



# ISO/IEC 27701

**TECHNIKI BEZPIECZEŃSTWA – ROZSZERZENIE DO ISO/IEC 27001 I ISO/IEC 27002  
W ZAKRESIE ZARZĄDZANIA INFORMACJAMI O OCHRONIE PRYWATNOŚCI –  
WYMAGANIA I WYTYCZNE**



# Dlaczego ISO/IEC 27701?

Certyfikacja ISO/IEC 27701 jest integralną częścią systemu zarządzania informacjami o ochronie prywatności (PIMS) i jest rozszerzeniem ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) i ISO/IEC 27002 (zarządzanie zabezpieczeniami).

## Co to jest ISO/IEC 27701?

Opierając się na pozostałych dwóch normach, ISO/IEC 27701 określa wymagania i wytyczne dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia PIMS specyficznego dla Twojej organizacji.

Przedstawia warunki i zalecenia związane z PIMS dla administratorów i podmiotów przetwarzających informacje umożliwiające identyfikację osób (PII), które są odpowiedzialne za przetwarzanie danych osobowych.

ISO/IEC 27701 ma zastosowanie do wszystkich organizacji, które są administratorami danych osobowych i/lub podmiotami przetwarzającymi, które przetwarzają PII w ramach systemu zarządzania bezpieczeństwem informacji (SZBI).

## Kluczowe korzyści

ISO/IEC 27701 może przyczynić się do:

- Podniesienia zaufania do zarządzania danymi osobowymi
- Większej przejrzystości między kluczowymi osobami
- Zawierania skutecznych umów biznesowych
- Zdefiniowania ról i obowiązków
- Osiągnięcia zgodności z przepisami dotyczącymi prywatności
- Zmniejszenia stopnia skomplikowania dzięki integracji z ISO/IEC 27001



# Koncentracja na obszarach krytycznych

ISO/IEC 27701 musi pracować dla Ciebie, abyś mógł osiągnąć oczekiwane wyniki. Od wymagań specyficznych dla PIMS po dodatkowe wskazówki dotyczące podmiotów przetwarzających dane osobowe, norma stawia szereg wymagań do spełnienia.

## Kluczowe obszary wymagań



### Zakres

Musisz zrozumieć wymagania i możliwości zastosowania swojego systemu zarządzania.



### Powołania normatywne

Konieczne jest zapoznanie się między innymi z następującymi dokumentami, przywoływanymi w treści normy:

- ISO/IEC 27000 i ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji)
- ISO/IEC 27002 (środki kontroli bezpieczeństwa informacji)
- ISO/IEC 29100 (ramy prywatności)



### Terminy i definicje

Ta sekcja zawiera kilka dodatkowych definicji użytych w normie, które nie są zawarte w normach ISO/IEC 27000 i ISO/IEC 29100.



### Wymagania ogólne

Należy zapoznać się z przeglądem struktury dokumentu i umiejscowieniem wymagań specyficznych dla PIMS, dotyczących ISO/IEC 27001 oraz ISO/IEC 27002.



### Zapisy specyficzne dla PIMS

W odniesieniu do systemu PIMS, należy zapoznać się z wymaganiami związanymi z ISO/IEC 27001 oraz wytycznymi dotyczącymi ISO/IEC 27002.



### Administratorzy i podmioty przetwarzające PII












Norma zawiera dwa punkty z dodatkowymi wytycznymi dotyczącymi administratorów i podmiotów przetwarzających dane osobowe.



# Docieranie do sedna

ISO 27701 zawiera kilka podstawowych koncepcji, które prawidłowo wdrożone mogą pomóc w uszczelnieniu organizacji.











## Niektóre podstawowe koncepcje

-  Kontekst Twojej organizacji
-  Strony zainteresowane
-  Problemy, ryzyka i szanse
-  Liderzy i właściciele ryzyka
-  Zagrożenia i szanse
-  Komunikacja
-  Udokumentowane informacje
-  Ocena wydajności
-  Plan zarządzania ryzykiem
-  Zabezpieczenia
-  Ciągłe doskonalenie

# Wdrażanie ISO/IEC 27701

Aby uzyskać wszystkie korzyści, niezbędne jest prawidłowe wdrożenie normy ISO/IEC 27701. Możemy wesprzeć Cię w osiągnięciu tego celu poprzez nasze szkolenia przygotowujące do wdrożenia.

## Najważniejsze zagadnienia związane z wdrożeniem

-  Zapewnienie wsparcia i zaangażowania najwyższego kierownictwa
-  Zaangażowanie całej organizacji i łańcucha dostaw poprzez komunikację wewnętrzną
-  Porównanie istniejących systemów z nowymi wymaganiami
-  Pozyskanie informacji zwrotnych od klientów i dostawców na temat obecnych systemów
-  Stworzenie zespołu wdrożeniowego
-  Zdefiniowanie ról (w tym podmiot przetwarzający i administrator danych), odpowiedzialności oraz harmonogramów
-  Korzystanie ze szkoleń i motywatorów, w celu pobudzenia zaangażowania pracowników
-  Tworzenie spójności poprzez zachęcanie innych w łańcuchu przetwarzania danych do używania ISO/IEC 27701
-  Dzielenie się wiedzą na temat standardu i szkolenia audytorów wewnętrznych
-  Regularne przeglądy systemu dla ciągłego doskonalenia



# Usługi SGS w zakresie ISO 27701

Dysponując doświadczeniem we wszystkich głównych branżach, rozumiemy największe problemy każdego sektora oraz dysponujemy umiejętnościami technicznymi i logistycznymi, aby zapewnić realne efekty.

## Co oferujemy?

Audyt zgodności z normą ISO/IEC 27701 od SGS, pomoże Twojej organizacji wyróżnić się z tłumu wspierając Cię w opracowywaniu i doskonaleniu procesów, rozwijaniu talentów pracowników oraz trwałych relacji z klientami.

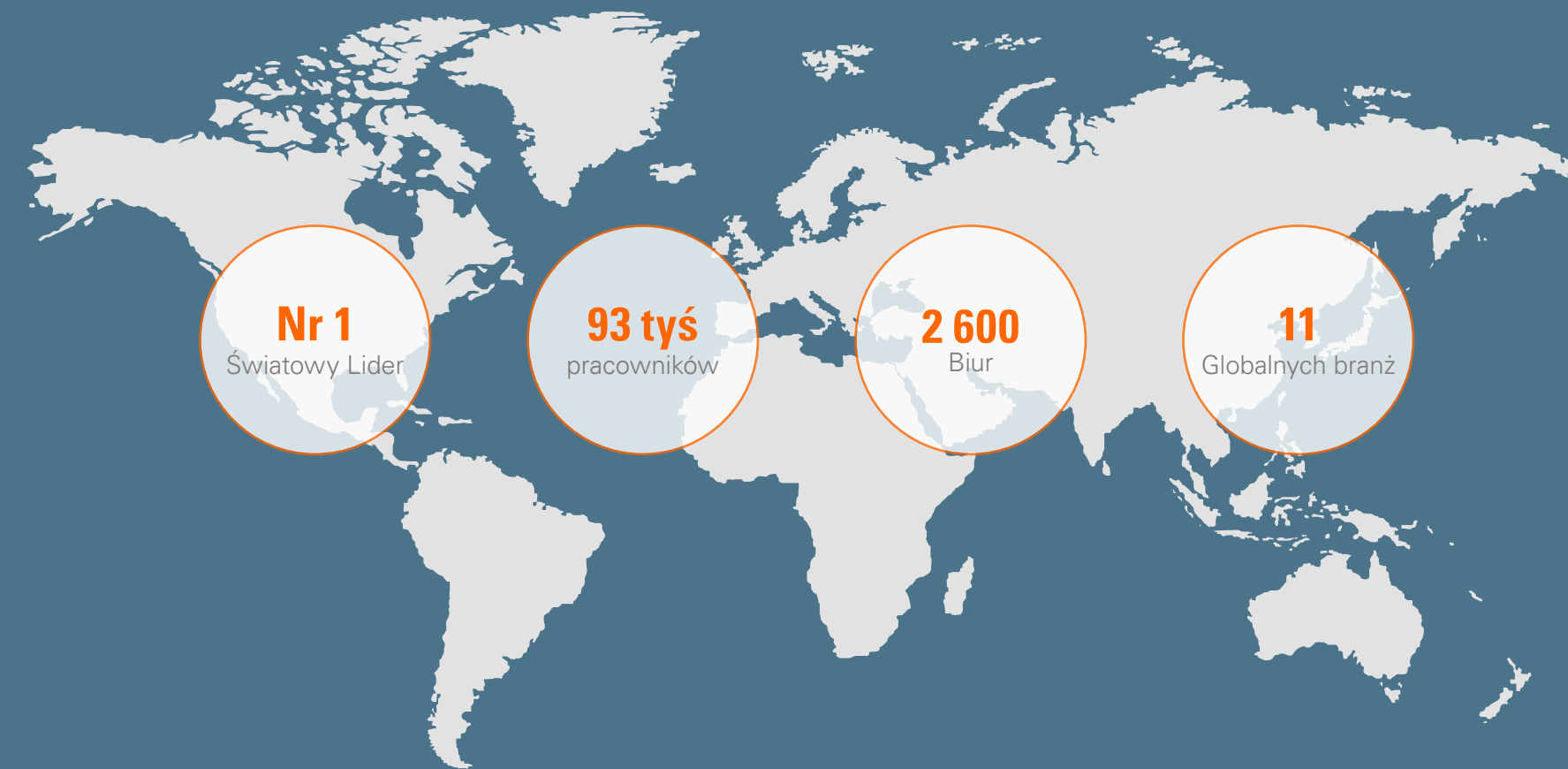
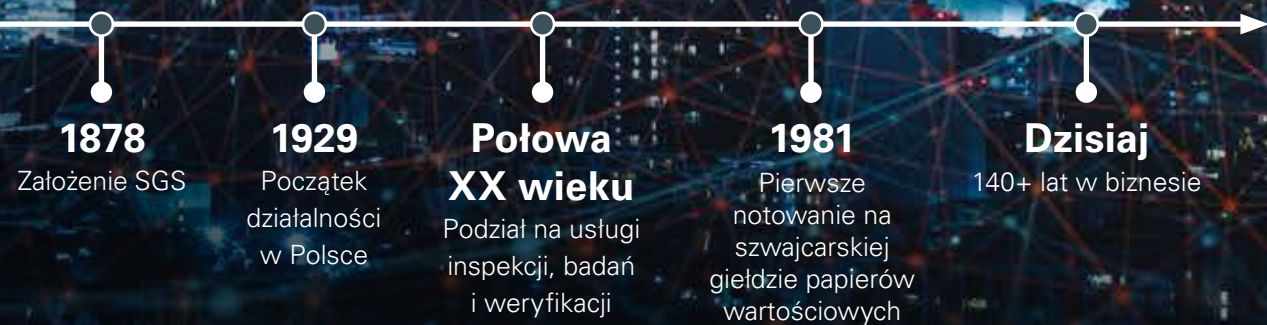
Ponadto oferujemy szereg usług uzupełniających, w tym:

- Szkolenie wprowadzające ISO/IEC 27701
- Kurs szkoleniowy dla audytorów wewnętrznych ISO/IEC 27701
- a także certyfikację, audyty i szkolenia w zakresie:
  - ISO/IEC 27001 – zarządzanie bezpieczeństwem informacji
  - ISO/IEC 20000 – zarządzanie usługami informatycznymi
  - ISO 22301 – zarządzanie ciągłością działania
  - ISO/IEC 27017 oraz ISO/IEC 27018 – usługi w chmurze
  - TISAX – bezpieczeństwo informacji w branży motoryzacyjnej
  - KSC (Krajowy System Cyberbezpieczeństwa)
  - ISO/IEC 19770 – zarządzanie zasobami IT
  - ISO/IEC 22237 (EN 50600) – certyfikacja Data Center
  - RODO (GDPR) – rozporządzenie o ochronie danych osobowych



# O SGS

## NASZA HISTORIA



## O SGS

SGS to wiodąca na świecie firma zajmująca się inspekcją, weryfikacją, testowaniem i certyfikacją. Firma SGS jest uznawana za światowy wzorzec jakości i uczciwości. Zatrudniając ponad 96 000 pracowników, SGS obsługuje sieć ponad 2600 biur i laboratoriów na całym świecie. Doskonalenie produktów, procesów, systemów i umiejętności ma fundamentalne znaczenie dla Twojego trwałego sukcesu i stabilnego wzrostu. Umożliwiamy ciągle doskonalenie i rozwój produktów, usług i łańcucha wartości poprzez podnoszenie wydajności, zarządzanie ryzykiem, lepsze spełnianie wymagań interesariuszy i zarządzanie zrównoważonym rozwojem. Działając na całym świecie, mamy doświadczenie w skutecznej realizacji złożonych międzynarodowych projektów na dużą skalę. Nasi pracownicy posługują się miejscowym językiem, rozumieją kulturę lokalnego rynku oraz działają globalnie w sposób spójny, niezawodny i efektywny.



**SGS Headquarters**  
1 Place des Alpes  
P.O. Box 2152  
1211 Geneva 1  
Switzerland

**SGS Polska Sp. z o.o.**  
Jana Kazimierza 3  
01-248 Warszawa  
Polska



**WWW.SGS.PL**

**WHEN YOU NEED TO BE SURE**

