Wzory i szablony dokumentacji RODO: Polityka ochrony danych

Jak powinna wyglądać skuteczna polityka ochrony danych zgodna z RODO? Jakie procedury powinna zawierać? Co zrobić, żeby nie była martwym dokumentem? Zapraszam do lektury!

Polityka bezpieczeństwa czy Polityka ochrony danych?

Zacznę od uporządkowania terminologii. Wiele osób posługuje się zamiennie dwoma terminami: **polityka bezpieczeństwa** i **polityka ochrony danych**.

Dlaczego tak się dzieje? Odpowiedź na tak postawione pytanie, stanowi poniższa tabela:

Akt prawny	Data obowiązywania	Stosowany termin	Co powinna zawierać?
Rozporządzenie MSWiA „w sprawie określenia podstawowych warunków technicznych i organizacyjnych”	15 lipca 1998	Polityka Zabezpieczenia Systemów Informatycznych	Określono w Rozporządzeniu
Rozporządzenie MSWiA „**w sprawie dokumentacji** przetwarzania danych osobowych (...)”	1 maja 2004	Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym	Określono w Rozporządzeniu
RODO	25 maja 2018	Polityka ochrony danych	Nie określono wprost zawartości

Podsumowując – na przestrzeni lat funkcjonowały w Polsce różne nazwy, kluczowego dla ochrony danych osobowych dokumentu.

Obecnie prawidłową nazwą jest **Polityka ochrony danych,** o której mowa w RODO – stosujmy zatem aktualną terminologię.

Czy polityka ochrony danych jest obowiązkowym dokumentem?

W najdłużej funkcjonującym polskim Rozporządzeniu z 29 kwietnia 2004 roku, było wskazane wprost – Polityka bezpieczeństwa oraz Instrukcja zarządzania to dokumenty, które **każdy** administrator danych musi wdrożyć.

RODO jest aktem prawnym znacznie bardziej elastycznym i unika jednoznacznej odpowiedzi na pytanie o obowiązkowość Polityki ochrony danych.

W samym tekście RODO znajdziemy następujące regulacje:

Motyw 79 preambuły

Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki.

Art. 24 ust. 2

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Co więcej, poza powyższymi zapisami, RODO przewiduje też szereg obowiązkowych procedur. A najlepszym według mnie miejscem na opisanie tych procedur, jest właśnie Polityka ochrony danych.

Z tworzenia Polityki ochrony danych, mogą na pewno zrezygnować najmniejsze podmioty.

Jednak w przypadku każdej dużej organizacji, posiadanie Polityki ochrony danych jest potrzebne do wykazania zgodności z RODO.

Oczywiście możemy zastosować rozwiązanie alternatywne i wszystkie wymagane przez RODO procedury zamieścić w innych wewnątrzorganizacyjnych dokumentach (regulamin pracy, polityki IT etc.).

Takie rozwiązanie jest mało praktyczne i sprawia, że procedury są bardzo rozproszone i znacznie trudniej nimi na bieżąco zarządzać.

Co powinna zawierać polityka ochrony danych zgodna z RODO?

RODO jest inteligentnym aktem prawnym, który ma regulować ochronę danych osobowych w Unii Europejskiej przez najbliższe 20 lat. Pomysł unormowania „na sztywno" treści Polityki ochrony danych, uznano za sprzeczny z głównymi założeniami RODO.

Polityki tworzone obecnie, na pewno będą różniły się od tych tworzonych za 10 lat.

Być może już za jakiś czas, tradycyjne Polityki ochrony danych zostaną zastąpione przez zbiory procedur i całe systemy informatyczne, służące do sprawnego zarządzania ochroną danych osobowych.

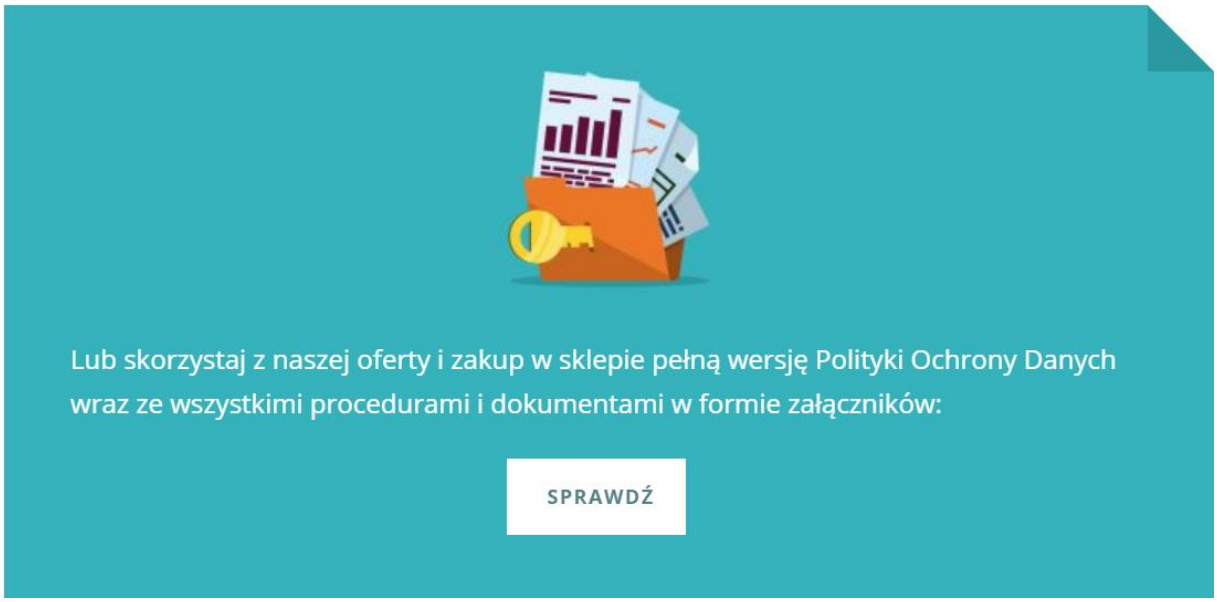
Na dzień dzisiejszy rekomendowana przeze mnie zawartość Polityki to przede wszystkim kluczowe i obowiązkowe procedury.

Poniżej przedstawiam tabelę z obowiązkowymi i rekomendowanymi procedurami, które łącznie składają się na Politykę ochrony danych zgodną z RODO:

Procedura	Status procedury	Funkcja procedury	RODO
Zasady retencji danych	Wymagany	Mówi w jaki sposób i kiedy usuwamy niepotrzebne już dane osobowe	Art. 5 ust. 1 lit. e)
Zasady privacy by design i privacy by default	Wymagany	Mówi o tym w jaki sposób zapewnić odpowiedni poziom bezpieczeństwa danych i prawa do prywatności np. przy nowych projektach IT	Art. 25
Struktura organizacyjna w zakresie ochrony danych osobowych	Wymagany	Kto i za co odpowiada w zakresie funkcjonowania systemu RODO (np. IOD, ASI etc.).	Art. 24 ust. 1, Art. 32 ust. 1
Procedura nadawania upoważnień	Wymagany	W jaki sposób, na jakich zasadach i komu nadajemy upoważnienia do przetwarzania danych osobowych	Art. 29

Procedura szkoleń	Mocno zalecany	W jaki sposób szkolimy personel uczestniczący w przetwarzaniu danych	Art. 39
Postępowanie z incydentami ochrony danych osobowych	Wymagany	Kto i w jaki sposób reaguje na incydenty ochrony danych osobowych	Art. 33
Ocena skutków dla ochrony danych osobowych (DPIA)	Wymagany	Kiedy i w jaki sposób oceniamy skutki dla ochrony danych	Art. 35
Realizacja praw osób, których dane dotyczą	Wymagany	Kto i w jaki sposób realizuje prawa osób, których dane dotyczą	Art. 7 ust. 3, Art. 12 - 22
Procedura audytu wewnętrznego	Mocno zalecany	Kto, w jaki sposób i kiedy kontroluje system ochrony danych osobowych w naszej organizacji.	Art. 24 ust. 1, Art. 32 ust. 1 lit. d), Art. 39 ust. 1 lit. b)
Kontrola podmiotów przetwarzających	Mocno zalecany	W jaki sposób i kiedy kontrolujemy procesorów	Art. 28 ust. 3 lit. h)
Opis środków bezpieczeństwa	Mocno zalecany	Jakie środki bezpieczeństwa stosujemy w sferze: organizacyjnej, technicznej, informatycznej	Art. 24 ust. 1, Art. 32 ust. 1
Plan ciągłości działania	Zalecany	Przygotowanie rozwiązań dla różnych zdarzeń mogących wpływać na ciągłość procesu biznesowego, z uwzględnieniem ochrony danych osobowych	Art. 5 ust. 1 lit. f), Art. 32 ust. 1 lit. b)
Procedury IT	Mocno zalecane	Sposób zarządzania infrastrukturą IT w której dochodzi do przetwarzania danych osobowych	Art. 24 ust. 1, Art. 32 ust. 1

W cyklu kolejnych artykułów opiszemy po kolei wszystkie wymagane przez RODO procedury i wskażemy praktyczne porady jak je przygotować. W naszym sklepie będą też czekały gotowe procedury dla tych z Państwa, którzy nie mają czasu na tworzenie ich od podstaw.



O czym jeszcze warto pamiętać, przygotowując politykę ochrony danych zgodną z RODO

Obecnie w Internecie znajdziemy ogromną ilość szablonów dokumentacji ochrony danych osobowych. Są one udostępniane odpłatnie i nieodpłatnie. Mają różną objętość i treść. Jak odnaleźć się w tym gąszczu? Gdzie znaleźć szablon idealny?

Po pierwsze – szablonów idealnych nie ma. Wzory dokumentów, które są dostępne w naszym sklepie, są efektem wielu lat pracy całego zespołu Lex Artist. Ale nawet te szablony, muszą być twórczo dostosowane do indywidualnych potrzeb Klienta.

Dlaczego? Ponieważ każdy administrator danych osobowych jest inny. Ma odmienne potrzeby i obszary wymagające poświęcenia szczególnej uwagi.

To trochę tak jak z Konstytucją. Teoretycznie, każdy polityk może przepisać Konstytucję największej światowej potęgi – Stanów Zjednoczonych, a następnie uchwalić ją w swoim kraju.

Pytanie tylko, z jakim efektem? Konstytucja amerykańska świetnie sprawdza się w Stanach Zjednoczonych. Ale czy równie dobrze sprawdziłaby się w Chinach, Rosji czy Polsce?

Co zatem jest kluczowe? Co sprawia, że jedne Polityki działają lepiej od innych?

Przede wszystkim zidentyfikowanie słabych i mocnych stron naszej organizacji oraz odpowiednie dopasowanie treści do indywidualnych potrzeb.

Ważna jest też pewna elastyczność. Możliwość zmiany Polityki w sytuacji, kiedy dany obszar nie działa sprawnie.

Analogia do Konstytucji nie jest przypadkowa. Polityka ochrony danych jest przecież Ustawą Zasadniczą naszej organizacji w obszarze ochrony danych osobowych.

To właśnie od treści Polityki ochrony danych, będzie zależała w dużym stopniu skuteczność systemu ochrony danych osobowych w Twojej organizacji.

Polityka ochrony danych – porady praktyczne

Niezależnie od kształtu i treści RODO procedur (dla każdej organizacji będą inne), możemy wskazać pewne uniwersalne reguły i zasady, które pomogą w lepszym funkcjonowaniu Twojej Polityki ochrony danych.

Definicje

Warto zdefiniować kluczowe pojęcia, takie jak dane osobowe czy ich przetwarzanie. Znaczenie pojęć może być tożsame z definicją wskazaną w RODO (zalecane rozwiązanie). Możemy również nieco zmodyfikować terminologię i dopasować ją do wewnętrznej struktury organizacyjnej. Zamieszczenie definicji pozwoli uniknąć chaosu terminologicznego i każdorazowego wyjaśniania powtarzających się pojęć.

Kto i za co odpowiada?

Przygotowując Politykę ochrony danych, powinniśmy zacząć od dyskusji i przemyślenia w gronie osób decyzyjnych wizji systemu ochrony danych osobowych.

Możemy (a w niektórych przypadkach musimy) powołać Inspektora Ochrony Danych (IOD), który będzie odpowiadał za część zadań związanych z ochroną danych osobowych.

Niezależnie od tego, czy IOD zostanie wybrany czy nie, musimy zdecydować, kto będzie odpowiadał za takie obszary jak:

- nadawanie upoważnień i szkolenie nowych pracowników

- reagowanie w przypadku incydentów
- przygotowanie oceny skutków dla ochrony danych osobowych (DPIA)
- audytowanie naszej organizacji i sprawdzanie czy RODO procedury działają w praktyce
- realizacja praw osób, których dane dotyczą
- kontakt z regulatorem

W Polityce ochrony danych, nie powinniśmy posługiwać się imionami i nazwiskami konkretnych osób. Jeśli np. za nadawanie upoważnień odpowiada IOD – Piotr Kowalski, to wystarczy, że w dokumentacji zaznaczymy, że za taki obszar odpowiada IOD.

Jeśli użyjemy konkretnego imienia i nazwiska, to przy każdorazowej zmianie na tym stanowisku, zaistnieje konieczność aktualizacji Polityki. Wiąże się to ze sformalizowaną drogą służbową i koniecznością uzyskania podpisu najwyższego kierownictwa, o co nie zawsze łatwo.

Podsumowując – najpierw ustalamy wspólnie z osobami decyzyjnymi ogólną wizję i koncepcję. A dopiero później nasze ustalenia materializujemy w postaci Polityki ochrony danych.

Załączniki

Dobra Polityka ochrony danych, tak samo jak dobra Konstytucja, powinna być na tyle ogólna, żeby nie trzeba było jej zbyt często aktualizować. Dokument jest podpisywany przez osobę uprawnioną do reprezentacji administratora danych osobowych, a my nie będziemy przecież chcieli niepokoić Prezesa ciągłymi prośbami o podpis aktualizacji.

Warto podzielić dokumentację na elementy zmienne (załączniki) oraz część „stałą" (ogólne zasady ochrony danych osobowych).

W części „stałej" powinniśmy wskazać zasady aktualizacji obu obszarów. Zdecydowanie polecam tutaj implementację możliwości modyfikowania załączników dokumentacji przez IODa lub osobę dedykowaną do opieki nad dokumentacją.

Każdorazowe zbieranie podpisów od Prezesa, na wielu stronach załączników bywa uciążliwe. Załączniki mogą zmieniać się dość często.

Co innego, jeśli chodzi o część „stałą" Polityki. Warto zadbać o to aby zmieniała się ona jedynie w wyjątkowych sytuacjach. Uzależnienie jej zmiany od podpisu Prezesa umożliwi kontrolę Administratora Danych nad kluczowymi zmianami.

Szablony kluczowych dokumentów

Kolejnym dobrym pomysłem jest dołączenie do treści Polityki (oczywiście w formie załączników), kluczowych dokumentów, z których będziemy często korzystać w naszej organizacji. Takim dokumentem może być na przykład szablon umowy powierzenia czy obowiązku informacyjnego.

W ten sposób nadamy Polityce bardziej użyteczny i praktyczny charakter.

Nie zwlekaj

O czym jeszcze warto pamiętać? Przede wszystkim o czasie. Lepiej przygotować Politykę, która będzie miała pewne braki, niż nie posiadać jej w ogóle. Zbytni perfekcjonizm zgubił już niejednego Administratora Danych. W poprzednim stanie prawnym, wielu ABIch wdrażało Politykę nawet kilka lat, wciąż czekając na brakujące załączniki czy pojedyncze procedury. A tymczasem brak podpisu Prezesa na Polityce ochrony danych oznacza, że dokument formalnie nigdy nie zaistniał.

Podsumowanie

Polityka ochrony danych jest potrzebna każdej dużej organizacji przetwarzającej dane osobowe. Dokument uporządkuje i ułatwi zarządzanie ochroną danych osobowych.

Skorzystajmy z elastyczności RODO, budując Politykę ochrony danych pasującą do naszych potrzeb.

Zachęcamy Państwa do dzielenia się wrażeniami z lektury Poradnika i do zadawania pytań w komentarzach.

Autor artykułu:

Przemysław Zegarek

Źródła:

- 10 letnie doświadczenie pełnienia funkcji ABI/IOD lub wsparcia ABI w ponad 100 organizacjach. Kilka tysięcy godzin szkoleniowych (w tym szkoleń dla ABI) i ponad 500 wdrożeń systemów ochrony danych osobowych,
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. z 2015 r., poz. 745) w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji,
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych).