Warszawa, 23.01.2024 r.

Program lojalnościowy zgodny z RODO – jak podejść do tematu?

Słowo wstępu

Programy lojalnościowe to jedno z powszechnie stosowanych na rynku narzędzi marketingowych. Rozwiązanie pozwala w sposób efektywny budować długotrwałe relacje z klientami, co ma przełożenie na sprzedaż oferowanych usług czy produktów przez firmę. Z drugiej strony, programy lojalnościowe mają wiele zalet dla klientów, m. in. pozwalają im być na bieżąco z ofertą firmy, nabywać usługi lub towary w atrakcyjnych cenach (zniżki dla uczestników programów lojalnościowych lub brak pobierania opłat za ich dostawy), umożliwiają dostęp do limitowanych usług lub towarów wyłącznie dla uczestników programu lojalnościowego – to tylko niektóre z funkcjonalności programów lojalnościowych obserwowanych na rynku.

Aby trafić do elitarnego grona lojalnych klientów danej firmy niezbędne jest przekazanie „jakiś" informacji, na podstawie których będziemy identyfikowani jako uczestnik programu lojalnościowego. Te informacje będą stanowić dane osobowe przetwarzane w celu prawidłowej obsługi procesu przetwarzania danych pt. „Program Lojalnościowy". ŻÓŁTA LAMPKA - niech to będzie punkt wyjścia dla dalszej treści publikacji.

Poniżej skupię się na kluczowych elementach, jakie należy brać pod uwagę przy tworzeniu oraz prowadzeniu programów lojalnościowych w perspektywie przetwarzanych danych osobowych. Mając jednak na uwadze, że programy lojalnościowe mogą przybierać różne formy, a sposób ich prowadzenia oraz stosowania zależy od indywidualnej działalności biznesowej każdej firmy, chciałbym zorientować publikację wokół programów lojalnościowych branży e-commerce oraz sprzedaży, oferowaniu usług w sposób „tradycyjny" – tj. sklepu, działającego stacjonarne.

Program lojalnościowy – rozkładamy na czynniki pierwsze

W zasadzie prawidłowe (w sposób „zgodny z RODO"), wdrożenie oraz prowadzenie programu lojalnościowego to nic innego, jak realizacja zasad *Privacy by Design* (ochrona danych w fazie projektowania) oraz *Privacy by Default* (stosowanie domyślnych ustawień ochrony danych osobowych). Obie stanowią treść art. 25 RODO.

Proste? Niekoniecznie? – to popatrz poniżej:

Zanim uruchomisz program lojalnościowy i przystąpisz do zbierania danych osobowych, wykonaj kilka działań.

Po pierwsze, zacznij od ustalenia CELU oraz W JAKI SPOSÓB ma być prowadzony program lojalnościowy, np.: a) oferowanie usług, towarów po bardziej atrakcyjnych cenach (kody rabatowe), b) przekazywanie newsletter'a (informacje handlowe), c) zbieranie punktów przez uczestników za zakupione usługi lub towary, a następnie możliwość ich wykorzystania na zakupy, d) oferowanie limitowanych usług, towarów, e) zakup usług, towarów w przedsprzedaży. Weź również pod uwagę możliwość rozwoju programu lojalnościowego, w tym uzupełnienie o nowe funkcjonalności.

Obecnie lwia część programów lojalnościowych nie może się obyć bez stosowania rozwiązań technologicznych (platformy sprzedażowe w formie on-line, w szczególności formularze członkowskie, poczta elektroniczna, systemy elektroniczne do obsługi programu, w tym aplikacje mobilne). Aktualny stan wiedzy technicznej i technologicznej (oferowane i funkcjonujące na rynku rozwiązania, systemy) należy wziąć pod uwagę przy analizowaniu, jak będzie prowadzony program lojalnościowy, aby nie odbiegał od standardów rynkowych, w szczególności w dziedzinie bezpieczeństwa danych osobowych.

Przeprowadzenie tej analizy na początku pozwoli na późniejsze zidentyfikowanie: a) jak oraz w jaki sposób będą przetwarzane dane osobowe, w szczególności z użyciem jakich narzędzi (kart lojalnościowych, systemów i ich funkcjonalności) tzw. charakter i kontekst przetwarzania, b) jaki będzie zakres niezbędnych danych przetwarzanych w celu prawidłowego prowadzenia programu lojalnościowego – będzie to stanowić podstawę dla prawidłowego zaprojektowania strumienia przetwarzanych danych osobowych.

Następnie zajmij się technicznymi elementami związanymi z prowadzeniem programu lojalnościowego. W tym celu musisz umieć sobie odpowiedzieć na poniższe pytania:

1. W jaki sposób będzie przebiegał proces zbierania danych, tj. z jakich kanałów komunikacji klienci będą mogli korzystać w celu przystąpienia do programu lojalnościowego? Np.: strona internetowa firmy, zapisanie się podczas zakupów online czy w salonie firmowym, kontakt telefoniczny, SMS itd.;

2. Jakie dane osobowe są niezbędne do osiągnięcia zidentyfikowanego wcześniej celu (trzy akapity wyżej), mając jednocześnie na uwadze zamierzony sposób prowadzenia programu lojalnościowego? Jeżeli uznasz, że jakieś dane nie są potrzebne do osiągnięcia celu, zrezygnuj z ich przetwarzania;

3. Jakie dane generowane przez uczestnika w związku z uczestnictwem i korzystaniem z programu lojalnościowego będą zbierane, np.: analizy statystyk sprzedażowych, w tym zawartości „koszyka" pod kątem ilości, wartości i częstotliwości zakupów, historia zakupów, geolokalizacja uczestników programu lojalnościowego, potwierdzenia realizacji usług, zakupu itp.? W jaki sposób będą wykorzystywane (przetwarzane), np.: w celu przyznawania i ustalania wartości rabatów?;

4. Jakie narzędzia (technologie) będą wykorzystywane do przetwarzania danych oraz jakie funkcjonalności są przez nie oferowane? Zwróć uwagę, czy narzędzia pochodzą od podmiotów zewnętrznych (dostawców, kontrahentów, np.: w ramach korzystania z gotowych rozwiązań oferowanych na rynku), czy mają charakter wewnętrzny (dedykowany dla firmy odpowiedzialnej za program lojalnościowy).

   WAŻNE! Jeżeli stwierdzisz, że podmiot dostarczający narzędzie ma dostęp do danych w nim zawartych (w szczególności danych uczestników programu lojalnościowego), konieczne może być zawarcie umowy powierzenia przetwarzania danych osobowych oraz weryfikacja stosowanych przez ten podmiot środków technicznych i organizacyjnych w celu bezpieczeństwa danych.

5. W jaki sposób będzie organizowane całe przedsięwzięcie prowadzenia programu lojalnościowego? Warto zwrócić uwagę m.in. na to:
   a) kto będzie odpowiedzialny za obsługę procesu tj. czy będzie to dedykowany zespół wewnętrzny firmy czy prowadzenie programu lojalnościowego zostanie zlecone podwykonawcy;
   b) kto będzie miał dostęp do danych gromadzonych w ramach programu lojalnościowego;
   c) czy jest możliwe oraz w jaki sposób realizowanie praw podmiotów danych w przypadku złożenia żądania przez uczestnika programu lojalnościowego, tj. m.in.:
      i. wycofanie zgody,
      ii. żądanie usunięcia danych,
      iii. żądanie wydania kopii danych,
      iv. żądanie zaprzestania dalszego przetwarzania,
      v. zgłoszenie sprzeciwu wobec przetwarzania jego danych osobowych

      w szczególności w kontekście wykorzystywanych narzędzi (pkt. 4 powyżej),

      WAŻNE! Upewnij się, że narzędzia, z których będziesz korzystać w związku z programem lojalnościowym, umożliwią automatyczne usuwanie danych po upływie okresu,

przez jaki dane mogą być legalnie przetwarzane (np.: po rezygnacji z członkostwa przez uczestnika).

d) czy dane mogą trafiać do tzw. państw trzecich (spoza EOG), tj. czy dochodzi do transferu danych osobowych – taka sytuacja może mieć miejsce w związku z korzystaniem z usług podmiotów trzecich lub wykorzystywanymi systemami IT albo w ramach dostępu do danych programu lojalnościowego przez inne spółki z grupy kapitałowej, mające siedzibę poza EOG;

Równocześnie pamiętaj o obowiązkach firmy jako administratora danych osobowych, które musisz spełnić. Do najważniejszych z nich zaliczają się m. in.:

- nadanie odpowiednich upoważnień do przetwarzania danych oraz odebranie oświadczeń o zachowaniu poufności od członków zespołu odpowiedzialnych za obsługę procesu;

- sporządzenie lub aktualizacja dokumentacji ochrony danych osobowych związanej z prowadzeniem programu lojalnościowego, w szczególności rejestru czynności przetwarzania;

- sporządzenie oraz przekazanie/publikacja informacji dla uczestników dotyczącej przetwarzania danych osobowych, zgodnie z art. 13 i 14 RODO (np. w formie części regulaminu/ogólnych warunków świadczenia usług lub jako część polityki prywatności na stronie internetowej);

- jeżeli konieczne – sporządzenie oraz odebranie zgód na przetwarzanie danych osobowych od uczestników programu lojalnościowego (np. w celu przekazywania informacji handlowych);

- zawarcie umów powierzenia przetwarzania danych osobowych z podmiotami zewnętrznymi wspierającymi lub obsługującymi proces w imieniu firmy;

- w przypadku przetwarzania danych na podstawie prawnie uzasadnionego interesu administratora przeprowadzenie tzw. „testu równowagi”;

- zidentyfikowanie zagrożeń dla bezpieczeństwa danych na podstawie ustalonych wcześniej informacji z pkt. 1 – 5 powyżej, a następnie wdrożenie odpowiednich środków technicznych i organizacyjnych, w szczególności technologicznych, dla zapewnienia ich bezpieczeństwa, w tym przeciwdziałania naruszeniom. Do takich zabezpieczeń można zaliczyć w szczególności: tworzenie backup’ów danych, stosowanie programów antywirusowych, szyfrowanie transmisji danych, odpowiednie poziomy uprawnień w systemach osób dopuszczonych do przetwarzania danych.

Podsumowanie

Powyższe opracowanie to oczywiście ogólne ujęcie kluczowych elementów jakie należy brać pod uwagę w celu prawidłowego „ustawienia” procesu ochrony danych osobowych w związku z wdrażaniem programów lojalnościowych. W każdym razie zaprezentowane kroki stanowią solidną podstawę dla wdrożenia programu lojalnościowego „zgodnie z RODO”.

Zaprojektowanie procesu przetwarzania danych osobowych, jakim jest program lojalnościowy, wymaga indywidualnego podejścia i może wymuszać dodatkową analizę lub dodatkowe działania, o czym należy pamiętać. Dlatego przestrzegamy przed kopiowaniem wprost rozwiązań funkcjonujących na rynku. Oczywiście możliwa jest inspiracja w zakresie zorganizowania programów lojalnościowych przez konkurencję, ale przejmowanie ich rozwiązań (w tym dokumentacji publikowanej na stronach www) i wdrażanie ich w takiej samej formie bez poprzedzającej analizy, to co do zasady prosta droga do naruszeń w sferze ochrony danych osobowych w naszej organizacji.

Adw. Paweł Wojciechowski, specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.