POLSKIE STOWARZYSZENIE MARKETINGU
POLISH MARKETING ASSOCIATION

Kodeks postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego (KODO)

Maj 2018

SPIS TREŚCI

WPROWADZENIE

1. Deklaracja

Mając na względzie, że dane osobowe stanowią jedno z najważniejszych dóbr osobistych oraz że rozwój technologii umożliwia coraz szybsze i bardziej kompleksowe posługiwanie się nimi, organizacje wykorzystujące w swojej działalności narzędzia marketingu bezpośredniego sygnujące niniejszy Kodeks uznają potrzebę porządkowania kwestii dotyczących wykorzystywania danych osobowych zgodnie z obowiązującymi zasadami prawa i najlepszymi praktykami rynkowymi w celu zapewnienia bezpieczeństwa podmiotom tych danych.

2. Cel ustanowienia Kodeksu

Niniejszy Kodeks stanowi uzupełnienie istniejących regulacji prawnych w zakresie ochrony danych osobowych i ma na celu ich doprecyzowanie, a także wskazanie najlepszych praktyk rynkowych w zakresie ich przetwarzania zgodnie z przepisami prawa i zasadami etyki.

Kodeks nie jest jedynie zbiorem sugerowanych rozwiązań i wytycznych, ale stanowi zbiór wartości i zasad, którymi kierują się organizacje wykorzystujące marketing bezpośredni . Podstawowymi zasadami działania organizacji, które przystąpiły do Kodeksu są etyka i rzetelność w przestrzeganiu zasad ochrony danych osobowych oraz prywatności konsumentów.

Przestrzeganie Kodeksu ma służyć budowie zaufania między konsumentem a kontaktującą się z nim organizacją i budowie dobrego wizerunku branży marketingu bezpośredniego. Stosowanie jego zapisów przez podmioty działające na rynku ma na celu podniesienie satysfakcji konsumentów z kontaktów realizowanych za pośrednictwem tej drogi komunikacji. Rezultatem przestrzegania najwyższych norm i standardów przez przedsiębiorców jest zwiększanie skuteczności wykorzystania marketingu bezpośredniego z korzyścią zarówno dla konsumentów, jak i organizacji korzystających z tych narzędzi.

3. Interesariusze

Niniejszy Kodeks adresowany jest w szczególności do członków Polskiego Stowarzyszenia Marketingu SMB oraz do wszelkich podmiotów, które na podstawie dobrowolnej deklaracji przystąpiły do stosowania Kodeksu. Kodeks ma również istotne znaczenie dla pozostałych przedsiębiorstw prowadzących działalność marketingową (na własną rzecz lub na rzecz zleceniodawcy), jako że może służyć jako źródło komplementarnej wiedzy o obowiązujących regulacjach w marketingu bezpośrednim oraz o zasadach ich właściwego i etycznego stosowania. Wreszcie Kodeks może stanowić ciekawe źródło wiedzy dla konsumentów i wszelkich innych osób, których dane osobowe są lub mogą być przetwarzane w celach marketingowych – pozwoli on zrozumieć, jakie dokładnie prawa przysługują tym osobom oraz w jaki sposób te prawa mogą być egzekwowane.

4. Słownik pojęć

W niniejszym kodeksie zastosowanie mają pojęcia, których definicje zawiera Załącznik 1.

ZBIERANIE DANYCH

1. Zakres i cel zbieranych danych

Zasady określania zakresu zbieranych danych w stosunku do celu

Zbierając dane osobowe, Administrator każdorazowo powinien z góry określić zakres danych, które zbiera (np. tylko imię, nazwisko i adres zamieszkania, albo numer telefonu, adres e-mail, numer PESEL, dane o stanie zdrowia, dane geolokalizacyjne itd.). Metodologia określenia zakresu pozostawiona jest każdorazowo swobodnej decyzji Administratora, niemniej każdorazowo Administrator powinien móc w sposób jasny i czytelny wykazać, że ustalony finalnie zakres jest adekwatny do celu, w jakim dane są zbierane.

Adekwatność w stosunku do celu oznacza, że Administrator zbiera tylko takie dane, które są rzeczywiście (w praktyce) niezbędne do realizacji zamierzonego celu przetwarzania. Mając na uwadze, że w praktyce stosowania określonych rozwiązań zakres danych dla tego samego celu może się zmieniać (zawężać lub rozszerzać), Administrator powinien dokonywać okresowej weryfikacji celowości zbierania zakresu danych osobowych.

W przypadku zbierania danych osobowych dla celów marketingowych uznaje się, że większość danych osobowych o klientach lub potencjalnych klientach może być adekwatna do celu marketingowego. Uzasadnione jest to dążeniem do przedstawienia klientowi lub potencjalnemu klientowi rozwiązania, oferty, która go rzeczywiście może zainteresować. Podmiot zbierający dane dla celów marketingowych powinien każdorazowo określić, jakie dane osobowe są niezbędne dla sprzedaży i promowania produktów lub usług.

Przykład: podczas zbierania danych osobowych w celu promocji przekąsek adekwatny dane zakres to : imię, nazwisko, adres zamieszkania, numer telefonu, adres e-mail, preferencje żywieniowe, sposób spędzania wolnego czasu, wykonywany zawód, data urodzenia i in. Jednocześnie w tym zakresie nieadekwatne do celu będzie zbieranie danych takich jak numer PESEL, skan/numer dowodu tożsamości, dane dotyczące przekonań religijnych, politycznych itp.

Wymaga podkreślenia, że w każdym przypadku przetwarzania danych w celach marketingowych ma miejsce przetwarzanie danych osobowych. Należy sprostować występujący niekiedy pogląd, że o ile przedsiębiorca nie wyodrębnił w swojej strukturze odrębnego zbioru danych dla celów marketingowych, to nie zbiera/nie przetwarza danych w tych celach. Przetwarzanie danych osobowych w celach marketingowych może być realizowane również wobec danych zawartych np. w zbiorze klientów, kontrahentów, czy też nawet pracowników. Istotne jest to, jakie operacje i w jakich celach są realizowane na danych osobowych, a nie ich struktura.

Zasady przetwarzania danych osobowych wrażliwych

Dane osobowe wrażliwe to szczególna kategoria danych. Są to dane osobowe, które z racji swego charakteru są szczególnie chronione w świetle podstawowych praw i wolności. Przepisy prawa nie przewidują ich zamkniętego katalogu i każdorazowo administrator powinien dokonać samodzielnej weryfikacji, czy zbierane lub posiadane dane osobowe mogą być uznane za wrażliwe. Należy uznać, że kategoria wrażliwości poszczególnych danych osobowych może zmieniać się w czasie wraz z rozwojem społeczeństwa informacyjnego. Administratorzy danych powinni

okresowo weryfikować, czy posiadane przez nich dane w określonym zakresie nie zaczęły być traktowane jako dane wrażliwe lub czy nie utraciły takiego charakteru.

Do kategorii danych osobowych wrażliwych zaliczyć można w szczególności:

1. pochodzenie rasowe i etniczne
2. przekonania polityczne
3. przekonania religijne lub światopoglądowe
4. informacje o stanie zdrowia
5. dane biometryczne
6. życie seksualne.

Przetwarzanie danych wrażliwych dla celów marketingowych jest możliwe pod warunkiem uzyskania uprzedniej wyraźnej zgody osoby, której dane dotyczą. Przetwarzanie takich danych może być uzasadnione (w ramach reguły adekwatności) na potrzeby promocji produktów lub usług, które są w jakiś sposób powiązane z danymi wrażliwymi osoby (np. przekonania religijne lub światopoglądowe w ramach promocji publikacji o określonej tematyce; przekonania polityczne w celu tworzenia komunikatów promujących określoną aktywność społeczną).

W tym miejscu dla usunięcia wątpliwości wskazuje się, że następujące działania na danych podejmowane w celach marketingowych nie stanowią przetwarzania danych wrażliwych:

1. przetwarzanie zdjęcia osoby lub potencjalnego klienta w celu np. rozpoznania go na potrzeby programu promocyjnego lub zaproponowania dostosowanej linii kosmetyków,
2. przetwarzanie danych o zakupionych wcześniej lub o obserwowanych w sieci produktach, czy usługach w celu przedstawienia klientowi lub potencjalnemu klientowi dostosowanej oferty sprzedaży (np. sprzedaż leków, usług medycznych, sprzedaż książek o określonej tematyce),
3. dane pochodzące z aktywności w sieci i wnioskowanie z nich,
4. zbieranie odpowiedzi na pytania w quizach, zbieranie danych podawanych w związku z udziałem w promocjach i programach lojalnościowych.

2. Podstawa prawna i faktyczna zbierania danych

Dane osobowe mogą być zbierane bezpośrednio przez Administratora lub za pośrednictwem Podmiotu Przetwarzającego, z którym Administrator zawarł umowę powierzenia przetwarzania danych, uwzględniającą m.in. zbieranie danych osobowych na rzecz Administratora.

W każdym przypadku zbierania danych osobowych Administrator lub odpowiednio Podmiot Przetwarzający powinni zapewnić, aby zbieranie to odbywało się na podstawie jednej z następujących przesłanek prawnych:

1. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. 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;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

6. 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.

Podstawą zbierania danych osobowych w celach marketingowych w przeważającej części przypadków będą: zgoda osoby, której dane dotyczą (ad. 1) oraz uzasadnione interesy administratora lub strony trzeciej (ad. 6). Nie budzi wątpliwości, że marketing produktów, usług lub generalnie działalności przedsiębiorstw i organizacji będących administratorami danych, jest niezbędnie konieczny dla rozwoju gospodarki.

Pomiędzy podstawami prawnymi przetwarzania danych osobowych dla celów marketingowych, jakimi są „zgoda" i „uzasadniony interes" nie czyni się rozróżnienia – żadna z tych podstaw nie ma charakteru preferowanego. W szczególności uznaje się, że pozyskanie wszelkich danych osobowych przy okazji oferowania lub dystrybucji produktów lub usług, prowadzenia akcji promocyjnych, portali internetowych, usług newsletter, ankiet satysfakcji klienta lub tym podobne, wiąże się w sposób bezpośredni i nierozerwalny z prowadzeniem działalności marketingowej Administratora wśród swoich klientów i potencjalnych klientów.

Jednocześnie należy podkreślić, że jeżeli Administrator zdecydował się wystąpić o zgodę na przetwarzanie danych osobowych w celach marketingowych i osoba fizyczna będąca konsumentem takiej zgody nie wyraziła, to następnie Administrator nie ma już prawa pozyskanych przy tym kontakcie danych osobowych przetwarzać dla celów marketingowych, powołując się na uzasadniony interes Administratora.

Zgoda jako wyłączna przesłanka zbierania i przetwarzania danych osobowych dla celów marketingowych jest wymagana dla szczególnych przypadków, w których Administrator nie może zasadnie powołać się na „uzasadniony interes". Dotyczy to w szczególności zbierania danych osobowych uznawanych za wrażliwe. Przykładowo - w sytuacji, w której Administrator oferuje towary lub usługi, dla których dane wrażliwe muszą być przetwarzane (np. dane genetyczne, szczegółowe informacje o stanie zdrowia), zbieranie takich danych i następnie wykorzystywanie ich dla celów marketingowych musi być poprzedzone uzyskaniem odrębnej zgody na takie wykorzystanie.

W Polsce szczególnym rodzajem danych są dane osobowe osób fizycznych prowadzących działalność gospodarczą, których dane osobowe są publicznie ujawnione m.in. w Centralnej Ewidencji i Informacji o Działalności Gospodarczej. Dane te mogą być zbierane przez Administratorów bezpośrednio z publicznie dostępnych rejestrów w celu ich wykorzystania dla potrzeb marketingowych lub w celu ich dalszej dystrybucji z powołaniem na „uzasadniony interes" administratora danych.

3. Pozyskiwanie danych ze źródeł zewnętrznych

Administrator obok uzyskania danych bezpośrednio od osoby, której dane dotyczą, może wejść w sposób legalny w posiadanie danych o określonej osobie do wykorzystania w celach marketingowych w szczególności poprzez:

- uzyskanie danych od innych Administratorów, którzy w ramach swojej działalności są uprawnieni do udostępniania posiadanych danych podmiotom trzecim dla określonych celów;

- uzyskanie danych z publicznie dostępnych źródeł, w tym opublikowanych w związku ze świadczeniem usług społeczeństwa informacyjnego;
- uzyskanie danych o osobie od innej osoby fizycznej, niebędącej Administratorem ani Podmiotem Przetwarzającym.

Uzyskanie danych osobowych od innego Administratora jest legalne pod warunkiem, że Administrator ten pozyskał dane zgodnie z prawem i wypełnił wszelkie przewidziane prawem obowiązki dla zgodnego z prawem udostępnienia danych innemu podmiotowi. Najpóźniej bezpośrednio przed otrzymaniem danych od innego Administratora należy dokonać niezbędnej analizy, czy Administrator uzyskał dane i dokonuje ich udostępnienia zgodnie z prawem. Analiza taka może polegać na dokonaniu sprawdzenia określonej próby rekordów z bazy, która ma zostać przekazana. Analizę może zastąpić:

a) powołanie się przez udostępniającego na fakt, że uzyskał on certyfikację lub jest sygnatariuszem kodeksu postępowania w rozumieniu art. 40 RODO,

b) w przypadku danych osobowych przedsiębiorców, w tym osób fizycznych prowadzących działalność gospodarczą – z uwagi na ich powszechną dostępność – wystarczające będzie uzyskanie od udostępniającego oświadczenia potwierdzającego legalność posiadania i udostępniania danych.

4. Obowiązek informacyjny

Przepisy RODO w art. 13, 14 oraz 21 ust. 4 przewidują szczegółowe informacje, które powinny być przekazywane osobom, których dane dotyczą. Obowiązek ten należy wypełnić wobec wszystkich konsumentów, których dane są zbierane.

Zgodnie z art. 12 RODO stosowne informacje powinny być podane zainteresowanym osobom w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Jednocześnie art. 13, 14 oraz 21 ust. 4 RODO przewidują bardzo szeroki katalog szczegółowych informacji, który ma zostać przekazany osobom, których dane dotyczą. W konsekwencji Administratorzy powinni bardzo starannie dobierać sposób przekazywania informacji, tak aby wypełniać oba powyższe, potencjalnie wzajemnie wykluczające się cele.

Jeżeli do domeny publicznej wejdą do powszechnego użytku oznaczenia graficzne stanowiące samodzielną formę przekazywania osobom niezbędnych informacji, Administrator powinien w miarę możliwości korzystać z tego rodzaju oznaczeń.

Do czasu wypracowania takich oznaczeń oraz tam, gdzie nie jest to uzasadnione, proponuje się, aby Administratorzy wypełniali obowiązek administracyjny w sposób opisany poniżej dla poszczególnych źródeł uzyskiwania danych o osobie.

Obowiązek informacyjny dla danych pozyskanych za pośrednictwem Internetu

W przypadku zbierania danych osobowych konsumentów przez Internet, gdzie osoba, której dane dotyczą, przekazuje swoje dane za pośrednictwem urządzenia końcowego (np. komputer, tablet, smartfon), obowiązek informacyjny powinien zostać zrealizowany z uwzględnieniem najlepszych praktyk oraz z uwzględnieniem Wytycznych Grupy Roboczej ds. art. 29 nr WP259 oraz WP260. Sugeruje się realizowanie obowiązku informacyjnego w następujący sposób:

1. Jeżeli w ramach formularza wyrażana jest jakakolwiek zgoda w rozumieniu art. 6 ust. 1 lit. a) RODO, lub zgoda na komunikację handlową, to zgoda taka powinna zostać poprzedzona co najmniej następującymi informacjami, dostępnymi w pierwszej warstwie tekstu:
   a) kto jest administratorem danych osobowych
   b) jaki jest cel przetwarzania danych
   c) jakie rodzaje danych będą zbierane i przetwarzane
   d) informacja o prawie do cofnięcia zgody ze wskazaniem, jak można takie cofnięcie wykonać
   e) informacje o wykorzystywaniu danych do podejmowania decyzji opartych wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, które to decyzje mogą mieć istotny skutek dla osoby fizycznej (warunkowo - jeżeli taki proces występuje)
   f) informacje o transferze danych do państwa trzeciego (warunkowo - jeżeli występuje; państwo trzecie to państwo leżące poza terytorium Europejskiego Obszaru Gospodarczego).
2. Pozostała część klauzuli informacyjnej może być dostępna odrębnie, z wykorzystaniem następujących rozwiązań:
   - poniżej formularza danych osobowych, który podlega wypełnieniu, a powyżej ikony akceptacji formularza - w formie rozwijanej klauzuli informacyjnej, która nosi tytuł np. „Informacje o danych osobowych", po najechaniu na którą lub po kliknięciu której użytkownikowi Internetu wyświetlana jest pełna treść informacji dotyczącej danych osobowych;
   - klauzula informacyjna lub jej część może znajdować się w tzw. drugiej i trzeciej warstwie – np. na odrębnej podstronie www, do której prowadzi co najmniej wyraźnie wyodrębniony link zawarty poniżej pól formularza (widoczny powyżej ikony akceptacji formularza);
   - pełna klauzula informacyjna może znajdować się w całości poniżej formularza danych osobowych, który podlega wypełnieniu, a powyżej ikony akceptacji formularza - w formie zwykłego tekstu, z którym użytkownik Internetu może się swobodnie zapoznać.

Przykład: na stronie www występuje formularz zapisania rejestracji w portalu ze zgodą na przesyłanie informacji handlowych drogą elektroniczną. Poniżej pól formularza, które wypełnia użytkownik, znajdują się informacje o tym: (a) kto jest administratorem danych osobowych, (b) jaki jest cel przetwarzania danych, (c) jakie rodzaje danych będą zbierane i przetwarzane, (d) informacja o prawie do cofnięcia zgody ze wskazaniem, jak można takie cofnięcie wykonać (nie ma tu informacji o udostępnianiu danych do państwa trzeciego ani o automatycznym podejmowaniu decyzji, bo takie procesy nie występują). Poniżej tej treści znajduje się klauzula zgody na przesyłanie informacji handlowej drogą elektroniczną, która wymaga wyraźnego zaznaczenia. Poniżej klauzuli zgody znajduje się zdanie „Informacja o tym, jak przetwarzamy Twoje dane". Po kliknięciu w nią użytkownikowi wyświetla się rozszerzona treść klauzuli informacyjnej zawierająca szereg dodatkowych informacji. Jednocześnie w ramach tej informacji mogą występować dalsze odesłania do innych stron, dokumentów, zawierających już bardzo precyzyjne informacje (np. pełny katalog odbiorców danych). Ikona akceptacji formularza znajduje się poniżej ww. klauzul i informacji.

3. W zakresie dyrektywy technicznej klauzuli informacyjnej, dla zapewnienia prawidłowej formy tej klauzuli:

- tekst klauzuli informacyjnej powinien być pisany czcionką nie mniejszą niż 6p, najlepiej czcionką bezszeryfową;
- język klauzuli informacyjnej powinien być możliwie najprostszy i jasny. Sugerowane jest korzystanie z prostych i krótkich podpunktów oraz posługiwanie się zdaniami prostymi. Tam, gdzie to możliwe i nie wprowadza w błąd, sugerowane jest posługiwanie się językiem potocznym, codziennym.

Obowiązek informacyjny dla danych pozyskanych za pośrednictwem telefonu

Wypełniając obowiązek informacyjny w rozmowie telefonicznej, należy przekazywać informacje rozmówcy w sposób wyraźny, w prostej i zwięzłej formie, w miarę możliwości codziennym językiem (o ile nie będzie to wprowadzało w błąd).

Jeżeli za pośrednictwem telefonu zbierana jest od rozmówcy zgoda w rozumieniu art. 6 ust. 1 lit. a) RODO lub zgoda na komunikację handlową, takiemu rozmówcy jeszcze przed wyrażeniem przez niego zgody należy podać z własnej inicjatywy co najmniej następujące informacje:

a) kto jest administratorem danych osobowych

b) jaki jest cel przetwarzania danych

c) jakie rodzaje danych będą zbierane i przetwarzane

d) prawo do cofnięcia zgody ze wskazaniem, jak można takie cofnięcie wykonać

e) informacje o wykorzystywaniu danych do podejmowania decyzji opartych wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, które to decyzje mogą mieć istotny skutek dla rozmówcy (warunkowo - jeżeli taki proces występuje)

f) informacje o transferze danych do państwa trzeciego (warunkowo - jeżeli występuje; państwo trzecie to państwo leżące poza terytorium Europejskiego Obszaru Gospodarczego).

Dopiero po przekazaniu tych informacji można uznawać, że następująca po tych informacjach zgoda rozmówcy zostaje udzielona w warunkach dostatecznego poinformowania (jest „świadoma").

Jeżeli rozmówca zaakceptuje takie rozwiązanie, pozostała treść obowiązku informacyjnego, który wynika z art. 13 RODO, może zostać przekazana poprzez przesłanie na adres e-mail rozmówcy pełnej klauzuli informacyjnej w formie elektronicznej (np. TXT, PDF) już po zakończeniu rozmowy lub podanie w trakcie rozmowy adresu strony www, na której rozmówca może zapoznać się z obowiązkiem informacyjnym.

W przypadku, gdy obowiązek informacyjny na życzenie rozmówcy w całości został spełniony w toku rozmowy telefonicznej, dobrą praktyką jest przesłanie dokumentu zawierającego klauzulę informacyjną na adres e-mail rozmówcy (o ile adres ten jest znany Administratorowi).

Przesłanie klauzuli informacyjnej nie stanowi komunikacji handlowej w rozumieniu art. 172 Prawa telekomunikacyjnego i art. 10 UŚUDE i tym samym jej przesłanie nie wymaga uzyskania odrębnej zgody podmiotu danych.

Obowiązek informacyjny dla danych pozyskanych pisemnie

W przypadku, gdy dane pozyskiwane są w formie pisemnej za pomocą formularza, którego wydawcą jest Administrator, formularz lub załącznik do formularza powinien posiadać stosowną klauzulę informacyjną.

W przypadku, gdy dane przekazane są bezpośrednio przez daną osobę na innym druku/na kartce (np. przesłanie reklamacji), obowiązek informacyjny powinien zostać spełniony najpóźniej przy składaniu osobie odpowiedzi na jej pismo. Obowiązek ten może zostać spełniony poprzez przesłanie pocztą tradycyjną lub pocztą elektroniczną dokumentu zawierającego klauzulę informacyjną.

Klauzula informacyjna, o której mowa w niniejszej części, powinna spełniać co najmniej następujące warunki co do formy:

- tekst klauzuli informacyjnej powinien być pisany czcionką nie mniejszą niż 6p, najlepiej czcionką bezszeryfową;
- język klauzuli informacyjnej powinien być możliwie najprostszy i jasny. Sugerowane jest korzystanie z prostych i krótkich podpunktów oraz posługiwanie się zdaniami prostymi. Tam, gdzie to możliwe i nie wprowadza w błąd, sugerowane jest posługiwanie się językiem potocznym, codziennym.

Obowiązek informacyjny dla danych pozyskanych w bezpośrednim kontakcie

W przypadku zbierania danych osobowych w relacji bezpośredniej (ustnej) klauzula informacyjna powinna zostać przedstawiona danej osobie w formie pisemnej (papierowej), a potwierdzeniem dokonania tej czynności powinno być podpisanie przez daną osobę egzemplarza klauzuli do akt podmiotu zbierającego dane.

Klauzula informacyjna, o której mowa w niniejszej części, powinna spełniać co najmniej następujące warunki co do formy:

- tekst klauzuli informacyjnej powinien być pisany czcionką nie mniejszą niż 6p, najlepiej czcionką bezszeryfową;
- język klauzuli informacyjnej powinien być możliwie najprostszy i jasny. Sugerowane jest korzystanie z prostych i krótkich podpunktów oraz posługiwanie się zdaniami prostymi. Tam, gdzie to możliwe i nie wprowadza w błąd, sugerowane jest posługiwanie się językiem potocznym, codziennym.

Obowiązek informacyjny dla danych pozyskanych od osób trzecich

W przypadku pozyskania danych od osób trzecich Administrator przekazuje danej osobie niezbędne informacje za pośrednictwem najbardziej stosownego kanału komunikacji – uwzględniając zakres posiadanych o osobie danych, cele przetwarzania oraz koszty przekazania. Z uwagi na powszechność oraz niskie koszty sugerowane jest wykorzystywanie w tym celu poczty e-mail.

Stosowne informacje mogą być przekazane przy okazji pierwszego kontaktu z daną osobą w ramach celu, w jakim dane zostały pozyskane. W takim przypadku klauzula informacyjna powinna wyraźnie odróżniać się od pozostałej treści przekazywanej danej osobie oraz powinna spełniać wszelkie warunki przewidziane dla klauzuli informacyjnej dla danego kanału komunikacji

(porównaj: obowiązki informacyjne dla kanału internetowego, telefonicznego, pisemnego oraz w bezpośrednim kontakcie).

Administrator może nie wykonywać obowiązku informacyjnego z powołaniem na art. 14 ust. 5 lit. b) RODO w przypadku, gdy pozyskał dane dotyczące przedsiębiorców od osób trzecich i jednocześnie w pozyskanej bazie danych nie ma informacji kontaktowych (adresów e-mail), które pozwalają na łatwe spełnienie obowiązku informacyjnego, a co za tym idzie dopełnienie obowiązku informacyjnego wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku Administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osób, których dane dotyczą, w tym udostępnia stosowne informacje publicznie , np. na własnej stronie internetowej.

5. Inne istotne zagadnienia

Utrwalanie oświadczeń

Administrator obowiązany jest zapewnić utrwalanie oświadczeń składanych przez osoby, których dane dotyczą, w zakresie wyrażanej przez nich zgody na określone wykorzystywanie danych osobowych.

W przypadku oświadczeń składanych w formie pisemnej są to przykładowo papierowe dokumenty oświadczeń lub ich kopie cyfrowe (skan).

W przypadku oświadczeń składanych telefonicznie są to przykładowo nagrania z rozmów.

W przypadku oświadczeń składanych drogą elektroniczną są to przykładowo informacje dotyczące sesji, w trakcie której zostało złożone oświadczenie (data i godzina oświadczenia, adres IP, z którego wyrażono oświadczenie, dane osobowe podane przy wyrażeniu oświadczenia).

Administrator, wywiązując się z obowiązku przekazania osobie, której dane dotyczą, wszelkich informacji związanych z przetwarzaniem jej danych osobowych, powinien zapewnić środki techniczne pozwalające mu udowodnić, że prawidłowo wywiązał się z tego obowiązku.

Informowanie o naruszeniu danych

Jeżeli doszło do naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych i nie znajdują zastosowania wyłączenia z art. 34 ust. 3 RODO, Administrator bez zbędnej zwłoki zawiadamia wszystkie te osoby o takim naruszeniu. Informacje, które powinny zostać podane w każdym takim przypadku, opisane są w art. 34 RODO.

Informacje w tym zakresie Administrator powinien wysłać do osób zainteresowanych bez zbędnej zwłoki, jak tylko finalnie określi pełen zakres naruszenia oraz występujących ryzyk. Sugerowane jest, aby takie zawiadomienie nastąpiło nie później niż w ciągu 72h od chwili stwierdzenia naruszenia.

Zawiadomienie powinno odbyć się z wykorzystaniem najszybszych środków komunikacji. W szczególności może się to odbyć poprzez przesłanie do osób zainteresowanych stosownych wiadomości e-mail. Jeżeli Administrator nie posiada adresów e-mail osób fizycznych, może się to odbyć poprzez przesłanie SMS z linkiem do odrębnej (dedykowanej) podstrony www zawierającej niezbędne informacje. Jeżeli administrator nie posiada ani adresu e-mail ani numeru telefonu, na który może przesłać SMS, Administrator powinien rozważyć wysłanie do wszystkich osób, których

dane dotyczą, stosownych komunikatów pocztą tradycyjną. Administrator może zrezygnować z tej formy komunikacji, jeżeli spełnione są warunki określone w art. 34 ust. 3 lit c) RODO, tj. wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak przypadku Administrator powinien wydać publiczny komunikat lub zastosować inny podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

WYKORZYSTYWANIE DANYCH

1. Profilowanie

Ogólne zasady Profilowania

Administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury Profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą oraz zapobiegający m.in. skutkom w postaci dyskryminacji.

Intencją administratora w Profilowaniu jest zapewnienie, aby kierowana w imieniu podmiotu/organizacji komunikacja reklamowa była jak najbardziej dopasowana do preferencji i oczekiwań odbiorcy. Kierowanie profilowanych komunikatów pozwala unikać marnowania czasu odbiorców. Daje to również oszczędności finansowe organizacji, która ze swoją komunikacją i ofertą zwraca się wyłącznie do osób, które rzeczywiście mogą podjąć określone, pożądane działania. Profilowanie w marketingu jest więc działaniem dającym korzyści profilującym oraz profilowanym.

Profilowanie w działalności marketingowej

Profilowanie w działalności marketingowej generalnie nie podlega regulacjom art. 22 RODO. Oznacza to, że profilowanie dla potrzeb marketingowych generalnie nie wymaga uzyskiwania od osoby, której dane dotyczą, odrębnej zgody. Profilowanie, którego rezultatem jest przedstawienie określonej reklamy lub promocyjnej oferty wyłącznie wybranym odbiorcom, potencjalnie najbardziej zainteresowani daną reklamą lub ofertą, nie stanowi sytuacji, o której mowa w art. 22 ust. 1 RODO.

Przykład: Wykorzystanie profilowania i automatycznych środków komunikowania po to, by wyodrębnić matki dzieci w wieku od lat 3 do lat 6 w danym regionie w celu zaproszenia ich na przedstawienie dziecięce, którego fundatorem jest producent żywności.

Profilowanie dla celów marketingowych na zasadzie wyjątku może wymagać uzyskania odrębnej zgody od osoby, której dane dotyczą, jeżeli realizowane jest w sposób kierunkowy, inwazyjny i z założenia jego rezultaty mogą mieć istotny, negatywny wpływ na daną osobę.

Przykład: Wykorzystywanie profilowania i automatycznych środków komunikowania w celu wyszukiwania osób, które mają kłopoty finansowe, są istotnie zadłużone, po to, by kierować do nich reklamy gier liczbowych lub loterii pieniężnych.

Jeżeli proces profilowania wymaga jednak w danym przypadku zgody osoby, której dane dotyczą (zastosowanie znajduje art. 22 ust. 1 RODO – decyzje oparte wyłącznie na zautomatyzowanym procesie przetwarzania), Administrator musi być w stanie udowodnić, że uzyskał uprzednią zgodę danej osoby na profilowanie jeszcze przed rozpoczęciem czynności profilowania. To oznacza, że Administrator ma obowiązek uzyskać zgody również od tych osób, wobec których finalnie w wyniku profilowania nie zdecyduje się podejmować takich czynności.

Jeżeli po procesie profilowania, ale przed podjęciem określonych dalszych działań, dochodzi do ingerencji człowieka w decyzje, wobec jakich osób i jakie działania będą podejmowane, to takie działania nie będą w żadnym przypadku uznawane za sytuację, o której mowa w art. 22 ust. 1 RODO.

Sugerowane jest, aby Administratorzy, dokonując oceny reguł przetwarzania danych osobowych w swojej organizacji, weryfikowali, jaki dokładnie będzie cel profilowania oraz czy planowane profilowanie nie będzie miało istotnego negatywnego wpływu na osoby, których dane będą przetwarzane. Działania te powinny kończyć się podsumowaniem określającym, czy profilowanie osób, których dane dotyczą, wymaga uzyskiwania od nich odrębnej zgody, czy też nie.

Profilowanie w celach marketingowych, pomimo że co do zasady nie wymaga odrębnej zgody, jest działaniem podlegającym pod regulacje RODO. W szczególności Administratorzy mają obowiązek posiadać prawną podstawę dla przetwarzania danych osobowych oraz powinni wypełniać wobec osób, których dane dotyczą, obowiązek informacyjny.

2. Wykorzystywanie danych w aktywnym marketingu bezpośrednim

Każde działanie marketingowe powinno zostać poprzedzone weryfikacją, czy będzie ono adresowane do Przedsiębiorców (B2B) czy do konsumentów (B2C). W zależności od adresatów komunikowania różne mogą być prawa i obowiązki stron. W działaniach marketingowych szczególną ochroną należy objąć dzieci i osoby o ograniczonej zdolności pojmowania.

Telemarketing

Sprzedaż telefoniczna wymaga przetwarzania danych osobowych co najmniej w zakresie numeru telefonu, na które wykonywane jest połączenie. Dane powinny pochodzić z pewnych i sprawdzonych źródeł, a Administrator powinien posiadać prawną podstawę dla przetwarzania takich danych osobowych (np. uzasadniony interes). Za praktyki niedozwolone i naruszające reguły ochrony danych osobowych uznaje się w szczególności:

- wykonywanie połączeń na numery wygenerowane losowo,
- wykonywanie połączeń na numery z posiadanej bazy danych i informowanie rozmówców, że połączenie zostało wykonane na numer wygenerowany losowo.

Wykonywanie do konsumenta połączeń telefonicznych, których celem jest prezentowanie komunikatów marketingowych, wymaga posiadania uprzedniej zgody takiego konsumenta. Obowiązek posiadania zgody jest niezależny od technologii wykorzystanej do wykonania połączenia (telefonia stacjonarna, komórkowa, z wykorzystaniem protokołu IP, wideorozmowa, programy typu Skype, lub tym podobne). Zgoda konsumenta powinna być wyrażona uprzednio – to jest przed przeprowadzeniem rozmowy o charakterze sprzedażowym.

Wykonywanie sprzedażowych połączeń telefonicznych do przedsiębiorcy nie wymaga posiadania uprzedniej zgody takiego przedsiębiorcy.

Wykonywanie sprzedażowych połączeń telefonicznych z tą samą lub podobną ofertą do tego samego konsumenta może być realizowane nie częściej niż co 1 miesiąc. W celu zapewnienia wykonania powyższego obowiązku Administrator zobowiązany jest dołożyć należytej staranności, aby osoby lub podmioty, którymi posługuje się dla realizacji marketingu telefonicznego, były wyposażone w system integrujący (mający postać oprogramowania lub procesu organizacyjnego) pozwalający na bieżąco monitorować wykonywane połączenia marketingowe.

Konsument powinien mieć możliwość uzyskania od telemarketera wszelkich informacji dotyczących: podmiotu Administratora, zakresu i celu przetwarzania jego danych, jak również innych informacji go dotyczących. W trakcie rozmowy konsument powinien mieć prawo wyrazić sprzeciw wobec wykonywania do niego w przyszłości tego rodzaju połączeń oraz wobec dalszego

przetwarzania jego danych osobowych dla celów marketingowych. Telemarketer powinien mieć możliwość odnotowania tego rodzaju sprzeciwu w sposób widoczny dla innych telemarketerów pracujących lub współpracujących z danym Administratorem.

W przypadku, gdy sprzeciw wobec komunikacji handlowej lub globalnie wobec przetwarzania danych osobowych w celach marketingowych jest zgłoszony bezpośrednio Administratorowi, który nie korzysta z Procesorów w procesie zbierania oświadczeń, powinien on uwzględnić rejestrację tego sprzeciwu we własnej bazie nie później niż w ciągu 3 (trzech) dni roboczych od chwili wpłynięcia sprzeciwu. Na zasadzie wyjątku termin ten może ulec wydłużeniu, jeżeli w danym okresie z przyczyn technicznych lub organizacyjnych taki termin nie jest możliwy (awaria systemu, wielość wpływających zgłoszeń itp.). Jeżeli w proces zbierania oświadczeń zaangażowani są Procesorzy, odnotowanie sprzeciwu w bazie, w sposób widoczny dla Administratora oraz wszystkich Procesorów powinno nastąpić nie później niż w terminie jednego miesiąca od chwili wpłynięcia oświadczenia o sprzeciwie.

Przedsiębiorcy mogą kontaktować się w celu przedstawienia oferty przeznaczonej dla konsumentów w dni robocze między godziną 08:00 i 20:00, a w soboty między godzina 10:00 i 16:00, chyba, że indywidualny rozmówca wcześniej zażyczył sobie inaczej. W uzasadnionych przypadkach, ze względu na specyfikę grupy docelowej dopuszcza się kontakt w innych godzinach.

Badania telefoniczne

Wykonywanie połączeń telefonicznych w celu badania satysfakcji klientów, w celu realizacji badań statystycznych lub tym podobnych nie wymaga posiadania odrębnej zgody konsumenta pod warunkiem, że tego rodzaju połączenia nie mają w rzeczywistości celu marketingowego. Połączenia tego typu można uznać za mające charakter marketingowy, jeżeli w trakcie rozmowy z inicjatywy konsultanta telefonicznego konsumentowi przedstawiana jest propozycja zawarcia umowy lub oferta sprzedaży towaru lub usługi.

W toku rozmowy możliwe jest uzyskanie od respondenta zgody na komunikację marketingową, jednak nawet w przypadku uzyskania takiej zgody konsultant telefoniczny nie może przedstawiać konsumentowi komunikatów marketingowych podczas tej samej rozmowy.

Przetwarzanie danych osobowych dla wykonywania telefonów w celu przeprowadzenia badania satysfakcji klienta znajduje swoją podstawę w uzasadnionym interesie Administratora. Jednocześnie rozmowa telefoniczna powinna być niedługa i nieinwazyjna.

Marketing drogą elektroniczną (e-mail, SMS, inne)

Sprzedaż za pośrednictwem narzędzi marketingu elektronicznego, takich jak e-mail, SMSy, komunikatory, wymaga przetwarzania danych osobowych co najmniej w zakresie, odpowiednio: adresu e-mail, numeru telefonu lub loginu komunikatora, na który wysyłana jest komunikacja marketingowa. Dane powinny pochodzić z pewnych i sprawdzonych źródeł, a Administrator powinien posiadać prawną podstawę dla przetwarzania takich danych osobowych (np. uzasadniony interes).

Wysyłanie komunikatów marketingowych za pośrednictwem narzędzi elektronicznych do konsumenta wymaga posiadania uprzedniej zgody takiego konsumenta. Obowiązek posiadania

zgody jest niezależny od technologii wykorzystanej do wysłania komunikatu. Zgoda konsumenta powinna być wyrażona uprzednio – to jest przed wysłaniem komunikatu marketingowego.

Zgodnie z art. 13 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) uprawnione jest przesyłanie do konsumentów informacji handlowych drogą elektroniczną bez uzyskania uprzedniej odrębnej zgody, w przypadku gdy taki konsument jest klientem administratora oraz administrator otrzymał od takiego konsumenta szczegółowe elektroniczne dane kontaktowe dla potrzeb poczty elektronicznej w kontekście sprzedaży produktu lub usługi. W takim przypadku komunikaty marketingowe mogą dotyczyć wyłącznie wprowadzania na rynek swoich własnych produktów podobnych lub usług pod warunkiem, że konsumenci zostali jasno i wyraźnie poinformowani o możliwości sprzeciwienia się, w sposób wolny od opłat i prosty, takiemu wykorzystywaniu elektronicznych danych kontaktowych w chwili ich zbierania oraz przy każdej okazji otrzymywania wiadomości, w przypadku konsumentów, którzy początkowo nie sprzeciwili się takiemu wykorzystywaniu.

Przesłanie komunikatu marketingowego drogą elektroniczną do przedsiębiorcy nie wymaga posiadania uprzedniej zgody takiego przedsiębiorcy.

Marketing pocztowy

Spersonalizowany marketing pocztowy (fizyczna przesyłka reklamowa do zidentyfikowanego odbiorcy) może być realizowany tylko pod warunkiem posiadania legalnej podstawy przetwarzania danych osobowych odbiorców dla celów marketingowych (zgoda odbiorcy lub uzasadniony interes Administratora).

Wysłanie informacji handlowej w ramach spersonalizowanego marketingu pocztowego nie wymaga uzyskania odrębnej zgody odbiorcy.

Marketing w kontakcie osobistym (np. stoisko handlowe, promocje sprzedaży, programy lojalnościowe)

W sytuacji zbierania danych osobowych w kontakcie bezpośrednim z daną osobą fizyczną w celach marketingowych (np. poprzez formularz rejestracji w programie lojalnościowym, wniosek o wydanie karty lojalnościowej) konieczne jest zachowanie następujących środków zapewniających zgodność z prawem, poufność i bezpieczeństwo przekazywanych danych:

- formularze mogą być wypełniane własnoręcznie przez osobę, która podaje dane osobowe lub przez upoważnioną do tego osobę (np. pracownika administratora lub procesora);
- w przypadku, gdy formularz wypełnia upoważniona osoba, a osoba podająca dane przekazuje ich treść ustnie, osoba upoważniona jest odpowiedzialna za to, aby zapewnić poufność przekazywanych danych, tj. aby dane te mogły być przekazane w sposób nie dający się łatwo podsłuchać przez osoby postronne (np. czekające w kolejce, przechodzące obok);
- dla każdej ze zgód wyrażanych w formularzu powinien być przewidziany odrębny checkbox;

- jeżeli w ramach formularza osoba go wypełniająca potwierdza zapoznanie się z określonymi dokumentami, dokumenty te powinny być rzeczywiście dostępne dla niej na miejscu do zapoznania się, bez presji czasu;
- przyjęty sposób zbierania danych powinien przewidywać metodę uwierzytelnienia przez osobę podającą dane, że to ona podała określone dane i wyraziła poszczególne zgody (np. podpis pod drukowanym formularzem, posłużeniem się podpisem elektronicznym lub innym znacznikiem pod dokumentem elektronicznym, dokonanie potwierdzenia przez daną osobę z wykorzystaniem poczty e-mail);
- wypełnione formularze powinny być od razu przechowywane w sposób zapewniający ich bezpieczeństwo przed dostępem osób niepowołanych lub nieupoważnionych. W szczególności niedozwolonym działaniem jest pozostawienie wypełnionych formularzy w sposób umożliwiający ich odczytanie przez osoby nieupoważnione.

3. Wykorzystywanie danych w pasywnym marketingu bezpośrednim - Infolinia

Osoba, która z własnej inicjatywy dzwoni na infolinię, może być klientem lub nie. Konsultant infolinii odbierający telefon ma prawo zweryfikować, czy osoba dzwoniąca jest już klientem podmiotu prowadzącego infolinię i w tym celu poprosić ją o podanie dodatkowych danych identyfikujących.

Osoba prowadząca rozmowę powinna przede wszystkim skoncentrować się na zaadresowaniu zagadnienia, z którym klient zadzwonił na infolinię (zainteresowanie określonym produktem, skorzystanie z pomocy helpdesk, inne). Pod warunkiem, że dzwoniący nie wyrażał sprzeciwu wobec przetwarzania jego danych osobowych dla celów marketingowych, osoba prowadząca rozmowę obok głównego celu rozmowy, może:

- dokonać aktualizacji danych osobowych klienta lub
- przedstawić dodatkową ofertę produktu lub usługi lub
- zapytać rozmówcę o zgodę na wykonywanie do niego telefonów marketingowych lub przesyłanie mu informacji handlowych drogą elektroniczną.

Przedstawiając dzwoniącemu dodatkową ofertę, konsultant infolinii ma prawo uwzględnić posiadane w bazie dane osobowe, w tym informacje o wcześniejszych preferencjach zakupowych, w celu lepszego dopasowania oferty do zainteresowań dzwoniącego.

W przypadku, gdy dzwoniący nie jest klientem podmiotu prowadzącego infolinię, stosuje się odpowiednio zapisy dotyczące prowadzenia rozmów z klientami oraz dodatkowo przedstawiciel infolinii ma prawo poprosić rozmówcę o podanie dodatkowych danych identyfikujących (obok posiadanego już numeru telefonu) – co uzasadnione jest prawidłowym rejestrowaniem czynności prowadzonych przez infolinię. W szczególności są to: imię, nazwisko oraz miejscowość zamieszkania. Wymaganie dodatkowych danych może być uzasadnione celem rozmowy, z jakim na infolinię zadzwonił rozmówca. Rozmówca ma prawo odmówić podania wskazanych danych osobowych (dobrowolność), przy czym w takim przypadku konsultant infolinii ma prawo podjąć decyzję o niekontynuowaniu rozmowy.

4. Inne przypadki i zasady wykorzystywania danych osobowych w marketingu

Lista Robinsonów

Dobrą praktyką dla każdego sygnatariusza niniejszego Kodeksu jest przestrzeganie programu Lista Robinsonów, którego szczegółowe zasady określa regulamin dostępny na stronie https://listarobinsonow.pl/page/regulaminy

Program ma na celu ochronę osób fizycznych, które nie życzą sobie otrzymywania niezamówionej, adresowanej do nich informacji handlowej. Użytkownik, który nie życzy sobie otrzymywać, adresowanej do niego Informacji handlowej, może zgłosić swój udział w programie poprzez zarejestrowanie swoich danych na Liście Robinsonów.

PRZEKAZYWANIE, POWIERZANIE i PRZENOSZENIE DANYCH

1. Reguły powierzania danych

Przetwarzanie danych w grupie przedsiębiorstw

Jeżeli administrator danych jest częścią grupy przedsiębiorstw, niezależnie od tego, czy jest podmiotem kontrolującym czy kontrolowanym, to może – ze względu na swój prawnie uzasadniony cel – przesyłać dane osobowe do pozostałych członków takiej grupy, a także przetwarzać dane osobowe otrzymane od pozostałych członków takiej Grupy do wewnętrznych celów administracyjnych samej grupy jak też poszczególnych jej członków. Uprawnienie to nie uchybia obowiązkowi wykonania wobec konsumentów, których dane dotyczą, obowiązku informacyjnego. Obowiązek ten, informujący o wszystkich podmiotach w grupie przedsiębiorstw może zostać wykonany przez jedno przedsiębiorstwo z grupy (np. już na etapie zbierania danych osobowych).

Powierzanie danych zleceniobiorcy/podwykonawcy krajowemu

Jeżeli Administrator powierza przetwarzanie danych podwykonawcy w związku z realizacją działań marketingowych, powinien korzystać wyłącznie z usług podwykonawcy, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawa ochrony danych osobowych i chroniło prawa osób, których dane dotyczą. Administrator może zobowiązać podwykonawcę do przestrzegania zasad ochrony danych nie mniej restrykcyjnych, niż gdyby Administrator realizował kampanię samodzielnie/we własnym zakresie.

1. Jeśli administrator danych chce zaangażować inny podmiot do przetwarzania danych w imieniu administratora, choćby już na etapie zbierania danych, a podmiot ma siedzibę i będzie przetwarzał dane w Polsce lub innym państwie członkowskim Unii Europejskiej czy Europejskiego Obszaru Gospodarczego, administrator może zaangażować taki podmiot do przetwarzania danych wyłącznie po zawarciu z nim umowy powierzenia przetwarzania danych lub innego instrumentu prawnego, zgodnie z art. 28 ust. 3 RODO.
2. Umowa powierzenia przetwarzania danych podmiotowi, który ma siedzibę i będzie przetwarzał dane w Polsce lub innym państwie członkowskim Unii Europejskiej czy Europejskiego Obszaru Gospodarczego, powinna:
   - być zawarta co najmniej w formie dokumentowej w rozumieniu art. 77^2-77^3 Kodeksu cywilnego, tj. poprzez oświadczenia woli utrwalone na nośniku informacji umożliwiającym zapoznanie się z jego treścią, złożone w sposób umożliwiający ustalenie osoby składającej oświadczenie, np. wiadomość e-mail lub skan podpisanego oświadczenia;
   - zawierać co najmniej wyraźne i egzekwowalne zobowiązanie podmiotu przetwarzającego do posiadania środków technicznych i organizacyjnych odpowiednich do wymogów RODO tak, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. Umowa powierzenia przetwarzania danych może zostać zawarta odrębnie od innej umowy pomiędzy administratorem danych oraz podmiotem przetwarzającym, z której wykonaniem wiąże się przetwarzania danych lub zostać ujęta jako element ww. innej umowy (np. jeden z paragrafów takiej umowy).

Powierzanie danych zleceniobiorcy/podwykonawcy zagranicznemu

Jeżeli Administrator powierza przetwarzanie danych w związku z realizacją kampanii promocyjnej podmiotowi zagranicznemu, powinien korzystać wyłącznie z usług podmiotu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

1. Jeśli Administrator chce zaangażować inny podmiot do przetwarzania danych w imieniu Administratora, choćby już na etapie zbierania danych, a podmiot ten ma siedzibę lub będzie przetwarzał dane w państwie trzecim, Administrator może zaangażować taki podmiot do przetwarzania danych tylko wówczas, jeśli zostaną spełnione wszystkie poniższe warunki:
   - przekazanie danych takiemu podmiotowi obędzie się w ramach jednej z przesłanek określonych w art. 45-49 RODO oraz na warunkach właściwych dla takiej przesłanki;
   - Administrator zawrze z ww. podmiotem umowę powierzenia przetwarzania danych zgodnie z art. 28 RODO.
2. Umowa powierzenia przetwarzania danych podmiotowi, który ma siedzibę lub będzie przetwarzał dane w państwie trzecim, powinna:
   - być zawarta co najmniej w formie dokumentowej w rozumieniu art. 77^2-77^3 Kodeksu cywilnego, tj. poprzez oświadczenia woli utrwalone na nośniku informacji umożliwiającym zapoznanie się z jego treścią, złożone w sposób umożliwiający ustalenie osoby składającej oświadczenie, np. wiadomość e-mail lub skan podpisanego oświadczenia;
   - wskazywać przesłankę przekazania danych do państwa trzeciego, na podstawie której takie przekazanie się odbywa oraz opisywać wyczerpująco, w jaki sposób spełnione są warunki RODO właściwe dla tej przesłanki;
   - zawierać co najmniej wyraźne i egzekwowalne zobowiązanie podmiotu przetwarzającego do posiadania środków technicznych i organizacyjnych odpowiednich do wymogów RODO tak, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

3. Umowa powierzenia przetwarzania danych może zostać zawarta odrębnie od innej umowy pomiędzy administratorem danych oraz podmiotem przetwarzającym, z której wykonaniem wiąże się przetwarzania danych lub zostać ujęta jako element ww. innej umowy (np. jeden z paragrafów takiej umowy).

Obowiązki Podmiotu Przetwarzającego

Podmiot, który ma zostać zaangażowany do przetwarzania danych w imieniu Administratora, choćby już na etapie zbierania danych, może przyjąć na siebie obowiązki w tym zakresie wyłącznie na podstawie umowy powierzenia przetwarzania danych lub innego instrumentu prawnego, zgodnie z art. 28 RODO. Podmiot Przetwarzający powinien przetwarzać dane, w tym zwłaszcza zapewnić im ochronę, co najmniej w taki sposób, jak gdyby sam był ich Administratorem.

2. Reguły przekazywania danych

Przekazywanie danych osobowych pomiędzy Administratorem a Podmiotem Przetwarzającym powinno odbywać się w sposób bezpieczny w ujęciu organizacyjnym oraz technicznym. Sugerowane jest, aby umowa powierzenia pomiędzy stronami określała, kto jest upoważniony do

przekazania lub odbioru danych w przedsiębiorstwie (o ile przekazanie odbywa się z wykorzystaniem oznaczonych osób) oraz jakimi środkami dane osobowe będą przekazywane.

W przypadku przekazywania danych osobowych w formie papierowej, dokumentacja powinna zostać przekazana bezpośrednio pomiędzy osobami upoważnionymi.

W przypadku przekazywania danych osobowych w formie elektronicznej, przekazanie powinno odbyć się przy wykorzystaniu jednego z następujących sposobów komunikacji:

- za pośrednictwem dedykowanego serwera (w tym rozwiązania chmurowe) zabezpieczonego przed dostępem osób trzecich, z uwzględnieniem szyfrowanej komunikacji z serwerem
- poprzez szyfrowaną wiadomość
- poprzez nieszyfrowaną wiadomość, o ile dostęp do plików zawierających dane osobowe wymaga podania hasła
- za pośrednictwem fizycznego nośnika danych (np. CD, DVD, szyfrowany pendrive)

W przypadku przekazywania danych z wykorzystaniem nieszyfrowanej wiadomości lub fizycznego nośnika danych sugerowane jest korzystanie z rozwiązań zawierających fizyczne zabezpieczenia, a jeżeli nie jest to możliwe, dostęp do plików z danymi powinien być chroniony hasłem. Hasło do plików musi zostać wysłane drugiej stronie innym środkiem komunikowania np. SMS)

Warunki, jakie muszą być spełnione, aby dokonać przekazania danych innemu administratorowi (np. sprzedaż bazy danych)

Jeżeli Administrator chce przekazać dane konsumenta innemu Administratorowi, powinien wykazać się podstawą prawną dla takiego działania. Podstawa prawna dla przekazania danych osobowych konsumenta innemu Administratorowi obejmuje w szczególności:

1. uprzednie poinformowanie osoby, której dane dotyczą, przy okazji zbierania danych o znanych na dany dzień odbiorcach lub kategoriach odbiorców danych osobowych; poinformowanie to musi nastąpić nie później niż przed pierwszym przekazaniem danych innemu Administratorowi;
2. posiadanie legalnej podstawy przetwarzania danych w celu ich dalszego przekazania (np. zgoda osoby, której dane dotyczą lub uzasadniony interes Administratora);
3. brak sprzeciwu osoby, której dane dotyczą, wobec przekazania jej danych osobowych Administratorom.

Informację o kategoriach innych podmiotów, którym będą przekazywane (przesyłane, udostępniane) dane do samodzielnego przetwarzania uważa się za dostateczną, jeśli określona zostanie branża, w której podmioty te prowadzą swoją działalność. Jeżeli branży jest więcej niż jedna, pełna lista branż może zostać określona na wskazanej stronie internetowej, a w przypadku formularzy papierowych - na odrębnej liście dostępnej w miejscu wypełniania formularza.

Proces i zasady udostępnienia danych oraz zakres wykorzystania powinny być uregulowane w podpisanej między administratorami umowie.

Udostępnienie danych pomiędzy Administratorami może zostać poprzedzone procesem deduplikacji, w toku której Administratorzy porównują swoje bazy danych w celu określenia, czy przekazanie/wymiana baz danych jest uzasadniona gospodarczo. Taka deduplikacja powinna odbyć się z wykorzystaniem małych próbek danych lub z wykorzystaniem pseudonimizacji (np. szyfrowanie z wykorzystaniem modułu kryptograficznego MD5). Bezpośrednio po takim sprawdzeniu każdy z Administratorów usuwa dane niezbędne dla deduplikacji. Tego rodzaju proces weryfikacyjny nie jest uznawany za proces udostępnienia danych.

Sprzeciw wobec przekazania danych osobowych odbiorcom danych może stanowić podstawę do odmowy realizacji świadczenia na rzecz danej osoby, o ile takie przekazanie jest niezbędne dla realizacji tego świadczenia (np. dostawa przesyłki kurierem) lub dane świadczenie realizowane jest bez odpłatności w zamian za możliwość przetwarzania i udostępniania danych osobowych.

Zawsze dopuszczalne jest w celach marketingowych przekazywane danych osobowych osób fizycznych prowadzących działalność gospodarczą z powołaniem na uzasadniony interes Administratora, o ile przekazywane dane osobowe są związane z ich działalnością gospodarczą. W przypadku przekazywania danych osobowych konsumentów w celach marketingowych Administrator powinien dokonać odrębnej analizy, czy przekazanie danych może odbyć się z powołaniem na uzasadniony interes Administratora, czy też Administrator powinien uzyskać odrębną zgodę osoby fizycznej.

Warunki przekazania danych do podmiotu krajowego/unijnego

W przypadku przekazywania (przesyłania, udostępniania) danych do samodzielnego (we własnym imieniu) przetwarzania podmiotowi, który nie ma siedziby ani nie będzie przetwarzał danych w państwie trzecim, nie wprowadza się żadnych dodatkowych warunków dla takiego przekazywania.

Warunki przekazania danych do podmiotu z kraju trzeciego

1. Przekazywanie (przesyłanie, udostępnianie) danych do samodzielnego (we własnym imieniu) przetwarzania podmiotowi, który ma siedzibę lub będzie przetwarzał dane w państwie trzecim wymaga spełnienia wszelkich wymogów RODO w zakresie przekazywania danych do państw trzecich.
2. Sygnatariuszom, którzy mają siedzibę lub będą przetwarzali dane w państwie trzecim, dane mogą być przekazywane na takich samych zasadach jak podmiotom, które nie mają siedziby ani nie będą przetwarzali danych w państwie trzecim.
3. W przypadku, gdyby Administrator danych planował przekazywanie danych konsumenta podmiotowi, który ma siedzibę lub będzie przetwarzał dane w państwie trzecim na podstawie zgody osoby, której dane dotyczą, zgoda taka powinna zostać wyrażona po uprzednim dokładnym poinformowaniu takiej osoby,do jakiego państwa trzeciego dane miałyby być przekazywane oraz jakie są prawne warunki ochrony danych w tym państwie.

3. Przekazywanie/Powierzanie danych operatorom usług pocztowych i kurierskich

Określenie warunków takiego powierzenia/przekazania

Udostępnienie kurierowi danych osobowych odbiorców przesyłek przez niego doręczanych w formie etykiet adresowych i/lub listy uzasadnione jest na podstawie uzasadnionego interesu Administratora i nie wymaga odrębnej zgody podmiotu danych.

Nie zwalnia to operatorów pocztowych ani firm kurierskich z obowiązku należnej ochrony przekazanych im w ten sposób danych osobowych.

1. W przypadku, gdy Administrator danych korzysta z usług operatorów pocztowych lub firm kurierskich, uznaje się, że ma prawo przekazywać takim podmiotom dane osobowe adresatów wymagane do zrealizowania usługi pocztowej/kurierskiej.
2. Jeśli nie występuje inna szczególna podstawa przetwarzania danych zgodnie z powyższym, Administrator ma zawsze prawnie uzasadniony interes w przekazywaniu do operatorów pocztowych lub firm kurierskich wymaganych przez nich danych osobowych adresatów, jeśli takie przekazanie jest niezbędne do spełnienia zobowiązania (wynikającego nawet ze zdarzeń lub aktów prawych innych niż umowa) Administratora wobec osoby, której dane dotyczą (np. wydania jej nagrody w akcji marketingowej).
3. W odniesieniu do danych osobowych adresatów, których przekazanie jest wymagane przez operatorów pocztowych lub firmy kurierskie dla doręczenia przesyłki (np. imię i nazwisko, adres do doręczenia przesyłki, numer telefonu, adres e-mail), administratorem takich danych jest operator pocztowy lub firma kurierska.
4. W odniesieniu do danych osobowych adresatów, których przekazanie nie jest wymagane przez operatorów pocztowych lub firmy kurierskie dla doręczenia przesyłki, a które są im przekazywane na potrzeby zrealizowania usług dodatkowych przy doręczeniu przesyłki (np. numer dowodu osobistego adresata dla celów potwierdzenia jego tożsamości lub wieku), operator pocztowy lub firma kurierska jest podmiotem przetwarzającym dane w imieniu administratora.

4. Przenoszenie danych

Na gruncie regulacji RODO osoba, której dane dotyczą ma prawo zgłosić żądanie do przeniesienia jej danych osobowych do innego Administratora. W przypadku zgłoszenia takiego żądania Administrator obowiązany jest wyeksportować posiadane dane osobowe do odrębnego pliku w powszechnie stosowanym formacie (np. XLSX, CSV). Przeniesieniu podlegają dane osobowe, które Administratorowi podała osoba fizyczna. Dotyczy to danych podanych przy okazji: rejestracji w serwisie, rozmowy telefonicznej, wypełniania kwestionariusza elektronicznego lub papierowego.

Przeniesieniu nie podlegają dane wydedukowane samodzielnie przez Administratora lub metadane, nie mające charakteru spersonalizowanego (np. dotyczące wyinterpretowanych preferencji zakupowych, zaszeregowania osoby do danego profilu z powołaniem na posiadane przez Administratora badania rynkowe, statystyczne).

PRZECHOWYWANIE DANYCH

1. Okres przechowywania danych przetwarzanych dla celów marketingowych

Przetwarzanie dla celów marketingowych co do zasady nie jest ograniczone czasowo. Administrator nie ma prawnego obowiązku usunięcia lub zanonimizowania danych przetwarzanych dla celów marketingowych z tego tylko powodu, że upłynął określony czas od daty ich zebrania.

Jednocześnie Administrator zobowiązany jest zapewnić, aby przetwarzane przez niego dla celów marketingowych dane pozostawały aktualne. Zobowiązanie to Administrator może realizować m.in. poprzez:

- skuteczne realizowanie komunikacji marketingowej nie rzadziej niż jeden raz w ciągu roku z wykorzystaniem posiadanych danych (poprzez skuteczne realizowanie komunikacji marketingowej rozumie się taką komunikację, która skutecznie dotarła do odbiorcy, a jej nadawca nie otrzymał informacji, że posiadane dane kontaktowe są nieaktualne);
- zgodne z prawem monitorowanie zachowania swoich klientów i podawanych przez nich danych (np. dane podawane na fakturach, dla potrzeb dostawy produktu, dla potrzeb realizowania płatności).

W przypadku braku kontaktu marketingowego oraz braku jakiejkolwiek transakcji na linii Administrator – osoba, której dane dotyczą, przez okres kolejnych 5 lat, Administrator obowiązany jest podjąć decyzję o zasadności pozostawienia danych osobowych w swojej bazie marketingowej.

Jeżeli dany podmiot zdecyduje się dalej nie przetwarzać określonych danych osobowych w celach marketingowych, może podjąć decyzję o przeniesieniu takich danych do swojej bazy archiwalnej, po to, aby takich danych więcej nie pobierać z publicznie dostępnych źródeł.

2. Dostęp do informacji

Każda osoba, której dane są przetwarzane przez Administratora, ma pełne prawo do uzyskiwania informacji o swoich danych osobowych przetwarzanych przez Administratora.

Prawo dostępu do informacji obejmuje wyłącznie dane podane przez osobę, której dane dotyczą oraz dane zebrane od osób trzecich. Prawo to nie obejmuje danych wytworzonych przez Administratora na podstawie zebranych danych (np. stwierdzone przez Administratora preferencje zakupowe).

Osoba, której dane dotyczą ma prawo w każdej chwili złożyć sprzeciw wobec przetwarzania jej danych osobowych w celach marketingowych. W takim przypadku Administrator ma obowiązek zaprzestać przetwarzania danych w powyższych celach i nie może z powołaniem na swój uzasadniony interes lub inną podstawę prawną przetwarzać dalej tych danych w celach marketingowych.

3. Aktualność danych

Administratorzy powinni czuwać, aby wszystkie przetwarzane przez nich dane osobowe były aktualne, to jest aby dane osobowe były rzetelne i prawidłowe. Administratorzy mają prawo kontaktować się co najmniej raz w roku z osobami, których dane przetwarzają, w celu zweryfikowania aktualności przetwarzanych danych. Kontakt taki nie powinien mieć charakteru

marketingowego, o ile Administrator nie posiada odrębnej podstawy prawnej dla wykorzystania danego środka komunikowania w celu marketingu bezpośredniego.

Każda osoba fizyczna ma prawo uzyskać informacje o tym, jakie jej dane osobowe Administrator przetwarza oraz ma prawo do ich aktualizowania.

4. Prawo do bycia zapomnianym

Prawo do bycia zapomnianym jest niezbywalnym prawem osoby, której dane dotyczą.

Osoba, której dane dotyczą, może żądać od Administratora, który upublicznił jej dane osobowe, nie tylko tego, aby usunął on jej dane osobowe, ale również aby Administrator przesłał do wszystkich znanych mu innych administratorów danych osobowych, którzy pobrali jej upublicznione dane, wezwanie do usunięcia tych danych, kopii tych danych osobowych lub ich replikacji.

W przypadku skorzystania z powyższego prawa przez daną osobę Administrator, który upublicznił dane osobowe, a który obecnie ma obowiązek usunięcia danych osobowych, podejmuje działania, by poinformować znanych mu administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Administrator realizuje te czynności w rozsądnych granicach, biorąc pod uwagę dostępną technologię i koszt realizacji. W szczególności Administrator powinien poinformować o takiej okoliczności wszystkie podmioty, którym w drodze umowy przekazał dane osobowe podmiotu danych, o ile kontakt z nimi w danym czasie drogą elektroniczną jest możliwy, a także podmiotom, co do których stwierdził, że opublikowały one dane osobowe danego podmiotu danych w sieci Internet, o ile jest w stanie określić podmiot będący administratorem tych danych osobowych oraz adres jego poczty elektronicznej.

Nieuprawnione jest publikowanie informacji o zgłoszeniu żądania usunięcia danych na swoich stronach internetowych lub w innych miejscach w celu dotarcia do możliwie szerokiego kręgu adresatów – tego rodzaju publikacja, wymagająca podania danych osoby, która zgłosiła żądanie, stanowi nieuprawniony sposób wykorzystywania jej danych osobowych.

Administrator może odmówić danej osobie prawa do bycia zapomnianym, o ile zachodzą przesłanki wyłączające prawo do żądania usunięcia danych osobowych. W praktyce marketingowej Administrator zobowiązany jest zawsze zachować dane osobowe dla przypadków:

1. przetwarzania danych na potrzeby podatkowe w związku z akcjami promocyjnymi;
2. rozliczalności gier hazardowych;
3. procesów sądowych.

Prawo do bycia zapomnianym w działalności marketingowej wiąże się z istotnymi problemami praktycznymi. W szczególności w ramach działalności marketingowej konieczne jest zapewnienie rozliczalności w zakresie źródeł uzyskania danych oraz uzyskania zgód na elektroniczną oraz telekomunikacyjną komunikację handlową. Jeżeli marketer zupełnie „zapomni" daną osobę, to w przyszłości nie będzie w stanie obronić się przed zarzutami tej osoby co do zgodności z prawem wcześniejszych działań w obszarze marketingu, a to może narazić marketera na istotne sankcje. W

celu uniknięcia powyższej sytuacji uznaje się, że Administrator jest uprawniony do stworzenia wewnętrznej „czarnej listy" osób, które skorzystały do prawa do bycia zapomnianym, do której dostęp będą mieli wyłącznie upoważnieni pracownicy, np. administrator systemów informatycznych oraz osoba odpowiedzialna w organizacji za dane osobowe (minimalny krąg osób). W ramach takiej czarnej listy mogą być przechowywane podstawowe dane osoby, która skorzystała z prawa do bycia zapomnianym oraz wszelkie dane oraz informacje pozwalające na zapewnienie rozliczalności działań Administratora.

Prawo do bycia zapomnianym może być realizowane poprzez anonimizację danych.

5. Pseudonimizacja

Pseudonimizacja to proces odwracalny, który polega na ograniczeniu możliwości powiązania zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą i tworzeniu w odniesieniu do tej osoby powiązań między różnymi zbiorami. Pseudonimizacja zmierza zatem do zwiększenia skuteczności systemu bezpieczeństwa przetwarzania danych, ale nie jest równoznaczna anonimizacji ani nie oznacza usunięcia danych osobowych.

Administrator może stosować technikę pseudonimizacji danych z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania, zakresu i celu przetwarzania danych oraz ryzyka i wagi naruszenia praw lub wolności osób fizycznych.

Pseudonimizacja może być szczególnie stosowana w następujących sytuacjach:

- gdy określone dane powinny być przechowywane na podstawie odrębnych przepisów prawnych, np. do przedstawienia określonych danych podczas kontroli przez upoważnione organy;
  przykład: organy celno-skarbowe, przeprowadzając kontrolę u organizatora loterii promocyjnej w zakresie stosowania ustawy o podatku dochodowym od osób fizycznych, jeśli nie toczy się postępowanie, nie mogą mieć wglądu w dane osobowe laureatów loterii;
- gdy dane osób fizycznych są powszechnie dostępne;
  przykład: w sytuacji, gdy osoby fizyczne prowadzące działalność gospodarczą wyraziły sprzeciw wobec przetwarzania ich danych, a istnieje możliwość ponownego ich przetwarzania (np. poprzez zaciągnięcie zaktualizowanej bazy danych z Centralnej Ewidencji i Informacji Działalności Gospodarczej)
- zmiana celu przetwarzania danych;
  przykład: dane zostały zebrane w celu zawarcia i wykonania umowy, a następnie Administrator danych rozpoczął przetwarzanie tych danych w celu przeciwdziałania oszustwom.

Zastosowanie przez Administratora techniki pseudonimizacji danych osobowych nie wymaga tworzenia lub wydzielania do odrębnej bazy danych, które zostały poddane pseudonimizacji. Dopuszcza się zastosowanie procedury pseudonimizacji jedynie w odniesieniu do niektórych rekordów, jak również wszystkich rekordów w bazie danych dotyczących danej osoby fizycznej, o ile w konkretnych okolicznościach będzie to celowe.

6. Anonimizacja

Anonimizacja jest procesem odrębnym od pseudonimizacji. W wyniku anonimizacji dochodzi do przetworzenia informacji w sposób uniemożliwiający zidentyfikowanie określonej osoby fizycznej. Anonimizacja może być stosowana w szczególności w celach archiwalnych lub statystycznych. Dane zanonimizowane nie stanowią danych osobowych i nie podlegają regulacjom RODO.

Przykład anonimizacji:

Dane osobowe: Izabela Nowak, zam. ul. Mickiewicza 13/26, 60- 858 Poznań, urodzona 11-04-1979 e-mail i.nowak@onet.pl zarejestrowana w serwisie 2012-03-12, zrezygnowała z rejestracji 2017-12-24.

Dane zanonimizowane: Ixxxxxx N1265, zam. w Poznaniu, e-mail: xxx@onet.pl, urodzona 11-04-1979, zarejestrowana w serwisie 2012-03-12, zrezygnowała z rejestracji 2017-12-24.

7. Bezpieczeństwo techniczne i organizacyjne danych

Zgodnie z ustawą o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych publikuje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Sygnatariusze Kodeksu mogą wywiązać się z obowiązku zapewnienia przetwarzanym danym osobowym bezpieczeństwa technicznego i organizacyjnego poprzez zastosowanie się do powołanych rekomendacji.

Sugerowane minimalne działania w obszarze bezpieczeństwa obejmują:

1) Zabezpieczenia fizyczne oraz organizacyjne
    a. pomieszczenia, gdzie są przetwarzane dane osobowe, powinny mieć możliwość ich zamknięcia w sposób uniemożliwiający wstęp osobom niepowołanym (klucze, zamki magnetyczne lub inne)
    b. jeżeli do pomieszczeń mają dostęp osoby o różnym zakresie upoważnienia do przetwarzania danych lub po godzinach pracy mają do nich dostęp osoby sprzątające, ochrona lub tym podobne to:
        i. w pokojach powinny znajdować się szafy zamykane na klucz na dokumenty papierowe zawierające dane osobowe. Dostęp do poszczególnych szaf (i odpowiednio kluczy) powinny mieć tylko osoby upoważnione do przetwarzania danych osobowych w nich przechowywanych;
        ii. w organizacji powinna obowiązywać polityka „czystych biurek”.
    c. ekrany komputerów powinny być ustawione w taki sposób, aby wglądu do nich nie miały osoby nieupoważnione albo ekrany powinny być wyposażone w specjalne rozwiązanie uniemożliwiające podejrzenie z boku treści na monitorach;
    d. biuro powinno być wyposażone w:
        i. alarm przeciwwłamaniowy;
        ii. alarm pożarowy;
        iii. gaśnice;
        iv. może być wykorzystywany monitoring (z tym, że monitoring nie może być dostępny w pomieszczeniach socjalnych oraz sanitarnych);
2) Zabezpieczenia IT:

a. dostęp do serwerowni powinien być ograniczony do minimalnej liczby osób; serwerownia powinna być generalnie pomieszczeniem zamkniętym w sposób uniemożliwiający wstęp osobom niepowołanym (klucze, zamki magnetyczne lub inne);
b. wszystkie stacje robocze (laptopy, komputery stacjonarne) powinny być wyposażone w moduł logowania, z wykorzystaniem indywidualnego loginu i hasła; hasła powinny mieć co najmniej 8 znaków, system powinien wymuszać zmianę hasła nie rzadziej niż co 120 dni i powinien pamiętać co najmniej 4 ostatnie hasła;
c. wszystkie urządzenia przenośne (np. smartfon, tablet), za pośrednictwem których następuje dostęp do danych (np. lista kontaktów, zdjęcia, dostęp do poczty e-mail), powinny mieć zabezpieczenie przed nieuprawnionym dostępem poprzez PIN lub hasło;
d. powinna istnieć polityka kopii zapasowych;
e. system powinien być wyposażony w niezbędny firewall, oprogramowanie antywirusowe,
f. oprogramowanie powinno być aktualne, w tym systemy operacyjne powinny funkcjonować w wersji utrzymywanej przez ich producenta;
g. poczta e-mail powinna być wysyłana i odbierana protokołami szyfrowanymi (np. SSL).

OCENA SKUTKÓW DLA OCHRONY DANYCH W DZIAŁALNOŚCI MARKETINGOWEJ

1. Czym jest „Ocena skutków dla ochrony danych” ? (eng. *Data protection impact assessment)*

Artykuł 35 RODO zobowiązuje Administratorów danych, aby w określonych przypadkach przed przystąpieniem do przetwarzania danych osobowych, dokonywali oni tzw. „oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych”. W ogólnym ujęciu prawodawca wymaga dokonywania takiej oceny „jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”. Prawodawca precyzuje, że Administrator zobowiązany jest wykonać „ocenę” w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych wrażliwych (art. 9 ust. 1 RODO) lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO); lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

2. „Ocena skutków dla ochrony danych” w działalności marketingowej

Generalnie dla większości czynności przetwarzania danych osobowych w działalności marketingowej nie ma obowiązku przeprowadzania procesu „Oceny skutków dla ochrony danych”. Czynności przetwarzania danych osobowych w granicach niezbędnych do przedstawienia oferty produktów lub usług, organizacji akcji promocyjnej, przygotowania materiału promocyjnego, nie wiążą się generalnie „z dużym prawdopodobieństwem wysokiego ryzyka naruszenia praw lub wolności osób fizycznych”.

W określonych przypadkach procesy przetwarzania danych osobowych dla potrzeb marketingowych mogą jednak wiązać się z takim prawdopodobieństwem ryzyka. W szczególności będzie dotyczyć sytuacji, w której spełnione są przynajmniej dwie z następujących przesłanek:

- Administrator w celach marketingowych zbiera i przetwarza dane w sposób systematyczny, na masową skalę, w tym z wykorzystaniem danych osobowych uzyskanych bezpośrednio od osoby, których dane dotyczą oraz z baz dostępnych publicznie; masowość skali przetwarzania można określić poprzez odwołanie do następujących czynników:
    - określenie liczby lub odsetka odpowiedniej populacji;
    - ilość danych i / lub zakres różnych przetwarzanych danych;
    - czas trwania lub trwałość działania przetwarzania danych;
    - zasięg geograficzny działalności przetwarzania

- Administrator zbiera i przetwarza w celach marketingowych dane osobowe wrażliwe lub dane dotyczące wyroków skazujących lub naruszeń prawa;
- Administrator dokonuje ewaluacji i scoringu, uwzględniając profilowanie i przewidywanie, w szczególności z aspektów dotyczących wydajności osoby, której dane dotyczą w pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub ruchów" (np. firma biotechnologiczna oferująca testy genetyczne bezpośrednio konsumentom w celu oceny i przewidywania ryzyka choroby / zdrowia, lub tworzenie profili zachowania;
- Administrator w sposób systematyczny monitoruje osoby, których dane dotyczą;
- Administrator przetwarza w celach marketingowych dane osobowe dzieci;
- Administrator dokonuje innowacyjnego wykorzystania lub stosowania rozwiązań technologicznych lub organizacyjnych;
- Administrator w toku swoich działań przekazuje dane osobowe poza granice Unii Europejskiej.

Jeżeli Administrator stwierdzi, że w ramach planowanego procesu przetwarzania danych osobowych spełnione są co najmniej dwie z powyższych przesłanek, zobowiązany jest zrealizować „Ocenę skutków dla ochrony danych" zgodnie z art. 35 RODO. Sugeruje się, aby dokonując „Oceny…" Administrator korzystał z wytycznych Grupy Roboczej ds. Art. 29 dostępnych pod adresem *ec.europa.eu/newsroom/document.cfm?doc_id=44137*.

STOSOWANIE KODEKSU / ADMINISTROWANIE

1. Przystąpienie do Kodeksu

Reguły przystąpienia

Każdy Przedsiębiorca realizujący działania z zakresu marketingu bezpośredniego (jako Administrator, jako Podmiot Przetwarzający, na własny rachunek, na zlecenie) może wyrazić wolę przystąpienia do Kodeksu.

W celu przystąpienia do Kodeksu i uzyskania rejestracji jako członka Sygnatariusza Kodeksu Przedsiębiorca musi wypełnić i wnieść oświadczenie o przystąpienia do Kodeksu. Wzór aktualnego oświadczenia, który stanowi Załącznik nr 2 do niniejszego Kodeksu, publikowany jest na stronie www.smb.pl.

Oświadczenie powinno zostać wypełnione przez Przedsiębiorcę zgodnie ze stanem faktycznym i prawnym występującym w jego strukturze. Następnie Przedsiębiorca podpisane oświadczenie (zgodnie z zasadą reprezentacji) doręcza na adres SMB (osobiście, pocztą, kurierem lub pocztą elektroniczną w przypadku posłużenia się przez Przedsiębiorcę kwalifikowanym podpisem elektronicznym).

Podpisanie i przesłanie na adres SMB oświadczenia o przystąpieniu do Kodeksu oznacza, że Przedsiębiorca zgadza na związanie regulacjami Kodeksu oraz potwierdza, że jego przedsiębiorstwo na dzień podpisania oświadczenia spełnia wszystkie warunki Przetwarzania Danych Osobowych stawiane przez Kodeks.

Biuro SMB rozpatruje zgłoszenie Przedsiębiorcy pod kątem jego prawidłowości oraz kompletności. W terminie 10 dni roboczych od otrzymania oświadczenia Biuro SMB informuje zgłaszającego o poprawności zgłoszenia albo o stwierdzonych brakach. W przypadku stwierdzenia jakiegokolwiek braku Zarząd Stowarzyszenia może wezwać Przedsiębiorcę do uzupełnienia braków w zakreślonym terminie.

Jeżeli Zarząd SMB ma wątpliwości co do prawdziwości oświadczenia, ma prawo zobowiązać Przedsiębiorcę do przedstawienia aktualnej opinii Jednostki Certyfikującej potwierdzającej zgodność Przetwarzania Danych Osobowych przez Przedsiębiorcę z niniejszym Kodeksem.

Jeżeli Zarząd SMB nie stwierdzi istnienia braków zgłoszenia, wpisuje przedsiębiorcę do publicznego rejestru Sygnatariuszy Kodeksu i wydaje zgłaszającemu przedsiębiorcy zaświadczenie o przystąpieniu do Kodeksu w terminie do 30 dni roboczych od daty otrzymania oświadczenia.

Stowarzyszenie może wprowadzić opłaty dla podmiotów chcących przystąpić do Kodeksu jak również opłaty roczne za pozostawanie w strukturze Kodeksu. Opłaty przeznaczone będą w szczególności na cele administrowania Kodeksem i na system monitorowania jego przestrzegania, na zwiększanie wiedzy i świadomości o danych osobowych wśród Sygnatariuszy, globalnie na rynku, a także na cele statutowe Stowarzyszenia. Wysokość opłat dla podmiotów będących członkami Stowarzyszenia oraz dla podmiotów nie będących członkami Stowarzyszenia może być różna. Bieżące informacje o opłatach są dostępne na stronie www.smb.pl.

Zaświadczenia o przystąpieniu do Kodeksu

Po wpisaniu do publicznego rejestru Sygnatariuszy Kodeksu Sygnatariusz może posługiwać się w swojej działalności informacją o przystąpieniu do Kodeksu jak również dokumentem

przyznanego zaświadczenia. Prawo to przysługuje przez okres pozostawania Sygnatariuszem Kodeksu przestrzegającym reguł niniejszego Kodeksu.

Okresowe sprawdzenia i audyty

Sygnatariusze Kodeksu zobowiązani są okresowo, jednak nie rzadziej niż 1 (jeden) raz na rok, dokonywać sprawdzenia zgodności swojej działalności z niniejszym Kodeksem oraz regulacjami RODO. Sprawdzenie takie, w zależności od posiadanej wiedzy, budżetu oraz środków organizacyjnych może być realizowane samodzielnie lub poprzez jednostkę zewnętrzną w stosunku do Sygnatariusza. Z dokonanego sprawdzenia Sygnatariusz ma obowiązek przesłać sprawozdanie do Stowarzyszenia SMB. Aktualne reguły dokonywania sprawdzeń oraz przesyłania sprawozdań będą na bieżąco publikowane i komunikowane przez Stowarzyszenie SMB poprzez stronę www.smb.pl. Stowarzyszenie może zadawać Sygnatariuszom dodatkowe pytania do przesyłanych przez nich sprawozdań. Sygnatariusz Kodeksu, który posiada aktualną certyfikację w rozumieniu art. 42 RODO, jest zwolniony z obowiązku realizowania okresowych sprawdzeń.

W przypadku istnienia wątpliwości co do zgodności działalności Sygnatariusza z regułami niniejszego Kodeksu lub RODO Stowarzyszenie ma prawo przeprowadzić audyt u tego Sygnatariusza z wykorzystaniem swoich lub zewnętrznych audytorów. Warunkiem przeprowadzenia audytu jest uprzednie zawiadomienie o tym fakcie Sygnatariusza z co najmniej 7-dniowym wyprzedzeniem. W przypadku potwierdzenia niezgodności działalności Sygnatariusza z niniejszym Kodeksem lub RODO Sygnatariusz może zostać obciążony dodatkowymi kosztami związanymi z przeprowadzonym audytem zgodnie z tabelą opłat dostępną na stronie www.smb.pl.

2. Okresowa weryfikacja Kodeksu

Zarząd Stowarzyszenia weryfikuje treść Kodeksu w oparciu o zmiany prawa ochrony danych osobowych na poziomie krajowym oraz na poziomie Unii Europejskiej. Zarząd Stowarzyszenia bierze również pod uwagę wnioski zgłaszane przez Sygnatariuszy oraz przez Prezesa Urzędu Ochrony Danych Osobowych.

Zarząd Stowarzyszenia ponadto weryfikuje Kodeks pod kątem zmian w praktyce stosowania prawa, zmian w orzecznictwie, zmian rynkowych oraz rozwoju technologicznego i przemysłowego. Zarząd dokonuje stosownej weryfikacji nie rzadziej niż raz na dwa lata.

3. Reguły dokonywania zmian w Kodeksie

W przypadku stwierdzenia, że Kodeks wymaga zmiany, Zarząd Stowarzyszenia przygotowuje projekt zmian do Kodeksu wraz z uzasadnieniem. W pracach nad zmianami mogą brać udział członkowie Stowarzyszenia SMB, Sygnatariusze, Prezes Urzędu Ochrony Danych Osobowych oraz inni interesariusze. Po wypracowaniu projektu zmian Zarząd Stowarzyszenia kieruje wniosek o dokonanie zmian w Kodeksie pod obrady walnego zebrania członków Stowarzyszenia SMB. Projekt zmian wymaga przyjęcia przez walne zebranie członków Stowarzyszenia SMB uchwałą podjętą większością głosów.

W przypadku podjęcia uchwały o przyjęciu projektu zmian w Kodeksie, Zarząd Stowarzyszenia kieruje proponowane zmiany do Prezesa Urzędu Ochrony Danych Osobowych w celu uzyskania jego formalnej akceptacji.

Po uzyskaniu formalnej akceptacji Prezesa Urzędu Ochrony Danych Osobowych dla zmian w Kodeksie Zarząd Stowarzyszenia publikuje uchwałę o zmianie Kodeksu wraz z tekstem jednolitym Kodeksu (po zmianach) na stronie internetowej www.smb.pl. Ponadto o dokonanej zmianie zawiadamiani są indywidualnie wszyscy Sygnatariusze Kodeksu.

Zarząd Stowarzyszenia w terminie do dwóch tygodni od wprowadzenia zmian w Kodeksie, wysyła Sygnatariuszom wzór oświadczenia o potwierdzeniu (przez Sygnatariusza) zmian w Kodeksie, w tym o potwierdzeniu dostosowania się Sygnatariusza do zmian w Kodeksie.

W przypadku niezaakceptowania zmian przez Sygnatariusza w terminie 2 miesięcy Zarząd Stowarzyszenia podejmuje decyzję o odebraniu statusu Sygnatariusza.

4. Reguły wnoszenia i rozpatrywania skarg/reklamacji

Komisja Etyki KODO

SMB powołuje Komisję Skargową, której zadaniem jest przyjmowanie i rozpatrywanie skarg na praktyki Sygnatariuszy Kodeksu.

Członków Komisji Etyki KODO powołuje Zarząd SMB spośród osób mających wiedzę i doświadczenie w zakresie reguł przetwarzania danych osobowych, w tym Kodeksu, oraz w zakresie marketingu bezpośredniego. Komisja Etyki KODO jest odpowiedzialna za: (1) rozpatrywanie skarg na niezgodność działań Sygnatariuszy z Kodeksem i (2) podejmowanie czynności egzekwujących przeciw Sygnatariuszowi dopuszczającemu się naruszeń Kodeksu.

Komisja Etyki KODO działa na podstawie przyjętego przez siebie regulaminu rozpatrywania skarg, zatwierdzonego przez Walne Zgromadzenie Członków Stowarzyszenia SMB.

Proces Skargowy

Każdy, kogo interes został naruszony w wyniku nieprzestrzegania postanowień niniejszego Kodeksu przez Sygnatariusza, może złożyć skargę na tego Sygnatariusza do Stowarzyszenia SMB. Skarga może zostać złożona poprzez formularz internetowy znajdujący się pod adresem www.smb.pl (z możliwością dołączenia załączników).

Skarga powinna zawierać co najmniej:

- oznaczenie składającego skargę: imię, nazwisko lub nazwę firmy, adres korespondencyjny, adres email lub telefon kontaktowy
- oznaczenie Sygnatariusza, którego działanie jest przedmiotem skargi
- opis okoliczności, w jakich doszło do naruszenia Kodeksu
- ewentualnie – żądania wnoszącego skargę.

Skarga przyjmowana jest do rozpoznania przez Komisję Etyki KODO. Komisja działa na podstawie statutu SMB i regulaminu przyjętego przez walne zebranie członków SMB. Komisja Etyki KODO może kontaktować się z wnoszącym skargę jak również z Sygnatariuszem, przeciwko któremu została wniesiona skarga, w celu uzyskania pełnej informacji o zaistniałej sytuacji.

Komisja Etyki KODO wydając rozstrzygnięcie określa, czy miało miejsce naruszenie Kodeksu przez Sygnatariusza czy też skarga była nieuzasadniona. Rozstrzygniecie zawiera zwięzłe uzasadnienie. Komisja Etyki KODO przekazuje rozstrzygnięcie zainteresowanym stronom oraz Zarządowi

Stowarzyszenia. Na podstawie rozstrzygnięcia Zarząd Stowarzyszenia może zdecydować o potrzebie podjęcia dalszych działań, w szczególności:

- wezwać Sygnatariusza do zaprzestania praktyk niezgodnych z Kodeksem;
- zobowiązać Sygnatariusza do przedstawienia aktualnej opinii Jednostki Akredytującej lub Jednostki Certyfikującej potwierdzającej zgodność Przetwarzania Danych przez Sygnatariusza z postanowieniami niniejszego Kodeksu;
- zawiesić przedsiębiorcę w prawach Sygnatariusza Kodeksu na zasadach określonych przez Zarząd Stowarzyszenia;
- wykreślić przedsiębiorcę z rejestru Sygnatariuszy Kodeksu;
- zakazać przedsiębiorcy ponownego przystąpienia do Kodeksu na okres do 3 lat w przypadku powtarzającego się rażącego łamania Kodeksu

Treść orzeczeń Komisji Skargowej jest publikowana na stronie www.smb.pl, przy czym w publicznie dostępnych orzeczeniach dane osób wnoszących skargę oraz dane przedsiębiorców, przeciwko którym skargi zostały wniesione, podlegają anonimizacji.

Prawo do wniesienia skargi nie wyłącza ani nie ogranicza prawa do szukania ochrony swoich interesów na podstawie innych przepisów prawa.

Stowarzyszenie SMB nie ponosi odpowiedzialności za stwierdzone niezgodności w przetwarzaniu danych osobowych przez Sygnatariusza Kodeksu.

Stowarzyszenie SMB może zdecydować się na przyjęcie i rozpatrzenie skargi złożonej na inny podmiot niż Sygnatariusz Kodeksu, o ile rozpatrzenie takiej skargi będzie miało istotne znaczenie dla edukacji rynku oraz konsumentów w zakresie prawidłowych reguł ochrony danych osobowych. W takim przypadku Komisja Etyki KODO będzie odpowiednio stosowała regulacje opisujące przebieg procesu skargowego dla Sygnatariusza Kodeksu, z tym że wobec podmiotu, który nie jest Sygnatariuszem, określone działania w postaci żądania udzielenia informacji oraz przesłuchania przedstawicieli, będą podejmowane wyłącznie za jego zgodą.

Stowarzyszenie w każdym przypadku zastrzega sobie prawo opublikowania informacji o skardze i sposobie jej rozpatrzenia.

5. Reguły występowania do Urzędu Ochrony Danych Osobowych o interpretacje

Zarząd Stowarzyszenia może wystąpić do Prezesa Urzędu Ochrony Danych Osobowych z wnioskiem o udzielenie interpretacji w zakresie zasad stosowania Kodeksu w przypadku podjęcia uzasadnionych wątpliwości co do zgodności z prawem określonych praktyk. Wniosek kierowany do Prezesa Urzędu Ochrony Danych Osobowych powinien zawierać precyzyjną treść zapytania oraz szczegółowy opis problemu, jaki w praktyce wiąże się z danym zagadnieniem.

Zarząd może wystąpić do Prezesa Urzędu Ochrony Danych Osobowych:

- z własnej inicjatywy;
- na wniosek co najmniej 5 Sygnatariuszy Kodeksu
- na wniosek co najmniej 5 członków Stowarzyszenia SMB
- na wniosek walnego zebrania członków Stowarzyszenia SMB podjętego w formie uchwały.

Zarząd Stowarzyszenia publikuje na stronie www.smb.pl treść zapytań kierowanych do Prezesa Urzędu Ochrony Danych Osobowych oraz treść odpowiedzi udzielonych przez ten organ.