GreenOnline

Polityka bezpieczeństwa

Wersja 1.4 – 14/03/2023

Niniejszy dokument bezpieczeństwa dotyczy strony www.opzeggen.nl. Strona internetowa www.contractterminator.pl jest inicjatywą firmy GreenOnline BV (www.greenonline.nl), zarejestrowanej w Izbie Handlowej pod numerem 34202424 w Amsterdamie (Holandia).

Kiedy korzystasz z naszych usług na www.contractterminator.pl lub jakiejkolwiek innej domenie, musimy oczywiście zapewnić, że odbywa się to w bezpieczny sposób. Wszyscy wiemy, że 100% bezpieczeństwa nigdy nie może być zagwarantowane, ale robimy wszystko w GreenOnline aby nasza platforma była jak najbezpieczniejsza.

Aplikacje są uruchamiane na serwerach w centrach danych na terenie Unii Europejskiej. Serwery te kupujemy od Amazon Cloud Services (AWS) ze względu na ich doświadczenie i certyfikaty, w tym ISO 27001, ISO 27017 (bezpieczeństwo w chmurze) i ISO 27018 (prywatność w chmurze). Serwery działają w swojej własnej sieci wewnętrznej, do której dostęp mają tylko upoważnieni pracownicy za pośrednictwem zarządzanej zapory sieciowej. Prowadzimy również stały monitoring aplikacji, a pracownicy są powiadamiani o nietypowych działaniach. Dbamy również o to, aby nasza infrastruktura była na bieżąco aktualizowana poprzez stosowanie łatek bezpieczeństwa.

Wszystkie dane są przechowywane "w spoczynku" zaszyfrowane (AES-256) i codziennie automatycznie archiwizowane. Wszystkie dane przesyłane pomiędzy Tobą a naszymi aplikacjami przechodzą przez szyfrowane połączenie HTTPS. Dostęp do danych mają tylko upoważnieni pracownicy. Dane te pozostają również przez cały czas na terenie Unii Europejskiej.

Aby zapobiec powszechnym i ważnym zagrożeniom bezpieczeństwa, takim jak ataki typu injection, cross-site scripting i cross-site request forgery, używamy frameworka, który minimalizuje te zagrożenia. Kod źródłowy aplikacji nie zawiera żadnych haseł ani innych danych uwierzytelniających. Konfiguracja ta jest zawsze przekazywana do aplikacji jako parametr zewnętrzny. W logach aplikacji hasła i inne dane uwierzytelniające są filtrowane tak, aby nie były w nich przechowywane.

Istnieje oddzielne środowisko do testowania nowych funkcji. Nie można na nim wykorzystywać żadnych danych osobowych ze środowiska produkcyjnego. Środowisko to jest chronione i dostępne tylko dla upoważnionych pracowników.