Rozliczalność – czyli o nowej filozofii w ochronie danych osobowych. Okiem prawników i programistów

Maciej Kubiak

Adwokat i wspólnik w Leśnodorski, Ślusarek i Wspólnicy

Maciej Dudek

Radca prawny w Leśnodorski Ślusarek i Wspólnicy

Paweł Huryn

Partner Zarządzający w HURO

---

25 maja 2018 roku zacznie obowiązywać rewolucyjna zmiana w zakresie ochrony prywatności i danych osobowych (ogólne rozporządzenie o ochronie danych), zwane również „RODO". RODO wymusza zmianę filozofii działania, stosowanych procedur, dokumentacji i systemów IT niemal w każdym przedsiębiorstwie i w każdej branży,

wprowadzając jednocześnie sankcje do 20 mln euro lub 4% światowego obrotu za poprzedni rok za nieprzestrzeganie nowych przepisów.

Dlaczego na pierwszym miejscu postawiliśmy „zmianę filozofii działania”? Dlatego, że RODO to nie garść wymogów do spełnienia, to zmiana podejścia do ochrony i relacji z ludźmi, których dane są przetwarzane. To też zmiana filozofii ochrony. Od maja 2018 r. nie wystarczy papierowa i teoretyczna polityka prywatności przechowywana w zakurzonym segregatorze. Nowe zasady ochrony danych muszą funkcjonować w codziennej działalności każdego przedsiębiorstwa i, co istotne, od firmy przetwarzającej dane (czyli praktycznie od każdego podmiotu na rynku) wymagana będzie **rozliczalność**.

Rozliczalność w rozumieniu RODO (art. 5) to ciążący na przedsiębiorcy obowiązek wykazania, że dane osobowe są przetwarzane w sposób, jaki wymaga tego RODO, a zatem:

a) zgodnie z prawem, rzetelnie i przejrzyście dla osoby, której dane dotyczą;
b) z ograniczeniem celu;
c) zgodnie z zasadą minimalizacji danych;
d) dane są prawidłowe, a w razie potrzeby uaktualniane;
e) z ograniczeniem przechowywania w czasie do niezbędnego minimum;
f) w sposób zapewniający bezpieczeństwo, w tym integralność i poufność.

Upraszczając i przekładając to na język biznesu, musimy być zatem w stanie wykazać, skąd mamy dane i na jakiej podstawie oraz w jakim celu je przetwarzamy, że wykonaliśmy obowiązek informacyjny oraz dbamy o to, aby były one prawidłowe, wiemy, jak długo możemy przetwarzać dane oraz że po tym okresie je usuwamy, kto ma do nich dostęp i dlaczego są one bezpieczne.

Jeśli zjawi się ktoś, kto powie, że nie wyrażał nigdy zgody na przetwarzanie przez przedsiębiorcę danych i nie miał od niego żadnej informacji, to na przedsiębiorcy będzie ciążył obowiązek wykazania, że te konkretne dane uzyskał np. na podstawie zgody udzielonej w konkretnym dniu i w konkretny sposób, że odbyło się to świadomie oraz, że zostały spełnione obowiązki informacyjne.

Formularz kontaktowy zgodny z RODO

Weźmy przykład formularza kontaktowego umieszczonego na stronie WWW. Poza przesłanymi przez użytkownika danymi (Jan Kowalski, +48 999 999 999, treść zapytania) datą, godziną oraz sposobem ich zebrania (formularz na stronie http://www...) konieczne może być wykazanie, jakie dokładnie treści zgód zaznaczał użytkownik („Wyrażam zgodę…”) oraz jak brzmiały teksty powiązane z obowiązkiem informacyjnym („Administratorem danych jest…”), nawet jeśli podlegały późniejszym zmianom.

Rozwiązania, które to umożliwiają (wersjonowanie rekordów w bazie danych, logowanie każdej wykonywanej operacji w ustrukturyzowany sposób umożliwiający raportowanie) nie są

niczym nowym. Ich zastosowanie we wszystkich systemach IT w tak krótkim czasie stanowi jednak duże wyzwanie. Nie tylko dla twórców oprogramowania (cykl wytworzenia, stabilizacji i dystrybucji nowej wersji rozwiązań może trwać wiele miesięcy), ale i dla przedsiębiorców (wdrożenie, przeszkolenie użytkowników, nowe procedury i sposób działania).

Dodatkowo same treści zgód i komunikatów także muszą ulec ewolucji. Powinny być napisane językiem prostym i zrozumiałym dla każdego, a jednocześnie przekazywać znacznie więcej informacji (imię i nazwisko inspektora ochrony danych, jakie kategorie danych przechowujemy, czy i komu przekazujemy dane, gdzie możemy uzyskać do nich dostęp, jak długo zamierzamy je przetwarzać). Niektórzy przedsiębiorcy rozważają nawet uzupełnienie komunikacji o tzw. „piktogramy", czyli komunikaty graficzne uzupełniające teksty.

Praca na zbiorach danych zgodna z RODO

Kolejny obowiązek ciążący na przedsiębiorcy to systematyczna ocena skutków dla ochrony danych (ang. DPI, *Data Protection Impact Assessment*), wymagana w przypadku wysokiego ryzyka. Oczywiście nie wystarczą szacowanie ryzyka i ocena wykonywana „w głowie". Każda operacja musi pozostawiać trwały ślad, tak aby móc udowodnić, kiedy i jak przebiegała ocena oraz jakie decyzje w związku z jej wynikiem podjęliśmy.

DPI to tylko jeden z przykładów pokazujących, że rozliczalność dotyczy nie tylko poszczególnych rekordów (Jan Kowalski). Równie ważna jest rozliczalność wszystkich działań podejmowanych w związku z tworzeniem i pracą na zbiorach danych osobowych (tzw. rejestrach czynności przetwarzania). Przykładowe pytania, na jakie powinniśmy być w stanie odpowiedzieć w przypadku kontroli, to:

a) Informacje „meta", na przykład: kto jest administratorem, jakie kategorie danych przetwarzamy, gdzie przechowujemy dane, jakie środki zabezpieczenia stosujemy, jak gromadzimy zgody, po jakim czasie dane będą usuwane?
b) Jak przebiegał proces akceptacji utworzenia rejestru? Kto i kiedy akceptował wniosek?
c) Komu powierzamy dane? Jakie umowy zawarliśmy? Czy umowy pozwalają na dalsze „podpowierzanie"?
d) Kogo, dlaczego i w jakim zakresie upoważniliśmy do przetwarzania danych? W jaki sposób szkolimy osoby mające dostęp do rejestru?
e) Jakie zapytania w związku z rejestrem otrzymaliśmy? Kiedy udzieliliśmy odpowiedzi?
f) W jaki sposób dbamy o usunięcie danych ze zbioru, gdy nie są już potrzebne (cykliczne przeglądy, system powiadomień, przypomnień i alertów, reguły wbudowane w konkretne systemy).

Pracy jest bardzo dużo. Toczące się obecnie w związku z RODO projekty można podzielić na kilka kategorii:

a) *Identify* – odpowiedź na pytanie, jakie dane i gdzie przetwarzamy?
b) *Describe* – utrzymanie aktualnych informacji o rejestrach (informacje „meta").

c) *Legal* – transformacja biznesu. Szkolenia, dostosowanie treści zgód i informacji, weryfikacja szablonów umów.
d) *Workflow* – automatyzacja procesów związanych z rejestrowaniem i tworzeniem zbiorów, nadawaniem upoważnień, zawieraniem umów, obsługą zapytań.
e) *Security* – wprowadzanie zabezpieczeń na poziomie infrastruktury lub aplikacji. Aby zapewnić zgodność infrastruktury z najwyższymi standardami, wielu przedsiębiorców decyduje się na wykorzystanie chmury.

RODO to nie bat na przedsiębiorców

Czy można w pełni przygotować się do RODO? Wiele zapisów pozostawia duże pole do interpretacji. RODO nie wskazuje, w jaki dokładnie sposób spełnić wymagania, mówi więcej o zasadach i zmianie filozofii działania przedsiębiorców. Powstają kolejne projekty branżowych kodeksów postępowania, mające ułatwić wdrażanie i dostosowanie się do nowych regulacji. Niejasność przepisów stanowi dla przedsiębiorców nie tylko wyzwanie, ale także szansę. W okresie przejściowym szczególnie istotne w kontekście sankcji może być wykazanie, że staraliśmy się jak najlepiej przygotować do zmian, nawet gdyby po drodze zdarzyły się potknięcia. RODO to nie bat na przedsiębiorców. Ma służyć nam wszystkim, bo każdy z nas może być w sytuacji nie tylko przedsiębiorcy, ale i klienta.