GreenOnline

Security Policy

Versie 1.4 – 14 maart 2023

Dit veiligheidsdocument is van toepassing op moneytoring.com, opzeggen.nl, opzeggen.be, kündigen.de, cancelar.es, resilieronline.fr, disdetteonline.it, kuendigen.ch, comment-resilier.be, contractterminator.pl is een initiatief van GreenOnline BV (www.greenonline.nl), ingeschreven bij de Kamer van Koophandel onder nummer 34202424 te Amsterdam (Nederland).
Wanneer u gebruik maakt van onze diensten op een van de alternatieve domeinen daarvan, moeten wij er uiteraard voor zorgen dat dit veilig gebeurt. We weten allemaal dat 100% veiligheid nooit gegarandeerd kan worden, maar we doen er binnen GreenOnline alles aan om ons platform zo veilig mogelijk te maken en te houden.

De applicaties draaien op servers in datacenters binnen de Europese Unie. We kopen deze servers van Amazon Cloud Services (AWS) vanwege hun expertise en certificeringen, waaronder ISO 27001, ISO 27017 (Cloud Security) en ISO 27018 (Cloud Privacy). De servers draaien in een eigen intern netwerk dat alleen toegankelijk is voor geautoriseerde medewerkers via een beheerde firewall. Ook monitoren we continu de applicaties en worden medewerkers op de hoogte gebracht van afwijkende activiteiten. Ook zorgen we ervoor dat onze infrastructuur up-to-date is door beveiligingspatches toe te passen.

Alle gegevens worden "at rest" versleuteld (AES-256) opgeslagen en er wordt dagelijks automatisch een back-up van gemaakt. Alle gegevens die tussen u en onze applicaties worden verzonden, gaan via een versleutelde HTTPS-verbinding. De gegevens zijn alleen toegankelijk voor geautoriseerde medewerkers. Ook deze gegevens blijven te allen tijde binnen de Europese Unie.

Om veelvoorkomende en belangrijke beveiligingsrisico's, zoals injectieaanvallen, cross-site scripting en cross-site request forgery, te voorkomen, gebruiken we een webframework dat deze risico's minimaliseert. De broncode van de applicaties bevat geen wachtwoorden of andere authenticatiegegevens. Deze configuratie wordt altijd als externe parameter doorgegeven aan de

applicaties. In de applicatielogs worden wachtwoorden en andere authenticatiegegevens gefilterd zodat ze niet in de logs worden opgeslagen.

Er is een aparte omgeving voor het testen van nieuwe features. Hierop mogen geen persoonlijke gegevens uit de productieomgeving worden gebruikt. Deze omgeving is afgeschermd en alleen toegankelijk voor geautoriseerde medewerkers.