Warszawa, 28.08.2024 r.

Newsletter w branży e-commerce – jak zrobić to zgodnie z RODO?

Tworzenie baz na potrzeby newslettera i sama jego wysyłka to wciąż jeden z najpopularniejszych i najefektywniejszych narzędzi marketingowych. Nic więc dziwnego, że korzystają z niego również sklepy internetowe. Poprzez newsletter można wysyłać informacje o nowościach w ofercie, specjalnych akcjach promocyjnych, itd. Przyznam szczerze, że sam również zapisany jestem do co najmniej kilku newsletterów w sklepach, w których zdarza mi się kupować np. gry wideo czy komiksy ☺ Dlaczego? Bo to dla mnie idealne rozwiązanie – dostaję na maila dokładnie to czym się interesuję, co śledzę i co potencjalnie mogę chcieć kupić.
Niestety i tutaj (tzn. przy tworzeniu baz newsletterowych) bardzo często spotykam się z sytuacją, że dany sklep nie do końca dobrze implementował wymogi wynikające z obowiązującego od maja 2018 r. ogólnego rozporządzenia o ochronie danych osobowych, czyli popularnego RODO.
W niniejszym artykule chciałbym zatem przedstawić kilka istotnych elementów, o które trzeba zadbać, by newsletter stał się – oprócz swych niewątpliwych walorów marketingowych – także narzędziem zgodnym ze wspomnianym wyżej RODO.

Zbieranie zgód od subskrybentów

Zacznijmy od podstaw, a dokładniej od podstaw prawnych, które dają nam (tj. właścicielom sklepów internetowych) prawo do przetwarzania danych osobowych. Taką przesłanką, która pozwala nam gromadzić dane będzie zgoda. Tyle, że taka zgoda musi spełniać pewne warunki. Chodzi m.in. o:

- Świadomą zgodę - formularz zapisu do newslettera powinien jasno określać, na co zgadza się użytkownik. Niby oczywiste, ale łatwo tu np. o zbyt ogólną zgodę np. „wyrażam zgodę na przetwarzanie danych osobowych”… i tyle. Zdecydowanie tak to wyglądać nie może.
- Osobną zgodę na różne cele - jeśli chcesz używać danych osobowych w różnych celach (np. do newslettera i analiz marketingowych), musisz uzyskać osobną zgodę na każdy z tych celów.
- Opcję opt-in (ale już nie koniecznie double opt-in) – zgoda musi być aktywnie wyrażona przez użytkownika, np. poprzez zaznaczenie checkboxa. Niedopuszczalne są checkboxy domyślnie zaznaczone.
- Łatwość rezygnacji z subskrypcji (czyli tzw. wycofanie zgody) - musisz zapewnić łatwy i szybki sposób na wypisanie się z newslettera, np. poprzez link w stopce każdego maila.

Transparentność i informacja

Ten punkt w zasadzie odnosi się do tzw. klauzul informacyjnych albo inaczej obowiązków informacyjnych. Ich celem jest przekazanie subskrybentowi pakietu informacji, które

pozwolą mu wiedzieć na czyją rzecz wyraża zgodę na przetwarzanie danych, w jakim celu, jakie przysługują mu uprawnienia, itd. Doskonałym narzędziem do przekazania tych informacji jest:

- Polityka prywatności – na jej temat dość dużo pisaliśmy na blogu iSecure, odsyłam np. do artykułu pt. „Jak (nie) pisać polityki prywatności – dobre praktyki".

Zasada minimalizacji danych

Zapewne nikt z nas nie chce podawać więcej informacji na swój temat niż jest to faktycznie konieczne, żeby osiągnąć dany rezultat (na gruncie RODO powiedzielibyśmy – zrealizować określony cel przetwarzania danych). Dlatego też unijny ustawodawca wprowadził bardzo ważną zasadę zwaną minimalizacją danych. To nic innego jak wymóg, by pobierać od subskrybentów jedynie te dane, które są absolutnie konieczne do realizacji celów newslettera (np. imię i adres e-mail). Krótko mówiąc - nie zbieraj danych, które nie są Ci do niczego potrzebne.

Bezpieczeństwo danych

W tym temacie spokojnie można napisać osobny artykuł, ograniczę się zatem do wskazania następujących wskazówek:

- Bezpieczne przechowywanie danych - zabezpiecz dane subskrybentów przed nieuprawnionym dostępem. Korzystaj z bezpiecznych serwerów, szyfrowania danych oraz regularnie aktualizuj oprogramowanie.
- Ograniczenie dostępu do danych osobowych - dostęp do danych powinny mieć tylko uprawnione osoby. Określ jasno role i odpowiedzialności związane z przetwarzaniem danych.

Ocena ryzyka i zasada rozliczalności

I znowu – tak na temat analizy ryzyka jak i dokumentacji RODO można napisać osobne teksty. Polecam np. ten artykuł: „Dobry moment, czyli co w trawie piszczy… Dokumentacja RODO w Twojej organizacji". Niemniej słowo komentarza jest tu niezbędne, a zatem:

- Analiza ryzyka - przeprowadź ocenę ryzyka związaną z przetwarzaniem danych osobowych w ramach newslettera. Określ potencjalne zagrożenia i podejmij odpowiednie środki zapobiegawcze. Tak, zdaję sobie sprawę, że brzmi to bardzo skomplikowanie i niestety w wielu przypadkach tak właśnie jest. Ale może choć trochę pomoże Ci ten tekst z naszego bloga: „Analiza ryzyka w procesach przetwarzania danych".
- Dokumentowanie procesów – w pewnym uproszczeniu: RODO mówi, że musisz umieć wykazać zgodność przetwarzania danych z ww. aktem prawnym. Prowadź zatem dokumentację wszystkich procesów związanych z przetwarzaniem danych osobowych w ramach newslettera. W razie kontroli RODO będziesz musiał udowodnić zgodność z przepisami.

Prowadzenie rejestru przetwarzania danych
Całkiem możliwe, że będziesz musiał prowadzić tzw. rejestr czynności przetwarzania. W kontekście newslettera musisz po prostu zadbać o to, by tego typu czynność (albo czynności – jeśli jest ich nieco więcej) została dodana do ww. rejestru. A jeśli chcesz wiedzieć jak taki rejestr prowadzić, rzuć okiem na artykuł: „Rejestr czynności przetwarzania danych osobowych – w jaki sposób go prowadzić?"

Korzystanie z zewnętrznych dostawców usług
Bardzo często prowadząc sklep internetowy, korzystać będziemy z usług zewnętrznych dostawców, którzy uczestniczą w przetwarzaniu danych osobowych. W przypadku newslettera często to będzie jakiś zewnętrzny system do przechowywania i wysyłania mailingów. W takim przypadku musisz pamiętać o umowie przetwarzania danych osobowych. Parę słów na ten temat piszemy np. tutaj: „Uregulowanie stosunku powierzenia".

Powyższa lista zdecydowanie nie wyczerpuje tematu, jednak daje solidne podstawy do tego, by zbudować bazę newsletterową i – co najważniejsze – wysyłać mailingi do subskrybentów takiego newslettera.

Michał Sztąberek – ekspert ds. ochrony danych osobowych, Prezes Zarządu w iSecure Sp. z o.o.