

## Informacje na temat zabezpieczeń

Bezpieczeństwo Twoich plików jest dla nas najważniejsze. Chcemy, aby każdy użytkownik Storino.pl miał pewność, że jego dane przechowywane są w sposób gwarantujący poufność i bezpieczeństwo. Uważamy, że każdy użytkownik ma prawo wiedzieć, w jaki sposób chronione są jego pliki, dlatego przygotowaliśmy dokument opisujący zabezpieczenia wykorzystywane przez nas w Storino.pl.

## Bezpieczne przechowywanie

W celu składowania danych Storino.pl korzysta z usługi Amazon S3 wchodzącej w skład Amazon Web Services (AWS). Amazon jest światowym liderem w dostarczaniu skalowalnych usług internetowych. Serwery Amazon zlokalizowane są w kilku centrach danych umieszczonych w różnych rejonach świata. Usługa S3 zapewnia trwałość danych na poziomie 99.999999999%, co oznacza, że Twoje dane są naprawdę bezpieczne. Więcej informacji na temat zabezpieczeń Amazon można znaleźć na [stronie Amazon Web Services](#). Pliki użytkowników, które przechowywane są na serwerze szyfrowane są przy pomocy algorytmu AES-256. Jest to taki sam standard szyfrowania, jaki stosowany jest przez wojsko do szyfrowania dokumentów o najwyższej klauzuli bezpieczeństwa.

## Bezpieczne transfery

Wysyłanie i odbieranie plików w Storino.pl odbywa się poprzez bezpieczny kanał SSL (Secure Sockets Layer) także z wykorzystaniem szyfrowania kluczem 256-bitowym (AES-256). Takie połączenie stanowi przyjęty standard bezpieczeństwa transmisji internetowej i jest wykorzystywane m.in. przez banki internetowe. Certyfikat SSL wystawiony został przez firmę GeoTrust. Więcej informacji na temat jakości usług firmy GeoTrust można znaleźć na stronie internetowej [www.geotrust.com](http://www.geotrust.com).

Wyjątek stanowią tutaj pliki udostępnione w postaci linków publicznych. Użytkownik samemu decyduje, które pliki chce upublicznić w Internecie. W tym przypadku transmisja nie jest szyfrowana.

## Bezpieczeństwo aplikacji

Aplikacja dla Windows została stworzona w oparciu o technologię .NET. Zespół Storino.pl dołożył wszelkich starań, aby zabezpieczyć aplikację. Aplikacja Storino.pl podpisana jest certyfikatem nadanym przez Thawte, co uniemożliwia modyfikację programu przez nieupoważnione osoby.

Aplikacja Storino.pl jest aktualizowana w sposób automatyczny. Zalecamy zawsze korzystać z aktualizacji – w ten sposób Twoja aplikacja posiada najnowsze funkcje.

Do działania aplikacja Storino.pl wymaga przechowywania meta danych na dysku komputera. Meta dane zawierają informacje o przechowywanych plikach takie jak nazwa, data, rozmiar oraz suma kontrolna pliku. Dostęp przez osoby trzecie do pliku meta danych nie stanowi zagrożenia dla użytkownika i nie umożliwia wykradzenia prywatnego hasła do serwisu.

Należy zaznaczyć, że pomimo zabezpieczeń stosowanych w Storino.pl nie da się uniknąć ryzyka związanego z tzw. 'czynnikiem ludzkim'. Są to oczywiście problemy niezależne od Storino.pl. Dlatego pamiętaj, aby nigdy nie stosować oczywistych haseł, które ktoś mógłby odgadnąć, nie zapisywać haseł na kartkach przyklejonych do klawiatury oraz po prostu uważać na kradzież swojego komputera. Zalecamy stosowanie haseł dłuższych niż 8 znaków oraz zawierających cyfry lub inne znaki alfanumeryczne.

## Prywatność

Pliki użytkowników przechowywane są w postaci zaszyfrowanej przy pomocy algorytmu AES-256. Poza szyfrowaniem nad Twoją prywatnością czuwają precyzyjne procedury bezpieczeństwa stosowane przez naszą firmę.

Przeglądanie zawartości plików przez pracowników Storino.pl jest zabronione. Pracownicy Storino.pl objęci są restrykcyjnymi procedurami pozwalającymi kontrolować kto i w jakim zakresie korzysta z zasobów serwera. Ograniczona liczba pracowników posiada uprawnienia do odczytu meta danych plików (jego nazwy, rozmiaru, daty modyfikacji oraz sumy kontrolnej). Jest to konieczne, aby móc zarządzać usługą Storino.pl oraz usprawniać ją.

