Fakty i mity na temat wdrożenia RODO w samorządach

Od 25 maja 2018 r. zacznie być stosowane nowe europejskie rozporządzenie w sprawie ochrony danych osobowych (RODO). Tak duża zmiana w przepisach skutkuje zalewem informacji dotyczących RODO, nie wszystkie jednak informacje są zgodne z prawdą.

Realizując projekty związane z wdrożeniem RODO dla różnego rodzaju przedsiębiorstw i instytucji (w tym administracji publicznej i samorządów), bardzo często słyszymy wiele twierdzeń związanych z RODO – czasem prawdziwych, ale często również mało precyzyjnych czy wręcz nieprawdziwych. W niniejszym tekście dokonaliśmy wyboru tych, które naszym zdaniem mają największe znaczenie praktyczne.

RODO mnie nie dotyczy, bo ja „nie mam" danych osobowych – MIT (prawdopodobnie)

Prawdopodobnie ponieważ to zależy od sytuacji konkretnego podmiotu. Wbrew pozorom takie stwierdzenie pada bardzo często na wczesnym etapie rozmów o RODO. Nasze doświadczenia pokazują, że takie stwierdzenie można usłyszeć nawet od działów HR dużych przedsiębiorstw.

Dane osobowe

Pojęcie danych osobowych w RODO jest bardzo zbliżone do tego jakie aktualnie obowiązuje w naszym porządku prawnym. Pojawiły się nowe elementy, które warto odnotować m.in.: numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy.

Definicja danych osobowych opiera się o trzy elementy:

- dane osobowe to informacja,
- dotycząca osoby fizycznej,
- zidentyfikowanej lub możliwej do zidentyfikowania.

Trudno zatem mówić o braku danych osobowych w przypadku podmiotu, który zatrudnia chociażby jednego pracownika. Co więcej, nawet jeżeli takiego zatrudnienia nie ma to przecież mogą być kontrahenci i klienci. Biorąc pod uwagę fakt, że dane przedsiębiorców ujawnionych w CEIDG nie zostały wyłączone spod regulacji RODO (i nic nie wskazuje, aby nawet na poziomie ustawodawstwa krajowego było to możliwe) – duża liczba przedsiębiorców może być zaskoczona faktem konieczności przygotowania się pod RODO właśnie z tej perspektywy.

Trzeba odnotować, że mimo zmieniających się w ostatnich latach regulacji prawnych odnośnie statusu danych osobowych tzw. jednoosobowych przedsiębiorców, znamy przykłady przedsiębiorców, którzy przez cały okres swojej działalności stosowali do tych danych reżim ustawy o ochronie danych osobowych (nie tylko w zawężonym zakresie wynikającym z ustawy o swobodzie działalności gospodarczej).

Prawo w zakresie ochrony danych osobowych jest jednakowe w całej Europie – MIT

Na poziomie zasad – tak. Na poziomie szczegółów, już nie zawsze. Samo RODO przewiduje kilkanaście artykułów, które dopuszczają odrębne uregulowania na poziomie państw członkowskich. Jednym z przykładów może być granica wieku dziecka. Już teraz wiadomo bowiem, że w Polsce planowane jest, aby był to próg 13 roku życia, dla porównania w Niemczech jest to próg, jak w RODO, czyli lat 16.

Inną, istotną różnicą może być kwestia limitowania administracyjnych kar pieniężnych nakładanych na administrację publiczną – w Niemczech jest całkowite wyłączenie tej grupy, w Polsce Ministerstwo Cyfryzacji w projekcie z marca 2017 r. zaproponowało limitację na poziomie 100.000 zł.

Jest jeszcze dużo czasu na rozpoczęcie procesu przygotowania – MIT

Okres wrzesień 2017 – maj 2018 to raptem 9 miesięcy. Nawet z perspektywy podmiotu, który zatrudnia kilkanaście osób, ma zawartych kilka umów powierzenia danych do przetwarzania, korzysta

z kilkunastu systemów informatycznych – okres ten może nie być wystarczający. Najbardziej czasochłonna część projektu tj. mapowanie danych osobowych, może okazać się (i tak zwykle jest) bardzo dużym wyzwaniem organizacyjnym, a przecież w większości przedsiębiorstw projekt pt. RODO nie będzie jedynym projektem w toku.

Ważne, aby być gotowym na 25 maja 2018 r. – MIT

W sumie to ważne, ale już tłumaczymy, dlaczego mit. Projekty RODO nie mają swojego magicznego końca. Projekty te zaczynają i kończą się na ludziach. Dostarczenie przez doradców najlepszych procedur, wzorów i klauzul nie wystarczy, jeżeli u podstaw organizacji nie legną zasady ochrony danych osobowych. Każdy organizm – czy to organizacja samorządowa, czy też przedsiębiorca organizacja samorządowa – żyje swoim życiem. Istotne jest takie przeprowadzenie procesu RODO, aby organizacja była w stanie realizować zasady RODO w kolejnych miesiącach aktywności.

Ryzyko, że dostanę karę pieniężną jest minimalne – FAKT / MIT

Można powiedzieć, że czas pokaże. Nikt tego nie wie. Im lepiej przygotowany jest podmiot, tym to ryzyko jest mniejsze – to jasne. Nie jest natomiast dobrą motywacją podchodzenie do RODO, jako wyłącznie obowiązku. RODO jest również szansą na budowanie przewagi konkurencyjnej, na uporządkowanie tego obszaru, na odzyskanie zasobów i czasu.

W projektach RODO jako element ryzyka trzeba koniecznie wziąć jeszcze inne elementy – m.in.: ryzyko postanowienia Prezesa Urzędu Ochrony Danych Osobowych dot. ograniczenia przetwarzania danych osobowych, ryzyko odpowiedzialności cywilnej (również w kontekście uprawnień organizacji pozarządowych), ryzyko zaktualizowanych przepisów przewidujących odpowiedzialność karną. Mówiąc brutalnie – zrobienie rezerwy na administracyjną karę pieniężną (nawet jeżeli dla administracji będzie to max 100.000 PLN) może nie być wystarczające.

RODO to wyłącznie kwestia IT – MIT

Nie wyłącznie. Obszar IT jest istotny. Musi być wzięty pod uwagę. Bardzo często kwestie technologiczne determinują w ogóle przebieg projektu. Podczas mapowania przedsiębiorca może uzyskać świadomość, że może transfer danych do USA w oparciu o (niepewny) *Privacy Shield* (dokument – porozumienie określający zasady wymiany danych osobowych pomiędzy państwami Unii Europejskiej a USA) to jednak coś nad czym warto się zastanowić. Dla rozwiązań przewidzianych RODO powstaje wiele rozwiązań IT – takich, które w większości przypadków mają pomóc np. w realizacji prawa do bycia zapomnianym czy *data portability (p*rawo do przenoszenia danych osobowych określone w art. 20 RODO).

Jestem podmiotem przetwarzającym dane osobowe na zlecenie, mnie ten projekt nie dotyczy – MIT

Dotyczy i to bardzo. Poza byciem procesorem jest wielce prawdopodobne, że taki podmiot jest również administratorem danych osobowych (np. jednostka administracji świadcząca usługi IT dla innych jednostek administracji publicznej, z jednej strony jest administratorem bo chociażby ma pracowników, z drugiej będzie procesorem bo przetwarza dane osobowe — swoich klientów – jednostek administracji publicznej). RODO nakłada na podmioty przetwarzające dane osobowe liczne obowiązki m.in. w zakresie notyfikacji naruszenia bezpieczeństwa danych osobowych czy wyznaczenie przedstawiciela.

Z wdrożeniem RODO trzeba czekać na przepisy krajowe – MIT

Nie trzeba. Nie powinno się. Biorąc pod uwagę czasochłonność procesów inwentaryzacji procesów przetwarzania danych osobowych, nie warto czekać. W skrajnym przypadku (na razie nic tego nie zapowiada), jeżeli na 25 maja 2018 r. nie będzie przepisów krajowych dot. ochrony danych osobowych, to RODO i tak się stosuje (może być egzekwowane).

Faktem jestem jednak, że przepisy krajowe i zatwierdzone kodeksy postępowania w poszczególnych branżach (w tym administracji), będą istotnym uzupełnieniem obrazu prawnego funkcjonowania w obszarze RODO i z pewnością w projektach RODO trzeba przewidzieć moment weryfikacji wypracowanych rozwiązań z przepisami krajowymi i sektorowymi. ▶

RODO to spora liczba nowych dokumentów – FAKT

Praktyka pokazuje, że to prawda. Wystarczy spojrzeć na potencjalną listę nowy dokumentów, które musi wytworzyć organizacja:

- procedura współpracy z organem nadzoru,
- przeprowadzenie oceny skutków dla ochrony danych,
- procedura realizacji prawa do sprostowania danych,
- procedura realizacji prawa do usunięcia danych,
- procedura realizacji prawa do ograniczonego przetwarzania,
- procedura realizacji prawa do przenoszenia danych,
- procedura realizacji prawa sprzeciwu,
- formularze do zgłoszenia naruszenia bezpieczeństwa,
- dokumenty dla DPO (Data Protection Officer – Inspektor Ochrony Danych) (umowa współpracy / zakres obowiązków),
- wzór umowy o powierzenie danych do przewarzania,
- wzór postanowień dot. powierzenie do przetwarzania do umieszczenia w innych umowach,
- wzór rejestru czynności przetwarzania danych,
- dokumenty do stosowania procedury *privacy by design,*
- dokumenty do stosowania procedury *privacy by default,*
- procedura weryfikacji podmiotu, któremu dane są powierzane do przetwarzania.

Wnioski

Niespodziewanie, tekst przyniósł więcej przykładów mitów aniżeli faktów. Jest to skutek niezamierzony przez autorów. Zapewne nie są to wszystkie, spośród przykładów, które można usłyszeć i zobaczyć w gazetach lub przestrzeni wirtualnej. Najbliższe miesiące zapewne przyniosą jeszcze więcej interesującego materiału do analizy.

Michał Kluska
associate w Zespole IP/TMT kancelarii
Domański Zakrzewski Palinka

Agnieszka Kaczmarek
associate w Praktyce Prawa Spółek,
Fuzji i Przejęć kancelarii
Domański Zakrzewski Palinka