Warszawa, 29.07.2025 r.

Czym jest polityka ochrony danych osobowych i dlaczego każda firma powinna ją mieć?

Ochrona danych osobowych stanowi obecnie jeden z fundamentów odpowiedzialnego prowadzenia działalności gospodarczej. Z uwagi na powszechność przetwarzania danych – zarówno klientów, kontrahentów, jak i pracowników – każda organizacja powinna nie tylko znać przepisy Rozporządzenia o ochronie danych osobowych (RODO), ale również posiadać odpowiednio skonstruowaną dokumentację wewnętrzną, w tym **politykę ochrony danych osobowych** (politykę bezpieczeństwa danych osobowych lub inny podobny dokument).

Choć samo RODO nie wymusza wprost obowiązku sporządzenia takiego dokumentu, polityka ochrony danych osobowych pozostaje w praktyce jednym z kluczowych środków służących spełnieniu wymogów rozliczalności (art. 5 ust. 2 RODO). Dokument ten nie tylko systematyzuje wewnętrzne procedury przetwarzania danych, lecz także wyznacza kierunki odpowiedzialności i umożliwia sprawne reagowanie na incydenty naruszenia ochrony danych.

Jaką funkcję pełni polityka ochrony danych osobowych?

Polityka ochrony danych osobowych (lub inny, o podobnej nazwie dokument, mówiący o tej tematyce) to **wewnętrzny dokument organizacji**, który opisuje przyjęte przez nią standardy w zakresie przetwarzania, zabezpieczania i zarządzania danymi osobowymi.

Dokument ten pełni funkcję:

- informacyjną – dla pracowników i kadry zarządzającej,
- dowodową – w relacji z organami nadzorczymi (PUODO),
- operacyjną – jako przewodnik po procedurach związanych z ochroną danych.

RODO nie wskazuje konieczności sporządzenia „polityki ochrony danych" jako obowiązkowego dokumentu. Jednak jego brak utrudnia wykazanie zgodności z zasadami rozliczalności i minimalizacji ryzyka naruszeń.

Co powinna zawierać polityka ochrony danych osobowych?

Nie istnieje wzorzec uniwersalny – każda polityka musi być dostosowana do specyfiki działalności danego podmiotu, jego struktury organizacyjnej oraz zakresu i celu przetwarzania danych. Mimo to, można wskazać katalog elementów, które powinny znaleźć się w każdej rzetelnej polityce.

Kluczowe elementy:

- Podstawa prawna dokumentu: odniesienie do RODO oraz ustawy o ochronie danych osobowych z 10 maja 2018 r.
- Słowniczek pojęć: ułatwiający interpretację przepisów wewnętrznych.
- Opis zasad nadawania, zmiany i cofania uprawnień do przetwarzania danych, wraz z procedurą podpisania oświadczenia o zachowaniu poufności.
- Opis zastosowanych zabezpieczeń fizycznych i technicznych: szyfrowanie, systemy kopii zapasowych, kontrola dostępu, monitoring systemowy.
- Wykaz lokalizacji przetwarzania danych: serwerownie, pomieszczenia biurowe, zasoby zewnętrzne.
- Opis rejestru czynności przetwarzania i rejestru kategorii czynności.

- Zakres odpowiedzialności poszczególnych osób za wdrożenie, monitoring oraz raportowanie nieprawidłowości.

Zakres polityki ochrony danych osobowych może zostać ograniczony do niezbędnego minimum, natomiast szczegółowe procedury operacyjne mogą być wdrażane w organizacji w formie odrębnych załączników – na przykład jako *procedura projektowania nowych procesów przetwarzania danych* lub *procedura dotycząca przetwarzania danych osobowych w relacjach z podmiotami zewnętrznymi* (np. dostawcami).

Rozdzielenie zagadnień z zakresu ochrony danych osobowych pomiędzy dokument główny (politykę) a szczegółowe procedury stanowiące jego załączniki może znacząco zwiększyć przejrzystość dokumentacji oraz ułatwić użytkownikom jej praktyczne stosowanie. Należy jednak pamiętać, że każda dokumentacja powinna być każdorazowo dostosowana do specyfiki i potrzeb danej organizacji – zarówno pod względem zakresu przetwarzanych danych, jak i struktury organizacyjnej oraz modelu operacyjnego.

Polityka ochrony danych osobowych ma **charakter dokumentu wewnętrznego** – nie podlega udostępnieniu osobom trzecim. Powinna być jednak:

- zabezpieczona przed nieautoryzowanym dostępem,
- zrozumiała dla wszystkich osób, które uczestniczą w procesach przetwarzania danych,
- kompatybilna z pozostałymi procedurami wewnętrznymi (np. instrukcją zarządzania systemem informatycznym, procedurą zgłaszania incydentów).

Kto odpowiada za wdrożenie polityki ochrony danych?

Zgodnie z RODO, pełną odpowiedzialność za zgodność przetwarzania danych osobowych z przepisami ponosi **Administrator Danych Osobowych (ADO)** – tj. podmiot decydujący o celach i środkach przetwarzania danych.

Wdrożenie polityki może zostać powierzone:

- wyspecjalizowanym działom compliance lub IT,
- zewnętrznym podmiotom doradczym.

Inspektor Ochrony Danych (IOD) odgrywa kluczową rolę w procesie wdrażania polityk dotyczących ochrony danych osobowych. Zgodnie z art. 38 ust. 1 RODO, IOD powinien być odpowiednio i niezwłocznie włączany we wszystkie kwestie dotyczące ochrony danych osobowych – w szczególności w zakresie tworzenia i opiniowania wewnętrznych regulacji.

W ramach swoich zadań, określonych w art. 39 RODO, Inspektor Ochrony Danych pełni funkcję doradczą wobec Administratora Danych Osobowych (ADO), w tym w zakresie oceny zgodności przyjmowanych polityk i procedur z obowiązującymi przepisami prawa. IOD może również rekomendować rozwiązania służące zapewnieniu skutecznej realizacji obowiązków wynikających z RODO, w tym prowadzenie szkoleń, opiniowanie dokumentacji czy udział w analizach ryzyka i DPIA.

Praktyczny charakter polityki

Dobra polityka ochrony danych osobowych nie powinna być jedynie ogólną deklaracją. Powinna być praktycznym narzędziem operacyjnym, które:

- zawiera odwołania do wszystkich dokumentów dotyczących ochrony danych (np. procedur DPIA, klauzul informacyjnych, umów powierzenia),

- wskazuje osoby odpowiedzialne za realizację obowiązków (rejestry, audyty, szkolenia, zgłoszenia incydentów),
- umożliwia jasne przypisanie ról i obowiązków – dzięki czemu można łatwo ustalić, kto odpowiada za jakie zadanie w razie naruszenia.

Osoby odpowiedzialne powinny być przypisane do zadań takich jak:

- prowadzenie i aktualizacja rejestrów (rejestry czynności przetwarzania, rejestr incydentów, rejestr wniosków osób, których dane dotyczą),
- przeprowadzanie analiz ryzyka i oceny skutków (DPIA),
- monitorowanie zgodności z RODO,
- wdrażanie zaleceń poaudytowych,
- organizacja i prowadzenie szkoleń,
- obsługa naruszeń bezpieczeństwa danych.

Dlaczego każda firma powinna posiadać ten dokument?

Brak formalnej polityki ochrony danych osobowych:

- utrudnia wykazanie zgodności z RODO,
- zwiększa ryzyko nieprawidłowości i sankcji administracyjnych,
- powoduje nieefektywność w reagowaniu na incydenty i żądania osób, których dane dotyczą,
- pogarsza wizerunek firmy w oczach klientów i kontrahentów.

Z kolei posiadanie aktualnej i wdrożonej polityki:

- buduje **przewagę reputacyjną**,
- zabezpiecza interesy prawne firmy,
- poprawia **wewnętrzną organizację przetwarzania danych**,
- ogranicza ryzyko nałożenia kar (nawet do 20 mln euro lub 4% rocznego obrotu).

Polityka ochrony danych osobowych to nie tylko dokument – to **podstawowy element systemu zgodności z RODO**. Umożliwia zarządzanie ryzykiem, zapewnia bezpieczeństwo informacji i wspiera transparentność działań. Każdy administrator – niezależnie od branży – powinien traktować jej wdrożenie jako **obowiązek i inwestycję w zaufanie**.

Nina Zacharska - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.