FOT.: THINKSTOCK

RODO – NOWE UNIJNE PRAWO TO RYZYKO CZY SZANSA DLA PRZEDSIĘBIORSTWA

Nie ma chyba przedsiębiorcy, który nie słyszałby, że od 25 maja 2018 r. zacznie obowiązywać nowe europejskie rozporządzenie w sprawie ochrony danych osobowych (RODO/GDPR). Przetwarzanie danych osobowych przejdzie na znacznie wyższy poziom znaczenia i ryzyka. Wbrew pozorom, czasu na przygotowanie się do zmienionej rzeczywistości prawnej jest bardzo mało.

Nowym rozporządzeniem powinni być zainteresowani przedsiębiorcy reprezentujący każdy sektor działalności gospodarczej, ponieważ dane osobowe występują praktycznie w każdym biznesie. Wystarczy zatrudniać chociażby jednego pracownika lub realizować wysyłkę newslettera. Nawet jeżeli firma nie zatrudnia ani jednej osoby, z pewnością posiada bazy dostawców, kontrahentów czy klientów. Często są to przedsiębiorcy prowadzący jednoosobową działalność gospodarczą, których dane (ujawnione w CEIDG) nie podlegają przepisom o ochronie danych osobowych. Jednak te same dane nie zostały wyłączone spod regulacji RODO. Dlatego każda firma przetwarzająca dane swoich kontrahentów czy klientów, którzy są przedsiębiorcami ujawnionymi w CEIDG, powinna przygotować się do stosowania RODO.

Wysokie kary

Rozporządzenie przewiduje m.in. możliwość nakładania sankcji finansowych przez organ nadzoru, Prezesa Urzędu Ochrony Danych Osobowych (PUODO), w wysokości nawet 20 mln euro (lub 4 proc. światowego obrotu), oraz ich zdecydowane egzekwowanie. Wystarczy powiedzieć, że w projekcie budżetu państwa na 2018 r. środki dla organu zajmującego się ochroną danych osobowych zwiększono o 238 proc. – co ma się przełożyć na większą niż dotąd jego aktywność.

Sankcje to jedna z głównych przyczyn zainteresowania się tematem ochrony danych osobowych przez firmy, które dotychczas mniej lub bardziej świadomie nie poświęcały tej dziedzinie większej uwagi.

Więcej praw i obowiązków

RODO przewiduje znaczne rozszerzenie katalogu praw pracowników, klientów, kontrahentów, czyli osób, których dane osobowe są przetwarzane. Jest to na przykład prawo do bycia zapomnianym i prawo do przenoszenia danych.

Wprowadza się także nowe instrumenty kontroli przetwarzania danych osobowych (np. rejestr czynności przetwarzania danych) oraz nakłada na administratora danych, czyli przedsiębiorcę, obowiązek implementowania nowych procedur związanych z przetwarzaniem danych osobowych (m.in. procedurę zgłoszenia naruszenia ochrony danych osobowych, współpracy z organem nadzorczym, procedury realizacji prawa do bycia zapomnianym czy prawa do przenoszenia danych).

Łącznie nowych procedur i dokumentów można naliczyć kilkanaście.

Projekt związany z RODO nie jest tylko zadaniem wewnętrznym w organizacji. Duże zmiany czekają cały sektor outsourcingu przetwarzania danych osobowych, powszechnie stosowanego np. w księgowości, procesach HR czy systemach IT. Po stronie przedsiębiorcy powoduje to konieczność zlokalizowania procesów, w których dochodzi do przekazywania danych osobowych na zewnątrz, i przygotowania odpowiedniej dokumentacji, co wiązać się będzie z aneksowaniem umów i przygotowaniem dodatkowej dokumentacji wewnętrznej.

Mimo tego że RODO reguluje znaczącą większość kwestii dotyczących przetwarzania danych osobowych, w Polsce prowadzone są prace nad nową ustawą o ochronie danych osobowych, która ma na celu doprecyzowanie niektórych postanowień nowego unijnego prawa. We wrześniu 2017 r. Ministerstwo Cyfryzacji, które pełni funkcję gospodarza implementacji RODO w Polsce, opublikowało projekt nowej ustawy o ochronie danych osobowych oraz projekt ustawy wprowadzającej zmiany w ponad 110 innych aktach prawnych (m.in. kodeks pracy, prawo bankowego).

Projekt ma szczególne znaczenie dla przedsiębiorców w zakresie regulacji obowiązku zgłaszania naruszeń bezpieczeństwa przetwarzania danych osobowych oraz odpowiedzialności cywilnej administratora danych w razie naruszenia praw podmiotu danych.

Projektowane regulacje wstępnie doprecyzowują obowiązki i procedurę postępowania w razie naruszenia przepisów ochrony danych osobowych, m.in. poprzez wprowadzenie przepisów w zakresie postępowania dowodowego czy określenia procedury postępowania przed PUODO w zakresie naruszenia. W odniesieniu do odpowiedzialności cywilnej projekt określa wzajemne obowiązki sądu okręgowego oraz PUODO w przypadku rozpoczęcia sporu cywilnego przez podmiot danych, w związku z naruszeniem przez administratora danych przysługujących mu praw.

Projekt zawiera ponadto regulacje dotyczące inspektora ochrony danych (IOD), a w szczególności zawiadamiania PUODO o powołaniu IOD i postępowaniu w odniesieniu do osób, które przed 25 maja 2018 r. pełniły już funkcję administratora bezpieczeństwa informacji. Z uwagi na przewidziany w RODO obowiązek powołania IOD przez „podmioty, których działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą", można uznać, że duża liczba przedsiębiorców może być zobowiązana do powołania IOD.

Interesującym dla przedsiębiorców instrumentem uławiającym wdrożenie nowych zasad międzynarodowych i krajowych są kodeksy postępowania. Jest to druga obok certyfikatów instytucja wprowadzona w tym celu do RODO. Kodeks postępowania umożliwia administratorowi danych spełnienie jednej z najważniejszych zasad: rozliczności. Stosowanie zatwierdzonego kodeksu postępowania jest, zgodnie z art. 83 RODO, brane pod uwagę przy wymierzaniu administracyjnej kary pieniężnej.

Techniczne wyzwania

RODO to jednak nie tylko prawo i procedury. To także technologia. Systemy informatyczne są istotnym elementem wspierającym działalność wielu przedsiębiorstw. Niezależnie od tego, czy stosowany system to ERP, CRM czy inny, wykorzystywane są one do przetwarzania danych, w tym danych osobowych. Systemy IT są również elementem szerszej infrastruktury IT, która w projektach RODO inwentaryzowana jest równolegle z obszarem prawnym i proceduralnym danego przedsiębiorstwa.

Najbardziej istotne wydaje się to, aby administrator danych osobowych miał możliwość realizowania uprawnień osób, których dane dotyczą – m.in. prawa do przenoszenia danych i prawa sprzeciwu. Dla wielu przedsiębiorców jest to największe ryzyko związane z RODO.

Równie ważne jak dostosowanie systemów IT jest uwzględnienie wymogów RODO we wdrożeniach, które aktualnie się toczą, a które będą funkcjonowały po 25 maja 2018 r. Z pewnością dla tych wdrożeń warto już teraz zastanowić się i zrealizować postulaty privacy by design oraz privacy by default. Ponadto elementem wymagającym rozważenia jest również ocena skutków (DPIA). O tych elementach w aktualnie prowadzonych projektach niestety często się zapomina.

Skoro mowa o systemach IT i oprogramowaniu, za pomocą którego przetwarzane są dane osobowe, to projekty związane z RODO często ujawniają prawdziwe luki w systemie zarządzania przedsiębiorstwem. Polegają one na braku precyzyjnych regulacji dotyczących np. instalowania nowego oprogramowania czy korzystania z własnego sprzętu do celów służbowych.

Biorąc pod uwagę, że liczba systemów IT (głównych i pomocniczych) w dużym przedsiębiorstwie może przekroczyć nawet 10 tys., a średnio jest ich kilkaset – zakres działań związanych z RODO wydaje się niezwykle szeroki. Istotna jest współpraca na linii doradca–ABI/IOD–IT, pozwalająca na priorytetyzację prac wdrożeniowych i skupienie się w pierwszej kolejności na krytycznych punktach widzenia ciągłości prowadzenia biznesu czy procesach.

Każdy administrator danych, każdy przedsiębiorca i każda instytucja powinni kompleksowo przygotować się na zmiany w zakresie ochrony danych osobowych wynikających z RODO. Proces wdrożenia, w zależności od rozmiaru organizacji, zajmuje od trzech do nawet 12 miesięcy i w zasadzie nigdy się nie kończy – nie chodzi bowiem o osiągnięcie zgodności z przepisami na dzień 25 maja 2018 r., lecz aby w późniejszym życiu gospodarczym danego przedsiębiorstwa podstawowe zasady wynikające z RODO i przepisów krajowych były efektywnie przestrzegane.

Michał Kluska

Michał Kluska

DZP więcej niż prawo

Agnieszka Kaczmarek

Agnieszka Kaczmarek

DZP więcej niż prawo