# RODO: trudna rzeczywistość polskiego biznesu

W maju 2018 r. dostosowanie do tzw. ogólnego rozporządzenia o ochronie danych, czyli Rozporządzenia 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 (DzUrz UE L 119 4 maja 2016 r., dalej: RODO) przypominało sceny z filmów katastroficznych. Mimo że przepisy wprowadzające obowiązki wynikające z RODO znane były od 2016 r., wiele firm odłożyło wdrożenie nowych przepisów na ostatnią chwilę. Apogeum nerwowości przypadło właśnie na maj 2018 r., kiedy odliczano dni do wejścia w życie rozporządzenia. Dodatkowo temat był podsycany w prasie, w której nie brakowało informacji o konsekwencjach w postaci kar finansowych z tytułu nieprzestrzegania RODO. Równolegle skrzynki mailowe przedsiębiorców zalewała fala informacji i ofert od firm doradczych zajmujących się dostosowaniem zasad ochrony danych osobowych do nowych regulacji.

W praktyce wielu przedsiębiorców nie zdążyło z wdrożeniem wszystkich niezbędnych działań do 25 maja 2018 r. Część z nich dalsze dostosowania związane z ochroną danych osobowych odłożyła na później. Wielu przedsiębiorców przyjęło zaś podstawowe dokumenty związane z RODO bez dostosowania ich do specyfiki swojej działalności, mając poczucie złudnego spokoju i oddalonego widma egzekucji.

## Ciągła ewolucja

Należy mieć świadomość, że ochrona danych osobowych zgodnie z RODO, podobnie jak to było pod rządami wcześniej obowiązujących krajowych przepisów, jest nieustannym procesem. Nie wystarczy jednorazowe przygotowanie dokumentacji, ponieważ wraz z rozwojem firmy powinny ewoluować również procedury, które dotyczą organizacji przetwarzania danych osobowych.

W tym roku w życie wszedł kolejny pakiet krajowych przepisów związanych z ochroną danych osobowych. Pojawiły się również pierwsze interpretacje i wytyczne organów. Z tego względu dokumenty, które mają zastosowanie w działalności firm, powinny być nieustannie dostosowywane do zmieniającego się otoczenia. RODO nie określiło sztywnych zasad postępowania, przyjmując, że procedury czy zabezpieczenia, które dla jednego przedsiębiorcy są właściwe, nie muszą się sprawdzić w przypadku innych podmiotów.

Przedsiębiorcy często nie wiedzą, jak właściwie interpretować niezrozumiałe przepisy. W dalszym ciągu odczuwają więc niepewność co do tego, jak ich działania ocenią organy dokonujące kontroli czy sądy. Sytuacji nie uspokajają rozbieżne sygnały płynące z Ministerstwa Cyfryzacji i Urzędu Ochrony Danych Osobowych, jak choćby w kwestiach dotyczących określania podstawy przetwarzania w procesie rekrutacji czy dopuszczalności prowadzenia badań trzeźwości.

## Niezbędna analiza ryzyka

Obecna sytuacja sprawia, że nietrudno o absurdy. Wiele firm na własnej skórze przekonało się, że „szafki RODO" są tylko dobrym chwytem marketingowym, nie gwarantując właściwego poziomu ochrony. Takiej gwarancji nie daje też sam fakt

powołania inspektora ochrony danych osobowych. Aby mieć pewność, że ochrona danych osobowych jest odpowiednia, trzeba zweryfikować wszystkie działania firmy w zakresie przetwarzania tych danych, a także ustalić, co może naruszyć ich bezpieczeństwo – np. komputery bez wygaszaczy ekranu pozostawiane w miejscu dostępnym dla klientów, mogą pozwolić na dostęp do danych osobom nieuprawnionym, a nieprzeszkolony z obsługi programu pracownik może nieświadomie skasować dane lub niewłaściwie je zmienić.

Dla przedsiębiorstw, które chcą zapewnić zgodność z RODO na stałe, niezbędnym narzędziem stały się cykliczne audyty procesów przetwarzania danych osobowych. Jednak audyt sam w sobie jest niewystarczający. Tylko tzw. analiza ryzyka, czyli ocena jakie zdarzenia mogą naruszyć bezpieczeństwo danych, pozwala ustalić, czy zabezpieczenia techniczne poszczególnych danych są właściwe, a stosowane procedury odpowiednie.

W ubiegłym roku dokumenty związane z ochroną danych osobowych bardzo często sporządzano bez inwentaryzacji procesów przetwarzania i bez analizy zdarzeń, które mogą naruszyć bezpieczeństwo danych. To oznacza, że opracowane procedury mogą nie być zgodne z RODO.

**Obowiązki informacyjne…**

W zeszłym roku wątpliwości związane z RODO pojawiały się w kolejności dobrze odzwierciedlającej etapy dostosowywania się rynku do tych regulacji. Pierwsze z nich dotyczyły treści obowiązków informacyjnych. Wiele podmiotów nie miało pewności, jak właściwie określić cele i podstawy przetwarzania danych oraz w jaki sposób ustalić okres ich przechowywania. Często wynikało to z braku dokładnego zidentyfikowania procesów przetwarzania – firmy musiały zacząć informować, zanim zdążyły w pełni przygotować się do RODO. Dodatkowo zasady przetwarzania danych osobowych muszą być opisane w sposób jasny i zrozumiały. Bez właściwego zrozumienia przepisów nie jest to proste.

**… wyzwaniem w marketingu**

Realizacja obowiązków informacyjnych wciąż stanowi wyzwanie przede wszystkim dla działań marketingowych i sprzedażowych. Liczba przetwarzanych w nich danych jest przeogromna, a specyfika przetwarzania często niejednorodna. Rośnie wykorzystanie nowych technologii – aplikacje zbierają coraz więcej danych od geolokalizacji i wizerunku po informacje o preferencjach i sposobie życia. Mimo deklaracji producentów oprogramowania, wiele systemów informatycznych nie spełnia wymagań stawianych przez RODO. Audyty ochrony danych osobowych często pobieżnie objęły bezpieczeństwo w tym obszarze. Świadomość, co wymaga jeszcze dostosowania, często jest więc niewystarczająca.

Problemy związane z przetwarzaniem danych osobowych dotyczą również wykorzystania mediów społecznościowych, np. instalacji wtyczek społecznościowych współpracujących z takimi serwisami jak Facebook czy LinkedIn. Niemało kłopotów sprawiają nadal tradycyjne kanały komunikacji, jak choćby infolinie czy zbieranie danych przy monitoringu wizyjnym.

**Wystarczy skrócone powiadomienie**

W lipcu 2019 r. Europejska Rada Ochrony Danych wydała wytyczne, w których potwierdziła dopuszczalność tzw. warstwowego obowiązku informacyjnego. Oznacza to możliwość podania podstawowych informacji o przetwarzaniu z odesłaniem do pełnego zakresu np. na stronę internetową. Dzięki temu nie powinno być już wątpliwości co do jego dopuszczalności i zasad konstrukcji. Przedsiębiorcom na pewno ułatwi to życie.

**Klient mówi: sprawdzam**

Jak wynika badań z przeprowadzonych przez Komisję Europejską w 28 państwach Unii Europejskiej, Polacy w porównaniu do innych Europejczyków mają dużą świadomość funkcjonowania przepisów dotyczących RODO. Zaledwie 36 proc. Europejczyków w ogóle wie, czym jest RODO. W Polsce taką świadomość ma aż 56 proc. badanych.

**56 proc.Badanych Polaków wie, czego dotyczą przepisy RODO**

Dla firm to ważna informacja. Ich klienci coraz częściej będą bowiem mówić „sprawdzam" i żądać odpowiedniej ochrony swoich danych osobowych. Dlatego przedsiębiorcy powinni pomyśleć o audytach weryfikacyjnych, tzn. sprawdzeniu zakresu i jakości posiadanych „dokumentów RODO" oraz sposobu, w jaki realizowane są zawarte w nich procedury. Audyt można rozszerzyć o symulacje incydentów według scenariuszy dedykowanych specyfice prowadzonej działalności. Testy bezpieczeństwa warto przeprowadzić w działach sprzedaży i marketingu oraz obsługi klienta. Kluczowe jest również zweryfikowanie przetwarzania danych osobowych pracowników. Te z firm, które do tej pory nie badały przetwarzania danych w swoich systemach, powinny pomyśleć także o zaudytowaniu przynajmniej wybranych, kluczowych systemów informatycznych pod kątem funkcjonalności wymaganych przez RODO i podatności na incydenty.

Wyniki audytów powinny dostarczyć informacji, na podstawie których będzie można przeprowadzić analizę ryzyka. Dopiero na podstawie informacji o rodzajach zagrożeń dla ochrony danych oraz ich ważności można określić, jakie procedury i dokumenty rzeczywiście są potrzebne.

Przedsiębiorcy muszą się liczyć z koniecznością korekty stosowanych rozwiązań z uwagi na zmiany w zakresie interpretacji przepisów. Nie mogą też zapominać jak istotne jest regularne prowadzenie szkoleń dla pracowników – zarówno z zasad wynikających z przepisów o ochronie danych osobowych, jak i sposobu stosowania wprowadzonych u nich polityk i procedur.

Powyższym wyzwaniom firmy będą musiały sprostać z uwzględnieniem bieżących, praktycznych problemów, jakie napotykają w swojej działalności. W dalszej części dodatku prezentujemy wybrane zagadnienia, które odnoszą się do stosowania RODO na co dzień. Ich lektura pozwoli lepiej zidentyfikować kwestie dotyczące ochrony danych osobowych, które wymagają szczególnej uwagi, a także kierunki, w jakich należy szukać rozwiązań dotyczących dostosowania prowadzonej działalności do wymogów prawa

Autor: Marcin Piszcz, wspólnik zarządzający Kancelarii Prawnej Piszcz i Wspólnicy sp.k.