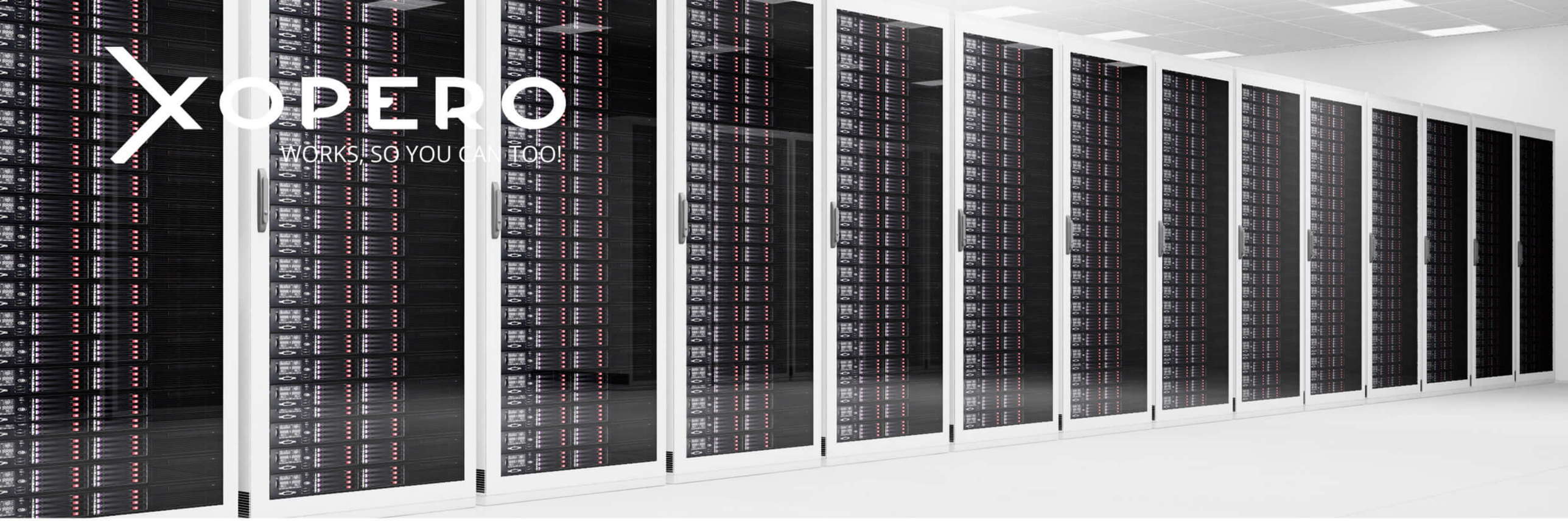

XOPERO WHITEPAPER

Standardy bezpieczeństwa

Dzięki 256 bitowemu szyfrowaniu, serwerom w niezależnych lokalizacjach oraz fizycznym zabezpieczeniom w centrach danych, gwarantujemy naszym klientom bezpieczeństwo danych na najwyższym poziomie.

AES 256
certyfikat SSL
dwie lokalizacje
Aktówka
forma rozproszona
weryfikacja poprawności

Backup danych

Wszystkie dane są szyfrowanie za pomocą algorytmu AES 256 i dopiero tak przygotowany plik jest wysyłany na serwer. Dodatkowo transmisja danych odbywa się za pośrednictwem protokołu HTTP, zabezpieczonego certyfikatem SSL. Dane, które trafiają do chmury są zapisywane w dwóch niezależnych lokalizacjach, co gwarantuje, że nawet w przypadku awarii jednego z serwerów, będą one zawsze dostępne.

Aplikacja Aktówki - umożliwiająca bezpieczną synchronizację i udostępnianie danych - za pomocą automatycznie generowanego klucza (który jest przechowywany na serwerach) szyfruje po stronie użytkownika synchronizowane pliki, niezależnie od wersji aplikacji z której on korzysta (WEB, Desktop, Mobile).

Wszystkie pliki backupowane do chmury są przechowywane w formie rozproszonej na jednym storage-u, czyli bez wydzielania przestrzeni na użytkownika. Zawsze podczas przywracania następuje weryfikacja poprawności danych. Co to oznacza? W trakcie wysyłki danych, po stronie klienta, liczona jest suma kontrolna CRC zaszyfrowanych danych; następnie podczas ich przywracania, program liczy sumy kontrolne sh1 dla każdego bloku niezaszyfrowanych danych; w ostatnim etapie program weryfikuje oba wyniki.

klucz domyśmy
klucz użytkownika

Szyfrowanie

Pliki użytkownika są cały czas zabezpieczane przed dostępem osób trzecich. Nasze produkty zapewniają najwyższy poziom ochrony danych, dzięki wykorzystaniu szyfrowania za pomocą klucza domyślnego oraz klucza nadawanego przez użytkownika systemu.

Klucz domyślny jest generowany automatycznie podczas pierwszego uruchomienia aplikacji i następnie przechowywany na serwerach (nie jest więc znany użytkownikowi, co wyklucza możliwość jego utraty).

Klucz użytkownika jest nadawany indywidualnie przez samego użytkownika (nie jest przechowywany na serwerach). Zapewnia on maksymalny poziom bezpieczeństwa danych, jednak w przypadku jego utraty użytkownik traci możliwość odzyskania wcześniej przesłanych danych.

centra danych w Polsce,
USA i Niemczech

Bezpieczne centra danych

Dane wysyłane do chmury trafiają do jednego z naszych centrów danych. Klient ma mozliwość wyboru, gdzie mają być przechowywane jego dane - w Polsce, w Niemczech lub w USA.

W Polsce współpracujemy z Asseco Data Systems, polskim gigantem na rynku usług IT. Centrum Danych Asseco Data Systems w Szczecinie gwarantuje dwie lokalizacje serwerów - Centrum Danych i Ośrodek Zapasowy - niezależne łącza operatorskie oraz najwyższy poziom zabezpieczeń.

Dodatkowo jest prowadzony całodobowy monitoring oraz pełna kontrola dostępu do pomieszczeń. Ciągłość działania w przypadku wystąpienia awarii zasilania, zapewniają dwie niezależne linie energetyczne, generator prądu i zasilacze awaryjne o dużej mocy, oraz systemy wczesnego wykrywania dymu i ognia oraz gaszenia gazem technicznym.

Certyfikaty

- **ISO 9001:2008**: certyfikacja ISO umożliwia ustawiczne doskonalenie systemów zarządzania jakością i procesów w przedsiębiorstwie, zgodnie z wymogami i potrzebami klientów,
- **AQAP 2110:2009**: jest to rozszerzenie normy i jakości serii ISO 9000, które określa wymagania dla kontraktów i dostaw dla wojska,
- **ISO/IEC 27001:2013**: dowód na spełnienie wymagań technicznych, personalnych i organizacyjnych w zakresie zarządzania bezpieczeństwem informacji,
- **PN-N 19001:2006 (WSK)**: potwierdza obrót wyrobami o znaczeniu strategicznym związanymi z systemami i projektami informatycznymi, utrzymaniem infrastruktury IT oraz usługami obsługi centrum danych.
- **WebTrust**: niezależny, światowy standard określający zbiór zasad i dobrych praktyk w zakresie bezpieczeństwa w Internecie, zapewniając użytkownikom najlepszą ochronę.

Bezpieczeństwo danych osobowych oraz danych wrażliwych

dane osobowe i dane wrażliwe pod szczególną ochroną

Spełniamy wszystkie zapisy polskiego prawa:

- ustawa z dnia 29 sierpnia 1997 r. o „Ochronie Danych Osobowych" (Dz. U. 2002 r. Nr 101 Poz. 926, ze zmianami),

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (dz. U. Z 2004 r. Nr 100, poz. 1024, ze zmianami),

oraz restrykcyjne wymogi GIODO w kwestii zabezpieczania danych osobowych i danych wrażliwych.

Obowiązki dostawcy i klienta

Nasza firma, jako dostawca usługi, nie przetwarza danych osobowych w rozumieniu art. 7, pkt 2 ustawy o „Ochronie danych osobowych"; jedynym podmiotem uprawnionym i zobowiązanym do tego typu działań jest klient, który decyduje o celach i środkach przetwarzania tychże danych,

Po stronie klienta (jako administratora danych) leży również obowiązek rejestracji zbioru danych w GIODO; w tym celu udostępniamy informacje na temat stosowanych metod zabezpieczeń. Za zapewnienie właściwego zabezpieczenia serwerów odpowiada Asseco Data Systems.

XOPERO
WORKS, SO YOU CAN TOO!

Jesteśmy jednym z największych producentów rozwiązań backupowych w Polsce, dostarczającym profesjonalne narzędzia do kompleksowego zabezpieczenia firmowych danych.

W naszej ofercie znajdują się rozwiązanie do backupu lokalnego, backupu do chmury, appliance backup, backup hybrydowy oraz disaster recovery i business continuity. Nasze produkty umożliwiają m.in. backup i przywracanie plików, folderów, stacji roboczych (endpointów), baz danych, skrzynek pocztowych, serwerów, lokalizacji sieciowych oraz środowisk wirtualnych.

Wśród klientów znajdują się firmy z segmentu MSP, administracja publiczna, finanse i bankowość, edukacja, medycyna, telekomunikacja oraz IT.