Magdalena Krawczyk, Grzegorz Pobożniak

Jak przygotować firmę do nowego systemu ochrony danych osobowych

Przedsiębiorcy będą zobligowani wykazać na żądanie urzędu, że określone rozwiązania zostały rozważone z punktu widzenia ich zgodności z ogólnymi zasadami przetwarzania danych, i przede wszystkim, że tym zasadom w pełni odpowiadają.

W połowie września ujrzał światło dzienne projekt nowej ustawy o ochronie danych osobowych, która ma służyć dostosowaniu polskiej regulacji systemu ochrony danych osobowych do rozwiązań przewidzianych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 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 (dalej: RODO). Rozporządzenie wchodzi w życie 25 maja 2018 roku. Polski ustawodawca chce wykorzystać zakreślony w rozporządzeniu okres dostosowawczy do efektywnego przygotowania się do stosowania rozporządzenia. Ministerstwo Cyfryzacji prowadzi konsultacje społeczne projektu ustawy wdrażającej RODO.

Nowa filozofia

Ambicją autorów rozporządzenia było wprowadzenie nowej filozofii ochrony danych osobowych, opierającej się na siedmiu fundamentach – zasadach dotyczących przetwarzania danych osobowych, które powinny znaleźć odzwierciedlenie w praktykach stosowanych przez organizacje w toku procesu przetwarzania danych. Szukając odpowiedzi na pytanie, jakie ramy prawne zmobilizują administratorów danych do podjęcia środków zapewniających ich rzeczywistą ochronę w praktyce, czyli jednym słowem – zapewnią realizację wspomnianych zasad, przyjęto strategię aktywnej ochrony.

W konsekwencji, osią reformy stała się zasada rozliczalności. Składają się na nią:

- zasada zgodności z prawem, rzetelności i przejrzystości,
- zasada ograniczenia celu przetwarzania danych,
- zasada minimalizacji danych,
- zasada prawidłowości danych,
- zasada ograniczenia przechowania danych,
- zasada integralności i poufności danych.

Ustawowe uregulowanie obowiązku raportowania rzeczywistych środków ochrony danych stanowi nowość w zakresie architektury systemu ochrony danych osobowych. Nigdy wcześniej na administratorach nie ciążyło blankietowe zobowiązanie wykazywania na żądanie organu zgodności podejmowanych praktyk z zasadami dotyczącymi przetwarzania. Przedsiębiorcy w myśl nowych przepisów będą zobligowani wykazać, że określone rozwiązania zostały rozważone z punktu widzenia ich zgodności z ogólnymi zasadami przetwarzania danych, i przede wszystkim, że tym zasadom w pełni odpowiadają.

Pora na sprawdzanie

Wywiązanie się z obowiązku raportowania zgodności praktyk i środków, w pierwszej kolejności wymaga dokonania przeglądu obowiązujących w organizacji polityk i procedur w zakresie przetwarzania danych, a także samych danych. Wprowadzenie mechanizmu rozliczalności skłania do dokonania we własnym dobrze pojętym interesie, nie tylko analizy zapisów wewnętrznych dokumentów dotyczących przetwarzania danych, ale przede wszystkim, rzetelnej oceny praktyki organizacji w tym zakresie. Ten wstępny etap może być porównany do swoistej inwentaryzacji, w ramach której winny być ustalone kategorie przetwarzanych danych, osób, których dane są przetwarzane, a także katalog akcji

podejmowanych względem tych danych, czyli szczegółowy ich opis i dokonywanych w związku z nimi czynności.

Wszystko to pozwoli zidentyfikować rodzaje operacji przetwarzania, które ze względu np. na posłużenie się nowymi technologiami, czy skalę przetwarzania, mogą implikować pewne ryzyka. Jeszcze przed rozpoczęciem przetwarzania, a zatem przed uzyskaniem danych od użytkownika, niezbędne może okazać się dokonanie oceny skutków dla ochrony danych (art. 35 RODO), którego celem jest określenie prawdopodobieństwa i powagi tego naprowadzonego ryzyka, przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować dane ryzyko, zapewniać ochronę danych osobowych, a w końcu, w myśl koronnej zasady rozliczalności, pozwoli wykazać przestrzeganie RODO.

Projekty i ustawienia

Dążąc do osiągnięcia dobrych praktyk prywatności, już na etapie projektowania systemu przetwarzania danych zadbać należy, aby wprowadzone do niego zostały odpowiednie rozwiązania, które zapewnią ochronę danych użytkowników i zagwarantują, że proces przetwarzania następował będzie w zgodzie z RODO. Mowa o zasadzie prywatności w fazie projektowania (*privacy by design* – art. 25 ust. 1 RODO), która każe aktywnie uwzględniać szereg przesłanek, o różnym prawdopodobieństwie występowania i wadze zagrożenia.

I tak, biorąc pod uwagę stan wiedzy technicznej, koszt wdrażania, a także charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator winien wdrożyć środki techniczne oraz organizacyjne w celu wykluczenia ryzyka naruszeń. Rozwiązania te winny być przy tym jak najlepiej dostosowane do rzeczywistych potrzeb administratora, to znaczy powinny być „szyte na miarę" danego procesu przetwarzania. Stąd, wstępnie względem projektowania systemu, nastąpić powinna ocena możliwych ryzyk i ich wpływu na ochronę danych.

Przeprowadzenie oceny przez pryzmat wskazanych powyżej wymogów ma miejsce również w stosunku do systemu, który już funkcjonuje. W tym zakresie, automatyzm przetwarzania wymaga przyjęcia założenia wstępnego w postaci najszerszej możliwej ochrony prywatności. Oznacza to, że ograniczenie prywatności użytkownika nastąpić może wyłącznie z jego własnej inicjatywy, i musi przyjąć postać podjęcia określonej aktywności (zasada prywatności w ustawieniach domyślnych – *privacy by default*).

Ciekawą alternatywą dla wykazania spełnienia wymogów standardu poszanowania prywatności tak w fazie projektowania, jak i sprawdzania adekwatności zakresu przetwarzania danych w systemie (ustawień domyślnych) będzie mechanizm certyfikacji. Trudno ocenić czy administratorzy będą powszechnie decydowali się na certyfikowanie swoich systemów, głównym zagrożeniem jest fakt, iż uzyskanie certyfikatu nie zwalnia administratora z przestrzegania wymogów rozporządzenia (art. 42 ust. 4 RODO).

Zmiany w dokumentacji

Przebudowa prawnych ram ochrony danych nie spowoduje całkowitego zdezaktualizowania się dokumentacji dotyczącej przetwarzania, obowiązującej w organizacjach w myśl aktualnych przepisów. W tym zakresie RODO wprowadza jednak wymóg legitymowania się nowymi, dodatkowymi dokumentami.

Aktualnie na administratorze danych spoczywa obowiązek posiadania polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym.

Rolą pierwszego dokumentu jest wskazanie środków bezpieczeństwa i procedur bezpiecznego przetwarzania informacji. Tam znajdziemy wykaz fizycznych i technicznych zabezpieczeń, miejsc, gdzie dane są przetwarzane oraz programów zastosowanych do przetwarzania danych osobowych. Instrukcja ma zaś na celu uporządkowanie procedur w zakresie nadawania uprawnień, uwierzytelniania, tworzenia narzędzi programowych.

RODO przewiduje

Ustawa o ochronie danych osobowych z 1997 r. przewiduje:

- posiadanie polityki bezpieczeństwa danych osobowych

- instrukcję zarządzania systemem informatycznym

- rejestr czynności przetwarzania udostępniany na żądanie organu nadzorczego – art. 30 RODO;

- dokumentację incydentów (naruszeń) – art. 33 ust. 5 RODO

- politykę i instrukcje wykazujące zgodność z RODO

W odniesieniu do obowiązków formalnych, pozytywna zmiana polega na zniesieniu uciążliwej dla administratorów procedury rejestracji i aktualizacji zbiorów danych osobowych. Sam fakt rejestracji nie gwarantował, że dane są należycie chronione. Ten aspekt w szczególności wymagał więc zmian, które miały przyczynić się do sztandarowego celu reformy, czyli przeniesienia ochrony danych z „teorii do praktyki", i pomóc nadzorowaniu i przestrzeganiu prawidłowości procesu przetwarzania. Alternatywą dla rejestracji będzie obowiązek prowadzenia przez przedsiębiorców dokumentacji czynności przetwarzania. Analiza ma tutaj przybierać czynność aktywną, pozostającą w toku w miarę przetwarzania danych – administratorzy obowiązani są na bieżąco analizować i przewidywać skutki przetwarzania.

Zgodnie z RODO, administrator będzie obowiązany dokumentować wszelkie naruszenia ochrony danych osobowych, uwzględniając okoliczności oraz skutki naruszeń, a także podjęte przez siebie działania zaradcze. Dokumentacja będzie służyła organowi nadzorczemu do sprawdzenia czy przestrzegane są obowiązki administratora, w tym obowiązek zawiadomienia organu o wystąpieniu incydentu naruszenia. Zalecanie jest wcześniejsze przygotowanie stosownej polityki reagowania na incydenty, a wraz z nią wzorów odpowiednich formularzy informacyjnych i planów naprawczych.

Przygotowanie tych dokumentów nabiera szczególnego znaczenia, ponieważ w przypadku zaistnienia incydentu naruszenia, administrator ma jedynie 72 godziny na przygotowanie kompletnego zawiadomienia do organu nadzorczego.

Lepiej zapobiegać niż leczyć

W myśl zasady, że lepiej zapobiegać, niż leczyć, niezależnie od wspomnianych powyżej dokumentów, z punktu widzenia prawidłowej realizacji zasady rozliczalności, rekomendowane jest uzupełnienie *workflow* w zakresie przetwarzania danych w organizacji o dodatkowe dokumenty wewnętrzne. Każda organizacja powinna więc skodyfikować instrukcję „krok po kroku" postępowania w sytuacjach potencjalnych zagrożeń. Wskazać można, że administrator winien wyczerpująco uregulować konsekwencje pobrania służbowej poczty na prywatne urządzenie mobilne pracownika, lub sposób postępowania w przypadku pozostawienia wydruków w nieodpowiednim miejscu, tak, że informacje mogą trafić w niepowołane ręce.

RODO wymaga, aby każda z podobnych sytuacji została odpowiednio wcześnie przewidziana, a administrator zapewnił na wypadek ich zaistnienia dokładne instrukcje. I tak, odpowiednio do podanego przykładu, byłyby to instrukcje wykorzystywania w pracy mobilnych urządzeń służbowych i prywatnych, czy obiegu dokumentów zapewniającego zachowanie ich poufności, które będą następnie pomocne dla wykazania, czyli znamiennego – rozliczenia, akcji podejmowanych w zakresie przetwarzania danych.

Zdaniem autorów

Spodziewane efekty - Grzegorz Pobożniak, adwokat, partner w Kancelarii Kubas Kos Gałkowski sp. p. sp.k.; Magdalena Krawczyk, adwokat, *senior associate* w Kancelarii Kubas Kos Gałkowski sp. p. sp.k.

Lektura motywów rozporządzenia wskazuje kierunek reformy, której głównym celem zdaje się być zapewnienie danym osobowym, a konkretnie prywatności – gwarantującej ich poufność,

eksponowanego miejsca w katalogu praw podstawowych. Tyle teorii. Ciągły wzrost wartości danych osobowych i zwiększenie się liczby zagrożeń przemawiają za potrzebą realnego wzmocnienia odpowiedzialności administratorów, którzy w myśl RODO mają podejmować konkretne działania i pełnić aktywną rolę w organizacji. Obowiązek rozliczalności ma stanowić gwarancję realizacji zasad dotyczących przetwarzania danych osobowych. Wydaje się, że to rozwiązanie będzie adekwatną odpowiedzią na skalę naruszeń i posłuży jako efektywne narzędzie dla egzekwowania przepisów przez organy nadzorcze.

Pierwotnie tekst ukazał się: Rzeczpospolita, 10.11.2017