

Mamy wzmocniać ochronę danych osobowych, a nie ją osłabiać

Dr Edyta Bielak-Jomaa: W najnowszym projekcie ustawy wdrażającej zrezygnowano z wielu planowanych wyłączeń obowiązków zapisanych w RODO. Mam nadzieję, że nikt nie będzie próbował ponownie ich wprowadzić. Przynajmniej w dotychczas zaproponowanym kształcie

Przedsiębiorcy wciąż nie wiedzą, w jakim stanie prawnym obudzą się 25 maja, bo nadal nie wiadomo, czy do tego czasu Sejm i Senat zdążą uchwalić regulacje wdrażające do naszego porządku prawnego RODO, czyli ustawę o ochronie danych osobowych i ustawę o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia, nowelizującą blisko 200 aktów prawnych. Przedsiębiorcy zastanawiają się, jak mają podejść do stosowania RODO. Przykładowo, w pierwotnych projektach tej drugiej ustawy dla wielu grup przewidziano wyłączenie z wykonywania obowiązku informacyjnego wynikającego z art. 13 RODO. Jeśli te przepisy nie zostaną uchwalone do 25 maja, to w jaki sposób mają postępować przedsiębiorcy?

Wielokrotnie zwracałam uwagę, że przepisy krajowe mają jedynie doprecyzować postanowienia ogólnego rozporządzenia o ochronie danych (RODO), a ponadto muszą być z nim zgodne. Unijne rozporządzenie jest bowiem aktem prawnym, który będzie stosowany bezpośrednio. Od dawna więc przy każdej okazji apeluję, by administratorzy z dostosowaniem się do nowych zasad ochrony danych osobowych nie czekali na polskie ustawy, bo ich podstawowe obowiązki reguluje RODO. To ono też określa podstawowe zasady obowiązujące przy przetwarzaniu danych osobowych.

Warto przy tym podkreślić, że o wyłączeniu stosowania unijnego rozporządzenia w całości w ogóle nie może być mowy. Zgodnie bowiem z art. 23 RODO państwo członkowskie może aktem prawnym ograniczyć zakres pewnych praw i obowiązków, ale ograniczenie to nie może naruszać „podstawowych praw i wolności” oraz musi być „w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym”, służącym ważnym – wskazanym w tym przepisie – celom, takim jak np. bezpieczeństwo narodowe czy publiczne, zapobieganie przestępczości albo ściganie przestępstw. A jeśli już w prawie krajowym wprowadza się ograniczenie, to w odpowiednim przepisie trzeba określić m.in. cele przetwarzania, kategorie danych, zakres wprowadzonych ograniczeń, zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi bądź przekazywaniu, zasady przechowywania itd. Czyli RODO dopuszcza wprowadzanie ograniczeń, jeśli spełnione są warunki wskazane w jego art. 23. Poza tym mamy chronić dane osobowe, a nie wyłączać tę ochronę.

Niektóre wyłączenia mogłyby ułatwić życie przedsiębiorcom...



DR EDYTA BIELAK-JOMAA
generalny inspektor ochrony danych osobowych (GIODO)

Rozumiem, że należy mieć na względzie rozwiązania pro-biznesowe, ale każde wyłączenie stosowania RODO powinno wskazywać wartość, która uzasadnia takie ograniczenie podstawowych praw obywateli, jakimi są prawo do prywatności i ochrony danych osobowych. Zresztą wydaje się, że RODO zapewnia właściwy balans pomiędzy prawami przedsiębiorców a prawami podmiotów danych, a wyłączenia, o których pani wspomniała, tę równowagę naruszały – i to na niekorzyść obywateli. Obecnie w projekcie ustawy wdrażającej zrezygnowano z nich i mam nadzieję, że w takim kształcie, w jakim były do tej pory, nikt nie będzie próbował ich wprowadzić.

A jeśli jakieś rozwiązania ograniczające stosowanie RODO zostaną przyjęte w przepisach krajowych w późniejszym terminie, np. na dalszym etapie trwających właśnie prac nad projektem ustawy wdrażającej? To administratorom gotowym do RODO łatwiej będzie dostosować się do takich zmian, a co najważniejsze – nikt nie zarzuci im, że działają niezgodnie z prawem. Trzeba bowiem pamiętać, że od 25 maja 2018 r. przepisy RODO muszą być stosowane i nie ma już żadnych okresów przejściowych.

Czy GIODO będzie od 25 maja karać za brak realizacji obowiązków wynikających z RODO?

Kary przewidziane w RODO to tylko jeden z instrumentów, który ma do dyspozycji GIODO w celu zapewnienia zgodności z przepisami rozporządzenia. Ponadto podkreślenia wymaga fakt, iż będą one dopiero ostatecznością. Ogólne rozporządzenie zawiera bowiem całą gamę różnych rozwiązań, które służą wzmocnieniu instytucji ochrony danych osobowych obywateli. Przykładowo należą do nich takie uprawnienia, jak: wydawanie ostrzeżeń administratorowi danych, udzielanie upomnień czy też nakazanie określonego zachowania, takiego jak np. spełnienie żądania osoby, której dane dotyczą.

Kary przewidziane w RODO, jak i ich wysokość w odniesieniu do przedsiębiorstw – do 20 mln euro lub do 4 proc. ich rocznego światowego obrotu – nie są przypadkowe. Mają bowiem mobilizować administratorów do jak najlepszej ochrony danych osobowych i przestrzegania przepisów RODO. Niemniej ich wysokość w każdym przypadku będzie uzależniona od indywidualnych okoliczności sprawy.

Na co w praktyce urząd będzie zwracał uwagę?

Istotne będą m.in. charakter, waga i czas trwania naruszenia. To, czy miało ono charakter umyślny, czy też nie, warunki, w jakich do niego doszło, liczba poszkodowanych osób czy rozmiar poniesionej przez nie szkody. Liczyć się też będzie, czy chodzi o pierwsze naruszenie, czy kolejne, jak zachował się administrator danych – czy np. sam zgłosił wyciek danych, czy też GIODO dowiedział się o tym z innych źródeł, np. z prasy. Jak zachował się administrator względem osób, których dane dotyczyły, czy np. poinformował je o wycieku. Jest wiele różnych okoliczności i każda z nich powinna być uwzględniona przy ustalaniu wysokości kary, o czym wprost stanowi art. 83 RODO. Niemniej jednak, jeśli będzie taka potrzeba, GIODO będzie je nakładać.

Jakie rady bądź wskazówki ma GIODO dla przedsiębiorców przetwarzających dane na niecałe dwa tygodnie przed rozpoczęciem stosowania RODO?

Przed wszystkim chciałybyśmy zaapelować, aby nie bali się RODO i nie postrzegali go jako dodatkowego obciążenia czy utrudnienia. Przepisy te nie są niczym strasznym, a ich stosowanie to nie czarna magia – szczególnie dla tych administratorów, którzy do tej pory należycie podchodzili do ochrony danych osobowych. W Polsce regulacje w tym zakresie obowiązują od 20 lat,

a RODO nie zmienia ich w sposób istotny. Nowe jest przede wszystkim podejście w spełnianiu tych obowiązków, które wyraża się m.in. w tym, iż daje ono administratorom danych dużą samodzielność. Wyznacza im cele, które mają osiągnąć, lecz nie narzuca sposobu, w jaki powinni to robić. Dzięki temu mają możliwość dopasowania swoich procesów przetwarzania danych osobowych czy stosowanych w tym zakresie rozwiązań do swojej specyfiki i kultury organizacyjnej.

Dlatego na RODO warto patrzeć jako na okazję do uporządkowania całej sfery związanej z przetwarzaniem danych osobowych. To także szansa na budowanie przewagi konkurencyjnej, gdyż dbałość o ochronę wykorzystywanych danych ma przełożenie na zaufanie zarówno klientów, jak i partnerów biznesowych.

Zachęcam więc, by przed 25 maja 2018 r. przedsiębiorcy raz jeszcze sprawdzili stan swojej gotowości.

Czyli co konkretnie powinni zrobić?

Warto, by przeanalizowali podjęte dotychczas działania, dokonali przeglądu procesów i procedur związanych z przetwarzaniem danych osobowych, by – jeśli okaże się to niezbędne – mogli jeszcze dokonać ostatnich korekt swoich działań. Pomocna w tym zakresie może być przygotowana przez GIODO publikacja pt. „Czy jesteś gotowy na RODO?”. Zwraca ona uwagę na najważniejsze zagadnienia i obszary, w których następować będą znaczące zmiany. Jest ona dostępna na stronie internetowej urzędu (<http://www.giodo.gov.pl/pl/1520281/10255>). Zachęcam, by poddać się temu sprawdzeniu i ocenić swoją gotowość do stosowania RODO.

Jednocześnie warto pamiętać, że to, iż 25 maja 2018 r. zaczniemy stosować RODO, a nasze działania będą w tym dniu zgodne z jego przepisami, nie oznacza, iż możemy spocząć na laurach. Wdrożenie RODO to nie jest jednorazowe działanie. Zapewnianie zgodności z nowymi przepisami to proces ciągły, to nowy sposób myślenia o ochronie danych, ich bezpieczeństwie w kontekście ciągle zmieniających się możliwości technologicznych i nowych zagrożeń. RODO wymusza działania długofalowe, które są niezbędne m.in. do tego, by z jednej strony we wszystkich firmowych procesach mocno zakorzenić zasady dbania o bezpieczeństwo danych osobowych, a z drugiej strony nieustannie doskonalić wdrożone polityki, procesy i zabezpieczenia techniczne.



Rozmawiała
Joanna Pieńczykowska