POLSKI KOMITET NORMALIZACYJNY

Jak zabezpieczyć dane osobowe w firmie?

Ochrona dzięki normom

Ochrona danych osobowych w systemach teleinformatycznych

Coraz więcej organizacji przetwarza dane osobowe, a ich ilość będzie już tylko rosnąć. Coraz większe są także oczekiwania społeczne co do ochrony i bezpieczeństwa danych osobowych. Aby organizacja mogła osiągnąć swoje cele, zwiększyć zaufanie klientów oraz działać zgodnie z wymaganiami prawnymi, powinna chronić dane osobowe.

Informacje o identyfikowalnych osobach

RODO[1] rozszerzyło pojęcie danych osobowych – są to wszystkie informacje, dzięki którym można zidentyfikować osoby fizyczne. „Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób".

[1] Ogólne rozporządzenie o ochronie danych osobowych 2016/679.

Co to jest PII?

Informacje o identyfikowalnych osobach (PII – Personal Identifiable Information) to różne zestawy danych, które pozwalają na bezsprzeczne wskazanie konkretnej osoby w przypadku pomyślnego połączenia danych przez algorytm.
Dane osobowe to również numery ID, informacje dotyczące lokalizacji, wskaźniki odnośnie do zdrowia fizycznego i psychicznego, statusu majątkowego oraz społecznego, a nawet dane genetyczne czy biometryczne, które pomogłyby zidentyfikować konkretną osobę.

Firma powinna wiedzieć, które informacje o identyfikowalnych osobach przetwarza, żeby je odpowiednio zabezpieczyć.


PII

DANE Z INTERNETU
media społecznościowe, hasła

DATA URODZENIA/MIEJSCE URODZENIA

DANE KONTAKTOWE
adres e-mail, adres fizyczny,
numery telefonów

DOKUMENT TOŻSAMOŚCI
paszport, prawo jazdy, akt urodzenia

DANE WERYFIKUJĄCE
nazwisko panieńskie matki,
szkoła średnia, imię zwierzęcia, hasła

GEOLOKALIZACJA
smartfon, aparat fotograficzny, GPS

NUMERY KONTA
numer konta bankowego,
ubezpieczenia, inwestycji

INFORMACJE MEDYCZNE
recepty, wyniki badań,
dokumentacja medyczna

Bezpieczeństwo i prywatność

Organizacje zbierające lub przetwarzające dane będą potrzebować wytycznych dotyczących ich ochrony, aby ograniczyć wystąpienie ryzyka naruszenia prywatności i ograniczyć skutki naruszeń odnoszących się do organizacji i zainteresowanych osób. Szczególnie przydatne pod kątem RODO dla osób zajmujących się zabezpieczaniem będą normy.

PKN opublikował normę PN-ISO/IEC 29151 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony informacji o identyfikowalnych osobach. Określono w niej cele zabezpieczeń, zabezpieczenia i wytyczne dotyczące wdrożenia zabezpieczeń w celu spełnienia wymagań zidentyfikowanych w trakcie szacowania ryzyka i oceny skutków związanych z ochroną informacji o identyfikowalnych osobach (PII).

Które normy można wykorzystać w procesie ochrony PII?

- PN-EN ISO/IEC 27001

Określa proces zarządzania bezpieczeństwem informacji i związane z nim wymagania, które mogą być wykorzystane jako podstawa ochrony PII.

- PN-EN ISO/IEC 27002

Podaje wytyczne dotyczące standardów bezpieczeństwa informacji w organizacji i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrożenia i zarządzania zabezpieczeniami, z uwzględnieniem środowisk, w których występują ryzyka w bezpieczeństwie informacji dla organizacji.

- ISO/IEC 27009 (Norma Międzynarodowa)

Określa wymagania dotyczące stosowania ISO/IEC 27001 w dowolnym określonym sektorze (pole, obszar zastosowania lub sektor rynku). Wyjaśnia, w jaki sposób uwzględnić wymagania dodatkowe do tych określonych w ISO/IEC 27001, jak zawęzić niektóre z wymagań określonych w ISO/IEC 27001 oraz jak dołączyć zabezpieczenia lub zestawy zabezpieczeń do tych wymienionych w Załączniku A do ISO/IEC 27001.

- PN-ISO/IEC 27018

Zawiera wytyczne dla organizacji działających jako podmioty przetwarzające PII, oferujące możliwość przetwarzania jako usługi w chmurze.

- PN-ISO/IEC 29134

Podaje wytyczne dotyczące identyfikowania, analizowania i szacowania ryzyk dla prywatności, podczas gdy PN-EN ISO/IEC 27001 i PN-ISO/IEC 27005 opisują metody identyfikowania, analizowania i oceny tych ryzyk w bezpieczeństwie.

Wszystkie normy można kupić w sklepie PKN **www.sklep.pkn.pl**

Ciągłe doskonalenie

Zagrożenia ewoluują, przybierają na sile i tym samym mogą nieść za sobą ogromne konsekwencje. Skąd pewność, że podejmowane przez organizację działania na rzecz ochrony informacji są wystarczające?

Warto dobrze planować i sprawdzać podejmowane działania. Warto uaktualniać wiedzę z zakresu zarządzania bezpieczeństwem informacji, cyberbezpieczeństwa, ciągłości działania i ryzyka.

PKN organizuje szkolenia z tego zakresu. Pełna oferta szkoleń znajduje się na stronie **wiedza.pkn.pl**.

Więcej informacji: www.pkn.pl

Polski Komitet Normalizacyjny
ul. Świętokrzyska 14
00-050 Warszawa
www.pkn.pl
wiedza.pkn.pl