KATARZYNA CZECHUŁA

radca prawny, KPRF Law Office

RODO a programy **lojalnościowe**

Z dniem 25 maja 2018r. ochrona danych osobowych osób fizycznych będzie podlegać przepisom Rozporządzenia z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o danych osobowych) („RODO" lub „Rozporządzenie").

RODO będzie mieć zastosowanie do wszystkich podmiotów, które m.in. oferują usługi lub towary w Unii. Wiele podmiotów, w celu uatrakcyjnienia swojej oferty i zbudowania bazy stałych, lojalnych klientów, oferuje usługi w ramach programów lojalnościowych. Dane osobowe klientów zebrane i przechowywane przez podmiot w związku z prowadzeniem programów lojalnościowych również podlegać będą regulacjom RODO.

W celu upewnienia się, że dane osobowe klientów są przetwarzane prawidłowo, w pierwszej kolejności podmiot oferujący program lojalnościowy powinien przeprowadzić audyt zgromadzonych danych przetwarzanych (tj. np. zgromadzonych, przechowywanych) w związku z prowadzeniem konkretnych programów lojalnościowych.

ZAKRES ZGROMADZONYCH DANYCH

Jedną z podstawowych zasad przetwarzania danych osobowych, wskazaną w RODO, jest minimalizacja danych. Zasada ta wymaga, by administrator (czyli podmiot decydujący o celach i sposobach przetwarzania danych) ograniczył ich przetwarzanie jedynie do tych danych, które są niezbędne do realizacji konkretnego celu. W szczególności, jeżeli celem programu lojalnościowego jest oferowanie w promocji określonych towarów osobom, które wyraziły zgodę na otrzymywanie newslettera wówczas żądanie przez podmiot podania adresu zamieszkania lub numeru PESEL wykracza poza zasadę minimalizacji danych, gdyż podanie tych danych nie jest niezbędne do realizacji celu programu. Administrator powinien zatem zweryfikować, czy zakres przetwarzanych przez niego danych nie jest zbyt szeroki i w konsekwencji powinien usunąć te z nich, które są zbędne w odniesieniu do konkretnego programu lojalnościowego.

PODSTAWA PRAWNA PRZETWARZANIA

W przypadku programu lojalnościowego, przystąpienie do niego najczęściej łączy się z obowiązkiem zaakceptowania regulaminu przez osobę przystępującą, a zatem podstawą prawną przetwarzania będzie zawarta umowa. W celu uniknięcia wątpliwości administratorzy bardzo często pobierają od uczestników zgodę na przetwarzanie danych osobowych. RODO wymaga, by taka zgoda była dobrowolna, wyrażona w sposób jednoznaczny – domyślnie zaznaczone okienko lub milczenie nie jest traktowane przez RODO jako wyrażenie zgody. Administrator jest zobowiązany wykazać, że pozyskane przez niego zgody spełniają wymagania RODO; jak wyjaśniła Grupa Robocza art. 29[1] w wytycznych dotyczących zgody na mocy RODO[2], Rozporządzenie nie wymaga od administratorów, którzy przetwarzają dane na podstawie zgody, aby automatycznie pozyskiwali nowe zgody od klientów/użytkowników – zgoda pozyskana dotychczas będzie nadal obowiązywać, o ile jest zgodna z warunkami RODO.

ZAKRES INFORMACJI PRZEKAZYWANYCH OSOBOM FIZYCZNYM

RODO wymaga, by każda osoba, której dane są przetwarzane, była poinformowana przez administratora m.in. o tym, kto w jakim celu i przez jaki czas je przetwarza. Przepisy RODO rozszerzają zakres obowiązku informacyjnego w odniesieniu do aktualnie obowiązujących przepisów, jednak jednocześnie art. 23 RODO umożliwia państwom członkowskim ograniczenie tego obowiązku – Ministerstwo Cyfryzacji zapowiedziało ograniczenie obowiązku informacyjnego wobec przedsiębiorców zatrudniających mniej niż 250 osób, ponieważ jednak nie ma jeszcze uchwalonych przepisów regulujących tę kwestię, zalecane jest śledzenie regulacji, a po ich uchwaleniu zweryfikowanie treści informacji dotychczas przekazanych uczestnikom programów lojalnościowych w celu ustalenia, czy konieczne jest ponowienie obowiązku informacyjnego.

ODBIORCY DANYCH OSOBOWYCH

Administrator, w niektórych przypadkach, może podjąć decyzję o zleceniu wykonywania poszczególnych czynności przetwarzania innym podmiotom (np. w zakresie mailingu), co w konsekwencji – na gruncie RODO – będzie traktowane jako powierzenie przetwarzania danych. Rozporządzenie w znacznie bardziej restrykcyjny sposób niż aktualnie obowiązująca ustawa reguluje wzajemne relacje administratora i podmiotu przetwarzającego (czyli podmiotu, który przetwarza dane osobowe na zlecenie administratora). Przede wszystkim RODO zastrzega, by administrator korzystał wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych, by spełnić jego wymogi. Po dokonaniu wyboru konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych zgodnie z zasadami wskazanymi w RODO.

WDROŻENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

RODO wymaga, by podmioty przetwarzające dane osobowe oszacowały ryzyko naruszenia praw lub wolności osób fizycznych podczas przeprowadzanego przez te podmioty przetwarzania (ryzyko to może wynikać np. z przypadkowego zniszczenia, utraty danych lub dostępu do danych osobowych przez osoby nieupoważnione), a następnie, uwzględniając to ryzyko (a także uwzględniając stan wiedzy technicznej), koszt wdrażania oraz charakter, zakres i cele przetwarzania, wdrożyły odpowiednie środki techniczne i organizacyjne, aby zapewnić bezpieczeństwo przetwarzania danych. RODO nie podaje żadnych uniwersalnych procedur, jakie administrator powinien wdrożyć, dlatego też konieczne jest, aby każdy z podmiotów przetwarzających dokonał samodzielnej analizy zagrożeń i wyboru środków niwelujących takie zagrożenia.

Administratorzy przetwarzający dane zebrane w ramach programów lojalnościowych powinni również być przygotowani do podejmowania czynności wskutek wykonywania przez osoby fizyczne przyznanych im uprawnień. Do takich uprawnień RODO zalicza np. prawo cofnięcia zgody, zgłoszenia sprzeciwu, prawo do żądania ograniczenia przetwarzania czy też nieuregulowane dotychczas prawo do bycia zapomnianym. Zgodnie z nowymi przepisami, administrator jest zobowiązany niezwłocznie udzielić informacji o podjętych na wniosek osoby działaniach, nie później jednak niż w ciągu miesiąca. To pokazuje, jak istotne jest posiadanie przez administratora, bieżącej wiedzy na temat zakresu i miejsc przetwarzania danych osobowych (np. miejsc w systemie informatycznym, gdzie dane są zapisane) każdego użytkownika programu lojalnościowego. Dodatkowe obowiązki RODO nakłada na administratorów, którzy korzystają z funkcji profilowania danych osobowych lub monitorowania zachowań uczestników programów lojalnościowych.

> *RODO wymaga, by każda osoba, której dane są przetwarzane, była poinformowana przez administratora m.in. o tym, kto w jakim celu i przez jaki czas je przetwarza.*

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu zebranych informacji np. do oceny preferencji danego klienta. Co do zasady, RODO przyznaje osobie fizycznej prawo do niepodlegania profilowaniu. Zastosowanie profilowania jest jednak możliwe, jeżeli np. jest niezbędne do wykonania umowy przez strony lub osoba fizyczna wyraziła zgodę na profilowanie. Niemniej jednak, jeżeli profilowanie jest dozwolone, administrator zobowiązany jest zapewnić osobie mu podlegającej co najmniej prawo do uzyskania interwencji ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania decyzji.

W szczególności, jeżeli monitorowanie zachowań użytkowników jest prowadzone na dużą skalę, jest systematyczne i regularne, wymaga wdrożenia przez administratora dodatkowych środków, takich jak obowiązek wyznaczenia inspektora ochrony danych.

Wskazane kwestie administrator powinien wziąć pod uwagę w odniesieniu do prowadzonych w dniu 25 maja 2018 r. programów lojalnościowych. Należy jednak pamiętać, że RODO nakłada obowiązek uwzględniania ochrony danych osobowych już w fazie projektowania czynności – administrator, planując zorganizowanie nowego programu lojalnościowego lub planując rozszerzenie dotychczasowego programu o kolejne akcje promocyjne, powinien uwzględnić ochronę danych osobowych przetwarzanych w takim programie lub w ramach promocji już na etapie planowania tego przedsięwzięcia. ■

Przypisy:

[1] Grupa Robocza ds. Ochrony osób Fizycznych w zakresie przetwarzania danych osobowych powołana na mocy dyrektywy 95/46/WE parlamentu Europejskiego i Rady z 24 października 1995r.

[2] Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 z 28.11.2017r. (17/PL WP 259)