Fakty i mity o RODO

Michał Kluska
Associate w kancelarii Domański Zakrzewski Palinka.

Stanisław Kastory
Associate w kancelarii 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. Nie wszystkie jednak podawane w mediach informacje są zgodne z prawdą.

Realizując projekty związane z wdrożeniem RODO dla różnego rodzaju przedsiębiorstw i instytucji, 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 przedsiębiorstwa czy instytucji. Wbrew pozorom, takie stwierdzenie pada bardzo często na wczesnym etapie w rozmowach z przedsiębiorcami. Nasze doświadczenia pokazują, że takie stwierdzenie można usłyszeć nawet od działów HR dużych przedsiębiorstw.

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 przedsiębiorcy, 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).

Pseudonimizacja i anonimizacja to to samo – Mit

To nie jest to samo. Najprościej mówiąc pseudonimizacja jest procesem odwracalnym. Anonimizacja tej cechy nie posiada.

Pseudonimizacja w RODO:

> „oznacza przetworzenie danych osobowych, w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej."

Na temat anonimizacji w RODO jest tylko jeden fragment w motywach (26):

> „zasady ochrony danych osobowych nie powinny mieć zastosowania do informacji anonimowych, czyli do informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować."

Więcej na temat można przeczytać w przyjętej w dniu 10 kwietnia 2014 r. przez Grupę Roboczą Art. 29 Opinii 5/2014 w sprawie technik anonimizacji[1].

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 przedsiębiorstwa, które 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 jest jedynym, który się toczy (PSD2, NIS, e-privacy...).

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 przedsiębiorca, czy też organizacja – żyje swoim życiem. Istotne jest takie przeprowadzenie procesu RODO, aby organizacja była w stanie realizować zasady RODO w kolejnych miesiącach aktywności.

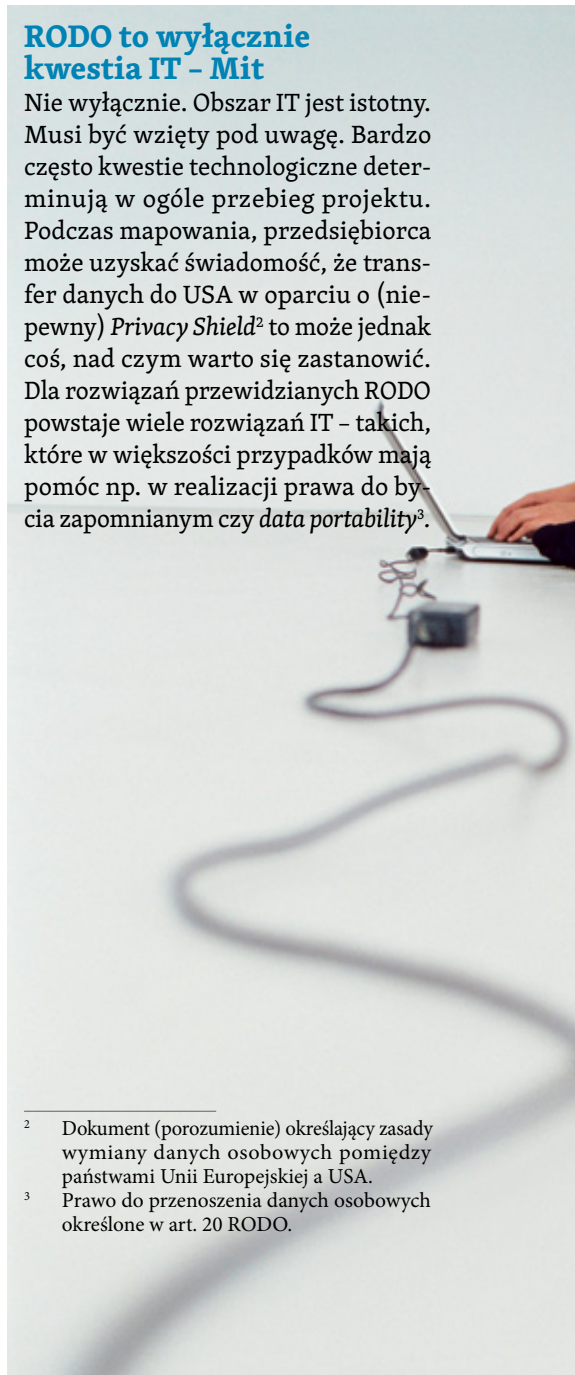
Ryzyko, że dostanę karę pieniężną jest minimalne – Fakt / Mit

Można powiedzieć, że czas pokaże. Nikt tego nie wie. Im lepiej przygotowane przedsiębiorstwo, 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 uprządkowanie 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 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 transfer danych do USA w oparciu o (niepewny) *Privacy Shield*[2] to może 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*[3].



[1] Nieoficjalne tłumaczenie: http://www.giodo.gov.pl/pl/1520203/7808, Plik źródłowy: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[2] Dokument (porozumienie) określający zasady wymiany danych osobowych pomiędzy państwami Unii Europejskiej a USA.

[3] Prawo 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. przedsiębiorca, który świadczy usługi platformy do email marketingu z jednej strony, jest administratorem bo chociażby ma pracowników, z drugiej będzie procesorem bo przetwarza

dane osobowe – adresy e-mail – swoich klientów). 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, 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 (oraz kodeksem postępowania, jeżeli zapadnie taka decyzja biznesowa).

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*[4],
- dokumenty do stosowania procedury *privacy by default*[5],
- procedura weryfikacji podmiotu, któremu dane są powierzane do przetwarzania.

Po 25 maja 2018 r. muszę mieć Inspektora Ochrony Danych Osobowych (IOD) – Mit

Taki obowiązek na poziomie RODO ma jedynie administracja publiczna. W kontekście biznesu, każdorazowo trzeba się będzie zastanowić nad przesłankami powołania IOD. Jeżeli już z takiego ćwiczenia wyjdzie nam obowiązek powołania IOD, to wciąż aktualne pozostają pytania o umiejscowienie w strukturze organizacyjnej, a także o ewentualny outsourcing tej funkcji. Jak zawsze, wszystko ma swoje plusy i minusy.

Wnioski

Niespodziewanie, tekst przyniósł więcej przykładów mitów aniżeli faktów. Było to niezamierzone przez autorów. Zapewne nie są to wszystkie, jakie można usłyszeć i zobaczyć w przestrzeni wirtualnej. Najbliższe miesiące, przed majem 2018 r., zapewne przyniosą jeszcze więcej interesującego materiału do analizy.

[4] Wymogi uwzględnienia ochrony danych w fazie projektowania zgodnie z art. 25 ust.1 RODO

[5] Wymogi ustanowienia domyślnej ochrony danych osobowych zgodnie z art. 25 ust. 2 RODO