Polityka bezpieczeństwa i instrukcja zarządzania

czy trzeba je prowadzić zgodnie z RODO

experto24.pl

Spis treści

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych to obecnie dwa najważniejsze dokumenty określające zasady ochrony danych osobowych. Wielu administratorów danych zastanawia się, czy także zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) można będzie je prowadzić, a jeżeli tak to, czy mogą zostać one w obecnym kształcie i o jakie informacje należy je zaktualizować.

Polityka bezpieczeństwa to jeden z podstawowych dokumentów, który dowodzi, że przetwarzanie danych odbywa się u administratora danych zgodnie z prawem. Co więcej, pozwala zapewnić, że pracownicy administratora danych są świadomi, jakie mają obowiązki w zakresie przetwarzania danych osobowych. Dokument ten dostarcza im konkretnych i praktycznych wskazówek, do których powinni się stosować przy wykonywaniu codziennych zadań. Aktualność tego dokumentu jest zatem niezwykle istotna, aby proces przetwarzania danych osobowych był prawidłowy.

Ogólne rozporządzenie o ochronie danych (RODO), podobnie jak polska ustawa o ochronie danych osobowych, wskazuje, że administrator danych musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby skutecznie chronić dane osobowe. Jednym z takich środków jest dokumentacja dotycząca przetwarzania danych osobowych.

Polskie przepisy zobowiązują administratora danych do wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Konkretne wskazówki, co taka dokumentacja powinna zawierać i jak ją prowadzić, znajdują się w rozporządzeniu ministra spraw wewnętrznych i administracji w sprawie dokumentacji przetwarzania

danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Dokumentacja ochrony danych osobowych według RODO

Ogólne rozporządzenie o ochronie danych (RODO), które będzie bezpośrednio stosowane w Polsce od 25 maja 2018 r., nie wprowadza formalnego obowiązku prowadzenia dokumentacji przetwarzania danych osobowych przez wszystkich administratorów. Jednak zgodnie z nim, aby wykazać, że jego regulacje są przestrzegane, administrator powinien przyjąć wewnętrzne polityki i wdrożyć odpowiednie środki, by zapewnić skuteczną ochronę danych osobowych.

Gdy RODO zacznie być stosowane, zastąpi polską ustawę o ochronie danych osobowych. Polski ustawodawca będzie mógł wprowadzić przepisy krajowe jedynie w zakresie, na jaki pozwala RODO (w szczególności będą one dotyczyły organów nadzorczych i zagadnień proceduralnych). Oznacza to, że wprawdzie formalnie administrator nie będzie musiał wdrażać polityki bezpieczeństwa, jednak polski organ nadzorczy będzie weryfikował, jak administrator dba o realizację obowiązków, które wynikają z RODO.

4 zasady wewnętrznej polityki administratora według RODO

Aby wykazać, że odpowiednie środki w celu skutecznej ochrony danych osobowych zostały wdrożone, administrator będzie musiał wprowadzić wewnętrzną politykę bezpieczeństwa. W razie kontroli taką politykę będzie mógł przedstawić organowi nadzorczemu. Wewnętrzna polityka administratora powinna być:

1) zgodna z zasadą uwzględniania ochrony danych w fazie projektowania (*privacy by design*),
2) zgodna z zasadą domyślnej ochrony danych (*privacy by default*),
3) proporcjonalna w stosunku do czynności przetwarzania danych osobowych,
4) napisana jasnym i przejrzystym językiem.

WAŻNE

Ogólne rozporządzenie o ochronie danych nakłada na administratora obowiązek przeanalizowania skutków podejmowanych operacji przetwarzania danych osobowych pod kątem ochrony danych osobowych. W szczególności taką ocenę administrator będzie musiał przeprowadzić, gdy będzie przetwarzać dane osobowe z użyciem nowych technologii. Taką analizę administrator powinien przeprowadzić jeszcze przed przystąpieniem do przetwarzania danych osobowych. Ogólne rozporządzenie o ochronie danych wskazuje przy tym na przykładowe sytuacje, w których tego rodzaju ocena będzie niezbędna (art. 35 RODO).

Przy określaniu sposobów przetwarzania, jak też w czasie samego przetwarzania, administrator musi wdrożyć odpowiednie środki techniczne i organizacyjne, biorąc pod uwagę:

- stan wiedzy technicznej,
- koszt wdrażania,
- charakter, zakres, kontekst i cele przetwarzania oraz
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

Zasada privacy by design i privacy by default

Administrator będzie miał obowiązek uwzględniania ochrony danych osobowych już w fazie projektowania swojej usługi, produktu czy aplikacji internetowej. Konieczność uwzględnienia ochrony danych w fazie projektowania (tzw. *privacy by design*) oznacza, że administrator będzie musiał w swój projekt biznesowy (jeśli będzie on opierał się na przetwarzaniu danych osobowych) wpleść mechanizmy i rozwiązania, które zapewnią ochronę danych osobowych. Ochrona danych będzie musiała niejako stanowić jego część składową.

Administrator będzie musiał przewidzieć, co może stać się z danymi osobowymi, które będzie przetwarzał, realizując określony projekt i jak zapobiec incydentom przy przetwarzaniu danych osobowych, np. wyciekowi danych. Ochrona danych osobowych może być wynikiem np. jak najszybszej pseudonimizacji danych osobowych, minimalizacji ich przetwarzania czy wdrożenia odpowiednich zabezpieczeń.

Zgodnie z ogólnym rozporządzeniem o ochronie danych administrator będzie musiał wdrożyć odpowiednie środki techniczne i organizacyjne, które zapewnią, że domyślnie będą przetwarzane tylko

te dane osobowe, które są niezbędne z punktu widzenia konkretnego celu przetwarzania (tzw. zasada *privacy by default*).

To, czy dane osobowe są niezbędne do osiągnięcia konkretnego celu przetwarzania, zależeć będzie od ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania czy ich dostępności. Chodzi tu zatem o ustawienia prywatności w urządzeniach, produktach lub usługach. Produkty czy usługi administratora powinny zawierać pierwotne ustawienia zapewniające ochronę danych osobowych (np. nie wymagać ich podawania). Zmiana tych ustawień powinna następować jedynie na wyraźne żądanie użytkownika takiego produktu.

WAŻNE

Administrator powinien zastosować odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane dane osobowe nie były udostępniane bez aktywności osoby, której dotyczą, nieokreślonej liczbie osób fizycznych.

Co musi znaleźć się w polityce bezpieczeństwa

Polityka bezpieczeństwa jako dokument, który odnosi się do zarządzania i zabezpieczania danych osobowych, powinna opisywać środki i mechanizmy świadczące o tym, że zasady *privacy by design* i *privacy by default* są u administratora danych przestrzegane.

Przede wszystkim administrator będzie musiał wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych. Dlatego tak ważne jest opracowanie indywidualnych dokumentów, takich jak polityka bezpieczeństwa.

Politykę bezpieczeństwa administrator może wdrożyć lub zaktualizować po uprzedniej analizie charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych, a także ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

UWAGA

Jeśli np. w prowadzonej działalności w szerokim zakresie administrator wykorzystuje dane osobowe, nie tylko może, ale powinien wprowadzić odpowiednią politykę ochrony danych. Będzie ona stanowiła dowód, że przeprowadzane u administratora operacje na danych osobowych odpowiadają wymogom ogólnego rozporządzenia o ochronie danych, a prawa osób fizycznych (użytkowników produktów czy usług) są respektowane. Polityka bezpieczeństwa powinna zawierać rozwiązania proporcjonalne (adekwatne) do czynności przetwarzania danych osobowych.

Poziom przewidzianych przez administratora w polityce bezpieczeństwa zabezpieczeń (środków technicznych i organizacyjnych) powinien być dostosowany do rodzaju prowadzonej działalności, zakresu i celów przetwarzania danych oraz ryzyka naruszenia danych osobowych. Im wyższe zagrożenie dla prywatności, tym bardziej zaawansowane środki zabezpieczające administrator powinien zastosować, a tym samym przewidzieć w swojej polityce bezpieczeństwa.

Ogólne rozporządzenie o ochronie danych nie wskazuje, w jaki sposób należy określić poziomy bezpieczeństwa przetwarzania danych osobowych. Nie podaje także konkretnych środków bezpieczeństwa niezbędnych dla ochrony danych osobowych na danym poziomie. Oznacza to, że administrator samodzielnie musi ocenić, jakie środki techniczne i organizacyjne będą proporcjonalne do ryzyka naruszenia danych osobowych w ramach działalności.

Polityka bezpieczeństwa powinna w sposób przejrzysty i jasny opisywać wszystkie szczegóły procesu przetwarzania danych, włączając podstawy prawne, rodzaj przetwarzanych danych i środki służące ochronie danych. Chodzi o to, aby mogła być ona stosowana w praktyce i nie zawierała abstrakcyjnych, niezrozumiałych rozwiązań. Przejrzysta polityka bezpieczeństwa będzie skutecznym środkiem ochrony danych osobowych i pozwoli administratorowi wykazać, że przetwarza dane osobowe zgodnie z wymogami ogólnego rozporządzenia o ochronie danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych według RODO

Ogólne rozporządzenie o ochronie danych nie zawiera konkretnych wskazówek, co powinna zawierać dokumentacja przetwarzania danych osobowych. Jednakże wskazuje, że dokumentacja taka powinna służyć zapewnieniu zgodności procesu przetwarzania danych osobowych z jego wymogami.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest jednym ze środków ochrony danych osobowych. Powinna zatem spełniać te wymagania, które ogólne rozporządzenie o ochronie danych odnosi do zabezpieczeń danych osobowych.

WAŻNE

Zgodnie z ogólnym rozporządzeniem o ochronie danych zastosowane przez administratora środki służące ochronie danych osobowych powinny być odpowiednie do stopnia ryzyka związanego z przetwarzaniem danych.

W ogólnym rozporządzeniu o ochronie danych podkreślono, że przetwarzanie danych osobowych powinno odbywać się w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia

bezpieczeństwa sieci i informacji. Administrator powinien wykazać, że wdrożył odpowiednie środki, aby zapewnić:

- odporność sieci lub systemu informatycznego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych,
- bezpieczeństwo usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa.

UWAGA

Umieszczone przez administratora w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych techniczne aspekty ochrony danych osobowych powinny być odpowiednie do stopnia zagrożenia bezpieczeństwa danych osobowych.

Jak ocenić, jaki stopień bezpieczeństwa wdrożyć

Jeśli administrator chce ocenić, czy przyjęty przez niego stopień bezpieczeństwa jest odpowiedni, musi uwzględnić w szczególności ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych.

Ponadto, aby osiągnąć odpowiedni poziom ochrony danych osobowych, administrator powinien wziąć pod uwagę stan wiedzy technicznej, koszty wdrażania zabezpieczeń oraz uwzględnić charakter i cele przetwarzania danych osobowych. Administrator samodzielnie musi ocenić, jakie zabezpieczenia będą proporcjonalne do ryzyka naruszenia danych osobowych przetwarzanych w ramach działalności. Pomocne mogą być:

- wytyczne i najlepsze praktyki dotyczące zarządzania bezpieczeństwem informacji, np. normy ISO, metodyka MARION,
- rekomendacje uznanych organizacji (The OWASP, ENISA),
- wytyczne i zalecenia Grupy Roboczej Art. 29, Europejskiej Rady Ochrony Danych Osobowych,
- zatwierdzone kodeksy postępowania czy
- zatwierdzone mechanizmy certyfikacji.

W praktyce oznacza to, że im bardziej działalność administratora ingeruje w prywatność osób fizycznych, tym więcej środków technicznych i organizacyjnych (lub bardziej zaawansowane środki) powinien wdrożyć. Dotyczy to także sposobu prowadzenia i zawartości instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jakie wymogi muszą spełniać środki bezpieczeństwa

Ogólne rozporządzenie o ochronie danych w kilku miejscach opisuje wymogi bezpieczeństwa danych osobowych, które powinny być przez administratora brane pod uwagę. Wprowadza zasadę uwzględniania ochrony danych w fazie projektowania (*privacy by design*) oraz zasadę domyślnej ochrony danych (*privacy by default*). Wskazuje, że środki ochrony danych osobowych powinny zapewnić:

- możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- poufność, integralność, dostępność i odporność systemów i usług przetwarzania,
- możliwość regularnego testowania, mierzenia i oceniania ich skuteczności.

Ogólne rozporządzenie o ochronie danych wymienia także przykładowe rodzaje zabezpieczeń, które mogą być stosowane w celu ochrony danych osobowych, np. pseudonimizację i szyfrowanie danych osobowych czy minimalizację przetwarzania danych osobowych.

W instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych administrator musi zatem uwzględnić wymogi bezpieczeństwa danych osobowych opisane w ogólnym rozporządzeniu o ochronie danych. Wymogi bezpieczeństwa danych osobowych wynikające z ogólnego rozporządzenia o ochronie danych mają wpływ na techniczne aspekty ochrony danych osobowych w systemach informatycznych np. w kontekście prawa dostępu do systemu czy szyfrowania danych osobowych.

Dokumentacja pomoże wykazać przestrzeganie RODO

Po 25 maja 2018 r. to administrator zadecyduje o formie i sposobie prowadzenia dokumentacji z zakresu przetwarzania danych osobowych. Jedyne, co musi mieć na względzie, to wynikające z ogólnego rozporządzenia o ochronie danych przypisane mu obowiązki. Ich realizację do celów dowodowych powinien obrazować stosowną dokumentacją. Administrator może zatem wdrożyć

jednolitą politykę wewnętrzną obejmującą kompleksowo kwestie regulowane dotąd w polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a dodatkowo uwzględnić w niej nowe obowiązki wynikające z ogólnego rozporządzenia o ochronie danych (np. procedurę zgłaszania naruszeń, procedurę oceny skutków przetwarzania danych).

Administrator może także pozostać przy funkcjonującym obecnie na gruncie polskich przepisów podziale na politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz w osobnych dokumentach wdrożyć procedury wymagane przez ogólne rozporządzenie o ochronie danych.

WAŻNE

Niezależnie od przyjętego rozwiązania administrator musi być świadomy, że dokumentacja przetwarzania danych osobowych powinna przede wszystkim stanowić skuteczny środek ochrony danych osobowych.

Co uregulować w instrukcji zarządzania systemem informatycznym

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna zawierać schematy postępowania, które mogą być skutecznie egzekwowane w organizacji administratora. To na administratorze spoczywa obowiązek wykazania, że procedury przyjęte w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych są realizowane w praktyce i że przetwarza dane zgodnie z wymogami ogólnego rozporządzenia o ochronie danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna zawierać jasne i konkretne rozwiązania, tak aby mogła być stosowana w praktyce. Nie może być celem samym w sobie. Wobec tego wypełnienie formalności i stworzenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie będzie automatycznie oznaczało, że administrator stosuje się do regulacji ogólnego rozporządzenia o ochronie danych.

Co można uznać za naruszenie ochrony danych

O tym, jak ważne są zabezpieczenia danych osobowych wynikające m.in. z instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, świadczy wprowadzenie w ogólnym rozporządzeniu o ochronie danych obowiązku powiadamiania o naruszeniu ochrony danych.

Administrator jest zobligowany do zgłoszenia właściwemu organowi nadzorczemu incydentu polegającego na:

- przypadkowym lub niezgodnym z prawem zniszczeniu, utracie, modyfikacji,
- nieuprawnionym ujawnieniu lub
- nieuprawnionym dostępie do przetwarzanych danych osobowych.

Zgłoszenia należy dokonać w miarę możliwości niezwłocznie, jednak nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Jeśli administrator przekaże zgłoszenie po upływie 72 godzin, będzie musiał wyjaśnić przyczyny opóźnienia. Zawiadomienie o naruszeniu ochrony danych osobowych nie jest wymagane w przypadku, gdy jest mało prawdopodobne, że naruszenie mogło spowodować zagrożenie dla praw i wolności osób, których dane dotyczą.

Nie tylko wejście nieupoważnionej osoby do systemu informatycznego, w którym są przetwarzane dane osobowe, ale też zagubiony laptop bądź telefon mogą stanowić naruszenie ochrony danych osobowych podlegające zgłoszeniu. Dlatego oprócz regulacji odnoszących się do zabezpieczeń, w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych administrator może umieścić schematy postępowania, które pozwolą na reagowanie w sytuacjach naruszeń ochrony danych osobowych.

UWAGA

Niedopełnienie obowiązku zgłoszenia naruszenia ochrony danych osobowych, gdy jest ono wymagane, może wiązać się z koniecznością poniesienia przez administratora kary finansowej, podobnie jak samo naruszenie.

Administrator danych już teraz powinien podjąć działania, aby dostosować się do wymagań ogólnego rozporządzenia o ochronie danych w sprawie ochrony danych osobowych. Powinien przeanalizować, czy konieczne jest wprowadzenie dodatkowych zabezpieczeń danych osobowych, czyli pseudonimizacji czy szyfrowania danych osobowych.

Możliwe, że aktualizacji będzie wymagała dotychczas obowiązująca instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, np. poprzez umieszczenie w niej procedur dotyczących naruszeń ochrony danych osobowych.

Podstawa prawna:

- rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024),
- rozporządzenie Parlamentu Europejskiego i Rady (UE) z 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).

Autor:
Agnieszka Kręcisz-Sarna,
radca prawny

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-7055-9
E-book nr:	2HH0666
Wydawnictwo:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł