GreenOnline

Politica di Sicurezza

Versione 1.4 – 14/03/2023

Il presente documento di sicurezza si applica ai siti web: moneytoring.com, opzeggen.nl, opzeggen.be, kündigen.de, cancelar.es, resilieronline.fr, disdetteonline.it, kuendigen.ch, comment-resilier.be, contractterminator.pl e sono un'iniziativa di GreenOnline BV (www.greenonline.nl) registrata presso la Camera di Commercio dei Paesi Bassi con il numero 34202424 e con la partita IVA NL8129.38.124.B01.

Quando vengono utilizzati i nostri servizi su uno qualsiasi dei domini alternativi, dobbiamo garantire che ciò avvenga in modo sicuro. Anche se la sicurezza non può mai essere garantita al 100%, noi di GreenOnline B.V. facciamo di tutto per rendere e mantenere la nostra piattaforma il più sicura possibile..

Le applicazioni vengono eseguite su server in centri dati all'interno dell'Unione Europea. Acquistiamo questi server da Amazon Cloud Services (AWS) per la loro esperienza e le loro certificazioni, tra cui ISO 27001, ISO 27017 (sicurezza del cloud) e ISO 27018 (privacy del cloud). I server vengono eseguiti in una rete interna a cui possono accedere solo i dipendenti autorizzati tramite un firewall gestito. Inoltre, monitoriamo costantemente le applicazioni e i dipendenti vengono avvisati in caso di attività anomale. Ci assicuriamo inoltre che la nostra infrastruttura sia aggiornata applicando le patch di sicurezza.

Tutti i dati vengono memorizzati "a riposo" in modo criptato (AES-256) e sottoposti a backup automatico su base giornaliera. Tutti i dati inviati tra lei e le nostre applicazioni passano attraverso una connessione HTTPS crittografata. I dati sono accessibili solo ai dipendenti autorizzati. Inoltre, questi dati rimarranno sempre all'interno dell'Unione Europea.

Per evitare rischi comuni e importanti per la sicurezza, come attacchi di tipo injection, cross-site scripting e cross-site request forgery, utilizziamo un framework web che riduce al minimo questi rischi. Il codice sorgente delle applicazioni non contiene password o altri dati di autenticazione. Questa configurazione viene sempre inviata alle applicazioni come parametro esterno. Nei log delle

applicazioni, le password e gli altri dati di autenticazione vengono filtrati in modo da non essere memorizzati nei log.

Esiste un ambiente separato per testare le nuove funzionalità. In questo ambiente non possono essere utilizzate informazioni personali provenienti dall'ambiente di produzione. Questo ambiente è protetto e accessibile solo ai dipendenti autorizzati.