

Czy wiadomości e-mail dotyczące porzuconych koszyków są zgodne z RODO?

W epoce cyfrowej, gdy zakupy online są nieodłączną częścią naszej codzienności, problem porzuconych koszyków w sklepach internetowych staje się coraz bardziej istotny. Codziennie setki, a nawet tysiące klientów przerywają proces zakupowy z różnych powodów - wysokie koszty dostawy, dodatkowe opłaty, brak preferowanego sposobu dostawy lub płatności, wystąpienie błędów systemowych, problemy z dostępem do Internetu lub po prostu zmiana zdania to tylko niektóre z nich.

W rezultacie opuszczamy stronę bez usuwania przedmiotów z koszyka. Z perspektywy sklepu, jeśli klient nie powróci do koszyka i nie sfinalizuje zakupów, oznacza to utratę potencjalnego dochodu. Dlatego sklepy internetowe podejmują działania mające na celu zachęcenie klientów do powrotu. Często wysyłają one przypomnienia o porzuconym koszyku, najczęściej w formie wiadomości e-mail, czasem dodatkowo oferując rabaty lub inne zachęty.

Jednak czy sklepy, przypominając nam o nieukończonych transakcjach, działają zgodnie z obowiązującymi przepisami, zwłaszcza w kontekście RODO?

Czym jest „porzucony koszyk”?

Porzucony koszyk to sytuacja, w której użytkownik dodaje produkt do koszyka, ale z jakiegoś powodu nie kupuje produktu i opuszcza stronę.

Właściciel sklepu internetowego widzi takie porzucone koszyki w panelu platformy sklepowej czy w Google Analytics i zaczyna się zastanawiać, co poszło nie tak.

Biorąc pod uwagę, że około 7 na 10 potencjalnych klientów¹ porzuca swoje koszyki przed dokonaniem zakupu, ponowne zaangażowanie nawet niewielkiego odsetka z nich za pośrednictwem tych e-maili może znacznie zwiększyć przychody sklepów online.

Czy wiadomości e-mail dotyczące porzuconych koszyków są zgodne z RODO?

Wysłanie użytkownikowi strony internetowej przypomnienia o porzuconym koszyku wymaga przetwarzania co najmniej jego adresu e-mail, a więc możemy je określić jako przetwarzania danych osobowych. Dlatego też musimy opierać to działanie na jednej z dopuszczalnych podstaw prawnych określonych w artykule 6 RODO:

- **art. 6 ust. 1 lit. b RODO – przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.**

Aby wykorzystać tę przesłankę, przetwarzanie danych musi być zainicjowane na żądanie osoby, której dane dotyczą, oraz musi mieć na celu zawarcie umowy. Tę podstawę przetwarzania moglibyśmy uzasadnić w sytuacji, gdy przyczyną niedokończenia zakupów były problemy techniczne lub problem z płatnością.

¹ zgodnie z badaniami Izby Gospodarki Elektronicznej.

Jednakże, jeśli klient zamknął stronę internetową i nie sfinalizował zakupu z nieznanymi nam przyczyn, nie możemy twierdzić, że wysyłając wiadomość, działamy na podstawie żądania klienta przed zawarciem umowy. Nie mamy bowiem pewności, jaka była intencja użytkownika.

- **art. 6 ust. 1 lit. a RODO – przetwarzanie odbywa się na podstawie zgody.**
Bezpieczniejszą podstawą, która nie wymaga analizowania powodów niedokończenia procesu zamówienia, jest zgoda osoby, która ma otrzymać informację o porzuconym koszyku. Zgoda ta, zgodnie z definicją wyrażoną w RODO, powinna być dobrowolna, świadoma, wyraźna i konkretna. Uzyskanie takiej zgody może być trudne i wymaga aktywnego działania, na przykład poprzez zaznaczenie odpowiedniego pola wyboru (checkbox). Wielu klientów, do których administrator chciałby skierować przypomnienie o porzuconym koszyku, może nie wyrazić takiej zgody.
- **art. 6 ust. 1 lit. f RODO – przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią.**

Uzasadniony interes administratora może obejmować kontakt z klientem, który z nieznanymi przyczyn zrezygnował z dokonania zakupów. Przypomnienie może być interpretowane jako próba zapewnienia pomocy w dokończeniu transakcji lub wsparcia w podejmowaniu decyzji. Niemniej jednak należy zachować ostrożność - niedopuszczalne jest wykorzystywanie adresu e-mail wprowadzonego jedynie w trakcie niesfinalizowanego zamówienia, który został zarejestrowany za pomocą plików cookie. Administrator powinien posiadać już wcześniej prawne uzasadnienie do przetwarzania adresu e-mail, na przykład w kontekście poprzednich zakupów lub założonego konta. Jeśli dane użytkownika nie są jeszcze obecne w bazie administratora, konieczne będzie uzyskanie zgody od użytkownika.

Analiza wskazanych powyżej podstaw prawnych przetwarzania wyraźnie wskazuje, że żadna z nich nie jest idealna czy uniwersalna – każda wymaga spełnienia dodatkowych warunków przez administratora czy odebrania konkretnych oświadczeń od klientów.

Najbezpieczniejszą podstawą przetwarzania będzie jednak zgoda, która w Polsce i tak musi być odebrana na podstawie ustawy o świadczeniu usług drogą elektroniczną czy prawa telekomunikacyjnego. Podobne wnioski płyną także z decyzji ICO, która jest pokrótce omówiona w końcowej części tego artykułu.

Jakie akty prawne poza RODO mogą mieć wpływ na porzucone koszyki?

W Polsce, oprócz RODO, podczas projektowania procesu dot. porzuconych koszyków należy wziąć pod uwagę jeszcze dwa akty prawne – ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Zgodnie z ustawą o świadczeniu usług drogą elektroniczną za **informację handlową** należy uznać m.in. *każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy*. Bez wątpienia przesłanie komunikatu o

porzuconym koszyku ma na celu zachęcenie odbiorcy do dokonania zakupu oraz, w efekcie, sprzedaż produktów znajdujących się w koszyku, co przekłada się na osiągnięcie celu handlowego.

Stosownie do art. 10 ustawy o świadczeniu usług drogą elektroniczną zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

Natomiast art. 172 ustawy – Prawo telekomunikacyjne reguluje, że *zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę*. Przepisy te jednoznacznie wskazują więc, że informacja handlowa może być wysyłana wyłącznie po uzyskaniu zgody użytkownika. Nie przewidziano w nich żadnej innej podstawy do działania.

Co ważne, zgoda wyrażona na podstawie ustawy Prawo telekomunikacyjne musi spełniać wszystkie wymagania określone w RODO – musi być dobrowolna, konkretna, świadoma i jednoznaczna.

Jak zgodnie z RODO wysyłać wiadomości e-mail dotyczące porzuconych koszyków?

Biorąc pod uwagę przepisy RODO, ale przede wszystkim ustawy o świadczeniu usług drogą elektroniczną i prawa telekomunikacyjnego, należy przede wszystkim odebrać właściwą zgodę, tak aby, jak najwięcej użytkowników mogło ją wyrazić jeszcze przed zamknięciem strony z niedokończonym zamówieniem.

Zgoda powinna jasno określać, kto jest odpowiedzialny za przetwarzanie danych, jakie konkretne dane będą przetwarzane oraz w jakich celach. Ważne jest również podkreślenie, że zgoda jest dobrowolna i może być cofnięta w dowolnym momencie. Aby zgoda była w pełni dobrowolna, musi być uzyskana oddzielnie dla każdego kanału komunikacji - klient powinien mieć możliwość wyrażenia zgody na marketing poprzez wiadomości e-mail niezależnie od zgody na marketing poprzez SMS.

Co równie istotne i niezbędne dla wykazania przestrzegania zasady rozliczalności, zgody muszą być dokładnie zapisane w systemie, aby w razie potrzeby można było udzielić wyjaśnień dotyczących daty udzielenia zgody oraz jej treści.

Należy także pamiętać o obowiązku wyrażonym w art. 13 RODO - spełnieniu obowiązku informacyjnego wobec klientów. Informacja o wysyłaniu przypomnień o porzuconych koszykach powinna być zawarta w polityce prywatności sklepu internetowego, a pierwszą warstwę tego obowiązku najlepiej umieścić w miejscu, gdzie zgoda jest udzielana przez klienta, np. w momencie podawania przez niego swojego adresu e-mail.

Natomiast komunikacja przesyłana do klienta, który wyraził na nią zgodę, nie powinna być uciążliwa ani nie powinna zawierać elementów krytyki za porzucenie koszyka wobec klienta. Celem komunikatu jest jedynie przypomnienie, a nie narzucanie klientowi konieczności powrotu na stronę.

Jakie konsekwencje grożą administratorom, którzy nieprawidłowo zaprojektują ten proces?

W przypadku naruszenia podstawowych zasad przetwarzania danych (art. 5 RODO), takich jak zgodność z prawem, rzetelność i przejrzystość, minimalizacja danych, jak również brak oparcia przetwarzania w jednej z przesłanek wskazanych w art. 6 albo art. 9 RODO administrator podlega administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu.

Jak istotne jest ustalenie odpowiedniej podstawy prawnej przetwarzania danych i zaprojektowanie procesu dot. porzuconych koszyków, może świadczyć grzywna nałożona przez ICO (brytyjski organ nadzorczy ds. ochrony danych osobowych) na American Express Services Europe Limited (dalej jako: Amex)². Amex został ukarany grzywną w wysokości 90 000 funtów na mocy RODO za wysłanie 4 milionów „wiadomości serwisowych”, które w ocenie ICO, stanowiły treści marketingowe.

W okresie od czerwca 2018 r. do maja 2019 r. Amex wysłał do swoich klientów (członków kart) ponad 50 milionów wiadomości e-mail, które sklasyfikował jako e-maile niezwiązane z usługami marketingowymi. Spośród nich 4 miliony e-maili wysłano do klientów, którzy zrezygnowali z komunikacji marketingowej.

Konsekwencją tej akcji wysyłkowej były 22 skargi przesłane przez odbiorców komunikacji do Amex oraz 3 skargi skierowane do ICO. ICO przeprowadziła dochodzenie i ustaliła, że niektóre wiadomości e-mail, które Amex sklasyfikował wewnątrz jako wiadomości serwisowe, zawierały materiały marketingowe.

W maju 2021 r. ICO ukarała Amex grzywną w wysokości 90 000 funtów za naruszenie przepisów dotyczących prywatności i komunikacji elektronicznej (PECR), które obowiązują obok ustawy o ochronie danych i brytyjskiego odpowiednika RODO. PECR w Wielkiej Brytanii podobnie jak ustawa o świadczeniu usług drogą elektroniczną w Polsce daje ludziom określone prawa do prywatności w odniesieniu do komunikacji elektronicznej.

Jakie wnioski administrator może wyciągnąć z decyzji ICO?

Przypadek Amex podkreśla, jak ważne jest zachowanie czujności w kwestii tego, jak cienka granica jest między e-mailem serwisowym a marketingowym. Wiadomości serwisowe zawierają rutynowe informacje, takie jak zmiany warunków i planów płatności, powiadomienia o przerwach w świadczeniu usług lub informacje dotyczące bezpieczeństwa produktów. Natomiast marketing bezpośredni to wszelkie komunikaty reklamowe lub materiały marketingowe skierowane do konkretnych osób, w tym także informacje o porzuconych koszykach.

To rozróżnienie ma kluczowe znaczenie, a te ostatnie powinny być wysyłane tylko do osób, które wyraziły zgodę na otrzymywanie marketingowych wiadomości e-mail – i na podstawie

² <https://www.rpc.co.uk/snapshots/data-protection/summer-2021/ico-fines-american-express-for-blurring-service-emails-with-marketing-emails/>



sektorowych przepisów w Wielkiej Brytanii, a także w Polsce, gdzie kwestię tę reguluje ustawa o świadczeniu usług drogą elektroniczną i prawo telekomunikacyjne.

Nina Zacharska - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.