Magdalena Podjacka
Karolina Smolarek
Grzegorz Olszewski

OCHRONA DANYCH OSOBOWYCH OKIEM E-COMMERCE MANAGERA

Warszawa 2022

Spis treści

Wykaz skrótów

art. – Artykuł

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.);

Ustawa o ochronie danych osobowych – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

UODO – Urząd Ochrony Danych Osobowych;

PUODO – Prezes Urzędu Ochrony Danych Osobowych;

EOG – Europejski Obszar Gospodarczy;

IOD – Inspektor ochrony danych;

UKE – Urząd Komunikacji Elektronicznej;

UOKiK – Urząd Ochrony Konkurencji i Konsumentów;

UŚUDE – Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344);

Prawo telekomunikacyjne – Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r. poz. 576 z późn. zm.);

Dyrektywa o prywatności i łączności elektronicznej – Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) z dnia 12 lipca 2002 r. (Dz.Urz.UE.L Nr 201, str. 37);

Kodeks cywilny – ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz.U. z 2020 r. poz. 1740 z późn. zm.);

TSUE – Trybunał Sprawiedliwości Unii Europejskiej.

Wstęp

Nie ulega wątpliwości, iż na każdym kroku zauważyć można jak dane osobowe stają się nieodłączną częścią zarówno biznesu, jak i życia prywatnego. Niniejsza publikacja „Ochrona danych osobowych okiem E-commerce Managera" to przewodnik, który wspiera czytelnika w zrozumieniu procesów przetwarzania danych osobowych oraz wymagań w zakresie dokumentacji ochrony danych osobowych, w szczególności z punktu widzenia osób odpowiedzialnych za prowadzenie działalności gospodarczej w branży e-commerce.

Pozycja ta opiera się na szeregu aktów prawnych, w szczególności Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 ochronie danych, tzw. RODO).

Problematyka ochrony danych osobowych powinna stanowić podstawowe zagadnienie leżące w sferze zainteresowań każdej organizacji, w szczególności za względu na ryzyko naruszeń ochrony danych osobowych, które mogą wiązać się z odpowiedzialnością finansową. Mając na uwadze powyższe, zaprojektowanie oraz wdrożenie skutecznego systemu ochrony danych powinno być uznane za kluczowe dla działalności każdego administratora oraz podmiotu przetwarzającego. Ma to zwłaszcza duże znaczenie dla tych podmiotów, które prowadzą swoją działalność w Internecie, a w dodatku przetwarzanie danych osobowych (np. klientów) jest dla nich niezbędne – ma to miejsce np. w działalności sklepów internetowych, które zdobywają coraz większą popularność.

Jak zostało wskazane na wstępie, niniejsza publikacja odnosi się do danych osobowych. Przez dane osobowe należy rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Zgodnie z RODO przez administratora rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Powyższa definicja wskazuje przede wszystkim na dwa konstytutywne elementy składające się na niniejsze zagadnienie, tj. ustalanie celów przetwarzania danych osobowych oraz ustalanie sposobów danych osobowych. Przykładowo, administratorem będzie pracodawca w odniesieniu do danych osobowych swoich pracowników lub przedsiębiorca w odniesieniu do danych osobowych swoich klientów.

Co do zasady, administrator może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu (tzw. procesorowi). Za podmiot przetwarzający uważa się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Co istotne, przetwarzając dane osobowe w imieniu administratora podmiot przetwarzający nie może realizować własnych celów przetwarzania danych osobowych. Dla przykładu, zlecenie czynności, które dotyczą przetwarzania danych osobowych może odnosić się do powierzenia archiwizacji, usług serwisowych systemów IT, usług chmurowych, czy zewnętrznych usług HR.

Mając na względzie powyższe podkreślamy jak ważne jest, aby dane osobowe były odpowiednio chronione, w szczególności zgodnie z postanowieniami RODO, które ma za zadanie zapewnić zachowanie wysokiego poziomu ochrony danych osobowych m.in. w związku z rozwojem technologicznym. Dlatego też postanowienia RODO nakładają na organizacje szereg obowiązków, w szczególności związanych z transparentnością, czy prawami osób, których dane osobowe są przetwarzane.

Zapraszamy do zapoznania się z całością publikacji, która w przystępny sposób omawia wybrane zagadnienia z zakresu regulacji dotyczących ochrony danych osobowych w codziennej działalności sektora e-commerce, jednocześnie zawierając wiele praktycznych wskazówek ułatwiających realizację tych wymogów, oraz przybliża zastosowanie prawa w praktyce i podpowiada, jak osiągnąć zgodność z regulacjami dotyczącymi ochrony danych osobowych w organizacji.

1. MARKETING W E-COMMERCE

Jednym z kluczowych aspektów prowadzenia działalności w formie sklepu internetowego jest skuteczny marketing swoich usług. Dzięki odpowiedniemu promowaniu przedsiębiorca może poszerzyć grono swoich klientów oraz szybciej dotrzeć do nich z przygotowaną ofertą. Z uwagi na specyfikę działalności e-commerce coraz większe znaczenie mają nowoczesne formy marketingu, dzięki którym można przekazywać komunikat promocyjny bezpośrednio poszczególnym jednostkom. Pozwalają one na lepsze dopasowanie oferty, trafniejszy wybór kręgu odbiorców oraz na szybki przekaz informacji, jednakże często wymagają pewnej ingerencji w prywatność użytkowników i mogą wiązać się z przetwarzaniem ich danych osobowych. Z uwagi na to, że wykorzystywanie danych w celach marketingowych pozwala administratorom na czerpanie z tego określonych zysków, powinno ono zostać zaplanowane szczególnie starannie, tak aby administrator mógł zapewnić, że nie dochodzi do naruszenia przepisów o ochronie danych osobowych.

Do najpopularniejszych środków marketingowych, przy których należy wziąć pod uwagę ochronę danych osobowych, można zaliczyć: newsletter, marketing telefoniczny (w tym SMS), organizowanie konkursów promocyjnych, a także reklamy behawioralne (dostosowywane do użytkownika).

1.1. Newsletter

1.1.1. Wprowadzenie

Newsletter to dodatkowa usługa świadczona na rzecz użytkowników przez różne podmioty działające w strefie internetowej, w tym sklepy internetowe. Polega

na cyklicznym przesyłaniu za pośrednictwem poczty elektronicznej określonych treści subskrybentom, tj. osobom, które dokonały zapisu na newsletter. W praktyce sklepów internetowych ten kanał komunikacji jest z reguły wykorzystywany do przekazywania informacji o nowych promocjach lub nowym asortymencie. Newsletter może też służyć budowaniu marki poprzez dzielenie się artykułami eksperckimi. Korzystanie z tej formy kontaktu z klientami można obecnie uznać za standard – tym bardziej istotne jest, aby takie rozwiązanie zostało wdrożone w sposób zgodny z prawem, zapewniający ochronę danych osobowych użytkowników.

1.1.2. Podstawa prawna

Uwagi ogólne

Przy każdej czynności przetwarzania administrator zobowiązany jest do ustalenia podstawy prawnej, na której opiera swoje działania. Katalog dopuszczalnych podstaw prawnych jest wskazany w art. 6 ust. 1 RODO (w odniesieniu do tzw. danych zwykłych) oraz w art. 9 ust. 2 RODO (w odniesieniu do tzw. danych wrażliwych). Przetwarzanie tzw. zwykłych danych osobowych jest zatem dopuszczalne (zgodne z prawem), gdy jest spełniony co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W przypadku danych wrażliwych ich przetwarzanie jest co do zasady zakazane, chyba że spełniony zostanie jeden z poniższych warunków:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach (chyba że przepisy prawa uniemożliwiają wyrażenie zgody);
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (jeżeli zezwala na to prawo lub porozumienie zbiorowe, a prawa podstawowe i interesy podmiotu danych są odpowiednio zabezpieczone);
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych (przy spełnieniu określonych warunków);
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego (pod warunkiem proporcjonalności celu i odpowiedniego zabezpieczenia praw podstawowych i interesów podmiotu danych);
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego (na podstawie przepisów prawa lub zgodnie z odpowiednią umową, z zastrzeżeniem odpowiednich warunków i zabezpieczeń);
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego (na podstawie przepisów prawa i przy zastosowaniu odpowiednich środków ochrony praw i wolności podmiotów danych);
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (pod warunkiem zgodności z prawem, proporcjonalności celu i odpowiedniego zabezpieczenia praw podstawowych i interesów podmiotu danych).

Przy ocenie podstawy prawnej przetwarzania danych osobowych w ramach newslettera początkowo przyjmiemy założenie, że w tym przypadku nie dochodzi do przetwarzania danych wrażliwych, a newsletter zawiera typowe treści marketingowe.

Prawnie uzasadniony interes

W zależności od ukształtowania treści i sposobu ich przekazywania w ramach newslettera usługę tę zazwyczaj oprzeć można albo na uzasadnionym interesie administratora danych lub innej osoby, albo na zgodzie podmiotu danych.

Prawnie uzasadniony interes jest niewątpliwie rozwiązaniem łatwiejszym do wdrożenia pod względem technicznym. W takim wypadku administrator jest jedynie zobowiązany do odpowiedniego poinformowania użytkowników o przetwarzaniu danych osobowych, jak również do zapewnienia możliwości wniesienia sprzeciwu. Należy jednak wskazać, że konieczne jest dokładne określenie, na czym polega prawnie uzasadniony interes oraz do kogo należy go odnosić (do administratora czy do innego podmiotu, a jeśli tak – to jakiego). Zgodnie z motywem 47 RODO taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Istotne jest też, że w przypadku planów oparcia danego procesu na prawnie uzasadnionym interesie, należy każdorazowo przeprowadzić tzw. „test równowagi", tj. przeprowadzić ocenę, czy określony prawnie uzasadniony interes jest nadrzędny wobec interesów i praw podstawowych osoby, której dane dotyczą. Przy ocenie należy wziąć pod uwagę to, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Co więcej, zgodnie z zasadą rozliczalności administrator powinien być w stanie wykazać, że przeprowadził taki test i na jego podstawie zdecydował, że prawnie uzasadniony interes będzie odpowiednią podstawą do przetwarzania danych osobowych.

Biorąc pod uwagę, że skorzystanie z newslettera wymaga zapisu i wiadomości są wysyłane wyłącznie do tych osób, które zgłoszą takie zapotrzebowanie, można stwierdzić, że użytkownicy sklepu internetowego, którzy decydują się skorzystać z usługi newslettera, mogą spodziewać się, że w tym celu nastąpi przetwarzanie ich danych osobowych. Co więcej, są to klienci sklepu lub osoby zainteresowane jego ofertą, więc istnieje tu wyraźny łącznik między tymi osobami a administratorem danych osobowych.

Dodatkowo motyw 47 RODO wyraźnie wskazuje, że za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego. Pozostają zatem do rozstrzygnięcia

dwie kwestie: czym jest marketing bezpośredni oraz czyich towarów lub usług ma on dotyczyć.

Ani RODO, ani polskie przepisy nie zawierają definicji legalnej marketingu bezpośredniego. Próby dookreślenia tego pojęcia podejmuje doktryna. Można więc uznać, że z perspektywy prawa ochrony danych osobowych za działania w zakresie marketingu bezpośredniego uznaje się natomiast wszelkie działania promujące produkty lub usługi, które skierowane są do osoby, której dotyczą dane osobowe, wykorzystywane w celu prowadzenia tej formy marketingu[1]. Zaliczenie formy newslettera do kategorii działań podejmowanych w celu marketingu bezpośredniego nie budzi raczej wątpliwości w praktyce – jest to bowiem kierowanie przygotowanej przez administratora oferty bezpośrednio na wskazany adres e-mail użytkownika.

Przytoczony powyżej motyw 47 RODO jako przykład prawnie uzasadnionego interesu podaje marketing bezpośredni, jednak nie odnosi go do żadnego konkretnego podmiotu (np. administratora). Często słyszy się o prawnie uzasadnionym interesie, jakim jest marketing własnych produktów i usług. Warto to jednak skonfrontować z treścią art. 6 ust. 1 lit f RODO, zgodnie z którym przetwarzanie jest zgodne z prawem, jeżeli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych. Wynika z tego, że administrator może legalnie przetwarzać dane osobowe również wtedy, gdy uzasadniony interes prawny ma ku temu inny podmiot. Przenosząc to na grunt sklepów internetowych i marketingu wydaje się, że na tej podstawie mogą być promowane również produkty i usługi partnerów biznesowych podmiotu prowadzącego sklep internetowy. Przygotowany newsletter mógłby zatem zawierać bezpośrednio ofertę sklepu, jak i innych podmiotów, mających ze sklepem biznesową relację, co może być bardzo istotne z praktycznego punktu widzenia. Należy przy tym poczynić bardzo ważne zastrzeżenie – w omawianej sytuacji podmiot trzeci nie ma żadnego władztwa nad danymi osobowymi użytkowników newslettera. Nie ma do nich dostępu, nie przygotowuje wiadomości samodzielnie. Dostarcza jedynie treści administratorowi, który zobowiązuje się je umieścić w przygotowywanym materiale marketingowym. Nie dochodzi więc jest udostępnienia danych osobowych podmiotowi trzeciemu, który mógłby samodzielnie z nich korzystać (np. poprzez dołączenie do swojej listy mailingowej).

[1] Artykuł 21, Nb 8 [w:] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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 ochronie danych). Komentarz, red. P. Litwiński, 2021, wyd. 1, Legalis.

Takie udostępnienie wymagałoby wyraźnego poinformowania użytkowników oraz uzyskania ich zgody.

Czasem bywa prezentowany pogląd, zgodnie z którym działania marketingowe na rzecz innego podmiotu wymagają zgody, podczas gdy marketing bezpośredni własnych produktów i usług może być prowadzony na podstawie prawnie uzasadnionego interesu. W ocenie autorki nie jest to jednak pogląd właściwy. Jeżeli są zatem spełnione przesłanki uzasadnionego interesu prawnego, będzie to wystarczająca podstawa prawna do przetwarzania danych osobowych. Niejednokrotnie zdarza się przecież, że w ramach jednego przekazu marketingowego sklep przekazuje oferty swoich parterów handlowych lub podmiotów powiązanych. Należy jednak zwrócić uwagę, że w sytuacji, gdy newsletter obejmuje też marketing bezpośredni produktów i usług podmiotów trzecich, test równowagi powinien zostać przeprowadzony szczególnie starannie. Wydaje się, że prezentowany pogląd to pozostałość po nieobowiązującej już ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która w art. 23 ust. 4 stanowiła, że za prawnie uzasadniony interes administratora należy uznać marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej. Zwracamy uwagę, że przepisy RODO nie zawierają już słowa „własnych" w odniesieniu do produktów lub usług.

Dane wrażliwe

Może się zdarzyć, że w celu wykonania usługi newslettera administrator będzie przetwarzał tzw. dane wrażliwe. Do tej kategorii danych osobowych art. 9 ust. 1 RODO zalicza dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Do przetwarzania takich danych osobowych może dojść w szczególności w sytuacji tych sklepów internetowych, które oferują szczególny rodzaj asortymentu – np. urządzenia medyczne bądź leki. Takie podmioty, chcące dopasować ofertę handlową zawartą w newsletterach do potrzeb poszczególnych grup odbiorców, mogą prosić ich o podanie pewnych informacji, aby możliwe było ich odpowiednie zakwalifikowanie za pomocą określonego kryterium zdrowotnego. Jeśli użytkownik przy zapisie na newsletter wskazuje, że cierpi na określone schorzenia, dochodzi do przetwarzania danych dotyczących zdrowia. Są to bowiem dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. W takim przypadku inaczej kształtują się dopuszczalne podstawy prawne

takiego przetwarzania danych osobowych. Nie ma wówczas możliwości oparcia przetwarzania danych na uzasadnionym interesie prawnym – konieczne będzie uzyskanie zgody podmiotu danych na podjęcie takich czynności. W ujęciu praktycznym będzie oznaczało to, że użytkownik ujawniający dodatkowe dane (należące do kategorii danych wrażliwych) będzie musiał wyrazić aktywną zgodę, spełniającą wymogi RODO, a więc np. zaznaczyć dodatkowy checkbox.

Jak widać, przetwarzanie danych należących do kategorii danych osobowych wrażliwych wpływa na sposób, a w jaki możliwe jest rozpoczęcie świadczenia usługi newslettera. Dokonując więc analizy, jaka forma wdrożenia będzie w danym przypadku odpowiednia, należy zweryfikować, jakie dane osobowe użytkowników są zbierane i czy administrator nie przetwarza również danych szczególnej kategorii. Dodatkowo należy wspomnieć, że sam fakt sprzedawania określonych produktów (np. leków, dewocjonaliów) nie przesądza jeszcze o tym, że handlujący nimi przedsiębiorca jest administratorem danych przetwarzającym szczególne kategorie danych osobowych (odpowiednio – dane dotyczące zdrowia, przekonania religijne)[2]. W takim przypadku należy jednak szczególnie starannie przeanalizować, czy może dochodzić do zbierania oraz dalszego przetwarzania takich danych (np. w przypadku powtarzających się zakupów określonych produktów, np. konkretnego leku), jak również tak zaprojektować system informatyczny, aby minimalizować ryzyko zbierania takich danych (o ile nie są one administratorowi konieczne).

W przypadku uznania, że będą gromadzone dane szczególnej kategorii (np. dane dotyczące zdrowia), należy zapewnić użytkownikowi możliwość wyrażenia odrębnej, wyraźnej zgody na przetwarzanie tych danych w celach marketingowych. W przypadku braku zgody użytkownik może mieć możliwość zapisania się na newsletter, ale bez spersonalizowanych treści, zatem ewentualne podanie określonych danych w formularzu przed udzieleniem zgody nie powinno zostać zapamiętane w systemie.

Zwracamy uwagę, że prawidłowo zebrana zgoda powinna mieć cechy określone w RODO, tj. być dobrowolna, konkretna, świadoma i jednoznaczna. Oznacza to, że użytkownik powinien podjąć decyzję zgodną ze swoją wolę, być poinformowany o okolicznościach związanych z przetwarzaniem jego danych osobowych oraz wyrażać zgodę na konkretne cele przetwarzania danych.

[2] por. B. Kaczmarek – Templin, RODO w e-commerce, red. D. Lubasz, 2018, s. 105–106.

1.1.3. Zakres danych i cele przetwarzania

W każdym procesie przetwarzania danych osobowych należy uwzględnić wszystkie zasady wynikające z RODO, w tym zasadę ograniczenia celu i zasadę adekwatności (szerzej o zasadach przetwarzania danych osobowych piszemy w rozdziale 5.).

Zasada ograniczenia celu oznacza, że administrator z góry określa cele przetwarzania danych osobowych. W omawianym przypadku będzie to wysyłka newslettera. Administrator nie może więc swobodnie wykorzystywać posiadanych danych osobowych w innych celach, bez podjęcia dodatkowych działań (poinformowania podmiotów danych i uzyskania ich zgody, jeśli będzie ona wymagana w danym przypadku). Oznacza to, że jeżeli dane osobowe zbierane są przez podmiot A na cele wysyłki newslettera, dane te nie mogą zostać wykorzystane np. do przekazania innemu podmiotowi lub kierowania do użytkownika innego rodzaju korespondencji.

Z kolei zgodnie z zasadą minimalizacji danych dopuszczalne jest przetwarzanie tylko takich danych osobowych, które są niezbędne do osiągnięcia określonego celu. Administrator powinien przetwarzać jak najmniej danych – tylko tyle, ile rzeczywiście potrzebuje. W przypadku usługi newslettera niewątpliwie niezbędny będzie adres poczty elektronicznej, który ma zostać dodany do bazy newslettera. Często spotyka się również pole do wskazania imienia, jak również możliwość wyboru przez użytkownika interesujących go zagadnień, grupy wiekowej itp., co pozwala na dopasowanie treści newslettera. Zakres przetwarzanych danych może być uzależnionych od konkretnych warunków biznesowych. Każdorazowo należy wiec zastanowić się, do czego są nam potrzebne określone dane osobowe i czy są one rzeczywiście niezbędne. Administrator jest zobowiązany do przeprowadzenia odpowiedniej analizy i dokonania oceny, czy dla jego potrzeb biznesowych niezbędne jest zbieranie danych w zakresie szerszym niż adres e-mail bądź imię. Należy przy tym zauważyć, że przetwarzanie szerszego zakresu danych musi być odpowiednio uzasadnione, a obowiązek wykazania, że są one niezbędne i zasada minimalizacji danych nie została złamana, ciąży zawsze na administratorze danych osobowych (zgodnie z zasadą rozliczalności).

1.1.4. Formy zapisu na newsletter

Możliwe są różne sposoby zapisu na newsletter, tzw. opt-in oraz double opt-in. Różnią się one technicznym sposobem dokonania zapisu, jednak ma to również swoje konsekwencje prawne.

Zapis typu opt-in polega na tym, że użytkownik musi podjąć wyraźną aktywność zmierzającą do wyrażenia chęci skorzystania z usługi newslettera

– np. wypełnienie i zatwierdzenie odpowiedniego formularza. Bezpośrednio po skutecznym podjęciu tej czynności użytkownik może już korzystać z newslettera – nie są wymagane kolejne kroki. Z kolei konstrukcja double opt-in przewiduje, że po podjęciu tej pierwszej aktywności użytkownik musi dokonać jeszcze jej potwierdzenia. W tym celu otrzymuje wiadomość e-mail, zawierającą z reguły link aktywacyjny, który należy kliknąć, aby sfinalizować zapis na newsletter. Dopiero wówczas użytkownik może zacząć otrzymywać wiadomości w ramach newslettera.

Najważniejszym plusem pierwszej metody jest łatwość i szybkość zapisu przez użytkownika. W przypadku użycia metody double opt-in użytkownik musi wykazać większe zaangażowanie, w związku z czym istnieje ryzyko, że nie podejmie dalszych działań potwierdzających i finalnie nie zapisze się na subskrypcję newslettera, co jest oczywiście skutkiem niepożądanym z perspektywy interesów sklepu internetowego, któremu zależy na jak najszerszym kręgu odbiorców. Z drugiej strony, dzięki double opt-in administrator ma pewność, że osoba, która zdecydowała się skorzystać z usługi newslettera, podejmuje tę decyzję świadomie. Co więcej, jednocześnie potwierdzony zostaje adres e-mail, co daje dwie korzyści: pewność, że adres e-mail jest prawidłowy (eliminuje to problem „pustych" adresów znajdujących się na liście mailingowej przygotowanej do wysyłki newslettera) oraz pewność, że zapisu powiązanego z konkretnym adresem e-mail dokonał właściciel tegoż adresu (mamy więc niejako potwierdzenie tożsamości użytkownika).

Zwracamy uwagę, że stosowaną wcześniej zasadą był zapis typu opt-out, polegający na tym, że do danego użytkownika można kierować treści marketingowe tak długo, jak nie wyrazi on sprzeciwu (w każdym komunikacie należało go informować o tym uprawnianiu). Na gruncie prawa europejskiego[3] kwestia ochrony użytkowników ewoluowała i ostatecznie przyjęto zasadę, że dla poczty elektronicznej (rozumianej szeroko, co obejmuje również np. wiadomości SMS/MMS) oraz automatycznych systemów wywołujących (zakres tego pojęcia jest sporny) powinna obowiązywać zasada opt-in, podczas gdy dla pozostałych form marketingu (w praktyce – połączeń głosowych, czyli telemarketingu) wybór należy do poszczególnych państw członkowskich UE i ich krajowego ustawodawstwa.

Zastosowanie modelu doble opt-in nie jest zatem wymogiem prawnym i pozostaje w sferze decyzji biznesowej każdego administratora. Niemniej jednak cechy tego modelu mogą okazać się pomocne dla wykazania zgodności z obowiązującymi przepisami i zapewnić lepszą kontrolę nad posiadaną bazą danych subskrybentów newslettera.

[3] Dyrektywa o prywatności i łączności elektronicznej.