Warszawa, dnia 15 listopada 2021 r.

Program lojalnościowy a przetwarzanie danych osobowych

Program lojalnościowy to nie tylko budowanie trwałych i pozytywnych relacji z klientami, ale również właściwie zabezpieczenie gromadzonych w tym celu danych osobowych. W praktyce zaprojektowanie programu lojalnościowego, bezpiecznego pod kątem przepisów o ochronie danych osobowych jest trudne i skomplikowane, ale pomimo tej niedogodności, przedsiębiorcy bardzo chętnie sięgają po tę formę reklamy i promocji. Jak zatem krok po kroku zbudować skuteczny, ale i odpowiednio zabezpieczony program lojalnościowy zgodny z zasadami RODO?

Krok pierwszy – oceń ryzyko

W zasadzie klauzule generalne RODO pozwalają administratorom danych w sposób pełny i zupełny szacować ryzyko związane z przetwarzaniem danych osobowych. Należy podkreślić, że samo szacowanie ryzyka powinno nastąpić już w momencie projektowania procesu programu lojalnościowego. Trzeba również zwrócić uwagę na skutki dla ochrony danych oraz rozwiązania w zakresie bezpieczeństwa. Nie wystarczy jednak samo wdrożenie mechanizmów chroniących dane osobowe. Każdy administrator powinien regularnie dokonywać kontroli i oceniać skuteczność zastosowanych narzędzi.

Podsumowując, przy wprowadzaniu programu lojalnościowego kluczowe jest wzięcie pod uwagę i zastosowanie dwóch naczelnych zasad: „privacy by design" oraz „privacy by default". Wytyczą one administratorom wskazówki w zakresie bezpieczeństwa wdrożenia programu lojalnościowego.

Krok drugi – zminimalizuj gromadzone dane

Jedną z kluczowych zasad RODO jest minimalizacja danych. Minimalizacja danych oznacza, że dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane. Administrator danych powinien zatem w każdym procesie przetwarzania danych osobowych pamiętać, aby ograniczać zakres gromadzonych danych osobowych. Wydaje się zatem, że aby przetwarzanie danych osobowych pozostawało w zgodzie z RODO, administrator danych powinien przetwarzać tylko te dane, które są niezbędne do osiągnięcia celu, w jakim pozyskał dane. Zasada ta znajduje swoje zastosowanie również we wdrażaniu rozwiązań dotyczących programu lojalnościowego. Zakres danych osobowych zbieranych w ramach tego rodzaju promocji, może zostać rozszerzony, gdy przy okazji przetwarzania danych osobowych ściśle w celu uczestnictwa w programie lojalnościowym, administrator zdecyduje się na zbieranie danych w innym celu, jak np. cele marketingowe.

Wymuszanie przez administratora podawania przez uczestnika programu lojalnościowego wielu danych osobowych, w tym w szczególności numeru PESEL, czy serii i numeru dokumentu tożsamości, wydaje się niezgodne z RODO, bowiem do realizacji wskazanego celu wystarczające będzie podanie np. imienia i nazwiska, danych kontaktowych, czy przypisanie numeru klienta i gromadzonych punktów w ramach przystąpienia do programu.

Krok trzeci – zastanów się nad podstawą prawną przetwarzania

Jedną z najbardziej problematycznych kwestii, jeśli chodzi o prawidłowe wdrożenie rozwiązań związanych z programem lojalnościowym, jest wybór właściwej podstawy prawnej przetwarzania danych osobowych zgodnie z art. 6 ust. 1 RODO.

Pierwszym i najważniejszym punktem implementacji jest regulamin programu lojalnościowego. To właśnie w tym dokumencie powinny pojawić się również postanowienia dotyczące ochrony danych osobowych. Jest to przede wszystkim mechanizm, który pozwala uczestnikowi zapoznać się z zasadami obowiązującymi w programie lojalnościowym, jak również stanowi dawkę wiedzy na temat

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

przetwarzania danych osobowych. W regulaminie przede wszystkim powinna znaleźć się informacja o celach i podstawach prawnych przetwarzania danych osobowych.

Dopuszczalne są dwie konstrukcje prawne programów lojalnościowych: przyrzeczenie publiczne bądź umowa. Wybór konstrukcji będzie determinował określenie prawidłowej podstawy prawnej przetwarzania danych osobowych. Bardziej praktyczną formą i częściej stosowaną w ramach wdrożenia programu lojalnościowego jest umowa. Potwierdza to również stanowisko judykatury, gdzie w wyrokach sądów wskazuje się na tzw. klauzule abuzywne, które mogą występować w regulaminach programów lojalnościowych. Z uwagi na takie rozumienie regulaminu, umowa adhezyjna będzie tym najwłaściwszym wyborem, jeśli chodzi o implementację rozwiązań w zakresie programu lojalnościowego.

Z uwagi na powyższe, jeśli program lojalnościowy opiera się na konstrukcji umowy, należy wskazać, że właściwą podstawą przetwarzania danych osobowych będzie niezbędność do wykonania umowy. Jeśli zaś program lojalnościowy został oparty na konstrukcji przyrzeczenia publicznego, podstawą prawną przetwarzania danych osobowych jest prawnie uzasadniony interes administratora danych. Z tej przesłanki prawnej wynika również możliwość m.in. dochodzenia roszczeń, czy wykorzystywania danych do celów marketingowych.

Ponadto, co warte uwagi, jeśli administrator danych zdecyduje się na zbieranie dodatkowych danych, niezwiązanych bezpośrednio z uczestnictwem w programie lojalnościowym, podstawą prawną przetwarzania danych będzie zgoda. Zgoda powinna spełniać wszelkie wymogi stawiane przez RODO, przede wszystkim musi być zgodą wyrażoną w pełni świadomie i dobrowolnie.

Nie należy też zapominać o podstawie prawnej, jaką jest przepis prawa, bowiem obowiązujące regulacje prawne mogą skutkować koniecznością przetwarzania danych w celach rozliczeniowych (kwestie podatkowe, księgowe).

Krok czwarty – spełnij obowiązek informacyjny

W regulaminie programu lojalnościowego powinna znaleźć się treść obowiązku informacyjnego. Zgodnie z przepisami RODO, każdy uczestnik programu lojalnościowego jako podmiot, którego dane są przetwarzane, musi zostać poinformowany o przetwarzaniu jego danych osobowych. Administrator zobowiązany jest wskazać m.in. swoją tożsamość i dane kontaktowe, dane kontaktowe inspektora ochrony danych, o ile został wyznaczony, cele przetwarzania oraz podstawy prawne, jak również czas przechowywania danych, czy informacje o przysługujących prawach.

Co ważne, treść obowiązku informacyjnego powinna wskazywać na wszystkie możliwe cele przetwarzania danych osobowych. Oznacza to, że w obowiązku informacyjnym programu lojalnościowego może znaleźć się informacja zarówno o przetwarzaniu danych w ramach programu lojalnościowego, jak również informacje dodatkowe np. o przetwarzaniu danych w celach marketingowych.

Klauzula informacyjna, aby była w pełni zgodna z przepisami RODO, powinna być skonstruowana w sposób jasny, czytelny i precyzyjny. Ma przedstawiać informacje uczestnikowi programu lojalnościowego prostym językiem, opisując wprost, dlaczego dane są gromadzone i przetwarzane.

Krok piąty – odpowiadaj na wnioski użytkowników

Odpowiedzi na wnioski podmiotów danych dotyczące realizacji przysługujących im praw stanowią jeden z fundamentalnych obowiązków administratorów danych. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki - najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania - podać tego przyczyny.

Prowadzenie programu lojalnościowego może wiązać się z licznymi zapytaniami kierowanymi od podmiotów danych. Przesyłanie przez administratora danych informacji o charakterze promocyjnym może skutkować zwiększoną ilością próśb osób, których dane dotyczą. Z tego względu, niezbędne jest wdrożenie bezpiecznego mechanizmu, który pozwoli administratorowi danych na sprawne i rzetelne konstruowanie odpowiedzi do podmiotów danych.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Jeśli zatem uczestnik programu lojalnościowego zdecyduje się wnieść sprzeciw wobec przetwarzania danych osobowych bądź chce skorzystać z prawa do wycofania zgody, należy przeanalizować złożony wniosek i przesłać do podmiotu danych w terminie 1 miesiąca odpowiedź. Jeśli sprawa wymaga dodatkowej weryfikacji, można wskazany termin przedłużyć o kolejne dwa miesiące. Każdorazowo należy informować podmiot danych o wyniku analizy jego prośby - bez znaczenia, czy wniosek zostanie rozstrzygnięty w sposób pozytywny, czy negatywny.

Trzeba mieć na względzie, że finalne rozstrzygnięcie wniosku może determinować konieczność podjęcia przez administratora danych dodatkowych działań, jak np. usunięcie danych osobowych.

Podsumowanie

Dołączenie do programu lojalnościowego przez podmiot danych często wiąże się z szeregiem dodatkowych uprawnień. Trzeba jednak pamiętać, że za każdym razem, gdy uczestnik decyduje się przystąpić do tego rodzaju promocji, jego dane osobowe zaczynają być przetwarzane. Administrator zatem, wdrażając rozwiązanie w postaci programu lojalnościowego, nie może pominąć zasad przetwarzania danych osobowych. Jego naczelnym obowiązkiem jest należyta ochrona danych uczestników programu.

Kinga Bieniek-Zawadzka, Specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł