RODO i spółka

Wielu administratorów danych założyło, że RODO jest jedynym nowym dokumentem regulującym przetwarzanie danych osobowych. Często przeoczają oni fakt, że rozporządzenie jest tylko ułamkiem przepisów dotyczących przetwarzania danych osobowych, które ulegną zmianie. – Michał Kluska, Agnieszka Kaczmarek

Michał Kluska,
associate w Domański, Zakrzewski, Palinka.

Agnieszka Kaczmarek,
associate w Domański, Zakrzewski, Palinka.

Od 25 maja 2018 r. zacznie być stosowane nowe europejskie rozporządzenie w sprawie ochrony danych osobowych (RODO). Nie ma chyba przedsiębiorcy, który nie słyszałby o nadchodzących zmianach.

Przetwarzanie danych osobowych (wszelkie operacje od gromadzenia danych osobowych aż po ich usunięcie) przejdzie na znacznie wyższy poziom istotności i ryzyka. Zmianami w tym zakresie zainteresowani powinni być przedsiębiorcy reprezentujący każdy sektor działalności gospodarczej, a w szczególności podmioty działające na rynku ubezpieczeniowym.

RODO jest elementem prawa administracyjnego, a najczęściej podnoszoną kwestią są wysokie kary finansowe, mimo wszystko zachęcamy do podejścia do tej regulacji jako szansy na uporządkowanie kwestii przetwarzania danych osobowych (w efekcie podniesienie efektywności i bezpieczeństwa).

Rozporządzenie przewiduje m.in. możliwość nakładania sankcji finansowych przez organ nadzoru (Prezesa Urzędu Ochrony Danych Osobowych, dalej: PUODO), na kwotę maksymalnie do 20 mln euro (lub 4% światowego obrotu) oraz ich zdecydowane egzekwowanie. W przypadku publicznych zakładów ubezpieczeń kary zostaną najprawdopodobniej obniżone do maksymalnej wysokości 100 tys. zł. Sankcje zdecydowanie stały się jednym z głównych impulsów do zainteresowania się tematem ochrony danych osobowych przez podmioty, które dotychczas traktowały tę dziedzinę z mniejszą uwagą (świadomie lub nie).

RODO przewiduje również znaczne rozszerzenie katalogu praw podmiotów danych (m.in. o prawo do bycia zapomnianym czy prawo do przenoszenia danych), wprowadzenie nowych instrumentów do kontroli przetwarzania danych osobowych (np. rejestru czynności przetwarzania danych) oraz nałożenie na administratora danych obowiązku implementowania nowych procedur związanych z przetwarzaniem danych osobowych (m.in. procedury zgłoszenia naruszenia ochrony danych osobowych, współpracy z organem nadzorczym czy procedury realizacji prawa do bycia zapomnianym czy prawa do przenoszenia danych).

OUTSOURCING A RODO

Duże zmiany czekają również instytucję powierzenia przetwarzania danych osobowych (outsourcingu), która jest powszechnie stosowana przez ubezpieczycieli w ramach swojej działalności (np. w ramach outsourcingu danych w zakresie niezbędnym do czynności wykonywanych przez pośredników ubezpieczeniowych).

RODO jednoznacznie stwierdza, że przetwarzanie danych osobowych może odbyć się na podstawie umowy lub innego instrumentu prawnego. Wprowadza tym samym bardziej sformalizowane zasady co do podstawy powierzenia przetwarzania danych niż te z ustaw o ochronie danych osobowych z 1997 r.

Rozporządzenie poszerza również znacznie zakres obowiązkowych elementów umowy o powierzenie przetwarzania danych m.in. o:

- określenie kategorii i rodzaju danych osobowych, które podlegają przetwarzaniu,
- określenie czasu trwania powierzenia przetwarzania,
- uregulowanie obowiązków procesora w związku z realizowaniem przez administratora danych praw podmiotów danych,
- zobowiązanie administratora danych do zapewnienia zachowania poufności przez pracowników przetwarzających dane,
- prawo audytu i kontroli procesora przez administratora danych lub wskazanego przez niego audytora,
- wzajemne uregulowanie odpowiedzialności administratora danych i procesora za przetwarzanie danych.

RODO reguluje również proces korzystania przez procesora z podwykonawców. W sytuacji, w której procesor korzysta z usług podwykonawcy, administrator danych ma dwie opcje działania.

Pierwsza z nich to wyrażenie ogólnej, pisemnej zgody na korzystanie przez procesora z usług podwykonawców. Po uzyskaniu takiej zgody procesor jest jedynie zobowiązany do poinformowania administratora danych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia podwykonawcy, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. W razie wyrażenia sprzeciwu przez administratora danych, procesor nie może korzystać z usług podwykonawcy.

Druga możliwość przewiduje każdorazowe wyrażanie przez administratora danych szczególnej, pisemnej zgody na korzystanie przez procesora z usług określonego podwykonawcy. W przypadku ubezpieczycieli korzystających z dużej liczby podwykonawców, drugie rozwiązanie mogłoby się wiązać z utrudnieniem w prowadzeniu działalności gospodarczej poprzez konieczność uzyskania od ogromnej liczby podmiotów zgód na korzystanie z usług nowych podwykonawców, a ich brak mógłby prowadzić do utrudnień w świadczeniu usług przez ubezpieczycieli.

Powyższe przykłady uwidaczniają, że RODO wprowadza zarówno wiele zmian w funkcjonujących już instytucjach przetwarzania danych osobowych, jak i wiele nowych instytucji i procedur nieznanych dotychczasowym przepisom. Idąc tym tropem, wielu administratorów danych założyło, że RODO jest jedynym nowym

dokumentem regulującym przetwarzanie danych osobowych. Często przeoczają oni fakt, że rozporządzenie jest tylko ułamkiem przepisów dotyczących przetwarzania danych osobowych, które ulegną zmianie z dniem 25 maja 2018 r.

NOWA USTAWA O OCHRONIE DANYCH OSOBOWYCH

Pomimo tego, że RODO reguluje znaczną większość kwestii dotyczących przetwarzania danych osobowych, w Polsce prowadzone są prace nad nową ustawą o ochronie danych osobowych, która ma na celu doprecyzowanie niektórych zapisów RODO. W marcu 2017 r. Ministerstwo Cyfryzacji, które pełni rolę „gospodarza" implementacji RODO w Polsce, opublikowało pierwszy projekt nowej ustawy o ochronie danych osobowych. Projektowana ustawa zastąpi dotychczas obowiązująca ustawę o ochronie danych osobowych.

Przedstawiony wstępny projekt odnosi się na razie tylko do niektórych regulacji RODO. Na dzień przygotowania tego artykułu projekt zawiera propozycje przepisów dotyczących m.in.:

- akredytacji i certyfikacji;
- postępowania w sprawie naruszenia przepisów o ochronie danych;
- europejskiej współpracy administracyjnej;
- postępowania kontrolnego;
- administracyjnych kar pieniężnych i odpowiedzialności cywilnej;
- inspektorów ochrony danych;
- granicy wieku dziecka, od której nie będzie wymagana zgoda rodzica bądź opiekuna prawnego.

Jak widać po zakresie przedmiotowym projektowanej ustawy, jej treść będzie miała szczególne znaczenie i wpływ na przetwarzanie danych osobowych przez ubezpieczycieli.

ZAKRES PRZEDMIOTOWY

Projekt ma szczególne znaczenie dla ubezpieczycieli w zakresie regulacji obowiązku zgłaszania naruszeń bezpieczeństwa przetwarzania danych osobowych oraz odpowiedzialności cywilnej administratora danych w przypadku naruszenia praw podmiotu danych. Projektowane regulacje wstępnie doprecyzowują obowiązki i procedurę postępowania w razie naruszenia przepisów ochrony danych osobowych m.in. poprzez wprowadzenie przepisów dotyczących 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 (dalej: IOD), a w szczególności zawiadamiania PUODO o powołaniu IOD czy postępowaniu w odniesieniu do osób, które przed dniem 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, na dużą skalę* (art. 37 ust. 1 pkt b RODO), można uznać, że ubezpieczyciele będą w zdecydowanej większości przypadków zobowiązani do powołania IOD. Powyższe zostanie oczywiście zweryfikowane przez praktykę organu nadzorczego, jednak zgodnie z wytycznymi Grupy Roboczej art. 29 wyznaczenie IOD powinno nastąpić nawet w podmiotach do tego niezobowiązanych.

Projekt nie zawiera w sobie jeszcze wszystkich rozwiązań, które będą regulowane nową ustawą. W ostatecznym projekcie powinny zostać zaimplementowane i uregulowane w szczególności jeszcze takie kwestie jak rejestry przetwarzania danych, pozostałe kwestie związane ze zgłaszaniem incydentów naruszenia ochrony danych osobowych czy ewentualna odpowiedzialność karna za niezgodne z przepisami przetwarzanie danych osobowych.

NOWE PRZEPISY SEKTOROWE

Projekt to nie jedyny nowy instrument prawny mający na celu zapewnienie prawidłowego wdrożenia RODO do polskiego porządku prawnego. Wraz z dniem rozpoczęcia stosowania RODO, zmianie powinna ulec ogromna liczba ustaw i innych aktów prawnych, regulujących przetwarzanie danych osobowych w sektorach takich jak np. bankowość czy właśnie ubezpieczenia.

Dostosowanie przepisów sektorowych jest kolejnym wyzwaniem stojącym przed przedsiębiorcami, Ministerstwem Cyfryzacji i innym resortami. Już teraz organizacje branżowe intensywnie uczestniczą w pracach legislacyjnych prowadzonych przez Ministerstwo Cyfryzacji, w ramach których przygotowywane są zmiany do przepisów sektorowych w zakresie przetwarzania danych osobowych czy ogólnobranżowe kodeksy postępowań.

Zmiany wypracowywane przez Ministerstwo Cyfryzacji oraz przedstawicieli organizacji branżowych zostaną przyjęte do porządku prawnego w formie ustawy, zawierającej w sobie zmiany dostosowujące sektorowe przetwarzanie danych osobowych do wymogów RODO.

„MIĘKKIE" AKTY PRAWA

W zakresie wydawania tzw. miękkich aktów prawa projekt przewiduje kompetencje PUODO do wydawania niewiążących dobrych praktyk w zakresie możliwych do zastosowania zabezpieczeń przetwarzania danych, w tym w odniesieniu do przetwarzania danych przez ubezpieczycieli. Ich wydawanie ma wpłynąć na zwiększenie poczucia pewności prawnej i tym samym zwiększyć stopień przestrzegania przez administratorów przepisów RODO. Należy podkreślić, że wspomniane dobre praktyki nie będą miały charakteru regulacyjnego, a jedynie informacyjny i w żaden sposób nie będą wiążące dla PUODO.

Kolejnym z instrumentów pomocnych w byciu zgodnym z przepisami RODO (i rozwiązaniami krajowymi) są kodeksy postępowania. Jest to jedna z dwóch instytucji wprowadzonych do RODO w tym celu (drugą są certyfikaty). Kodeks postępowania umożliwia administratorowi danych spełnienie jednej z najważniejszych zasad przewidzianych w RODO, czyli rozliczności. Ponadto fakt stosowania zatwierdzonego kodeksu postępowania jest, zgodnie z art. 83 RODO, brany pod uwagę przy wymierzaniu administracyjnej kary pieniężnej.

W PRZEDDZIEŃ RODO

Każdy administrator danych, niezależnie od sektora działalności, powinien kompleksowo przygotować się na zmiany w zakresie ochrony danych osobowych wynikające z RODO. Należy podkreślić, że proces wdrożenia RODO, w zależności od rozmiaru organizacji, zajmuje od 3 do nawet 12 miesięcy, więc czasu na działania pozostało niewiele. W niektórych organizacjach już teraz wiadomo, że przed majem 2018 r. ten projekt się nie zakończy. W zasadzie projekty RODO jako takie nigdy się nie kończą, bo nie chodzi w nich 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. ❑