Rzeczpospolita z 7.04.2018

Co zmienia RODO w ochronie danych osobowych

Jarosław Kamiński, adwokat Warszawa, Rödl & Partner
Marta Wiśniewska, radca prawny Warszawa, Rödl & Partner

Przedsiębiorcy już za półtora miesiąca powinni zmienić dotychczasowe podejście do ochrony i przetwarzania danych osobowych. Wypełnienie minimalnych wymogów określonych w przepisach prawa już nie wystarczy. Każdy podmiot, który przetwarza dane osobowe, będzie musiał po 25 maja wprowadzić wewnętrzne procedury i środki techniczne, zapewniające adekwatny stopień bezpieczeństwa przetwarzanych danych.

Wszystko będzie zależeć od poziomu ryzyka utraty lub ujawnienia danych w konkretnej firmie. Oznacza to, że każdy pracownik działu HR, sprzedaży, marketingu, księgowości, IT oraz każdy, kto ma czynny wpływ na przetwarzanie danych osobowych w swoim miejscu pracy, musi wiedzieć, czym jest RODO i jaki ma wpływ na jego pracę.
RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych) określa, jak firmy powinny podejść do ochrony przetwarzanych danych oraz jak powinny zadbać o ich bezpieczeństwo. Dotyczy to nie tylko administratorów danych, ale także firm, które przetwarzają dane na zlecenie administratora (np. firm outsourcingowych).

KOGO DOTYCZY

RODO ma na celu ujednolicenie prawodawstwa i procedur związanych z ochroną danych osobowych na terenie całej Unii Europejskiej. Jednak nowe przepisy stosuje się nie tylko do przetwarzania danych osobowych w związku z działalnością prowadzoną przez przedsiębiorców na terenie UE, niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. RODO może dotyczyć także firm, które nie mają swoich jednostek organizacyjnych w UE. Wystarczy, że przetwarzają one dane w związku z oferowaniem towarów lub usług osobom fizycznym w UE lub monitorowaniem ich zachowania, o ile ma to miejsce na terenie UE.

PRZYKŁAD

RODO nie stosuje się do przetwarzania danych osobowych dotyczących osób prawnych (np. spółek kapitałowych), w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (nazwa firmy, jej adres, siedziba, dane kontaktowe na stronie internetowej). RODO będzie mieć jednak zastosowanie, jeśli firma przetwarza dane konkretnej osoby (np. szefa sprzedaży, dyrektora finansowego, kierownika produkcji) w formie np. imienia, nazwiska, adresu email, numeru telefonu kontaktowego.

RODO nie tylko zmienia podejście do ochrony i przetwarzania danych osobowych, lecz także istotnie wzmacnia pozycję osób fizycznych.
Zwiększa również obowiązki administratorów oraz podmiotów przetwarzających i przyznaje nowe uprawnienia organom nadzorczym: obecnie GIODO, a w przyszłości UODO – Urząd Ochrony Danych Osobowych.

KLUCZOWA ZMIANA

Na podmioty przetwarzające dane RODO nakłada obowiązek przeprowadzenia samooceny, która polega na oszacowaniu ryzyk związanych z przetwarzaniem danych, w tym w systemach informatycznych (ang. risk-based approach). W praktyce oznacza to konieczność gruntownej weryfikacji przetwarzanych danych, szczegółowej oceny zagrożeń związanych z przetwarzaniem konkretnych danych osobowych oraz zaplanowania odpowiednich środków technicznych i organizacyjnych, m.in. zabezpieczeń i mechanizmów w celu zminimalizowania zagrożeń.

Aby zabezpieczyć przetwarzane dane osobowe, administratorzy danych i podmioty przetwarzające będą musiały zrobić wszystko, co uznają za właściwe na podstawie własnych sposobów przetwarzania danych oraz przeprowadzić swoją analizę ryzyka dla ochrony danych.

Ponadto, będą musiały wykazać, że przyjęte rozwiązania, środki techniczne i organizacyjne są odpowiednie dla danego przypadku przetwarzania danych osobowych.

DOTKLIWE KARY

Za nieprzestrzeganie nowych przepisów przewidziane są administracyjne kary finansowe. Mogą one zostać nałożone przykładowo za niepowołanie inspektora ochrony danych lub też za przetwarzanie danych osobowych bez podstawy prawnej, np. w procesie rekrutacji kandydatów do pracy). Ich wysokość sięga nawet 20 mln euro lub do 4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa).

NOWE OBOWIĄZKI DLA FIRM

RODO wprowadza obowiązek monitorowania i raportowania do organu nadzorczego o naruszeniach ochrony danych osobowych w terminie 72 godzin po stwierdzeniu takiego naruszenia, a w niektórych wypadkach także obowiązek zawiadomienia osób fizycznych, których naruszenie dotyczy.
Incydent ochrony danych osobowych to naruszenie, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.

Kolejny obowiązek to regularne testowanie bezpieczeństwa. Jednak tutaj administrator danych będzie mógł sam zdecydować, jak często i jakimi metodami powinien sprawdzać skuteczność wprowadzonych zabezpieczeń oraz w jaki sposób monitorować incydenty.

RODO obliguje administratorów danych do opracowania i wdrożenia adekwatnych procedur postępowania i środków bezpieczeństwa. Nie narzuca jednak żadnego standardu w tym zakresie, a pełna odpowiedzialność za dobór procedur i środków bezpieczeństwa spoczywa na administratorze danych.

Konieczne będzie także przeprowadzenie analizy ryzyka. Z uwagi na wysokie kary finansowe oraz coraz liczniejsze incydenty związane z wyciekiem danych, najlepsze praktyki wskazują na konieczność przeprowadzenia własnej, wewnętrznej analizy ryzyka przez każdego administratora a także procesora danych. Celem takiej analizy ma być m.in. zinwentaryzowanie własnych systemów i procesów oraz wdrożenie stosownych środków zaradczych formalno-prawnych. Wybrane podmioty obejmie obowiązek przeprowadzenia formalnej tzw. oceny skutków dla ochrony danych osobowych. Będzie to dotyczyło nie tylko banków, spółek ubezpieczeniowych czy spółek internetowych, ale również startupów, które na dużą skalę wykorzystują systemy śledzące zachowania użytkowników w Internecie w celu targetowania ich określonymi informacjami lub reklamami.

W określonych przypadkach obowiązkowe będzie wprowadzenie funkcji inspektora ochrony danych, który będzie punktem kontaktowym zarówno dla organu nadzorczego, jak i dla osób, których dane są przetwarzane.

Na firmie ciążyć będzie obowiązek zwiększania świadomości pracowników w temacie ochrony danych osobowych. Pracownicy muszą być świadomi obowiązujących w danej organizacji procedur i zasad związanych z ochroną i przetwarzaniem danych osobowych, umieć rozpoznać próbę cyberataku, wiedzieć, jak powiadomić przełożonego itd. Są to istotne kwestie mające na celu wykazanie zgodności działań danego przedsiębiorstwa z RODO.

Obowiązkowe będzie również przeformułowanie klauzul dotyczących zgody na przetwarzanie danych w oparciu o nowe przepisy, w szczególności także rozszerzony zakres obowiązku informacyjnego.

W miejsce dotychczasowego obowiązku rejestracji baz danych osobowych w GIODO pojawi się obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania danych osobowych. Będzie on dotyczył organizacji zatrudniających co najmniej 250 osób lub organizacji, w których przetwarzanie danych może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje dane wrażliwe, np. medyczne.

RODO wymaga także uzyskania zgody opiekunów prawnych w przypadku świadczenia usług wobec dzieci poniżej 16. roku życia. Obecny projekt nowej polskiej ustawy o ochronie danych osobowych obniża tę granicę do 13. roku życia.

...I NOWE PRAWA DLA OSÓB FIZYCZNYCH

Nowe przepisy istotnie wzmacniają pozycję osób fizycznych, którym będzie przysługiwało nowe prawo, tzw. prawo do bycia zapomnianym. Korzystając z tego prawa, osoba, której dane dotyczą, będzie mogła zażądać od administratora niezwłocznego usunięcia danych, które jej dotyczą. Co więcej, w przypadku upublicznienia tych danych, to na administratorze będzie ciążył obowiązek podjęcia działań, by poinformować administratorów przetwarzających te dane osobowe, że konkretna osoba żąda usunięcia wszelkich łącza do jej danych, ich kopii lub ich replikacji.

ZDANIEM AUTORÓW

Jarosław Kamiński, adwokat, senior associate w warszawskim biurze Rödl & Partner;
Marta Wiśniewska, radca prawny w warszawskim biurze Rödl & Partner

Im dalej w las, tym więcej drzew

To ostatni dzwonek, aby rozpocząć przygotowania do nowych wyzwań i zmian. Doświadczenie pokazuje, że po przeprowadzeniu odpowiedniej weryfikacji własnej firmy pod kątem przetwarzania danych osobowych często okazuje się, że oprócz konieczności wprowadzenia nowych rozwiązań i zmiany dokumentacji, niezbędne jest także dostosowanie do nowych przepisów ogólnego modelu biznesowego, w tym rozwiązań technicznych oraz stosunków z podmiotami trzecimi, czyli klientami oraz dostawcami.

Źródło: http://www.rp.pl/Firma/304079991-Co-zmienia-RODO-w-ochronie-danych-osobowych.html