et sont automatiquement sauvegardées quotidiennement. Toutes les données envoyées entre vous et nos applications passent par une connexion HTTPS cryptée. Seuls les employés autorisés peuvent accéder aux données. Ces données resteront également à tout moment au sein de l'Union européenne.

Pour éviter les risques de sécurité courants et importants, tels que les attaques par injection, le cross-site scripting et la falsification de requêtes cross-site, nous utilisons un framework Web qui minimise ces risques. Le code source des applications ne contient pas de mots de passe ou d'autres données d'authentification. Ces paramètres sont toujours transmis aux applications en tant que paramètres

externes. Dans les journaux d'application, les mots de passe et autres données d'authentification sont filtrés afin qu'ils n'y soient pas stockés.

Il existe un environnement distinct pour tester les nouvelles fonctionnalités. Aucune information personnelle de l'environnement de production ne peut y être utilisée. Cet environnement est protégé et n'est accessible qu'aux employés autorisés.