GreenOnline
Security Policy
Version 1.4 – 14/03/2023

This security document applies to websites: moneytoring.com, opzeggen.nl, opzeggen.be, kündigen.de, cancelar.es, resilieronline.fr, disdetteonline.it, kuendigen.ch, comment-resilier.be, contractterminator.pl are an initiative of GreenOnline BV (www.greenonline.nl) registered in the Chamber of Commerce in The Netherlands with the number 34202424 and with the VAT number NL8129.38.124.B01.

When you use our services on any of its alternate domains, we must of course ensure that this is done safely. We all know that 100% security can never be guaranteed, but we do everything within GreenOnline B.V. to make and keep our platform as secure as possible.

The applications run on servers in data centers within the European Union. We purchase these servers from Amazon Cloud Services (AWS) for their expertise and certifications, including ISO 27001, ISO 27017 (Cloud Security) and ISO 27018 (Cloud Privacy). The servers run in their own internal network that can only be accessed by authorized employees via a managed firewall. We also constantly monitor the applications and employees are notified of abnormal activities. We also ensure that our infrastructure is up-to-date by applying security patches.

All data is stored "at rest" encrypted (AES-256) and backed up automatically on a daily basis. All data sent between you and our applications go through an encrypted HTTPS connection. The data is only accessible to authorized employees. This data will also remain within the European Union at all times.

To prevent common and important security risks, such as injection attacks, cross-site scripting and cross-site request forgery, we use a web framework that minimizes these risks. The source code of the applications does not contain any passwords or other authentication data. This configuration is always passed to the applications as an external parameter. In the application logs, passwords and other authentication details are filtered so that they are not stored in the logs.

There is a separate environment for testing new features. No personal information from the production environment may be used on this. This environment is protected and accessible only to authorized employees.