Rzeczpospolita z 31.03.2017

Dane osobowe: firmy muszą zacząć szkolenia

Jarosław Kamiński, adwokat Warszawa, Rödl & Partner
Adam Wódź, IT Security Manager, Cybercom Poland

Wyzwaniem dla administratorów danych będzie wdrożenie takich środków technicznych i organizacyjnych, które w najlepszy sposób ochronią dane osobowe przed incydentami związanymi z ich bezpieczeństwem. Dobór tych środków spocznie w całości na przedsiębiorcach.

Zgodnie z postanowieniami RODO firmy mają jeszcze 14 miesięcy na przygotowanie się do nadchodzących zmian zarówno pod kątem prawnym jak i technicznym (informatycznym). W tym okresie wskazane byłoby, aby administratorzy danych (kadra zarządzająca i osoby odpowiedzialne za procesy przetwarzania danych osobowych) zapoznali się z nowymi regulacjami, obowiązkami i wytycznymi oraz sankcjami, jakie grożą za nieprzestrzeganie lub niewdrożenie przepisów RODO.
W szczególności zalecane jest, aby firmy dokonały jeszcze przed 25 maja 2018 r.:

- weryfikacji przesłanek i podstaw przetwarzania danych osobowych;
- weryfikacji konieczności i zasadności powołania Inspektora Ochrony Danych Osobowych;
- analizy i weryfikacji dokumentacji kadrowej i zasad procesu rekrutacji;
- ustalenia kategorii i zbiorów przetwarzanych danych osobowych;
- audytu przetwarzania danych pod kątem RODO i rekomendacji do wdrożenia w przyszłości;
- przeprowadzenia szkoleń dla pracowników w zakresie nowych zasad przetwarzania danych na gruncie RODO;
- weryfikacji stron internetowych pod kątem przetwarzania danych i rekomendacji zmian na gruncie RODO;
- weryfikacji umów powierzenia przetwarzania danych osobowych oraz propozycji nowych postanowień pod kątem RODO;
- weryfikacji stosowanych klauzul informacyjnych oraz propozycji nowych klauzul na gruncie RODO;
- weryfikacji stosowanych klauzul zgody na przetwarzanie danych oraz propozycji nowych klauzul na gruncie RODO;
- opracowania wstępnej dokumentacji związanej z ochroną danych na gruncie RODO oraz systematycznej (cyklicznej, np. raz na kwartał) weryfikacji pod kątem nowych wytycznych i wskazówek organów nadzorczych.

Dodatkowo, RODO przewiduje, że pewne szczególne kwestie mogą i powinny zostać uregulowane w ramach ustawodawstwa krajowego. Zatem, konieczne będzie także monitorowanie zmian w polskiej ustawie o ochronie danych oraz ewentualne wdrożenie jej zasad w firmach (np. w zakresie kwestii pracowniczych).

Wyzwania dla IT

Zmiany wynikające z RODO nie ograniczają się wyłącznie do zagadnień i interpretacji prawnych. Nowomianowany inspektor ochrony danych (lub administratorzy danych w razie braku powołania inspektora ochrony danych) będzie musiał umieć sprawować także pieczę nad procedurami bezpieczeństwa systemów informatycznych wykorzystywanych do przetwarzania danych osobowych. A procedury te, w porównaniu z obecnie obowiązującym ustawodawstwem, przejdą poważną metamorfozę i mocno zyskają na znaczeniu.

Przeprowadzenie analizy ryzyka

Według nowych wytycznych przetwarzanie danych osobowych nie będzie w ogóle możliwe bez przeprowadzenia dogłębnej analizy jego potrzeb, zakresu i ryzyk z nim związanych. W kontekście systemów IT szczególne znaczenie będzie miała oczywiście ta ostatnia analiza. Obowiązek jej przeprowadzenia spocznie bezpośrednio na administratorze danych, przy czym decyzje i procedury ustalone w wyniku analizy ryzyka będą obowiązywały nie tylko administratora, ale także podmioty przetwarzające – czyli ewentualnych podwykonawców zaangażowanych w przetwarzanie danych osobowych.
Ryzyko związane z ewentualnymi incydentami upublicznienia lub utraty danych trzeba będzie ocenić na podstawie aktualnego stanu wiedzy technicznej i znajomości realnych zagrożeń. A zatem każda firma będzie musiała we własnym zakresie przeprowadzić rozpoznanie aktualnej sytuacji w „świecie" ataków na dane, po czym najlepiej udokumentować proces pozyskania tych informacji. Należy przy tym pamiętać, że nie może to być działanie

jednorazowe, lecz zaplanowany z góry proces wymagający cyklicznej powtarzalności. Wiadomo bowiem, że zagrożenia dla danych osobowych zmieniają się bardzo dynamicznie i to, co dzisiaj uznajemy za bezpieczny standard, jutro może okazać się wielką luką w systemie bezpieczeństwa, która narazi nasze dane na niekontrolowany wyciek. Jako przykład możemy przyjąć chociażby niedawne wykrycie podatności w protokole szyfrowania SSL, który przez wiele lat był wykorzystywany jako podstawowe zabezpieczenie transmisji wrażliwych danych na stronach internetowych.
Wzorcowo wdrożony proces analizy zagrożeń powinien uwzględniać zatem stałe monitorowanie informacji o wykrytych lukach w bezpieczeństwie systemów i aplikacji oraz o „trendach" w skutecznych atakach hackerskich, a także – co najważniejsze – umożliwiać szybką reakcję na pojawiające się zagrożenia o wysokim stopniu ryzyka dla bezpieczeństwa danych osobowych, także poza przyjętą wcześniej regularnością przeprowadzania analizy ryzyka. Nietrudno się bowiem domyśleć, że najwięcej skutecznych ataków na dane następuje w ciągu kilku pierwszych dni po upublicznieniu informacji o wykrytej luce bezpieczeństwa. Hackerzy zdają sobie sprawę, że ich skuteczność zależy wtedy od opieszałości administratorów IT w instalowaniu „łatek" bezpieczeństwa dostarczanych przez producentów podatnych aplikacji czy systemów. Przedsiębiorcy, zwłaszcza ci przetwarzający duże zbiory danych osobowych lub dane szczególnie wrażliwe, powinni zatem być gotowi do podjęcia skutecznej walki nie tylko z atakującymi, ale także z czasem.

Wdrożenie zabezpieczeń

Kolejnym wyzwaniem dla administratorów stanie się wdrożenie takich środków technicznych i organizacyjnych, które w najlepszy sposób ochronią dane osobowe przed incydentami związanymi z ich bezpieczeństwem. Dobór tych środków spocznie w całości na przedsiębiorcach, przy czym w swoich analizach będą oni mogli uwzględnić koszty wdrożenia poszczególnych rodzajów zabezpieczeń i ich wpływ na realne obniżenie poziomu ryzyka dla danych.
W praktyce będzie to zapewne wyglądało tak, że przedsiębiorca, który uzna, że przetwarzany przez niego zakres danych osobowych nie jest obarczony dużym ryzykiem ewentualnego naruszenia praw osób fizycznych, będzie mógł zrezygnować z wdrażania zaawansowanych systemów bezpieczeństwa (np. SIEM) i wybrać jedynie takie rozwiązania, które uzna za optymalne w stosunku poziomu gwarantowanej ochrony do kosztów jej wdrożenia. Oczywiście taki proces decyzyjny także będzie musiał być odpowiednio udokumentowany. Można się już domyślać, że podczas ewentualnej kontroli organ nadzorczy poprosi w pierwszej kolejności nie tylko o dokument polityki bezpieczeństwa, ale także właśnie o dokumentację przeprowadzonych procesów analizy ryzyka i wyboru adekwatnych środków bezpieczeństwa.
A to jeszcze nie wszystko! RODO wyraźnie wskazuje także konieczność regularnego testowania, mierzenia i oceniania skuteczności wdrożonych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych. Nie wystarczy zatem w dokumentacji uzasadnić swój wybór środków bezpieczeństwa, lecz także opracować, wdrożyć i udokumentować proces cyklicznej weryfikacji, że wybór ten jest trafny i zapewnia odpowiedni poziom bezpieczeństwa.

Monitorowanie incydentów

Jednak najbardziej wymagającą dla przedsiębiorców zmianą wydaje się być wprowadzenie obowiązku monitorowania wszelkich incydentów związanych z bezpieczeństwem przetwarzanych danych osobowych. Administrator będzie miał jedynie 72 godziny na zgłoszenie organowi nadzorczemu wykrytego wycieku danych, włączając w to czas potrzebny na konieczną analizę skali problemu – określenie liczby i rodzaju danych, które wyciekły. Jeśli z jakiegoś powodu administrator spóźni się z powiadomieniem, to będzie musiał przedstawić pisemne usprawiedliwienie tego faktu. Jeżeli zaś wyciek mógłby skutkować „wysokim ryzykiem naruszenia praw lub wolności osób fizycznych" (czyli dotyczyłby danych wrażliwych lub umożliwiających np. podszycie się pod daną osobę w celu wzięcia kredytu), to administrator będzie miał obowiązek poinformowania o zagrożeniu także poszczególne osoby, których to ryzyko dotyczy. W przypadku wycieku znacznej liczby danych powiadomienia takiego będzie można dokonać za pomocą mediów.
A zatem do konieczności monitorowania informacji o zagrożeniach i skuteczności systemów zabezpieczających dojdzie jeszcze jeden obowiązek – stałe monitorowanie incydentów związanych z bezpieczeństwem danych. Wiąże się to z potrzebą przeprowadzenia różnorakich działań, które powinny być dostosowane do możliwości poszczególnych przedsiębiorstw. Na pewno warto będzie w pierwszej kolejności podnieść poziom świadomości zagrożeń wśród pracowników – tak, aby ewentualny incydent został w ogóle rozpoznany i niezwłocznie zgłoszony administratorowi.

Jarosław Kamiński, adwokat i senior associate w warszawskim biurze Rödl & Partner

Sankcje dla przedsiębiorców

Naruszenie przepisów RODO będzie oznaczać dla przedsiębiorców określone sankcje zarówno cywilnoprawne (odszkodowanie za poniesioną szkodę), jak i administracyjne (w zależności od naruszenia aż do 20 mln euro, a w przypadku przedsiębiorstwa – do 4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa). Dodatkowo, państwa członkowskie mają obowiązek przyjąć przepisy określające inne sankcje za naruszenie RODO, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym oraz podjąć wszelkie środki niezbędne do ich wykonania.

Rozporządzenie Ogólne o Ochronie Danych

Rozporządzenie 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 (RODO) wejdzie w życie 25 maja 2018 r. Nowe przepisy obowiązywać będą bezpośrednio, tj. nie będą one zasadniczo wymagać implementacji do polskiego porządku prawnego. Przepisy RODO wzmacniają pozycję osób fizycznych, nakładając jednocześnie nowe obowiązki na przedsiębiorców i organy nadzoru w zakresie ochrony danych.
Już dziś przedsiębiorcy (w tym grupy przedsiębiorców) powinni przygotować się na wyzwania i zmiany, które będą konieczne w celu dostosowania ich modelu biznesowego (w tym rozwiązań technicznych) do nowych regulacji w zakresie ochrony i przetwarzania danych osobowych, niezależnie od skali, rodzaju, zakresu i celu przetwarzania danych osobowych.
Celem uchwalenia RODO jest ujednolicenie w całej Unii Europejskiej poziomu ochrony danych i zapewnienie poczucia pewności prawnej w zakresie przetwarzania danych osobowych.

Nowe obowiązki dla przedsiębiorców

Przepisy RODO przewidują m.in. wprowadzenie:
- rozszerzonej formuły zgody na przetwarzanie danych;
- rozszerzonego zakresu obowiązku informacyjnego;
- rejestru czynności przetwarzania;
- zmiany statusu Administratora Bezpieczeństwa Informacji na Inspektora Ochrony Danych;
- zmienionej definicji danych wrażliwych;
- zwiększenia uprawnień osób, których dane dotyczą.

Z kolei, nowe obowiązki po stronie przedsiębiorców pojawią się, w szczególności w następujących obszarach:
- nowego podejścia do ochrony danych osobowych (risk-based approach);
- ułatwienia dla grup przedsiębiorstw;
- uregulowania zasad profilowania;
- prawa do przenoszenia danych do innego usługodawcy;
- wprowadzenie kar administracyjnych i ich zdecydowanego egzekwowania;
- raportowania o własnych naruszeniach i prawa osoby, której dane dotyczą do informacji o naruszeniu ochrony danych;
- przetwarzania danych dziecka tylko za zgodą opiekuna.

Dodatkowo, na administratorów danych RODO nakłada obowiązek uwzględnienia najnowszych osiągnięć technicznych oraz kosztów wdrożenia rozwiązań w zakresie ochrony danych zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i podczas przetwarzania przy wdrożeniu odpowiednich środków i procedur technicznych oraz organizacyjnych w taki sposób, aby przetwarzanie gwarantowało ochronę praw osoby, której dane są przetwarzane.
Źródło: http://www.rp.pl/Kadry/303319986-Dane-osobowe-firmy-musza-zaczac-szkolenia.html#ap-8