Ready to RODO – czyli jak przygotować się do nowego rozporządzania w 9 krokach?

24.08.2017

25 maja 2018 roku w życie wchodzi rozporządzenie o ochronie danych osobowych (RODO). Dokument unifikuje kwestie związane z ochroną danych osobowych na terenie Unii Europejskiej, co oznacza, że wszystkie przedsiębiorstwa i instytucje działające na terenie UE będą obowiązywać te same procedury.

Nowe rozporządzenie nie definiuje wprost jakich narzędzi użyć aby być zgodnym z nowym prawem. Zgodnie z przyjętym w dokumencie podejściem opartym na ryzyku (risk based approach) to w jaki sposób organizacja dostosuje się do zmian zależy tylko i wyłącznie od niej. Nowe podejście mówi nam natomiast o tym, że to przedsiębiorstwo jest odpowiedzialne za właściwe zidentyfikowanie i zabezpieczenie danych osobowych, które przechowuje.

Wydawać się może, że maj 2018 to odległy termin. Nic bardziej mylnego. Dostosowanie organizacji do nowych przepisów w zakresie danych osobowych to poważne wyzwanie, wymagające zarezerwowania dużej ilości czasu. Zgodnie z raportem przedstawionym przez Fundację „Wiedza to Bezpieczeństwo", blisko 50% organizacji nie rozpoczęło jeszcze, bądź w ogóle nie wie w jaki sposób przygotować się do RODO. [1]

Jakie kroki należy zatem podjąć aby przygotować organizację na 25.05.2018?

1. Zbudowanie świadomości

Wiedza na temat wejścia w życie nowego rozporządzenia to podstawa. Przede wszystkim informacja o nowych wymaganiach musi trafić do osób zarządzających, tak aby mogli oni wystarczająco wcześnie przygotować na nią organizację. Poza kadrą kierowniczą, informacja powinna dotrzeć także do wszystkich pracowników, przede wszystkim tych, którzy mają na co dzień do czynienia z danymi osobowymi.

2. Dokonanie identyfikacji

Proces dostosowania do RODO należy rozpocząć od szczegółowej inwentaryzacji obszarów organizacji, w których występują dane osobowe. Następnie powinniśmy odpowiedzieć sobie na kilka pytań: Gdzie dane osobowe występują? Kto ma do nich dostęp? Jakie operacje może na nich wykonywać? Jakie są źródła pozyskiwania danych? Czy są udostępniane poza organizację i w jakim celu?

3. Zidentyfikowanie zagrożeń

Dane osobowe narażone są na dostanie się w niepowołane ręce. W związku z tym należy zidentyfikować wszystkie możliwe miejsca ich wycieku.

4. Przegląd dokumentacji

Punkt ten dotyczy przeglądu dotychczasowej dokumentacji i procedur: klauzul, pozyskiwania zgód na przetwarzanie danych, powierzanie danych osobowych osobom trzecim. RODO na nowo określa jakich informacji musi udzielić organizacja zbierając dane osobowe oraz jakie zgody powinna pozyskać.

5. Wprowadzenie nowych procedur

RODO wymusza zaplanowanie i wdrożenie nowych procesów wewnątrz organizacji tak aby maksymalnie zapewnić bezpieczeństwo pozyskiwanych, przetwarzanych i powierzanych danych osobowych. Należy przygotować procedury związane z takimi procesami jak: informowanie w zakresie danych osobowych, pozyskiwanie, przenoszenie, kasowanie, kopiowanie danych, incydenty czy przekazywanie danych to państw trzecich.

6. Dostosowanie narzędzia IT

Dane osobowe zwykle przechowujemy w różnego rodzaju systemach informatycznych np. klasy ERP. To w nich gromadzone są informacje o zatrudnionych pracownikach (systemy kadrowo-płacowe) czy też kontakty zebrane podczas działań marketingowych i sprzedażowych prowadzonych przez organizację (systemy CRM). Dlatego też jednym z najistotniejszych kroków w ramach przygotowania do RODO jest przeprowadzenie audytu wykorzystywanych systemów informatycznych. Przede wszystkim systemy IT, w których przechowujemy dane, muszą spełniać wyśrubowane normy bezpieczeństwa, zabezpieczające je przed ewentualnymi atakami hackerskimi. Informacja o częstotliwości wykonywania testów penetracyjnych, pozwoli ocenić czy dostawca rozwiązania IT regularnie dba o bezpieczeństwo dostarczanego produktu. Zgodnie z przyjętą w rozporządzeniu zasadą privacy by default, systemy informatyczne mają zapewniać ochronę danych osobowych na poziomie pierwotnych ustawień. Zasada wymaga domyślnych ustawień systemu zapewniających możliwie najszerszą ochronę prywatności wszystkich użytkowników, a zmiana powinna następować tylko i wyłączenie na wyraźne żądanie użytkownika, wymagając od niego podjęcia aktywnego działania. Drugim aspektem jest przygotowanie systemów pod kątem funkcjonalnym (obsługa procesów przetwarzania danych, zamieszczenie informacje o źródle pozyskania danych, przechowywanie zgód, kasowanie danych czy właściwa konfiguracja systemu uprawnień do zarządzania danymi). W obu tych kwestiach warto skomunikować się ze swoim dostawcą rozwiązań IT i upewnić się że system z którego korzystamy będzie na RODO przygotowany.

7. Zabezpieczenie kopii zapasowych

Należy pamiętać, że wprowadzone przez RODO normy bezpieczeństwa dotyczą nie tylko systemów w których przechowujemy i przetwarzamy dane osobowe (np. system ERP), ale również wszystkie miejsca w których przechowujemy ich kopie zapasowe. Oznacza to konieczność rewizji aktualnie stosowanych mechanizmów zarządzania kopiami bezpieczeństwa danych firmy.

8. Powołanie Inspektora Ochrony Danych Osobowych

W miejsce dotychczasowych Administratorów Bezpieczeństwa Informacji (ABI) organizacja będzie zobowiązana do powołania Inspektora Danych Osobowych. Stworzenie nowego stanowiska będzie obligatoryjne dla wszystkich instytucji publicznych (z wyłączeniem sądów), organizacji, których główna aktywność polega na regularnym i automatycznym przetwarzaniu danych osobowych poprzez monitorowanie na dużą skalę osób, których dane są przetwarzane oraz organizacji, których główna działalność polega na przetwarzaniu wrażliwych danych osobowych oraz danych dotyczących przestępstw i skazań za przestępstwa. Inspektor na co dzień monitoruje zgodność procedur z wymogami rozporządzenia.

9. Stały monitoring

Właściwe przygotowanie organizacji na wejście w życie rozporządzenia wymaga podjęcia działań odpowiednio wcześniej. Należy jednak pamiętać, że ochrona danych osobowych jest procesem ciągłym. Dlatego też, po wejściu w życie rozporządzenia, należy stale monitorować procesy zachodzące w organizacji i na bieżąco weryfikować czy dane osobowe są odpowiednio chronione.

RODO określa wysokość kar finansowych za uchybienia związane z nieprzestrzeganiem obowiązków wynikających z rozporządzenia. Wysokość kar uzależniona jest od skali naruszeń i może wynieść do 10 mln euro, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego obrotu światowego z poprzedniego roku obrotowego lub do 20 mln euro a w przypadku przedsiębiorstwa do 4% jego całkowitego rocznego obrotu światowego z poprzedniego roku obrotowego. W obu przypadkach zastosowanie będzie miała kara wyższa.

Do rozporządzenia o ochronie danych osobowych przygotowują się wszystkie organizacje mające do czynienia z danymi osobowymi. Mikroprzedsiębiorstwa jak i globalne korporacje, sektor prywatny oraz publiczny. Niezależnie od skali wielkości organizacji, to ostatni dzwonek aby rozpocząć przygotowania na zmiany jakie czekają nas od 25.05.2018.

Konrad Spryńca

[1] Red. M. Danielewicz, „*Co wiemy o ochronie danych osobowych*”, Warszawa 2017, s.21