GreenOnline

Informationssicherheitspolice

Version 1.4 - 14/03/2023

Dieses Sicherheitsdokument gilt für die Websites: moneytoring.com, opzeggen.nl, opzeggen.be, kündigen.de, cancelar.es, resilieronline.fr, disdetteonline.it, kuendigen.ch, comment-resilier.be, contractterminator.pl. Diese sind eine Initiative von GreenOnline BV (www.greenonline.nl), eingetragen bei der Handelskammer in den Niederlanden unter der Nummer 34202424 und mit der Umsatzsteuernummer NL8129.38.124.B01.

Wenn Sie unsere Dienste auf einer der alternativen Domains nutzen, müssen wir natürlich dafür sorgen, dass dies sicher geschieht. Wir alle wissen, dass eine hundertprozentige Sicherheit nie garantiert werden kann, aber wir tun innerhalb von GreenOnline B.V. alles, um unsere Plattform so sicher wie möglich zu machen und zu halten.

Die Anwendungen laufen auf Servern in Datenzentren innerhalb der Europäischen Union. Wir kaufen diese Server von Amazon Cloud Services (AWS), da sie über das nötige Fachwissen und die entsprechenden Zertifizierungen verfügen, darunter ISO 27001, ISO 27017 (Cloud-Sicherheit) und ISO 27018 (Cloud-Datenschutz). Die Server laufen in einem eigenen internen Netzwerk, auf das nur autorisierte Mitarbeiter über eine verwaltete Firewall zugreifen können. Außerdem überwachen wir die Anwendungen ständig, und die Mitarbeiter werden über ungewöhnliche Aktivitäten informiert. Zudem stellen wir sicher, dass unsere Infrastruktur auf dem neuesten Stand ist, indem wir Sicherheits-Patches anwenden.

Alle Daten werden "im Ruhezustand" verschlüsselt (AES-256) gespeichert und täglich automatisch gesichert. Alle Daten, die zwischen Ihnen und unseren Anwendungen gesendet werden, laufen über eine verschlüsselte HTTPS-Verbindung. Die Daten sind nur für autorisierte Mitarbeiter zugänglich. Auch diese Daten bleiben stets innerhalb der Europäischen Union.

Um häufige und wichtige Sicherheitsrisiken wie Injektionsangriffe, Cross-Site-Scripting und Cross-Site-Request-Forgery zu vermeiden, verwenden wir ein Web-Framework, das diese Risiken minimiert. Der Quellcode der Anwendungen enthält keine Passwörter oder andere Authentifizierungsdaten. Diese

Konfiguration wird den Anwendungen immer als externer Parameter übergeben. In den Anwendungsprotokollen werden Passwörter und andere Authentifizierungsdaten gefiltert, damit sie nicht in den Protokollen gespeichert werden.

Für das Testen neuer Funktionen gibt es eine separate Umgebung. In dieser dürfen keine persönlichen Informationen aus der Produktionsumgebung verwendet werden. Diese Umgebung ist geschützt und nur für autorisierte Mitarbeiter zugänglich.