ZNACZENIE ZARZĄDZANIA PRYWATNOŚCIĄ DLA BEZPIECZEŃSTWA KLUCZOWYCH DANYCH

Niedawna fala incydentów związanych z naruszeniem danych w globalnych organizacjach zwiększyła apetyt konsumentów na bardziej rygorystyczne środki ochronne. W tym artykule poznasz podstawy skutecznego systemu zarządzania prywatnością danych w celu ich zabezpieczenia.

DYCHOTOMIA PRYWATNOŚCI/OCHRONY DANYCH

Chociaż pojęcia te bywają używane zamiennie, „prywatność danych" i „ochrona danych" pełnią różne funkcje. Rozróżnienie między tymi dwoma terminami jest więc niezbędne do określenia, co oznacza skuteczny system zarządzania prywatnością.

Prywatność danych" obejmuje zarządzanie ilością danych udostępnianych, gromadzonych i wykorzystywanych, zwłaszcza z osobami trzecimi.

Z drugiej strony „ochrona danych" zabezpiecza takie informacje przed możliwością ujawnienia, uszkodzenia lub całkowitej utraty. Określa warunki prawidłowego gromadzenia, wykorzystywania lub modyfikacji danych, co jest niezbędne dla zachowania prywatności danych w organizacji.

PRYWATNOŚĆ DANYCH – ZASADY

Zasady przetwarzania danych, zgodnie z rozporządzeniem UE 2016/679 (RODO):

- **Zgodność z prawem, rzetelność i przejrzystość** – dane osobowe musza być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- **Ograniczenie celu** – dane osobowe musza być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami;
- **Minimalizacja danych** – dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

PRYWATNOŚĆ DANYCH – ZASADY – CD

- **Prawidłowość** – dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

- **Ograniczenie przechowywania** – dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia RODO w celu ochrony praw i wolności osób, których dane dotyczą;

- **Integralność i poufność** – przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

ISO/IEC 27701

System zarządzania informacjami o prywatności ISO/IEC 27701 (PIMS) został stworzony, aby pomóc organizacjom w lepszym poruszaniu się w wymaganiach prawnych dotyczących prywatności.

Wprowadzony przez specjalistów ds. prywatności i audytorów wewnętrznych/zewnętrznych, PIMS rozważa szczegółowo operacyjne środki kontroli, które uwzględniają wiele wymogów regulacyjnych i RODO. Daje to możliwość potencjalnej certyfikacji i wykazania zgodności.

PROCES WDRAŻANIA ISO 27001

Certyfikacja ISO 27001 jest zalecana organizacjom niezależnie od ich wielkości oraz tego, czy taka organizacja jest administratorem lub podmiotem przetwarzającym dane. Pomaga we wdrożeniu odpowiednich środków kontroli w celu ochrony danych osobowych, znacznie zmniejszając ryzyko naruszenia danych w następujący sposób:

- ISO 27001 nakazuje organizacjom przeprowadzenie dokładnej oceny ryzyka, identyfikującej słabe punkty i potencjalne zagrożenia, które mogą zagrozić danym znajdującym się pod opieką organizacji.

PROCES WDRAŻANIA ISO 27001 – CD

- Wyraźnie określa środki kontroli mające na celu zmniejszenie zagrożeń bezpieczeństwa danych. Natomiast organizacje są zobowiązane do określenia, które aktywa są wrażliwe lub wymagają ochrony.

Ostatecznie, organizacja powinna ocenić, czy ma rzeczywistą potrzebę certyfikacji ISO 27001 + ISO 27701 przed ich uzyskaniem. W przypadkach, gdy firmy mają do czynienia ze sprzedawcami lub dostawcami danych, powinny rozważyć złożenie wniosku o certyfikację ISO 27001 + ISO 27701, aby uniknąć odpowiedzialności wynikającej z potencjalnych przypadków naruszenia danych.

ROZWIĄZANIA SGS

Ankieta przeprowadzona przez IBM wykazała, że 95% wszystkich naruszeń bezpieczeństwa jest wynikiem błędu ludzkiego. Niezwykle ważna jest identyfikacja potencjalnych zagrożeń oraz wdrażanie prawidłowych procedur przechowywania swoich kluczowych danych.

SGS oferuje szeroki zakres usług, które pomagają organizacjom w skuteczny i efektywny sposób chronić integralność swoich danych i systemów. Współpraca z SGS w celu uzyskania certyfikatu systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001 oznacza sprawniej przebiegające procesy, lepsze wykorzystanie naturalnych zdolności pracowników i trwalsze relacje z klientami.

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 przystępny cenowo.

Dowiedz się więcej o usługach SGS związanych z ISO 27001

Sprawdź listę szkoleń Akademii SGS w zakresie ISO 27001

Jeżeli masz jakieś pytania zapraszamy do kontaktu.

KONTAKT

pl.certyfikacja@sgs.com

+48 22 329 22 93

www.sgs.pl

#SGSinPoland

#SGSinPoland

WHEN YOU NEED TO BE SURE

SGS