

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

(wersja do konsultacji społecznych, po zmianach z 23.03.2020 r.)

SPIS TREŚCI

WPROWADZENIE 5

Deklaracja 5

Cel ustanowienia Kodeksu 5

Zakres terytorialny stosowania 5

Interesariusze 5

Działania objęte przedmiotem Kodeksu 6

Słownik pojęć 6

Wyznaczenie inspektora ochrony danych przy przetwarzaniu danych osobowych do celów marketingu bezpośredniego 7

PRZEJRZYSTE PRZETWARZANIE DANYCH OSOBOWYCH W MARKETINGU BEZPOŚREDNIM. JAK REALIZOWAĆ OBOWIĄZEK INFORMACYJNY? 7

Dyrektywy ogólne dla obowiązku informacyjnego 7

Obowiązek informacyjny przy zbieraniu danych osobowych od osób, których dane dotyczą 8

Internet 9

Telefon 10

Na piśmie 12

W bezpośrednim kontakcie 12

Obowiązek informacyjny przy zbieraniu danych osobowych od osób trzecich (z innego źródła niż osoba, której dane dotyczą) 12

Agencje bazodanowe i publiczna platforma informacyjna 13

ŹRÓDŁA DANYCH OSOBOWYCH W MARKETINGU BEZPOŚREDNIM 14

Dane niezbędne do celów marketingu bezpośredniego 14

Podstawa prawna przetwarzania danych do celów marketingowych 16

Dodatkowe wyjaśnienia dla pozyskiwania danych od osób trzecich 18

ROZLICZALNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO 20

NAJCZĘŚCIEJ WYSTĘPUJĄCE FORMY MARKETINGU BEZPOŚREDNIEGO 21

Telemarketing przy połączeniach wychodzących – tzw. *outbound calls* 21

Telemarketing przy połączeniach przychodzących – tzw. *inbound calls* 22

Marketing bezpośredni drogą elektroniczną (e-mail, SMS, czat, inne) 22

Marketing bezpośredni pocztą tradycyjną (tzw. *Direct Mailing*) 23

Marketing bezpośredni w kontakcie osobistym (np. w punktach sprzedaży lub podczas promocji, targów i im podobnych wydarzeń) 23

Promowanie podmiotów trzecich 24

Profilowanie w działaniach marketingu bezpośredniego 24

Badania rynkowe 26
PRZEKAZYWANIE DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO 27
Zlecanie przetwarzania danych innemu podmiotowi 27
Role głównych podmiotów zaangażowanych w przetwarzanie danych osobowych w akcji promocyjnej 33
operatorom usług pocztowych i kurierskich 34
Przekazywanie danych osobowych innemu marketerowi do samodzielnego przetwarzania (np. sprzedaż bazy danych) 34
Ogólne reguły bezpieczeństwa przy przekazywaniu danych do celów marketingu bezpośredniego 35
PRZECHOWYWANIE DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO 36
Okres przechowywania danych przetwarzanych do celów marketingu bezpośredniego 36
Aktualność danych 37
Anonimizacja 37
Bezpieczeństwo techniczne i organizacyjne przy przetwarzaniu danych, w tym przy ich przechowywaniu 38
PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ W KONTEKŚCIE MARKETINGU BEZPOŚREDNIEGO 39
Prawo wycofania zgody na przetwarzanie danych do celów marketingu bezpośredniego 39
Prawo wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego 40
Prawo dostępu do informacji o przetwarzaniu danych do celów marketingu bezpośredniego 41
Prawo do usunięcia danych przetwarzanych do celów marketingu bezpośredniego („prawo do bycia zapomnianym”) 42
Pozostałe prawa osób, których dane dotyczą 44
INFORMOWANIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH PRZY MARKETINGU BEZPOŚREDNIM 44
STOSOWANIE KODEKSU I ADMINISTROWANIE 46
Monitorowanie przestrzegania Kodeksu 46
Przystąpienie i partycypacja w Kodeksie, jak również możliwość posługiwania się zaświadczeniem Sygnatariusza Kodeksu, są odpłatne. 47
Proces Skargowy 47
Sankcje nakładane przez organ monitorujący 48
Reguły dokonywania zmian w Kodeksie 48

WPROWADZENIE

Deklaracja

Mając na względzie, że dane osobowe oraz prywatność stanowią jedne z najważniejszych dóbr osobistych oraz że rozwój technologii umożliwia coraz szybsze i bardziej kompleksowe posługiwanie się danymi osobowymi, organizacje realizujące marketing bezpośredni, sygnujące niniejszy Kodeks, uznają potrzebę uporządkowania kwestii dotyczących przetwarzania danych osobowych zgodnie z obowiązującymi zasadami prawa i najlepszymi praktykami rynkowymi w celu zapewnienia bezpieczeństwa osobom, których dane dotyczą.

Cel ustanowienia Kodeksu

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

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

Przestrzeganie Kodeksu ma służyć budowie zaufania między odbiorcą marketingu bezpośredniego a kontaktującą się z nim organizacją, a także wspierać budowanie dobrego wizerunku branży marketingu bezpośredniego. Stosowanie jego postanowień przez podmioty działające na rynku ma na celu podniesienie satysfakcji odbiorców marketingu bezpośredniego. Rezultatem przestrzegania najwyższych norm i standardów przez przedsiębiorców jest zwiększanie skuteczności marketingu bezpośredniego z korzyścią zarówno dla odbiorców tego marketingu, jak i organizacji korzystających z tych narzędzi.

Zakres terytorialny stosowania

Kodeks adresowany jest do organizacji i przedsiębiorstw działających w branży marketingu bezpośredniego na terytorium Rzeczypospolitej Polskiej. Odnosi się zatem wyłącznie do czynności przetwarzania ograniczonych do ww. terytorium i ma zastosowanie wyłącznie na szczeblu krajowym.

Kodeks nie reguluje czynności przetwarzania prowadzonych w kilku państwach członkowskich w rozumieniu art. 40 ust. 7 RODO, a wszelkie jego postanowienia, które mogą odnosić się do transgranicznego charakteru przetwarzanych danych, należy interpretować jako postanowienia adresowane do organizacji i przedsiębiorstw w zakresie ich działalności w Polsce.

Interesariusze

Niniejszy Kodeks adresowany jest do wszelkich podmiotów, które na podstawie dobrowolnej deklaracji przystąpiły do stosowania Kodeksu.

Kodeks ma również istotne znaczenie dla pozostałych przedsiębiorstw i organizacji prowadzących marketing bezpośredni (we własnym imieniu lub na zlecenie innych przedsiębiorstw lub organizacji). Może służyć jako źródło wiedzy o obowiązujących regulacjach w marketingu bezpośrednim oraz o zasadach ich właściwego i etycznego stosowania.

Kodeks może stanowić źródło wiedzy dla odbiorców marketingu bezpośredniego i wszelkich innych osób, których dane osobowe są lub mogą być przetwarzane do celów marketingu bezpośredniego. Pozwoli on zrozumieć, jakie prawa przysługują tym osobom oraz w jaki sposób te prawa mogą być egzekwowane.

Działania objęte przedmiotem Kodeksu

Niniejszy Kodeks dotyczy działań marketingu bezpośredniego, a więc przede wszystkim prowadzenia komunikacji za pomocą jakichkolwiek środków bezpośredniego kontaktu, która obejmuje treści marketingowe, reklamowe lub promocyjne i jest skierowana do konkretnego odbiorcy.

Niniejszy Kodeks dotyczy również działań marketingowych polegających na:

a) organizowaniu akcji marketingowych (np. konkursy, loterie, sprzedaże promocyjne, programy lojalnościowe);
b) pozyskiwaniu danych osobowych po to, aby budować bazy danych do celów przyszłych działań marketingowych, a zwłaszcza marketingu bezpośredniego.

Wskazane powyżej działania marketingowe są realizowane przez podmioty branży marketingu bezpośredniego, a zwłaszcza przez członków Polskiego Stowarzyszenia Marketingu SMB.

Z komentarzem [1]: Wprowadzony został nowy fragment określający jasno, jakich działań dotyczy Kodeks.

Słownik pojęć

W niniejszym Kodeksie zastosowanie mają pojęcia, których definicje zawiera art. 4 Rozporządzenia 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 (zwane dalej w niniejszym Kodeksie „RODO").

„Podmiot przetwarzający", o którym mowa w art. 4 pkt 8 RODO zwany jest w niniejszym Kodeksie „**procesorem**".

W postanowieniach niniejszego Kodeksu posłużono się pojęciem „**marketer**", przez które należy rozumieć każdy podmiot realizujący działania marketingu bezpośredniego bez względu na to, czy robi to samodzielnie dla własnych celów, czy też w imieniu innego podmiotu lub na jego zlecenie. Adresatami postanowień niniejszego Kodeksu są bowiem wszelkie podmioty realizujące marketing bezpośredni, niezależnie od swojej roli w zakresie ochrony danych osobowych (administrator albo procesor). Administrator ostatecznie decyduje o celach i sposobach przetwarzania danych, ale zapewnienie prawidłowego przetwarzania danych jest zadaniem zarówno administratora, jak i procesora.

Z komentarzem [2]: Zastosowaliśmy nowe podejście redakcyjne – tak, aby uniknąć sytuacji, w której podmioty działające przeważnie jako procesorzy nie czuły się „zwolnione" z obowiązków, skoro większość postanowień Kodeksu była pierwotnie adresowana do „administratorów"

Ponadto, w Kodeksie posłużono się następującymi pojęciami charakterystycznymi dla działań marketingu bezpośredniego:

a) **marketing bezpośredni** – komunikacja odbywająca się za pomocą jakichkolwiek środków bezpośredniego kontaktu (w tym e-mail, telefon, SMS, komunikatory internetowe, kontakt osobisty, powiadomienia w aplikacji mobilnej, przesyłka adresowa, przesyłka bezadresowa zawierająca formularz do podania danych osobowych itp.), która obejmuje treści marketingowe, reklamowe lub promocyjne i jest skierowana do konkretnego odbiorcy;
b) **komunikat marketingowy** – każda treść, której celem jest skłonienie odbiorcy komunikatu do nabycia towaru lub usługi, niezależnie od wykorzystanych środków komunikowania; przykłady komunikatów marketingowych:
   - oferta kupna towaru lub usługi;
   - reklama danego towaru lub usługi, nawet jeżeli nie jest połączona z ofertą, ani nie określa ceny towaru lub usługi;

- zaproszenie na spotkanie promujące towary lub usługi;
- komunikat promujący akcję marketingową lub wydarzenie.

c) **zgoda na otrzymywanie komunikatów marketingowych** – zgoda potencjalnego odbiorcy marketingu bezpośredniego na to, aby określony podmiot kierował do tego odbiorcy komunikaty marketingowe z wykorzystaniem telefonu, e-maila lub innych środków komunikacji elektronicznej oraz telekomunikacyjnych urządzeń końcowych tego odbiorcy; uzyskanie takiej zgody spełnia jednocześnie wymóg zarówno art. 10 ustawy o świadczeniu usług drogą elektroniczną, jak i art. 172 ustawy – Prawo telekomunikacyjne.

Z komentarzem [3]: Postanowienia o komunikatach technicznych i obsługowych zostało przesunięte do merytorycznej części Kodeksu.

Z komentarzem [4]: Pojęcie profilowania jest szczegółowo opisana w merytorycznej części Kodeksu.

Wyznaczenie inspektora ochrony danych przy przetwarzaniu danych osobowych do celów marketingu bezpośredniego

Podmiot, który do celów marketingu bezpośredniego przetwarza w sposób trwały dane osobowe co najmniej 10 000 (dziesięciu tysięcy) osób, ma obowiązek wyznaczyć inspektora ochrony danych, o którym mowa w art. 37 ust. 1 RODO. Nie ma znaczenia, czy takie przetwarzanie jest realizowane w charakterze administratora czy procesora (tj. w imieniu innego podmiotu). Przetwarzanie danych osobowych do celów marketingu bezpośredniego w sposób trwały oznacza przetwarzanie danych osobowych wskazanej liczby osób przez okres co najmniej kolejnych 6 (sześciu) miesięcy.

Z komentarzem [5]: Zgodnie z sugestiami Urzędu wprowadziliśmy dodatkowe postanowienie dotyczące obowiązku wyznaczenia IOD.

PRZEJRZYSTE PRZETWARZANIE DANYCH OSOBOWYCH W MARKETINGU BEZPOŚREDNIM. JAK REALIZOWAĆ OBOWIĄZEK INFORMACYJNY?

Dyrektywy ogólne dla obowiązku informacyjnego

1. Marketer powinien stosować następujące, generalne reguły realizowania obowiązku informacyjnego wobec osób, których dane dotyczą:

a) tekst pisemnej klauzuli informacyjnej powinien być pisany czcionką o czytelnej wielkości i proporcjonalną do innych komunikatów, którym towarzyszy klauzula informacyjna, najlepiej czcionką bezszeryfową;

Przykłady:
1. *Dla kuponu loteryjnego o wymiarach 7x5 cm wystarczająca będzie czcionka o rozmiarze 6.*
2. *Na broszurze reklamowej wielkości kartki A4 czcionka klauzuli powinna odpowiadać standardowej czcionce zastosowanej w broszurze, jednak nie powinna być mniejsza od rozmiaru 8.*

b) język klauzuli informacyjnej powinien być możliwie najprostszy i jasny; sugerowane jest korzystanie z prostych i krótkich podpunktów oraz posługiwanie się zdaniami prostymi;

c) tam, gdzie to możliwe i nie wprowadza w błąd, sugerowane jest posługiwanie się językiem potocznym, codziennym;

d) klauzula informacyjna nie wymaga powoływania pełnych tytułów aktów prawnych oraz numerów dzienników urzędowych; jeśli jednak dane są przetwarzane dlatego, że jest to niezbędne do wywiązania się z obowiązku prawnego, w klauzuli informacyjnej powinien być wskazany konkretny przepis nakładający ten obowiązek poprzez podanie jednostki redakcyjnej aktu prawnego (np. artykuł),

e) klauzula informacyjna w tzw. „pierwszej warstwie" nie wymaga podawania dokładnego adresu siedziby administratora, ale powinna zawierać dane kontaktowe do niego, np. adres e-mail lub link do formularza kontaktowego.

Przykład nieprawidłowego języka przekazywania informacji:
Zgodnie z wymogami art. 13 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady 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. L 119 z 4.5.2016, str. 1—88) informujemy, że administratorem danych osobowych jest XYZ sp. z o.o., ul. Przykładowa 0, 00-000 Miasto, zarejestrowana w rejestrze przedsiębiorców Krajowego Rejestru Sądowego XIV Wydział Gospodarczy pod numerem KRS 9A8B7C6D543. Dane osobowe są przetwarzane w celu realizacji złożonego zamówienia. Podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. b Rozporządzenia Parlamentu Europejskiego i Rady 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. L 119 z 4.5.2016, str. 1-88).

Przykład prawidłowego języka przekazywania informacji:
Administratorem Twoich danych osobowych jest XYZ Sp. z o.o. z siedzibą w Mieście (daneosobowe@xyz.pl). Przetwarzamy Twoje dane osobowe do celów marketingowych. Więcej informacji na xyz.pl/dane.

2. Marketer powinien stosować odpowiednio powyższe zasady przy opracowywaniu treści zgody, które ma wyrażać osoba, której dane dotyczą.

Przykład negatywny klauzuli zgody:
Niniejszym wyrażam zgodę na przetwarzanie przez firmę XYZ sp. z o.o., ul. Przykładowa 0, 00-000 Miasto, zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego XIV Wydział Gospodarczy pod numerem KRS 9A8B7C6D543 moich danych osobowych do celów marketingowych, zgodnie z art. 6 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady 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. L 119 z 4.5.2016, str. 1—88).

Przykład pozytywny klauzuli zgody:
Zgadzam się przetwarzanie moich danych osobowych do celów marketingowych przez firmę XYZ Sp. z o.o. z siedzibą w Mieście.

3. Udostępnienie osobie, której dane dotyczą, klauzuli informacyjnej z pośrednictwem środków komunikowania się na odległość (np. e-mail, SMS, komunikator) nie stanowi przesyłania informacji handlowej w rozumieniu art. 10 ustawy o świadczeniu usług drogą elektroniczną ani wykorzystywania automatycznych systemów wywołujących lub telekomunikacyjnych urządzeń końcowych do celów marketingu bezpośredniego w rozumieniu art. 172 Prawa telekomunikacyjnego. Jej przesłanie nie wymaga zatem uzyskania odrębnej zgody osoby, której dane dotyczą, a proces informowania realizowany jest z powołaniem na obowiązek wynikający z przepisów prawa (art. 6 ust. 1 lit. c RODO w zw. z art. 13 lub art. 14 RODO).

Obowiązek informacyjny przy zbieraniu danych osobowych od osób, których dane dotyczą

Internet

W przypadku zbierania danych osobowych przez Internet, gdy osoba, której dane dotyczą, przekazuje swoje dane za pośrednictwem urządzenia końcowego (np. komputer, tablet, smartfon), obowiązek informacyjny powinien zostać zrealizowany z uwzględnieniem poniższych reguł.

4. Jeżeli w ramach formularza wyrażana jest jakakolwiek zgoda na przetwarzanie danych osobowych lub zgoda na otrzymywanie komunikatów marketingowych, to zgoda taka powinna zostać poprzedzona co najmniej następującymi informacjami, dostępnymi w tzw. „pierwszej warstwie" tekstu:
   a) kto jest administratorem danych osobowych;
   b) jaki jest cel przetwarzania danych;
   c) jakie dane (jaki rodzaj danych) będą zbierane i wykorzystywane (o ile są to dane inne niż te, które samodzielnie podaje osoba, której dane dotyczą);
   d) w przypadku dobrowolnej zgody na przetwarzanie szczególnych kategorii danych (tzw. danych wrażliwych) – jakie kategorie takich danych będą przetwarzane;
   e) o dobrowolności podania danych i wyrażenia zgody na ich przetwarzanie, a także prawie do cofnięcia zgody wraz ze wskazaniem, w jaki sposób zgodę można wycofać;
   f) jeżeli występuje – 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
   g) jeżeli występuje – informacje o tym, że dane będą przekazywane do państwa trzeciego (poza Europejski Obszar Gospodarczy) i możliwych zagrożeniach z tym związanych, o ile nie została wydana decyzja stwierdzająca odpowiedni stopień ochrony lub brak odpowiednich zabezpieczeń zgodnie z art. 46 RODO.

   Tylko jeżeli są przekazywane powyższe informacje można uznawać, że zgoda rozmówcy zostaje udzielona w warunkach dostatecznego poinformowania (jest świadoma).

5. Pozostała część klauzuli informacyjnej może być dostępna odrębnie, z wykorzystaniem następujących rozwiązań:
   a) poniżej pól formularza, który ma być wypełniony, a powyżej ikony akceptacji formularza – w formie rozwijanej klauzuli informacyjnej, która nosi tytuł np. „Informacje o ochronie danych osobowych", po najechaniu na którą lub po kliknięciu której użytkownikowi wyświetlana jest pełna treść informacji dotyczącej ochrony danych osobowych;
   b) 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);
   c) pełna klauzula informacyjna może znajdować się w całości poniżej formularza, który ma być wypełniony, a powyżej ikony akceptacji formularza – w formie zwykłego tekstu, z którym użytkownik może się swobodnie zapoznać.

Przykład:
Na stronie www występuje formularz rejestracji w serwisie internetowym wraz ze zgodami na otrzymywanie komunikatów marketingowych na podany adres e-mail. Marketer nie przetwarza szczególnych kategorii danych, nie przekazuje danych do państw trzecich, ani nie wykorzystuje danych do podejmowania decyzji opartych wyłącznie na automatycznym przetwarzaniu, które mogą mieć istotny skutek dla osoby fizycznej. Poniżej pól formularza znajdują się informacje:

Administratorem Twoich danych jest XYZ Sp. z o.o. z siedzibą w Mieście (daneosobowe@xyz.pl). Twoje dane będziemy przetwarzać w celu prowadzenia Twojego konta w serwisie. Jeśli się na to zgodzisz, będziemy wysyłać na Twój adres e-mail komunikaty marketingowe dotyczące naszych usług. Masz prawo w każdej chwili wycofać zgodę np. pisząc na daneosobowe@xyz.pl. Więcej informacji o przetwarzaniu Twoich danych znajdziesz tutaj.

Słowo „tutaj" stanowi aktywny i bezpośredni link do pełnej klauzuli informacyjnej. Po jego kliknięciu użytkownikowi wyświetla się rozszerzona treść klauzuli informacyjnej zawierająca szereg dodatkowych informacji, które są wymagane przepisami prawa. Jednocześnie w ramach tej informacji mogą występować dalsze odesłania do innych stron, dokumentów, zawierających już bardzo precyzyjne informacje (np. pełny katalog odbiorców danych).

Poniżej tej treści znajduje się klauzula zgody na otrzymywanie komunikatów marketingowych, która dla swojej ważności wymaga wyraźnego zaznaczenia. Zaznaczenie tej zgody jest dobrowolne.

◯ **Zgadzam się na przesyłanie ofert usług XYZ Sp. z o.o. na mój adres e-mail.**

Przycisk potwierdzający wysłanie formularza znajduje się poniżej ww. klauzul i informacji. Mogą im towarzyszyć inne oświadczenia, takie jak akceptacja regulaminu portalu.

Telefon

6. Wypełniając obowiązek informacyjny w rozmowie telefonicznej marketer (czyli zatrudniany przez niego konsultant) powinien przekazywać rozmówcy informacje w sposób wyraźny, w prostej i zwięzłej formie, w miarę możliwości codziennym językiem (o ile nie będzie to wprowadzało w błąd).

7. Jeżeli za pośrednictwem telefonu marketer (czyli zatrudniany przez niego konsultant) uzyskuje od rozmówcy zgodę w rozumieniu art. 6 ust. 1 lit. a RODO, 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 dane (jaki rodzaj danych) będą zbierane i wykorzystywane (o ile są to dane inne niż te, które samodzielnie podaje osoba, której dane dotyczą);
   d) w przypadku dobrowolnej zgody na przetwarzanie szczególnych kategorii danych (tzw. danych wrażliwych) – jakie rodzaje takich danych będą zbierane i przetwarzane;
   e) dobrowolności podania danych i wyrażenia zgody na ich przetwarzanie, a także prawie do cofnięcia zgody ze wskazaniem, jak można takie cofnięcie wykonać;
   f) jeżeli występuje – informacje o wykorzystywaniu danych do podejmowania decyzji opartych wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, które to decyzje mogą mieć istotny skutek dla rozmówcy;
   g) jeżeli występuje – informacje o tym, że dane będą przekazywane do państwa trzeciego (poza Europejski Obszar Gospodarczy i możliwych zagrożeniach z tym związanych, o ile nie została

wydana decyzja stwierdzająca odpowiedni stopień ochrony lub brak odpowiednich zabezpieczeń zgodnie z art. 46 RODO.

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

8. Jeżeli rozmówca zaakceptuje takie rozwiązanie, pozostała treść obowiązku informacyjnego, który wynika z art. 13 ust. 1-2 RODO, może zostać przekazana poprzez przesłanie na adres e-mail rozmówcy pełnej klauzuli informacyjnej w formie elektronicznej (np. TXT, PDF) po zakończeniu rozmowy lub poprzez podanie w trakcie rozmowy adresu strony www, na której rozmówca może zapoznać się z pełną klauzulą informacyjną.

Przykład fragmentu rozmowy:
Konsultant: Reprezentuję firmę kosmetyczną XYZ Sp. z o.o. z siedzibą w Mieście, przy ulicy [komunikat podawany przy założeniu, że ta informacja nie pojawiła się na wcześniejszym etapie rozmowy]. Czy byłaby Pani zainteresowana otrzymywaniem informacji o naszych nowościach produktowych? W tym celu będą nam potrzebne Pani imię, nazwisko, numer telefonu oraz adres e-mail.
Rozmówczyni: Tak, jestem zainteresowana.
Konsultant:. Może Pani w każdej chwili zrezygnować z otrzymywania takich informacji pisząc do nas na adres daneosobowe@xyz.pl, dzwoniąc na naszą infolinię 987654321 lub pisemnie na adres naszej firmy. Czy chciałaby Pani, abym przeczytała Pani teraz pełną informację o zasadach przetwarzania danych, czy wystarczy jej przesłanie do Pani mailem?
Rozmówczyni: Poproszę o jej przesłanie na mój adres e-mail: adres@e-mail.pl.

9. Zapytanie swojego dotychczasowego klienta o zgodę na otrzymywanie komunikatów marketingowych nie wymaga ponownego podawania informacji, które ten klient już zna.

Przykład fragmentu rozmowy:
Konsultant: Na zakończenie chciałabym jeszcze zapytać, czy chciałby Pan otrzymywać od nas newsletter zawierający naszą aktualną ofertę. Do tego będę jednak potrzebować dodatkowo Pana adres e-mail. W razie czego może Pan w każdej chwili odwołać swoją zgodę, klikając w link dostępny w stopce każdego naszego newslettera.
Klient: Z chęcią. Mój adres e-mail to: xyz@e-mail.pl
Konsultant: Dziękuję. W ciągu 5 minut na Pana adres e-mail przyjdzie link aktywacyjny. Po jego kliknięciu newsletter zostanie aktywowany.

10. 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 marketerowi).

11. W praktyce mają miejsce przypadki, w których firma w toku rozmowy telefonicznej chce przedstawić rozmówcy określoną ofertę, ale nie uzyskała wcześniej odrębnej zgody na otrzymywanie komunikacji marketingowej. W takim przypadku – w celu umożliwienia normalnej komunikacji międzyludzkiej – uprawnione jest zapytanie, czy rozmówca jest zainteresowany przedstawianiem mu w danym momencie określonej oferty produktu lub usługi danego podmiotu.

Jeżeli rozmówca wyraża zgodę – marketer (czyli zatrudniany przez niego konsultant) może przedstawić mu taką ofertę. Po zakończeniu części dotyczącej danej oferty i normalnej rozmowy z nią związanej marketer (czyli zatrudniany przez niego konsultant) powinien przedstawić te informacje, o których mowa w pkt 7 niniejszego Kodeksu, które nie są jeszcze znane rozmówcy po przeprowadzonej rozmowie. W dalszej części możliwe jest zapytanie, czy rozmówca wyraża ogólną zgodę na otrzymywanie w przyszłości komunikacji marketingowej.

Warunkiem zastosowania powyższego rozwiązania jest to, aby:

a) w celu przedstawiania oferty nie były zbierane ani wykorzystywane żadne dodatkowe dane o rozmówcy mające charakter szczególnych kategorii danych (tzw. wrażliwych);
b) rozmówca miał pełną świadomość, z kim prowadzi rozmowę oraz w każdej chwili mógł przerwać rozmowę albo poprosić o przedstawienie pełnych informacji dotyczących sposobu przetwarzania jego danych.

Na piśmie

12. W przypadku, gdy dane pozyskiwane są w formie pisemnej za pomocą formularza, taki formularz lub załącznik do niego powinien posiadać stosowną klauzulę informacyjną albo odesłanie do miejsca, gdzie klauzula informacyjna jest łatwo dostępna (np. do strony internetowej). Warunkiem zastosowania odesłania jest to, aby przeciętny odbiorca klauzuli informacyjnej miał łatwy dostęp do miejsca takiego odesłania.

W pozostałym zakresie marketer powinien odpowiednio stosować wytyczne dotyczące realizowania obowiązku informacyjnego przy zbieraniu danych osobowych za pośrednictwem Internetu.

W bezpośrednim kontakcie

13. W przypadku zbierania danych osobowych w relacji bezpośredniej (ustnie), marketer powinien być gotowy przedstawić klauzulę informacyjną w formie pisemnej (papierowej). Może to zostać zrealizowane poprzez udostępnienie każdej osobie kopii egzemplarza klauzuli albo poprzez wywieszenie treści klauzuli w miejscu łatwo dostępnym dla osoby, której dane są zbierane (np. w bezpośrednim sąsiedztwie stanowiska promocyjnego).

Przykład:
Firma na swoim stoisku promocyjnym na targach zbiera dane osób zainteresowanych jej ofertą, po to, aby móc im wysłać swój prospekt. Firma na swoim stoisku wywiesiła do wglądu tekst klauzuli informacyjnej oraz przyjęła dwa możliwe sposoby zbierania danych: ustne podanie swoich danych kontaktowych przez zainteresowaną osobę hostessie albo wrzucenie swojej wizytówki do specjalnej puszki opisanej hasłem „Wrzuć tutaj swoją wizytówkę, a odezwiemy się do Ciebie".

W pozostałym zakresie marketer powinien odpowiednio stosować wytyczne dotyczące realizowania obowiązku informacyjnego przy zbieraniu danych osobowych za pośrednictwem telefonu.

Obowiązek informacyjny przy zbieraniu danych osobowych od osób trzecich (z innego źródła niż osoba, której dane dotyczą)

14. W przypadku pozyskania danych osobowych od osób trzecich (z innego źródła niż osoba, której dane dotyczą), marketer ma obowiązek przekazać danej osobie niezbędne informacje wymagane przez art. 14 ust. 1-2 RODO za pośrednictwem najbardziej stosownego kanału komunikacji, uwzględniając zakres posiadanych o tej osobie danych, cele przetwarzania oraz koszty przekazania tej informacji. Z uwagi na powszechność oraz niskie koszty, sugerowane jest wykorzystywanie w tym celu poczty e-mail.

15. Informacje przekazywane osobom, których dane dotyczą po zebraniu ich danych od osób trzecich (z innego źródła niż osoba, której dane dotyczą) powinny w szczególności akcentować następujące informacje:
a) kto jest administratorem danych osobowych;

b) jaki jest cel przetwarzania danych;
c) z jakiego źródła dane osobowe zostały zebrane;
d) jakie kategorie danych zostały zebrane.

Pozostała część klauzuli informacyjnej przekazywanej zgodnie z art. 14 ust. 1-2 RODO może być dostępna odrębnie, w tzw. drugiej i trzeciej warstwie – np. na odrębnej podstronie www, do której prowadzi co najmniej wyraźnie wyodrębniony link zawarty w tzw. pierwszej warstwie obejmującej informacje opisane powyżej.

Przykład:
Administratorem Twoich danych osobowych jest XYZ Sp. z o.o. z siedzibą w Mieście (daneosobowe@xyz.pl). Otrzymaliśmy Twój adres do dostarczenia przesyłki od firmy ABC i przetwarzamy go, aby dostarczyć Ci przesyłkę. Więcej informacji o przetwarzaniu Twoich danych osobowych znajdziesz tutaj.

Słowo „tutaj" stanowi aktywny i bezpośredni link do pełnej klauzuli informacyjnej.

16. Informacje dotyczące przetwarzania danych marketer powinien przekazać przy okazji pierwszego kontaktu z daną osobą w ramach celu, w jakim dane osobowe zostały pozyskane, ale nie później niż w ciągu miesiąca od pozyskania tych danych. 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.

Agencje bazodanowe i publiczna platforma informacyjna

17. Sygnatariusze Kodeksu będący podmiotami specjalizującymi się w przetwarzaniu dużych zbiorów informacji handlowych (agencje bazodanowe, brokerzy danych itp.) mogą realizować obowiązek informacyjny z wykorzystaniem dedykowanej platformy internetowej prowadzonej pod adresem xxxxx (dalej: **Platforma**) – dla procesów zbierania danych z rejestrów publicznych, list, aktów lub dokumentów, które mogą być znane każdemu lub są dostępne publicznie (źródła publiczne).

18. Informacje handlowe, o których mowa w pkt 17 Kodeksu, obejmują dane osobowe osób fizycznych związane z prowadzoną działalnością lub zajmowaną funkcją (reprezentanci, wspólnicy, członkowie organów, przedstawiciele, jednoosobowe działalności). Informacje handlowe nie obejmują konsumentów ani danych, o których mowa w art. 9 oraz 10 RODO.

Platforma prowadzona jest przez Polskie Stowarzyszenie Marketingu SMB.

19. Na Platformie publikowane są następujące informacje:
a) dane podmiotów, o których mowa w pkt 17 Kodeksu uwzględniające: nazwę, adres siedziby, dane teleadresowe, adres e-mail inspektora ochrony danych, adres strony www;
b) odbiorcy lub kategorie odbiorców danych osobowych, którzy również jako administratorzy danych, mogą uzyskać dostęp do danych;
c) wszelkie możliwe transfery danych osobowych do klientów zlokalizowanych w krajach trzecich;
d) kategorie przetwarzanych danych;
e) prawnie uzasadniony interes realizowany w procesie, którym może być monitorowanie i zapobieganie oszustwom, gwarancja bezpieczeństwo i niezawodność usług świadczonych przez klientów, działalność marketingowa, handlowa, gospodarcza i finansowa, zgodnie z przepisami art. 6 ust. 1 lit. f) RODO;
f) okres przechowywania danych;

g) informacje o zautomatyzowanym przetwarzaniu danych obejmujące profilowanie osób, których dane dotyczą;
h) informacje o przysługujących prawach, w tym sposobie ich realizacji, z uwzględnieniem prawa do złożenia skargi do organu nadzoru.

20. Każdy z podmiotów, o których mowa w pkt 17 Kodeksu ma obowiązek zamieścić na swojej stronie w widocznym miejscu:
a) informację o Platformie oraz jej adresie (link) z opisem jej funkcjonalności;
b) pełną treść klauzuli informacyjnej związanej z prowadzeniem działalności, zgodnej z art. 14 RODO.

21. Platforma nie może służyć do spełniania obowiązku informacyjnego dla przypadków zbierania danych bezpośrednio od osób, których dane dotyczą.

22. Informacje handlowe, o których mowa w pkt 18 Kodeksu, mogą być udostępniane przez podmioty, o których mowa w pkt 17 Kodeksu zainteresowanym podmiotom, bez odrębnej zgody osoby, której dane dotyczą.

ŹRÓDŁA DANYCH OSOBOWYCH W MARKETINGU BEZPOŚREDNIM

Dane niezbędne do celów marketingu bezpośredniego

23. Zbierając dane osobowe do celów marketingu bezpośredniego, marketer powinien z góry określać zakres danych, które zamierza zbierać.

Przykład:
Wydawnictwo o tematyce rowerowej zbiera dane o swoich klientach, w stosunku do których chce przeprowadzić prostą kampanię telemarketingową i e-mailingową, informującą o swoim nowym produkcie. Wydawnictwo określa, że dla tego procesu niezbędne są: imię, nazwisko, adres e-mail, numer telefonu, informacje o dotychczasowych produktach kupowanych od Wydawnictwa przez klienta.

Przykład:
Agencja bazodanowa prowadzi działalność w obszarze agregowania i dalszego udostępniania informacji o osobach prowadzących działalność gospodarczą, które są dostępne w publicznych źródłach. Agencja na podstawie analizy zakresu danych, jakiego będą oczekiwać jej klienci, podejmuje decyzję o zbieraniu następujących danych: imię, nazwisko, firma, adres siedziby, adresy placówek, numer NIP, Regon, PKD, numer telefonu, adres e-mail, adres strony internetowej, status prowadzonej działalności, informacje o pozostawaniu w spółce cywilnej, informacja o ewentualnej rozdzielności majątkowej małżeńskiej.

Marketer powinien móc w sposób jasny i czytelny wykazać, że ustalony zakres danych jest niezbędny do działań marketingu bezpośredniego, które ten marketer chce realizować.

Z komentarzem [6]: Iza Biskup
Zgodnie z zasadą minimalizacji (art. 5 lit. c RODO) administrator powinien przetwarzać tylko te dane, które są niezbędne do realizacji danego celu.
Brakuje informacji w jakich konkretnych przypadkach można pozyskiwać poszczególne dane osobowe w tym w szczególności numer PESEL.

Z komentarzem [7R6]: Przedstawione poniżej przykłady budzą wątpliwości. Może wystąpić ryzyko, że będą stosowane bezrefleksyjnie, bez odniesienia do konkretnego celu i kontekstu. Nie wskazują precyzyjnie celu i niezbędności zbierania poszczególnych danych, np. wskazano datę urodzenia, podczas gdy czasami wystarczający jest wiek osoby lub też przedział wiekowy. Wskazywany jest też równocześnie np. nr telefonu i e-mail, podczas gdy dla konkretnego celu wykorzystywany może być wyłącznie e-mail.
W naszej ocenie warto rozbudować wskazówki dla administratorów na czym polega zasada minimalizacji danych oraz podkreślić potrzebę precyzyjnego określenia celu przetwarzania.

Z komentarzem [8R6]: Przykłady zostały skorygowane.

Przykład:
Podczas zbierania danych osobowych w celu promocji przekąsek (e-mail marketing, telemarketing, przesyłki tradycyjne) marketer uznał za adekwatny następujący zakres danych osobowych: imię, nazwisko, adres zamieszkania, numer telefonu, adres e-mail, preferencje żywieniowe. Nieadekwatne do celu będzie zbieranie danych takich, jak: numer PESEL, skan/numer dowodu tożsamości, dane dotyczące przekonań religijnych, politycznych itp.

24. Marketer powinien okresowo weryfikować, czy ustalony przez niego pierwotnie zakres danych jest adekwatny do celów marketingu bezpośredniego, które ten marketer realizuje lub chce realizować.

Przykład:
Dealer samochodowy po roku dokonuje ewaluacji swojej bazy marketingowej i stwierdza, że pierwotnie wpisał do niej informacje o wykonywanym zawodzie, mając na uwadze możliwość prezentowania dedykowanych ofert poszczególnym grupom zawodowym. Finalnie dealer ani razu nie wykorzystał tych danych i nie planuje ich wykorzystania, ponieważ zrezygnował z tego typu ofert. Dealer powinien usunąć z bazy marketingowej tego rodzaju dane.

25. Przetwarzanie szczególnych kategorii danych (tzw. danych wrażliwych) oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych do celów marketingu bezpośredniego jest dopuszczalne tylko wówczas, jeżeli dane te są w danym przypadku adekwatne.

Przykłady adekwatności:

1. *Przetwarzanie informacji o przekonaniach religijnych lub światopoglądowych dla promowania wydawnictwa o tematyce religijnej.*
2. *Przetwarzanie informacji o przekonaniach politycznych w celu kierowania komunikatów promujących określoną aktywność społeczną.*
3. *Przetwarzanie informacji dotyczących zdrowia w celu promowania produktów lub usług medycznych.*

Przykłady nieadekwatności:

1. *Przetwarzanie informacji o orientacji seksualnej w celu promowania jogurtu.*
2. *Przetwarzanie informacji o chorobach układu krążenia w związku z marketingiem bezpośrednim usług telefonicznych.*

26. Następujących przypadków nie uznaje się za przetwarzanie szczególnych kategorii danych (tzw. danych wrażliwych):

a) przetwarzanie zdjęcia osoby lub potencjalnego klienta np. w celu zaproponowania dostosowanej linii kosmetyków, przedstawienia wizualizacji określonego produktu w zestawieniu z wizerunkiem klienta, rozpoznania podstawowych i łatwo rozpoznawalnych cech klienta (np. płci oraz przedziału wiekowego) na potrzeby weryfikacji, czy może on wziąć udział w programie promocyjnym;

b) przechowywanie zdjęcia przesłanego w ramach zgłoszenia do konkursu lub innej akcji marketingowej, zawierającego wizerunek uczestnika lub innych osób znajdujących się na zdjęciu;

c) przetwarzanie danych o zakupionych wcześniej lub o obserwowanych w sieci produktach lub usługach w celu przedstawienia klientowi lub potencjalnemu klientowi dostosowanej oferty sprzedaży;

Z komentarzem [9]: W jaki sposób miałoby być prowadzone rozpoznanie cech płciowych i wiekowych? Czy obejmowałoby automatyczną analizę?

Z komentarzem [10R9]: Zgodnie z pkt 80. Wytycznych EROD nr 3/2019 ws. przetwarzania danych za pośrednictwem urządzeń video, wersja 2.0 (z dnia 29 stycznia 2020) – automatyczna identyfikacja cech typu płeć czy wiek nie stanowi przetwarzania danych wrażliwych.

Przykład:
Konsument kupuje lekarstwa lub suplementy diety w aptece internetowej. Zbieranie informacji o preferencjach zakupowych przez aptekę internetową w celu proponowania konsumentowi w przyszłości produktów podobnych (o podobnym składzie, działaniu) nie jest uznawane za przetwarzanie danych wrażliwych i działanie takie nie wymaga wyraźnej zgody. Jeśli jednak ta sama apteka internetowa zestawia informacje o kupowanych przez klienta lekach w celu ustalenia prawdopodobnej choroby/schorzenia, na które klient cierpi, po to, aby przedstawić mu dopasowaną ofertę, konieczne będzie uzyskanie uprzedniej, odrębnej i wyraźnej zgody osoby, której dane dotyczą.

d) dane pochodzące z aktywności w sieci i wnioskowanie z nich;

e) nieintencjonalne wejście w posiadanie danych o wrażliwym charakterze, jeżeli nie będą dalej wykorzystywane przez marketera danych w normalnym toku działalności

Przykład:
Producent produktów spożywczych realizuje konkurs, którego treścią jest przedstawienie w formie krótkiego tekstu zalet danego produktu spożywczego. Dziesięć najlepszych zgłoszeń wygra nagrody. Jeden z uczestników konkursu przesyła zgłoszenie, w którym pisze, że dany produkt spożywczy jest dla niego najlepszy, ponieważ pomaga mu na jego chore serce. W takim przypadku marketer może rozpoznać takie zgłoszenie konkursowe normalnie, bez konieczności uzyskiwania dodatkowej zgody na przetwarzanie szczególnej kategorii danych od zgłaszającego oraz bez konieczności odrzucenia zgłoszenia jako zawierającego dane, których marketer nie może przetwarzać. Jednocześnie dane pozyskane w ten sposób nie mogą być przetwarzane w innych celach (chyba, że marketer pozyska w tym zakresie odrębną wyraźną zgodę uczestnika oraz dane te będą adekwatne do planowanego celu).

27. Zgoda na przetwarzanie szczególnych kategorii danych (tzw. danych wrażliwych) musi być wyraźna. W przypadku dzieci zgody takiej powinni udzielać ich rodzice lub opiekunowie prawni. Zgody na przetwarzanie danych wrażliwych nie można wywodzić z oświadczeń o innej treści lub wnioskować z działań osoby, której dane dotyczą. Najlepszym i rekomendowanym przez niniejszy Kodeks sposobem uzyskiwania wyraźnej zgody jest uzyskanie odrębnego, wyraźnego oświadczenia od osoby, której dane dotyczą, że wyraża ona zgodę na przetwarzanie w konkretnym celu określonych szczególnych kategorii danych (tzw. danych wrażliwych), które jej dotyczą.

Podstawa prawna przetwarzania danych do celów marketingowych

28. W każdym przypadku zbierania danych osobowych marketer powinien zapewnić, aby zbieranie to odbywało się na podstawie jednej z podstaw prawnych wskazanych w RODO.

29. Marketer może przetwarzać pozyskane przez siebie dane swoich klientów lub potencjalnych klientów również do celów marketingowych na podstawie klauzuli prawnie uzasadnionego interesu administratora danych.

Przykład:
Marketer przy organizacji akcji promocyjnej uzyskał od uczestnika dane identyfikacyjne, dane teleadresowe, informacje o zainteresowaniach i wykonywanym zawodzie (podanie tych danych, było w danym przypadku uzasadnione charakterem konkursu skierowanego do danej grupy zawodowej). Marketer ma prawo wykorzystać uzyskane w ten sposób dane również dla potrzeb swoich działań marketingowych w przyszłości.

Z powołaniem na klauzulę swojego prawnie uzasadnionego interesu marketer nie może przetwarzać szczególnych kategorii danych ani danych, o których mowa w art. 10 RODO (danych osobowych dotyczących wyroków skazujących i czynów zabronionych).

30. Podstawą przetwarzania danych do celów marketingu bezpośredniego w przeważającej części przypadków będą: zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO) albo realizacja prawnie uzasadnionych interesów marketera jako administratora lub strony trzeciej (art. 6 ust. 1 lit. f RODO).

31. Pomiędzy podstawami prawnymi przetwarzania danych osobowych do celów marketingowych nie ma różnicy jakościowej. Żadna z tych podstaw nie jest preferowana lub domyślna. Jeżeli jednak marketer zdecydował się uzyskać zgodę na przetwarzanie danych osobowych do celów marketingu bezpośredniego i osoba, której dane dotyczą, takiej zgody nie wyraziła, to marketer nie może przetwarzać danych osobowych tej osoby do celów marketingu bezpośredniego z powołaniem na swój prawnie uzasadniony interes.

32. Zgoda jako wyłączna podstawa przetwarzania danych osobowych do celów marketingowych jest wymagana, gdy marketer nie może zasadnie opierać się na klauzuli prawnie uzasadnionego interesu. Dotyczy to przetwarzania danych osobowych uznawanych za szczególne kategorie danych (tzw. dane wrażliwe), jak również danych, o których mowa w art. 10 RODO.

> ***Przykład:***
> *Marketer oferuje towary lub usługi, dla których promocji chce wykorzystywać szczególne kategorie danych (np. dane genetyczne, szczegółowe informacje o stanie zdrowia). Wykorzystanie takich danych do celów marketingowych tego marketera musi być poprzedzone uzyskaniem odrębnej, wyraźnej zgody od osoby, której dane dotyczą.*

33. Z powołaniem na klauzulę uzasadnionego interesu nie powinno odbywać się również przetwarzanie danych do celów marketingowych, które spełnia warunki określone w art. 22 RODO. W takim przypadku zgoda jest wyłączną podstawą przetwarzania danych osobowych.

> ***Przykład:***
> *Marketer chce wykorzystać system sztucznej inteligencji do profilowania swoich klientów w taki sposób, aby wybrać wyłącznie tych, którzy mają największą szansę stać się stałymi klientami danej marki. Na podstawie przeprowadzonego profilowania system informatyczny przesyła do wybranych osób zniżki na produkty marki lub imienne zaproszenia do udziału w zamkniętej loterii promocyjnej.*

34. Marketer ma również obowiązek uzyskać uprzednią zgodę potencjalnego odbiorcy na realizowanie określonych działań marketingu bezpośredniego, jeśli wyraźnie wymaga tego przepis prawa (np. art. 172 ustawy – Prawo telekomunikacyjne).

35. Działaniami marketingu bezpośredniego nie jest kierowanie do odbiorców komunikatów technicznych lub obsługowych. Są to takie komunikaty, których:
    a) odbiorcą jest osoba, którą łączy z nadawcą komunikatu relacja prawna lub faktyczna (np. odbiorca jest klientem nadawcy);
    b) celem jest zapewnienie prawidłowej obsługi ww. osoby w ramach wspomnianej relacji prawnej lub faktycznej, np. obsługa transakcji, przeprowadzenie akcji promocyjnej lub badanie satysfakcji klienta.

    Nadawca komunikatu nie musi uzyskiwać uprzedniej zgody odbiorcy na przesyłanie do niego komunikatów technicznych i obsługowych.

Przykłady komunikatów technicznych i obsługowych:

(1) *E-mail z potwierdzeniem realizacji zamówienia lub z potwierdzeniem rejestracji na portalu internetowym.*

(2) *Kontakt z klientem w sprawie zbliżającego się zakończenia umowy (np. subskrypcji oprogramowania) w celu poinformowania o możliwych konsekwencjach braku przedłużenia umowy (np. utrata możliwości korzystania z programu) i zaproszenia do zapoznania się z możliwościami jej przedłużenia.*

(3) *Kontakt z osobą, która zgłosiła już udział w akcji promocyjnej w celu związanym z bieżącą obsługą akcji, a zwłaszcza kontakt z laureatem nagrody w celu powiadomienia o wygranej.*

(4) *Wszelkie odpowiedzi na korespondencję przesłaną przez klienta, z jego inicjatywy (np. odpowiedzi na reklamacje, zapytania).*

36. Dla realizacji akcji promocyjnej (np. konkursu, loterii promocyjnej) podstawą prawną przetwarzania danych osobowych na potrzeby realizacji tej akcji jest art. 6 ust. 1 lit. b RODO. Przepis ten należy stosować również do akcji promocyjnych realizowanych w trybie tzw. przyrzeczenia publicznego (art. 919-921 Kodeksu cywilnego).

Z komentarzem [11]: Iza Biskup
Błędna podstawa prawna do przetwarzania danych. W przypadku przeprowadzenia konkursu niezbędna jest zgoda uczestnika (6 ust. 1 lit. a RODO)

Przykład:
Marketer realizuje konkurs konsumencki, który ma swój regulamin. Zgodnie z regulaminem w konkursie Jury ma wyłonić 5 najlepszych prac plastycznych – pomysłów na nowe logo dla produktu marketera. Regulamin przewiduje, że dla laureatów przewidziane są nagrody, a w zamian za nagrody laureaci przeniosą na marketera autorskie prawa majątkowe do swoich prac. Uczestnik przystępując do konkursu i zgłaszając swoją pracę jest zobowiązany zaakceptować regulamin konkursu (jako warunek wzięcia w nim udziału). W takim przypadku przetwarzanie danych na potrzeby konkursu wiąże się z charakterem obligacyjnym dla obu stron.

Dodatkowe wyjaśnienia dla pozyskiwania danych od osób trzecich

37. Marketer może pozyskiwać dane osobowe do celów marketingu bezpośredniego nie tylko od osoby, której dane dotyczą. Może w sposób legalny i równorzędny wejść w posiadanie danych o określonej osobie od osób trzecich.

Przykłady:

1. *Uzyskanie danych od innego administratora, który w ramach swojej działalności jest uprawniony do udostępniania posiadanych danych podmiotom trzecim dla określonych celów.*
2. *Uzyskanie danych z publicznie dostępnych źródeł, w tym opublikowanych w związku ze świadczeniem usług społeczeństwa informacyjnego.*
3. *Uzyskanie danych od innej osoby fizycznej niebędącej administratorem ani podmiotem przetwarzającym (np. informacje od konsumenta o członkach jego rodziny, o jego znajomych).*

38. 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 udostępnienia danych innemu podmiotowi.

39. W przypadku udostępniania danych osobowych dotyczących konsumentów przyjmuje się generalną zasadę, że podstawą udostępnienia do celów marketingowych powinna być zgoda osób, których dane dotyczą. W przypadku pozostałych danych osobowych (dane przedsiębiorców, przedstawicieli spółek lub organizacji) podstawą prawną udostępnienia danych może być prawnie uzasadniony interes.

Z komentarzem [12]: Należy rozgraniczać osoby fizyczne prowadzące działalność gospodarczą, które zgodnie z RODO mają taki sam poziom ochrony jak konsumenci.

Przykład:
Agencja bazodanowa pozyskała dane osobowe konsumentów. Warunkiem udostępnienia danych osobowych innym podmiotom w ich celach marketingowych jest uzyskanie od konsumentów zgody na udostępnienie tych danych podmiotom trzecim określonym co do kategorii.

40. Marketer otrzymujący bazę danych potencjalnych odbiorców marketingu bezpośredniego od innego podmiotu powinien dokonać niezbędnej analizy, czy podmiot ten 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.

Przykład:
Marketer przed otrzymaniem danych osobowych konsumentów sprawdza: (1) wzór/wzory stosowanej przez udostępniającego zgody na dalsze udostępnienie danych; (2) wzór/wzory stosowanej klauzuli informacyjnej.

Rozliczalność posłużenia się przez udostępniającego tymi wzorami powinna być zweryfikowana wobec próby 20 losowo wybranych rekordów (np. skany formularzy pisemnych; dane z systemu informatycznego).

1. Marketer otrzymujący dane od innego administratora nie ma obowiązku dokonywać ww. analizy, jeżeli:
a) udostępniający jest podmiotem certyfikowanym w rozumieniu art. 42 RODO;
b) udostępniający jest sygnatariuszem niniejszego Kodeksu.

41. Dane osobowe osób fizycznych prowadzących działalność gospodarczą oraz osób fizycznych będących przedstawicielami lub członkami organów spółek handlowych, których dane osobowe są ujawnione publicznie (m.in. w Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz Krajowym Rejestrze Sądowym) mogą być zbierane przez marketerów bezpośrednio z publicznie dostępnych rejestrów w celu ich wykorzystania do celów marketingu bezpośredniego lub w celu ich dalszej dystrybucji z powołaniem na prawnie uzasadniony interes administratora danych. Dane zebrane z takich źródeł uznaje się za dane zebrane z innego źródła niż od osoby, której dane dotyczą.

W przypadku danych osobowych przedsiębiorców, w tym osób fizycznych prowadzących działalność gospodarczą – z uwagi na ich powszechną dostępność – marketer przyjmujący nie ma obowiązku dokonywania analizy zbioru. W przypadku zbierania danych osobowych z publicznie dostępnych, zaufanych źródeł, przyjmuje się domniemanie ich udostępnienia w zgodzie z przepisami prawa.

Za zaufane źródła pochodzenia danych osobowych przedsiębiorców, przedstawicieli oraz członków organów spółek handlowych przyjmuje się w szczególności wszelkie publiczne rejestry oraz strony internetowe prowadzone lub nadzorowane przez tych przedsiębiorców (w tym firmowe strony i wizytówki w serwisach społecznościowych).

ROZLICZALNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO

42. Marketer przeprowadza działania marketingu bezpośredniego w taki sposób, aby był w stanie wykazać zgodność tych działań z przepisami o ochronie danych osobowych. Dotyczy to między innymi przekazywania osobom, których dane dotyczą, wszelkich wymaganych informacji związanych z przetwarzaniem ich danych osobowych przy zastosowaniu odpowiednich środków organizacyjnych lub technicznych – czyli takich, które będą możliwe do zweryfikowania pod kątem tego, czy rzeczywiście są stosowane.

Obowiązek rozliczalności przetwarzania danych osobowych polega na tym, że marketer powinien przechowywać takie informacje o swoich działaniach związanych z przetwarzaniem danych osobowych, które będą pokazywać, że marketer systemowo spełnia wymagania RODO, np. obowiązek informacyjny wynikający z art. 13 lub art. 14 RODO. Systemowo, to znaczy metody działania administratora są zgodne z RODO. Marketer może wykazać, że spełnia obowiązek informacyjny względem osób, których dane dotyczą np. w ten sposób, że opracował i wdrożył w tym zakresie efektywną procedurę.

Przykład:
Marketer na konferencjach organizuje konkursy wizytówkowe. Uczestnictwo w konkursie potwierdza się wyłącznie poprzez wrzucenie do urny swojej wizytówki. Obowiązek informacyjny może zostać spełniony poprzez zamieszczenie informacji o ochronie danych osobowych uczestników konkursu w bezpośrednim sąsiedztwie urny.
Na potrzeby spełnienia wymogu rozliczalności marketer w swojej dokumentacji może zachować wzorcowy regulamin takiego konkursu wizytówkowego oraz wzorcową klauzulę informacyjną, która jest umieszczana w sąsiedztwie urny. Ponadto, zespół odpowiedzialny za promocję na konferencjach otrzymał polecenie każdorazowego ich stosowania.

Obowiązek rozliczalności przetwarzania danych osobowych nie polega na tym, że marketer musi trwale odnotowywać wszelkie swoje czynności (w ramach których wykonuje obowiązki RODO) w każdym indywidualnym przypadku osoby, której dane dotyczą. Nie jest obowiązkiem marketera zbieranie indywidualnych dowodów na to, że konkretnej osobie, której dane dotyczą, udzielił wymaganych informacji o ochronie jej danych osobowych.

43. Zakres informacji, które marketer powinien zachować, aby wykazać zgodność swojego działania z przepisami o ochronie danych osobowych będzie się różnić w zależności od obowiązku wynikającego z RODO. W przypadku, gdy marketer opiera przetwarzanie danych osobowych do celów marketingu bezpośredniego na zgodzie osoby, której dane dotyczą, ma obowiązek utrwalać i przechowywać informacje pozwalające wykazać, że zgoda została wyrażona oraz, że spełnia ona wymagania określone w RODO. RODO wymaga bowiem, aby zgoda była m. in. świadoma, jednoznaczna i konkretna, dlatego niezbędna jest pewność, że konkretna osoba, której dane marketer przetwarza, wyraziła na to zgodę.

W przypadku zgód wyrażanych w formie pisemnego oświadczenia ich utrwalenie oraz przechowywanie może polegać na archiwizacji papierowych dokumenty oświadczeń lub na wykonaniu ich kopii cyfrowej (skanów).

W przypadku zgód wyrażanych w formie ustnych oświadczeń (najczęściej w rozmowie telefonicznej), ich utrwalenie oraz przechowywanie może polegać na nagrywaniu rozmów i archiwizacji nagrań.

W przypadku zgód wyrażanych w formie oświadczenia złożonego drogą elektroniczną, ich utrwalenie oraz przechowywanie może polegać zachowaniu i archiwizowaniu następujących informacji:

Z komentarzem [13]: Kwestia do rozwinięcia. W braku wyjaśnienia konieczne może okazać się usunięcie.

Z komentarzem [14R13]: Kwestie rozliczalności zostały znacznie rozbudowane.

a) treści oświadczenia;
b) danych dotyczących sesji, w trakcie której zostało złożone oświadczenie (data i godzina oświadczenia, adres IP, z którego wyrażono oświadczenie, dane osobowe podane przy wyrażeniu oświadczenia);
c) informacje, które zostały przedstawione osobie, której dane dotyczą przed wyrażeniem zgody.

Z komentarzem [15]: Rozdział o naruszeniach (incydentach) został przeniesiony w inne miejsce Kodeksu oraz istotnie rozbudowany z uwzględnieniem dotychczasowych uwag Urzędu.

NAJCZĘŚCIEJ WYSTĘPUJĄCE FORMY MARKETINGU BEZPOŚREDNIEGO

Z komentarzem [16]: Rozdział o dotyczący konkretnych działań marketingu bezpośredniego (wykorzystanie danych) został istotnie zmieniony i rozbudowany z uwzględnieniem dotychczasowych uwag Urzędu.

44. Każde działanie marketingu bezpośredniego powinno zostać poprzedzone weryfikacją, czy będzie ono adresowane do przedsiębiorców (B2B) czy do konsumentów (B2C). W zależności od odbiorców przyszłej komunikacji marketingowej różne mogą być prawa i obowiązki marketera oraz osób, których dane dotyczą. W działaniach marketingu bezpośredniego szczególną ochroną należy obejmować osoby, które tego wymagają ze względu na swój wiek, stan zdrowia lub inne podobne okoliczności. Dotyczy to zwłaszcza dzieci oraz osób w podeszłym wieku.

Telemarketing przy połączeniach wychodzących – tzw. *outbound calls*

45. Telefoniczny marketing bezpośredni wymaga przetwarzania danych osobowych co najmniej w zakresie numeru telefonu, na który wykonywane jest połączenie. Dane powinny pochodzić z pewnych i sprawdzonych źródeł, a marketer powinien posiadać prawną podstawę dla przetwarzania takich danych osobowych (np. swój prawnie uzasadniony interes). Za praktyki niedozwolone i naruszające reguły ochrony danych osobowych uznaje się w szczególności:
   a) wykonywanie połączeń na numery wygenerowane losowo,
   b) wykonywanie połączeń na numery z posiadanej bazy danych i informowanie rozmówców, że połączenie zostało wykonane na numer wygenerowany losowo.

46. Wykonywanie połączeń telefonicznych, których celem jest prezentowanie komunikatów marketingowych, wymaga uzyskania uprzedniej zgody odbiorcy takich połączeń. Obowiązek uzyskania zgody jest niezależny od technologii wykorzystanej do wykonania połączenia (telefonia stacjonarna, komórkowa, z wykorzystaniem protokołu IP, wideorozmowa lub tym podobne). Zgoda musi być wyrażona uprzednio – to jest przed wysłaniem komunikatu marketingowego.

47. Wykonywanie sprzedażowych połączeń telefonicznych z tą samą lub podobną ofertą do tego samego odbiorcy nie może być realizowane częściej niż co jeden miesiąc. Aby to zapewnić, marketer zobowiązany jest dołożyć należytej staranności, aby osoby lub podmioty, którymi posługuje się dla realizacji telemarketingu były wyposażone w system integrujący (np. oprogramowanie lub proces organizacyjny), który pozwoli na bieżąco monitorować wykonywane połączenia marketingowe.

48. Jeśli w trakcie rozmowy rozmówca skieruje do konsultanta pytanie dotyczące ochrony danych osobowych, konsultant powinien udzielić mu co najmniej następujących, podstawowych informacji:
   a) kto jest administratorem danych;
   b) w jaki celu dane są przetwarzane;
   c) gdzie można uzyskać więcej informacji na temat ochrony danych osobowych.

49. W trakcie rozmowy odbiorca marketingu bezpośredniego może cofnąć swoją zgodę na telemarketing lub wyrazić sprzeciw wobec dalszego przetwarzania jego danych osobowych do celów marketingu bezpośredniego. Konsultant ma obowiązek takie cofnięcie zgody lub sprzeciw odnotować w sposób, dzięki któremu żądania rozmówcy zostaną wykonane. Marketer zapewnia, aby odnotowanie cofnięcia zgody lub sprzeciwu przez konsultanta odbywało się w taki sposób, aby było widoczne dla innych konsultantów pracujących dla marketera lub podmiotu zewnętrznego działającego w imieniu marketera.

2. Marketer powinien odnotować i uwzględnić sprzeciw nie później niż w ciągu w ciągu miesiąca od zgłoszenia sprzeciwu. Jeżeli z przyczyn technicznych lub organizacyjnych taki termin nie jest możliwy (np. awaria systemu, wysoka liczba wpływających zgłoszeń itp.), może ulec wydłużeniu. Takim przypadku marketer powinien w ciągu miesiąca od zgłoszenia sprzeciwu poinformować o wydłużeniu terminu osobę, której dane dotyczą wraz z podaniem przyczyny wydłużenia terminu oraz podaniem terminu, w którym sprzeciw zostanie uwzględniony.

50. Telefoniczny marketing bezpośredni w celu przedstawienia oferty przeznaczonej dla konsumentów może być realizowany w dni robocze pomiędzy godziną 8:00 a 20:00, a w soboty pomiędzy godziną 10:00 a 16:00, chyba, że odbiorca takiego marketingu wcześniej zażyczył sobie, aby kontakt miał miejsce w innych godzinach. W uzasadnionych przypadkach, ze względu na specyfikę grupy docelowej, dopuszcza się kontakt w innych godzinach.

Telemarketing przy połączeniach przychodzących – tzw. *inbound calls*

51. Konsultant powinien w pierwszej kolejności odpowiedzieć na problem, z którym klient zadzwonił do contact center (np. zainteresowanie określonym produktem, skorzystanie z pomocy helpdesk itp.).

Jeśli dzwoniący nie wyrażał wcześniej sprzeciwu wobec przetwarzania jego danych osobowych do celów marketingu bezpośredniego, konsultant po zrealizowaniu zasadniczego celu rozmowy może:

a) poprosić osobę dzwoniącą o potwierdzenie aktualności jej danych osobowych i w razie potrzeby dokonać ich zmiany;
b) przedstawić dodatkową ofertę produktu lub usługi;
c) zapytać osobę dzwoniącą o to, czy wyraża zgodę na otrzymywanie komunikatów marketingowych.

52. Przedstawiając osobie dzwoniącej dodatkową ofertę, konsultant może uwzględnić posiadane w bazie dane osobowe, w tym informacje o wcześniejszych preferencjach zakupowych, w celu lepszego dopasowania oferty do zainteresowań ww. osoby.

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

53. Prowadzenie marketingu bezpośredniego drogą elektroniczną (np. e-mail, SMS, komunikatory internetowe), wymaga przetwarzania danych osobowych co najmniej w zakresie adresu elektronicznego odbiorcy (np. adresu e-mail, numeru telefonu lub nazwy użytkownika komunikatora), na który kierowana jest komunikacja marketingowa. Takie dane kontaktowe powinny pochodzić z pewnych i sprawdzonych źródeł, a marketer powinien posiadać prawną podstawę dla przetwarzania takich danych osobowych (np. swój prawnie uzasadniony interes).

54. Wysyłanie komunikatów marketingowych drogą elektroniczną do osoby, której dane dotyczą wymaga uzyskania jej uprzedniej zgody. Obowiązek uzyskania zgody jest niezależny od

technologii wykorzystanej do wysłania komunikatu. Zgoda osoby, której dane dotyczą musi być wyrażona uprzednio – to jest przed wysłaniem komunikatu marketingowego.

55. Na zasadzie wyjątku od obowiązku uzyskania uprzedniej zgody, zgodnie z przepisami Unii Europejskiej (art. 13 ust. 2 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 lub przepis go zastępujący) marketer może przesyłać komunikaty marketingowe do klienta drogą elektroniczną bez uzyskania uprzedniej zgody, w przypadku gdy marketer otrzymał od takiego klienta 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 własnych podobnych produktów lub usług marketera pod warunkiem, że klienci 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 klientów, którzy początkowo nie sprzeciwili się takiemu wykorzystywaniu.

Marketing bezpośredni pocztą tradycyjną (tzw. *Direct Mailing*)

56. Adresowany indywidualnie marketing pocztowy (czyli przesyłka reklamowa do zidentyfikowanego odbiorcy) może być realizowany tylko pod warunkiem posiadania podstawy prawnej przetwarzania danych osobowych odbiorców do celów marketingu bezpośredniego (zgoda odbiorcy lub prawnie uzasadniony interes marketera). Prowadzenie marketingu bezpośredniego pocztą tradycyjną (tzw. Direct Mailing) nie wymaga uzyskania odrębnej zgody odbiorcy (inaczej niż w przypadku marketingu bezpośredniego drogą telefoniczną lub elektroniczną).

Marketing bezpośredni w kontakcie osobistym (np. w punktach sprzedaży lub podczas promocji, targów i im podobnych wydarzeń)

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

Formularze służące do zbierania danych mogą być wypełniane własnoręcznie przez osobę, która podaje dane osobowe lub przez upoważnioną przez marketera osobę (np. pracownika marketera). W przypadku, gdy formularz wypełnia upoważniona przez marketera osoba, a osoba, której dane dotyczą podaje swoje dane 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).

Przykłady:

1. *Osoba upoważniona wpisuje do formularza dane podawane ustnie przez osobę, której dane dotyczą. Ponieważ w pobliżu przebywają osoby postronne, osoba upoważniona prosi o zapisanie poszczególnych informacji na kartce i następnie przepisuje do formularza, a kartkę zwraca osobie, której dane dotyczą.*
2. *Osoba upoważniona wpisuje do formularza dane podawane ustnie przez osobę, której dane dotyczą. W pewnym momencie do osoby tej podchodzi osoba postronna i chce rozpocząć rozmowę. Osoba upoważniona odwraca formularz na niezapisaną stronę albo przykrywa go innym przedmiotem – tak, aby nie można było podejrzeć danych wpisanych do formularza.*

Jeśli w formularzu zawarte są oświadczenia zgód osoby, której dane dotyczą, dla każdej ze zgód wyrażanych w formularzu powinno być przewidziane odrębne pole do zaznaczenia, miejsce na podpis lub powinna zostać zastosowana inna forma pozwalająca ustalić, że każda zgoda została wyrażona odrębnie.

Jeśli w ramach formularza osoba go wypełniająca potwierdza zapoznanie się z określonymi dokumentami, dokumenty te powinny być rzeczywiście dostępne dla niej na miejscu, bez presji czasu.

Wypełnione formularze powinny być przechowywane w sposób zapewniający ich bezpieczeństwo przed dostępem osób niepowołanych lub nieupoważnionych.

Z komentarzem [17]: Fragment o Liście Robinsonów został usunięty ze względu na negatywny stosunek regulatorów.

Promowanie podmiotów trzecich

58. Jeśli marketer przetwarza dane osobowe jako administrator, może przetwarzać te dane również w celu promowania podmiotów trzecich (np. swoich partnerów biznesowych, swoich klientów) bez ujawniania tym podmiotom trzecim ww. danych.

    Tego rodzaju działanie może odbywać się na podstawie zgody osoby, której dane dotyczą lub w ramach prawnie uzasadnionego interesu marketera jako administratora. Jeśli marketer chce realizować takie przetwarzanie, ma obowiązek informować o tym osoby, których dane dotyczą podczas zbierania danych albo, odrębnie, przed podjęciem decyzji o takim przetwarzaniu danych.

59. Podjęcie przez marketera działań e-mail marketingu lub telemarketingu na rzecz podmiotów trzecich również podlega zasadom opisanym w niniejszym Rozdziale. Zgoda na otrzymywanie komunikacji marketingowej oferty podmiotów trzecich nie musi mieć charakteru odrębnego dla każdego przyszłego partnera biznesowego lub klienta.

Przykład zgody:
Zgadzam się na kontakt telefoniczny i mailowy do celów marketingowych ze strony XYZ Sp. z o.o. w Warszawie z ofertami tej firmy oraz z ofertami jej partnerów biznesowych.

Z komentarzem [18]: Rozdział dotyczący przekazywania danych został istotnie zmieniony i rozbudowany z uwzględnieniem dotychczasowych uwag Urzędu.

Profilowanie w działaniach marketingu bezpośredniego

60. Przy prowadzeniu marketingu bezpośredniego może dochodzić do profilowania, czyli zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących jej osobistych preferencji lub zainteresowań.

Przykład:
Sprzedawca sprzętu elektronicznego może dokonać analizy informacji o klientach, którzy w ciągu ostatniego miesiąca kupili od niego określony model telefonu.
Następnie, do wszystkich takich klientów, którzy dodatkowo wyrazili wcześniej zgodę na otrzymywanie komunikacji marketingowej, sprzedawca może przesłać wiadomość e-mail zawierają ofertę różnych modeli etui dedykowanych dla zakupionego modelu telefonu.

61. Profilowanie w działaniach marketingu bezpośredniego ma na celu zapewnienie, aby kierowana do odbiorcy komunikacja marketingowa była jak najbardziej dopasowana do jego preferencji i oczekiwań. Kierowanie profilowanych komunikatów marketingowych pozwala unikać marnowania czasu odbiorców poprzez prezentowanie im komunikatów (np. ofert), co do których istnieje możliwość, że nie będą budziły zainteresowania odbiorcy. Daje to również oszczędności finansowe organizacji, ponieważ ze swoją komunikacją marketingową zwraca się wyłącznie do osób, co do których jest bardziej prawdopodobne, że odpowiedzą na komunikację (np. skorzystają z oferty).

Profilowanie w marketingu jest więc działaniem dającym korzyści zarówno osobom, których dane dotyczą (profilowanym), jak i marketerom (profilującym).

Przykład:
Sprzedawca sprzętu elektronicznego regularnie wysyła do osób, które wyraziły na to zgodę, komunikację marketingową obejmującą informację o jego ofercie na dany okres. Kolejna planowana przez sprzedawcę komunikacja marketingowa ma być skupiona na ofercie telewizorów. Przed wysyłką komunikacji sprzedawca dokonuje analizy informacji o klientach, którzy w ciągu ostatniego miesiąca kupili od niego telewizor. Następnie, do wszystkich takich klientów sprzedawca nie wysyła komunikacji marketingowej, ponieważ jest mało prawdopodobne, aby takie osoby były zainteresowane zakupem nowego telewizora, skoro niedawno kupiły takie urządzenie.

62. W każdym przypadku, gdy dochodzi do profilowania do celów marketingu bezpośredniego, należy zapewnić, aby nie prowadziło ono do naruszenia praw lub wolności osób objętych profilowaniem, a zwłaszcza do ich dyskryminacji.

63. Jeśli dochodzi do profilowania do celów marketingu bezpośredniego, to w zdecydowanej większości przypadków nie wywołuje ono wobec osoby, której dane dotyczą skutków prawnych ani nie wpływa na taką osobę w podobny sposób. W związku z tym nie stanowi podejmowania decyzji, o których mowa w art. 22 RODO.

Oznacza to, że profilowanie do celów marketingu bezpośredniego w zdecydowanej większości przypadków nie musi być oparte na wyraźnej zgodzie osoby, której dane dotyczą. Może być oparte na tym, że jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez marketera 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.

Profilowanie, którego rezultatem jest przedstawienie określonej reklamy lub promocyjnej oferty wyłącznie wybranym odbiorcom, potencjalnie najbardziej zainteresowanym daną reklamą lub ofertą, nie stanowi sytuacji, o której mowa w art. 22 ust. 1 RODO.

Przykład:
Producent żywności (lub inny podmiot w jego imieniu) wyodrębnia matki dzieci w wieku od lat 3 do lat 6 w danym regionie po to, aby zaprosić je do udziału w programie lojalnościowym realizowanym przez producenta zdrowej żywności dla dzieci.

64. W niektórych przypadkach profilowanie do celów marketingu bezpośredniego może jednak wpływać na osobę, której dane dotyczą w sposób podobny do skutków prawnych, a więc stanowić podejmowanie decyzji, o których mowa w art. 22 RODO. Będzie tak wówczas, gdy jest realizowane w sposób kierunkowy, inwazyjny i z założenia jego rezultaty mogą mieć istotny, negatywny wpływ na daną osobę.

Przykład:
Wykorzystywanie profilowania w celu wyszukiwania osób, które mają kłopoty finansowe lub są istotnie zadłużone po to, aby kierować do nich bezpośrednio reklamę wysokooprocentowanych produktów finansowych, gier liczbowych lub loterii pieniężnych.

3. Tego rodzaju profilowanie do celów marketingu bezpośredniego nie może być realizowane w sposób wyłącznie zautomatyzowany (bez ludzkiej interwencji) – chyba, że marketer uzyska najpierw wyraźną zgodę od osoby, której dane dotyczą. W takim przypadku marketer musi być w stanie wykazać, że przed rozpoczęciem profilowania uzyskał taką wyraźną zgodę. Oznacza to, że marketer ma obowiązek uzyskać zgodę również od takiej osoby, wobec której finalnie – w wyniku profilowania – nie zdecyduje się podejmować działań marketingowych.

Jeżeli po przeprowadzeniu profilowania, ale przed podjęciem dalszych działań marketingu bezpośredniego, dochodzi do interwencji ludzkiej w decyzję, wobec których 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.

W każdym przypadku marketer powinien ocenić, jaki dokładnie będzie cel profilowania oraz czy planowane profilowanie nie będzie miało istotnego negatywnego wpływu na osoby, których dane dotyczą. Efektem tego działania powinno być podsumowanie określające, czy profilowanie wymaga uzyskiwania wyraźnej zgody osób, których dane dotyczą, czy też nie.

Badania rynkowe

65. Prowadzenie bezpośredniego kontaktu w celu badania satysfakcji klientów oraz w celu badań statystycznych lub tym podobnych nie wymaga uzyskania uprzedniej zgody. Warunkiem jest to, że tego rodzaju działania nie mogą mieć w rzeczywistości ukrytego celu marketingowego. Kontakty tego typu można uznać za mające charakter marketingowy, jeżeli z inicjatywy marketera przedstawiana jest propozycja zawarcia umowy lub oferta sprzedaży towaru lub usługi.

66. W ramach kontaktu w celu badania satysfakcji klientów oraz w celu badań statystycznych lub tym podobnych możliwe jest uzyskanie od osoby, której dane dotyczą zgody na otrzymywanie komunikatów marketingowych, jednak nawet w przypadku uzyskania takiej zgody konsultant telefoniczny nie może przedstawiać komunikatów marketingowych podczas tego samego kontaktu (np. tej samej rozmowy).

67. Przetwarzanie danych osobowych dla prowadzenia kontaktu w celu przeprowadzenia badania satysfakcji klienta oraz w celu badań statystycznych lub tym podobnych znajduje swoją podstawę w prawnie uzasadnionym interesie marketera jako administratora. Jednocześnie rozmowa telefoniczna powinna być niedługa i nieinwazyjna.

PRZEKAZYWANIE DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO

Zlecanie przetwarzania danych innemu podmiotowi

68. Przy realizowaniu marketingu bezpośredniego może dochodzić do wielu sytuacji, w których marketer korzysta z usług innego podmiotu. Usługi te najczęściej obejmują działania, w których dochodzi do przetwarzania danych osobowych.

Przykłady

1. *Agencja interaktywna otrzymuje dostęp do bazy adresów e-mail sprzedawcy produktów branży FMCG. Jej zadaniem jest projektowanie i realizowanie kampanii e-mail marketingowych z wykorzystaniem adresów osób, które wyraziły zgodę na takie działania marketingu bezpośredniego.*
2. *Towarzystwo ubezpieczeniowe zleca zewnętrznemu dostawcy obsługę infolinii (contact center) służącej do obsługi zapytań o produkty ubezpieczeniowe tego towarzystwa. Przez infolinię może również dochodzić do przygotowania umów ubezpieczenia.*
3. *Producent artykułów budowlanych zleca agencji marketingowej zorganizowanie loterii promocyjnej promującej sprzedaż nowej marki jego produktów.*
4. *Twórca oprogramowania do zarządzania projektami zleca agencji interaktywnej zbieranie danych kontaktowych osób zainteresowanych korzystaniem z tego oprogramowania poprzez prowadzenie strony internetowej, która zawiera formularz kontaktowy, dzięki któremu osoby zainteresowane mogą zostawić swoje dane z prośbą o kontakt ws. oferty.*

4. W takich sytuacjach będzie dochodziło do przetwarzania danych w imieniu marketera będącego administratorem danych (dalej również jako „marketer-administrator") przez zewnętrznego dostawcę usług jako marketera będącego procesorem (dalej również jako „marketer-procesor").

69. Jeżeli marketer-administrator zleca działania marketingu bezpośredniego, powinien korzystać wyłącznie z usług takiego dostawcy, 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. Poziom ochrony danych przez marketera-procesora przy marketingu bezpośrednim nie może być niższy niż wówczas, gdyby marketer-administrator realizował marketing bezpośredni samodzielnie. Dlatego przed zleceniem działań marketingu bezpośredniego marketer-administrator powinien dokonać oceny, czy marketer-procesor zapewnia ww. gwarancje.

Ocena musi się opierać na rzetelnych informacjach, a stopień zaawansowania analizy powinien być proporcjonalny do ryzyka związanego z przetwarzaniem danych do celów marketingu bezpośredniego. Marketer-administrator nie może w każdym przypadku opierać się wyłącznie na ogólnej pisemnej gwarancji przyszłego marketera-procesora (składanej np. w umowie dotyczącej przetwarzania danych), że ten gwarantuje wdrożenie odpowiednich środków. Jeśli przetwarzanie danych do celów marketingu bezpośredniego może wiązać się z wyższym poziomem ryzyka, marketer-administrator powinien przedsięwziąć dalej idące kroki mające na celu zweryfikowanie rzetelności działań marketera-procesora i jego gotowości do przestrzegania reguł wynikających z RODO.

Kluczowe czynniki ryzyka, jakie marketer-administrator powinien wziąć pod uwagę przy wyborze, w jakim stopniu weryfikować marketera-procesora to:

a) kategorie osób, których dane mają być przetwarzane (np. to, czy mają być przetwarzane dane dzieci lub osób starszych);

b) kategorie danych, które mają być przetwarzane (np. to czy mają być przetwarzane dane o życiu prywatnym, dane finansowe, szczególne kategorie danych i im podobne kategorie zasługujące na wyższy poziom ochrony);
c) ilość danych, do których dostęp będzie miał marketer-procesor (np. to, czy dane mają być przetwarzane na dużą skalę);
d) system informatyczny, z którego będzie korzystać marketer-procesor lub urządzenia, z których będzie korzystać marketer-procesor (np. to, czy będzie przetwarzał dane we własnym systemie i na własnych urządzeniach, poza bieżącą kontrolą marketera-administratora);
e) przedmiot i czas trwania przetwarzania, a także charakter i cel przetwarzania (np. to, czy może dochodzić do rodzajów przetwarzania, które mogą powodować wysokie ryzyko dla osób, których dane dotyczą[1];
f) dotychczasowy przebieg współpracy (np. to, czy marketer-administrator wcześniej współpracował z marketerem-procesorem i czy przy tej współpracy występowały jakiekolwiek błędy lub nieprawidłowości ze strony marketera-procesora).

70. Marketer-procesor w każdym przypadku może wykazać, że zapewnia wystarczające gwarancje poprzez stosowanie niniejszego Kodeksu lub poprzez stosowanie zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO. Za wystarczające gwarancje w zakresie bezpieczeństwa danych osobowych uznawane jest również posiadanie przez marketera-procesora certyfikatu zgodności z normą ISO/IEC 27001.

71. Jeśli marketer-procesor nie przystąpił do stosowania żadnego kodeksu postępowania, o którym mowa w art. 40 RODO ani zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, marketer-administrator powinien w każdym przypadku wystąpić do procesora o przedstawienie informacji o tym, jakie dokładnie środki techniczne i organizacyjne stosuje marketer-procesor po to, by przetwarzanie spełniało wymogi prawa ochrony danych osobowych i chroniło prawa osób, których dane dotyczą oraz dlaczego środki te są według marketera-procesora odpowiednie.

72. Jeśli przetwarzanie danych do celów marketingu bezpośredniego może wiązać się z wyższym poziomem ryzyka, marketer-administrator powinien rozważyć dalej idące działania mające na celu weryfikację, czy marketer-procesor rzeczywiście zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawa ochrony danych osobowych i chroniło prawa osób, których dane dotyczą. Takie dalej idące działania mogą obejmować w pierwszej kolejności przeprowadzenie wstępnego, szczegółowego audytu marketera-procesora w sposób „zdalny", czyli poprzez zadanie procesorowi poniższych pytań (mogą być ujęte w formie tabelarycznego formularza).

l.p.	Pytanie	Odpowiedź procesora
1.	Czy procesor posiada doświadczenie w świadczeniu usług związanych z marketingiem	

[1] Tzn. jednego z rodzajów przetwarzania o których mowa w:
a) Wytycznych Grupy Roboczej art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 (WP248 rev.01) zatwierdzonych przez Europejską Radę Ochrony Danych zgodnie z art. 68 RODO - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236;
b) Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (Monitor Polski 2019 r. poz. 666 - http://monitorpolski.gov.pl/MP/2019/666).

	bezpośrednim? Jeśli tak, jak bogate jest to doświadczenie? Czy procesor otrzymał referencje od innych administratorów, w imieniu których przetwarzał dane? Jeśli tak, prosimy o ich przedstawienie.	
2.	Czy procesor wyznaczył wewnętrznie osobę odpowiedzialną za dbanie o to, by przetwarzanie spełniało wymogi prawa ochrony danych osobowych i chroniło prawa osób, których dane dotyczą? Od kiedy taka osoba jest wyznaczona? Jak można się z nią skontaktować? Czy taka osoba została wyznaczona formalnie jako inspektor ochrony danych?	
3.	W jaki sposób procesor wyznaczył wewnętrzne reguły postępowania w zakresie ochrony danych osobowych? Dlaczego właśnie ten sposób wyznaczenia tych reguł został wybrany?	
4.	Czy procesor przetwarza dane osobowe w imieniu innych administratorów? Jeśli tak – czy prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu tych administratorów? Jaką ma on postać i jakie rodzaje informacji zawiera (procesor może przesłać szablon stosowanego u siebie dokumentu)?	
5.	Czy procesor ustalił procedury dotyczące realizowania praw osób, których dane dotyczą, a zwłaszcza procedurę uwzględniania sprzeciwu wobec przetwarzania danych osobowych do celów marketingu bezpośredniego albo realizacji prawa do wycofania zgody na takie przetwarzanie?	
6.	Czy procesor ustalił procedury dotyczące postępowania na wypadek naruszenia ochrony danych osobowych (incydentu bezpieczeństwa)?	
7.	Czy procesor ustalił wewnętrzne reguły korzystania ze sprzętu w celu przetwarzania danych (np. komputerów, telefonów)? W jakiej formie zostały one przekazane pracownikom?	
8.	W jaki sposób zabezpieczane są pomieszczenia, w których działa procesor? Czy są zamykane na klucz? Czy jest stosowany	

	alarm przeciwwłamaniowy i przeciwpożarowy?	
9.	Czy pracownicy lub współpracownicy procesora są regularnie szkoleni z reguł ochrony danych osobowych? Jak często? Czy zobowiązali się do zachowania danych osobowych w tajemnicy?	
10.	Jakie środki kontroli dostępu i uwierzytelnienia stosuje procesor? Jakie reguły haseł są stosowane?	
11.	Czy procesor stosuje szyfrowanie danych przesyłanych oraz danych „w spoczynku”? Jakie metody szyfrowania są stosowane?	
12.	W jaki sposób procesor chroni dane osobowe przetwarzane na swoich urządzeniach, zwłaszcza mobilnych (laptopy, telefony)? Jakie systemy operacyjne stosuje? Jakie programy antywirusowe są stosowane? Jakie są reguły aktualizacji oprogramowania?	
13.	W jaki sposób procesor chroni dane osobowe przesyłane w ramach sieci zewnętrznych lub wewnętrznych?	
14.	Jakimi zasadami kieruje się procesor tworząc kopie zapasowe danych, które przetwarza?	
15.	Jakimi zasadami kieruje się procesor w zakresie niszczenia/kasowania danych?	
16.	Z jakimi podwykonawcami współpracuje procesor? Komu planuje ujawniać dane, które przetwarza lub będzie przetwarzał w imieniu administratora?	
17.	Czy kiedykolwiek stwierdzono prawomocną decyzją organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez procesora?	
18.	Czy procesor korzysta z usług podmiotów, które mogą przetwarzać dane poza Europejskim Obszarem Gospodarczym (np. z USA)? Na jakiej podstawie dokonuje transferu danych poza EOG?	

5. W dalszej kolejności marketer może również podjąć decyzję o przeprowadzeniu audytu „na miejscu” u procesora, w tym zwłaszcza zweryfikować zgodność z rzeczywistością informacji przedstawionych w odpowiedzi ww. pytania. W razie potrzeby, ww. audyty powinny być okresowe ponawiane.

Powyższe działania zostały wymienione w ten sposób, że każde kolejne jest dalej idącym działaniem weryfikującym. Wybór, które z tych działań zastosować należy do marketera-administratora. Dokonując wyboru marketer-administrator musi uwzględnić ryzyko związane z przetwarzaniem danych w jego imieniu przez marketera-procesora.

73. Przed rozpoczęciem przetwarzania przez marketera-procesora danych w imieniu marketera-administratora powinna zostać zawarta pomiędzy nimi umowa. Taka umowa dotycząca przetwarzania danych (tzw. umowa powierzenia) powinna zawierać wszystkie elementy istotne dla zapewnienia prawidłowej współpracy marketera-administratora i marketera-procesora w zakresie przetwarzania danych, a zwłaszcza elementy określone w art. 28 RODO. Są to następujące elementy:

(1) określenie przedmiotu i czasu trwania przetwarzania – czyli jakiego rodzaju usługi związane z przetwarzaniem danych ma świadczyć marketer-procesor i przez jaki okres;

(2) określenie charakteru i celu przetwarzania – czyli na czym dokładnie ma polegać przetwarzanie danych przez marketera-procesora w imieniu marketera-administratora (należy unikać ogólnych, enigmatycznych lub generycznych sformułowań, np. „w celu prowadzenia współpracy" lub w „celu świadczenia usług");

(3) określenie rodzaju danych osobowych oraz kategorii osób, których dane dotyczą (np. dane klientów w postaci adresów e-mail oraz numerów telefonów)

(4) regułę, że marketer-procesor może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie marketera-administratora, czyli tylko dlatego, że zlecił mu to marketer-administrator (zlecenie może mieć charakter ogólny, ale przetwarzanie musi następować dlatego, że chce tego marketer-administrator); jeśli obowiązek przetwarzania danych nakłada na marketera-procesora prawo Unii lub prawo państwa członkowskiego, któremu podlega marketer-procesor, wówczas przed rozpoczęciem przetwarzania marketer-procesor informuje marketera-administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

(5) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych przez marketera-procesora (np. jego pracownicy) zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

(6) obowiązek podejmowania przez marketera-procesora wszelkich środków bezpieczeństwa danych wymaganych na mocy art. 32 RODO, czyli wybór odpowiednich środków technicznych i organizacyjnych zapewniających poufność, integralność i dostępność danych;

(7) obowiązek przestrzegania przez marketera-procesora warunków korzystania z usług innego (dalszego) procesora, o których mowa w art. 28 ust. 2 i 4 RODO;

(8) obowiązek pomagania (w miarę możliwości oraz biorąc pod uwagę charakter przetwarzania) marketerowi-administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO (np. prawa sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego);

(9) obowiązek pomagania marketerowi-administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO stosownie do charakteru przetwarzania oraz dostępnych

dla marketera-procesora informacji, w tym zwłaszcza obowiązek niezwłocznego informowania marketera-administratora o wszelkich stwierdzonych przez marketera-procesora naruszeniach ochrony danych osobowych (incydentach) oraz ich okolicznościach;

(10) obowiązek usunięcia lub zwrócenia marketerowi-administratorowi przez marketera-procesora wszelkich danych osobowych po zakończeniu świadczenia usług związanych z przetwarzaniem oraz usunięcia wszelkich ich istniejących kopii – zależnie od decyzji marketera-administratora, chyba że prawo Unii lub prawo Rzeczypospolitej Polskiej nakazują przechowywanie danych osobowych marketerowi-procesorowi;

(11) obowiązek udostępniania marketerowi-administratorowi przez marketera-procesora wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiania marketerowi-administratorowi lub audytorowi upoważnionemu przez marketera-administratora przeprowadzania audytów, w tym inspekcji, i przyczyniania się do nich.

(12) obowiązek niezwłocznego informowania marketera-administratora, jeżeli zdaniem marketera-procesora wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub Rzeczypospolitej Polskiej o ochronie danych.

(13) obowiązek prowadzenia przez marketera-procesora rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu marketera-administratora.

6. Strony powinny ustalić w umowie ww. elementy w sposób jasny i konkretny. Mogą również w umowie dotyczącej przetwarzania danych osobowych do celów marketingu bezpośredniego wprowadzić bardziej szczegółowe reguły współpracy, np. dokładnie określać sposób, w jaki marketer-administrator może przeprowadzać audyty przetwarzania danych przez marketera-procesora. W żadnym wypadku takie szczegółowe reguły nie mogą jednak prowadzić do tego, aby wykonywanie praw i obowiązków marketera-administratora było w praktyce niemożliwe lub istotnie utrudnione (np. nadmiernie zawyżone opłaty z tytułu przeprowadzania audytów).

74. Obowiązek zawarcia umowy dotyczącej przetwarzania danych (tzw. umowy powierzenia) spoczywa w równym stopniu na obu stronach, czyli na marketerze-administratorze oraz na marketerze-procesorze. Obie strony powinny dążyć do zawarcia odpowiedniej umowy przed rozpoczęciem przetwarzania danych przez marketera-procesora w imieniu marketera-administratora. Nie jest tak, że tylko marketer-administrator jest odpowiedzialny za zawarcie takiej umowy.

W praktyce branży marketingu bezpośredniego bardzo często stosowane są różnego rodzaju wzory umów dotyczących przetwarzania danych przez marketera-procesora w imieniu marketera-administratora. Tego rodzaju wzory przygotowują i stosują zarówno podmioty działające jako administratorzy, jak i jako procesorzy. Nie ma jednak znaczenia dla ważności umowy to, od której ze stron „pochodzi" wzór umowy. W każdym przypadku treść umowy musi spełniać wymagania RODO, a zwłaszcza zawierać elementy określone w art. 28 RODO.

75. Umowa dotycząca przetwarzania danych w imieniu marketera-administratora (tzw. umowa powierzenia) może być zawarta w formie pisemnej, a ponadto również:
a) 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;

b) w trybie przewidzianym w art. 384 Kodeksu cywilnego, tj. poprzez posłużenie się przez jedną ze stron wzorcem umowy dotyczącej przetwarzania danych w imieniu marketera-administratora i spełnieniem się warunków do związania stron treścią tego wzorca.

76. Umowa dotycząca przetwarzania danych w imieniu marketera-administratora może zostać zawarta odrębnie od innej umowy, z której wykonaniem wiąże się przetwarzanie danych lub zostać ujęta jako element ww. innej umowy (np. jeden z paragrafów takiej umowy).

77. Jeśli marketer-administrator chce zaangażować do przetwarzania danych procesora z siedzibą w państwie trzecim, może to zrobić tylko wówczas, jeśli poza wcześniej wymienionymi zostaną dodatkowo spełnione poniższe warunki:
a) przekazanie danych takiemu podmiotowi obędzie się w ramach jednej z przesłanek określonych w art. 45-49 RODO oraz na warunkach właściwych dla takiej przesłanki;
b) umowa dotycząca przetwarzania danych w imieniu marketera-administratora będzie 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.

W przypadku przekazywania danych do podmiotu z kraju trzeciego sugerowanym rozwiązaniem jest zastosowanie przez strony umowy zatwierdzonych przez Komisję Europejską Standardowych Klauzul Umownych.

78. Jeśli marketer realizuje działania marketingu bezpośredniego w imieniu innego podmiotu jako procesor i chce podzlecić niektóre z działań innemu podmiotowi (dalszemu procesorowi), powinien analogicznie stosować wszystkie reguły opisane w niniejszym Kodeksie. Dodatkowym warunkiem podzlecenia takich działań jest jednak to, aby administrator wyraził na to zgodę (ogólną lub dla konkretnego dalszego procesora).

Przykład:
Przekazanie danych przez agencję marketingową (procesora) do swojego podwykonawcy (dalszego procesora) w Indiach jest możliwe, jeżeli agencja zawrze ze swoim podwykonawcą umowę zgodną w swojej treści z postanowieniami Załącznika do Decyzji Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady).

Role głównych podmiotów zaangażowanych w przetwarzanie danych osobowych w akcji promocyjnej

79. W przypadku realizacji konkretnej akcji promocyjnej (np. konkursu, sprzedaży premiowej, programu lojalnościowego, loterii promocyjnej lub audioteksowej), w której występują:
a) podmiot zlecający przeprowadzenie danej akcji (promujący swoją markę, produkty lub usługi), oraz
b) agencja marketingowa jako formalny organizator takiej akcji
– role ww. podmiotów zaangażowanych w proces przetwarzania danych osobowych przedstawiają się następująco.

Administratorem danych uczestników, które są przetwarzane do celów marketingowych oraz w celu realizacji danej akcji, jest podmiot zlecający przeprowadzenie akcji (klient agencji marketingowej).

Agencja marketingowa, mimo że jest formalnym organizatorem danej akcji promocyjnej, jest procesorem – podmiotem przetwarzającym w imieniu administratora dane osobowe uczestników tej akcji do celów marketingowych oraz w celu realizacji tej akcji.

80. Agencja marketingowa będąca formalnym organizatorem danej akcji promocyjnej jest jednocześnie samodzielnym administratorem danych wybranych kategorii uczestników akcji promocyjnej, w zakresie, w jakim:
    a) przepisy prawa (np. podatkowego lub regulujące organizację gier hazardowych) nakładają bezpośrednio na taką agencję obowiązek dokonania określonych działań (np. rozliczeń podatkowych, ewidencjonowania wydawanych nagród lub realizacji określonych czynności sprawozdawczych względem organów administracji publicznej);
    b) agencja przetwarza dane osobowe osób składających reklamacje dotyczące przeprowadzenia danej akcji marketingowej w celu ustalenia, a następnie zaspokojenia roszczeń albo obrony przed roszczeniami, które są kierowane bezpośrednio do niej jako organizatora.

Przekazywanie danych operatorom usług pocztowych i kurierskich

81. Przekazywanie kurierowi danych osobowych odbiorców przesyłek przez niego doręczanych w formie etykiet adresowych i/lub listy nie wymaga odrębnej zgody osoby, której dane dotyczą, ponieważ doręczenie przesyłki za pośrednictwem kuriera jest elementem przetwarzania danych, które ma inną podstawę prawną, np.:
    a) jest niezbędne do wykonania zobowiązań, które organizator akcji promocyjnej ma wobec uczestnika takiej akcji i adresata przesyłki (np. zobowiązanie wysyłania nagrody przyznanej w akcji promocyjnej);
    b) jest niezbędne do wypełnienia obowiązku prawnego ciążącego na organizator akcji promocyjnej (np. obowiązek wysłania informacji podatkowej nagrodzonemu uczestnikowi akcji promocyjnej).

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

82. W przypadku, gdy marketer korzysta z usług operatorów pocztowych lub firm kurierskich, ma prawo przekazywać takim podmiotom dane osobowe adresatów wymagane do zrealizowania usługi pocztowej/kurierskiej.

    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.

    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, operator pocztowy lub firma kurierska jest podmiotem przetwarzającym dane w imieniu administratora. Takie usługi dodatkowe mogą obejmować:
    a) potwierdzenie tożsamości lub wieku odbiorcy przesyłki oraz zebranie informacji o numerze dowodu osobistego;
    b) przekazanie adresatowi przesyłki umowy do podpisania oraz przyjęcie od razu podpisanego egzemplarza umowy w celu zwrotnego przesłania go do nadawcy.

Z komentarzem [19]: Zapis ten opiera się na stanowisku ICO.
UODO prosi o dodanie przypadku z umową, która jest otwierana przy kurierze.

Z komentarzem [20R19]: Czy zostanie to uzupełnione zgodnie z sugestią?

Z komentarzem [21R19]: Postanowienie zostało rozbudowane o przykłady.

Przekazywanie danych osobowych innemu marketerowi do samodzielnego przetwarzania (np. sprzedaż bazy danych)

83. Jeżeli marketer chce przekazać dane osobowe innemu marketerowi do samodzielnego przetwarzania (np. sprzedaż bazy danych), powinien mieć podstawą prawną dla takiego działania. Podstawa prawna dla przekazania danych osobowych innemu marketerowi obejmuje w szczególności:
    a) 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 marketerowi;
    b) posiadanie podstawy prawnej przetwarzania danych w celu ich dalszego przekazania (np. zgoda osoby, której dane dotyczą lub uzasadniony interes marketera);
    c) brak sprzeciwu osoby, której dane dotyczą, wobec przekazania jej danych osobowych innym marketerom, o ile nie istnieją ważne, prawnie uzasadnione podstawy do dalszego przetwarzania danych, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, w tym ustalenie, dochodzenie lub obrona roszczeń.

84. Informację o kategoriach innych podmiotów, którym będą przekazywane (przesyłane, udostępniane) dane do samodzielnego przetwarzania jest dostateczna, 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 łatwo dostępnej w miejscu wypełniania formularza.

85. Proces i zasady udostępnienia danych oraz sposób późniejszego wykorzystania danych przez drugiego z marketerów (otrzymującego dane) powinny być uregulowane w podpisanej pomiędzy marketerami umowie.

86. Udostępnienie danych pomiędzy marketerami może zostać poprzedzone procesem deduplikacji, w ramach której marketerzy porównują swoje bazy danych w celu określenia, czy przekazanie/wymiana baz danych jest uzasadniona prawnie (minimalizacja danych) oraz gospodarczo. W ramach deduplikacji marketerzy porównują swoje bazy w celu znalezienia duplikatów. Duplikatami są dane osobowe, które się powtarzają, czyli znajdują się w obu bazach danych. Jeśli duplikat występuje, jego przekazanie nie powinno następować, ponieważ nie jest to uzasadnione prawnie – zgodnie z zasadą minimalizacji dane powinny być ograniczone do niezbędnych. Ponadto, im więcej takich duplikatów występuje, tym mniej uzasadniona gospodarczo jest przekazanie/wymiana baz danych, ponieważ nie prowadzi do wzbogacenia bazy marketera otrzymującego dane.

    W celu zapewnienia bezpieczeństwa danych, deduplikacja powinna odbyć się z wykorzystaniem pseudonimizacji (np. tak, aby marketer otrzymujący mógł jedynie sprawdzić otrzymaną bazę pod kątem duplikatów ze swoją bazą, ale żeby nie mógł odczytać pozostałych danych, które nie są duplikatami). Bezpośrednio po takim sprawdzeniu każdy z marketerów usuwa dane przekazane w ramach procesu deduplikacji. Tego rodzaju proces weryfikacyjny nie jest uznawany za proces udostępnienia danych.

87. Zawsze dopuszczalne jest do celów marketingowych przekazywanie danych osobowych osób fizycznych prowadzących działalność gospodarczą z powołaniem na prawnie uzasadniony interes marketera, o ile przekazywane dane osobowe są związane z ich działalnością gospodarczą. W przypadku przekazywania danych osobowych konsumentów do celów marketingowych marketer powinien dokonać odrębnej analizy, czy przekazanie danych może odbyć się z powołaniem na uzasadniony interes marketera, czy też marketer powinien uzyskać odrębną zgodę konsumentów.

Ogólne reguły bezpieczeństwa przy przekazywaniu danych do celów marketingu bezpośredniego

88. Przekazywanie danych osobowych do celów marketingu bezpośredniego powinno odbywać się w sposób bezpieczny pod względem organizacyjnym oraz technicznym. Umowa pomiędzy stronami powinna określać, kto jest upoważniony do przekazania lub odbioru danych w organizacji (o ile przekazanie odbywa się z wykorzystaniem oznaczonych osób fizycznych) 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 może odbyć się w szczególności przy wykorzystaniu jednego z następujących sposobów komunikacji:

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

7. Wszelkie hasła umożliwiające uzyskanie dostępu do plików zawierających dane osobowe muszą być przekazywane odbiorcy innym środkiem komunikowania (np. SMS).

89. W związku z postępem technologicznym możliwe jest również zastosowanie innych form wymiany danymi, pod warunkiem że pozwolą one zapewnić odpowiedni poziom zabezpieczenia tych danych.

PRZECHOWYWANIE DANYCH OSOBOWYCH DO CELÓW MARKETINGU BEZPOŚREDNIEGO

Z komentarzem [22]: Rozdział dotyczący przechowywania danych został istotnie zmieniony i rozbudowany z uwzględnieniem dotychczasowych uwag Urzędu.

Okres przechowywania danych przetwarzanych do celów marketingu bezpośredniego

90. Przetwarzanie danych do celów marketingu bezpośredniego nie jest z góry ograniczone do konkretnego okresu wyrażonego w dniach, miesiącach czy latach. Marketer nie ma prawnego obowiązku usunięcia lub zanonimizowania danych przetwarzanych do celów marketingu bezpośredniego tylko z tego powodu, że upłynął określony czas od daty ich zebrania. Nie jest to sytuacja analogiczna np. do przechowywania danych osobowych w dokumentacji księgowej przez z góry wyrażony w latach okres wymagany przepisami o rachunkowości.

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

a) 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 dotarła do odbiorcy, a jej nadawca nie

otrzymał informacji, że posiadane dane kontaktowe są nieaktualne; nieskutecznym realizowaniem komunikacji marketingowej jest np. *hard bounce* czyli niedostarczenie komunikatu e-mailowego z tego powodu, że nie istnieje skrzynka, której adres podano);

b) 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).

91. W przypadku, gdy w ustalonym przez marketera czasie nie będzie występował kontakt marketingowy oraz brak będzie jakichkolwiek transakcji na linii marketer-osoba, której dane dotyczą, marketer obowiązany jest podjąć decyzję o zasadności pozostawienia danych osobowych w swojej bazie marketingowej. Jeśli marketer nie znajduje żadnej podstawy dla dalszego przetwarzania takich danych do celów marketingu bezpośredniego, powinien je usunąć.

92. Marketer ustala okres przetwarzania danych osobowych do celów marketingu bezpośredniego samodzielnie, z uwzględnieniem specyfiki rynku, na którym działa, specyfiki produktu lub usługi, które promuje, oczekiwań osób, których dane dotyczą oraz innych czynników występujących w danej branży. Marketer musi być jednak w stanie wykazać, dlaczego ustalił taki, a nie inny okres przetwarzania danych osobowych do celów marketingu bezpośredniego.

> ***Przykład:***
> *Dealer w branży samochodowej sprzedał samochód osobowy nowemu klientowi. Dealer wie, że średnio klienci wymieniają samochód co 5-6 lat. Dlatego dealer zachował dane klienta i po upływie 5 lat ma prawo skontaktować się z klientem w celu zapytania, czy klient jest zainteresowany ofertą salonu i dalej kontynuować rozmowy, jeżeli z zachowania klienta będzie wynikała taka chęć. Jeżeli z kolei klient wskaże kategorycznie, że nie ma chęci rozmawiać z dealerem i kupił sobie już inny nowy samochód (lub tym podobne odpowiedzi), dealer powinien uważnie rozważyć, czy potrafi uzasadnić dalsze przetwarzanie danych takiego klienta do celów marketingu bezpośredniego. Jeżeli zdecyduje się dalej nie przetwarzać określonych danych osobowych, może podjąć decyzję o przeniesieniu takich danych do swojej bazy archiwalnej, po to, aby takich danych więcej nie pobierać z publicznie dostępnych źródeł.*

93. Odrębnym problemem w obszarze okresu przechowywania danych jest czas, przez jaki marketer danych powinien przechowywać informację o tym, że dana osoba wyraziła sprzeciw wobec przetwarzania jej danych do celów marketingu bezpośredniego oraz powiązane z tym sprzeciwem dane osobowe. Dla potrzeb niniejszego Kodeksu przyjmuje się, że okres 3 (trzech) lat przechowywania danych na potrzeby uwzględniania sprzeciwu wobec komunikacji marketingowej jest uzasadniony i wystarczający.

Z komentarzem [23]: Postanowienia dotyczące praw osób, których dane dotyczą zostały przeniesione do nowego, osobnego rozdziału.

Aktualność danych

94. Marketerzy powinni czuwać, aby wszystkie przetwarzane przez nich dane osobowe były aktualne, tzn. aby dane osobowe były rzetelne i prawidłowe. Marketerzy mają prawo kontaktować się co najmniej raz w roku z osobami, których dane przetwarzają, w celu zweryfikowania aktualności przetwarzanych danych. Jeśli marketer w ciągu roku nabierze uzasadnionego podejrzenia, że dane mogą być nieaktualne (np. osoba, której dane dotyczą prowadzi z własnej inicjatywy kontakt z marketerem z użyciem innej danej kontaktowej), marketer ma prawo skontaktować się *ad hoc* z taką osobą w celu zweryfikowania aktualności przetwarzanych danych.

95. Kontakt w celu zweryfikowania aktualności przetwarzanych danych nie może być uciążliwy dla osób, których dane dotyczą oraz nie może mieć charakteru marketingowego, o ile marketer nie

posiada odrębnej podstawy prawnej dla wykorzystania danego środka komunikowania w celu marketingu bezpośredniego.

Anonimizacja

96. W wyniku anonimizacji dochodzi do przetworzenia informacji w sposób uniemożliwiający zidentyfikowanie określonej osoby fizycznej. Anonimizacja może być stosowana w szczególności do celów 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: xxxxxxa N1265, zam. w Poznaniu, e-mail: xxx@xxxx.pl, urodzona xx-xx-1979, zarejestrowana w serwisie 2012-03-12, zrezygnowała z rejestracji 2017-12-24.

Bezpieczeństwo techniczne i organizacyjne przy przetwarzaniu danych, w tym przy ich przechowywaniu

97. Zgodnie z ustawą o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych publikuje w Biuletynie Informacji Publicznej na swojej stronie 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.

98. Sugerowane minimalne działania w obszarze bezpieczeństwa obejmują:
   a) zabezpieczenia fizyczne oraz organizacyjne
      - pomieszczenia, gdzie są przetwarzane dane osobowe, powinny mieć możliwość ich zamknięcia w sposób uniemożliwiający wstęp osobom niepowołanym (klucze, zamki magnetyczne lub inne)
      - 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:
        ✓ 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;
        ✓ w organizacji powinna obowiązywać polityka „czystych biurek".
      - 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;
      - biuro powinno być wyposażone w:
        ✓ alarm przeciwwłamaniowy;
        ✓ alarm pożarowy;
        ✓ gaśnice;
      - może być wykorzystywany monitoring (przy czym należy spełnić wszelkie warunki dla stosowania tego sposobu przetwarzania danych osobowych);
   b) zabezpieczenia IT:

- 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);
- 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 zapobiegać ponownemu ustanowieniu jednego z 4 ostatnich haseł;
- 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 (np. poprzez PIN lub hasło);
- powinna istnieć polityka kopii zapasowych;
- system powinien być wyposażony w niezbędny firewall oraz oprogramowanie antywirusowe,
- oprogramowanie powinno być aktualne, w tym systemy operacyjne powinny funkcjonować w wersji utrzymywanej przez ich producenta;
- poczta e-mail powinna być wysyłana i odbierana protokołami szyfrowanymi (np. SSL).

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ W KONTEKŚCIE MARKETINGU BEZPOŚREDNIEGO

Z komentarzem [24]: Nowy rozdział przygotowany z uwzględnieniem dotychczasowych uwag Urzędu.

99. W związku z przetwarzaniem danych osobowych, osoby, których te dane dotyczą mogą realizować szereg praw określonych w rozdziale III RODO. W kontekście działań marketingu bezpośredniego na szczególną uwagę zasługują następujące prawa:
    a) prawo wycofania zgody na przetwarzanie danych do celów marketingu bezpośredniego;
    b) prawo wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego;
    c) prawo dostępu do informacji o przetwarzaniu danych do celów marketingu bezpośredniego;
    d) prawo do usunięcia danych („prawo do bycia zapomnianym").

    Niniejszy rozdział Kodeksu porusza kluczowe aspekty realizowania powyższych praw w kontekście działań marketingu bezpośredniego.

100. Za realizację praw osób, których dane dotyczą odpowiada marketer-administrator. Marketer-procesor, który przetwarza dane w imieniu marketera-administratora ma obowiązek pomagać mu (w miarę możliwości oraz biorąc pod uwagę charakter przetwarzania) poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z ww. obowiązku. Oznacza to przede wszystkim, że marketer-procesor ma obowiązek niezwłocznie przekazywać marketerowi-administratorowi żądania zgłaszane przez osoby, których dane dotyczą. Szczegółowy zakres takiego wsparcia może zostać ustalony w stosownej umowie dotyczącej przetwarzania danych osobowych przez marketera-procesora w imieniu marketera-administratora. Jeżeli nie ustalono szczegółowych zasad działania w tym obszarze, marketer-procesor nie ma prawa samodzielnie (bez wiedzy i zgody marketera-administratora) odpowiadać na żądanie osoby, której dane dotyczą.

Prawo wycofania zgody na przetwarzanie danych do celów marketingu bezpośredniego

101. Jeśli marketer opiera przetwarzanie danych osobowych do celów marketingu bezpośredniego na zgodzie osoby, której dane dotyczą, musi zapewnić możliwość wycofania takiej zgody w sposób równie łatwy ja ten, w który zgoda została wyrażona. Marketerzy powinni kierować się w tym zakresie regułą swego rodzaju „symetrii". Zgodnie z tą regułą jeśli można wyrazić zgodę w określony sposób, to powinna być zapewniona możliwość wycofania zgody w ten sam sposób.

Przykład prawidłowego działania:
Marketer na swojej stronie internetowej stosuje formularz służący do pozostawienia przez klienta danych kontaktowych i wyrażenia zgody na przetwarzanie danych do celów marketingu bezpośredniego. Na tej samej stronie internetowej w dedykowanej podstronie o intuicyjnej nazwie (np. „Ochrona danych osobowych") dostępny jest również formularz służący do podania danych identyfikujących klienta i odwołania zgody na przetwarzanie danych do celów marketingu bezpośredniego. Marketer uwzględnia również zgłoszenia odwołania zgody poprzez swoją infolinię oraz skrzynkę e-mail dedykowaną do obsługi korespondencji związanej z ochroną danych osobowych (np. daneosobowe@firma.pl).

Przykład nieprawidłowego działania:
Marketer na swojej stronie internetowej stosuje formularz służący do pozostawienia przez klienta danych kontaktowych i wyrażenia zgody na przetwarzanie danych do celów marketingu bezpośredniego. Aby wycofać tę zgodę osoba, której dane dotyczą musi pobrać ze strony marketera specjalny formularz, w którym musi podać powód odwołania swojej zgody. Taki wypełniony formularz osoba, której dane dotyczą musi przesłać marketerowi za pośrednictwem listu poleconego za zwrotnym potwierdzeniem odbioru.

102. Wycofanie zgody na przetwarzanie danych osobowych do celów marketingu bezpośredniego powinno być równie łatwe jak jej wyrażenie niezależnie od tego, jakiego przetwarzania ta zgoda dotyczy. Obejmuje to zwłaszcza zgodę na otrzymywanie komunikacji marketingowej, a także zgodę na takie profilowanie do celów marketingu bezpośredniego, które wywołuje wobec osoby, której dane dotyczą skutki prawne lub wpływa na taką osobę w podobny sposób.

Prawo wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego

103. Jeśli marketer opiera przetwarzanie danych osobowych do celów marketingu bezpośredniego na przesłance swojego prawnie uzasadnionego interesu, to osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych do ww. celów, w tym wobec profilowania. W razie wniesienia takiego sprzeciwu, marketer nie może już dalej przetwarzać danych do celów marketingu bezpośredniego.

104. Osoba, której dane dotyczą nie może wnieść sprzeciwu wobec przetwarzania jej danych, jeśli przetwarzanie jej danych osobowych jest oparte na innej podstawie prawnej niż prawnie uzasadniony interes marketera (np. wówczas, gdy przetwarzanie danych jest niezbędne do zrealizowania świadczenia wobec określonej wynikającego z jej udziału w akcji promocyjnej, polegającego na dostawie nagrody kurierem). Sprzeciw wobec przekazania danych osobowych odbiorcom danych może stanowić podstawę do odmowy spełnienia określonego świadczenia, jeśli takie świadczenie realizowane jest bez dodatkowej odpłatności w zamian za możliwość przetwarzania i udostępniania danych osobowych.

105. W celu realizowania prawnego obowiązku uwzględniania sprzeciwów osób, których dane dotyczą wobec przetwarzania ich danych do celów marketingu bezpośredniego, marketer może prowadzić wewnętrzną listę osób, które wniosły taki sprzeciw (tzw. „lista sprzeciwów" lub „lista negatywna"). W ramach takiej listy mogą być przechowywane podstawowe dane osoby, która wniosła sprzeciw oraz wszelkie informacje pozwalające na uwzględnianie tego sprzeciwu w przyszłych działaniach marketingu bezpośredniego oraz zapewnienie rozliczalności działań marketera. Praktyczne wykorzystanie takiej listy może polegać np. na tym, że marketer przez wysyłką kampanii marketingowej będzie zawsze filtrował listę odbiorców wiadomości (komunikatów) marketingowych pod kątem tego, czy znajdują się na liście osób, które wniosły sprzeciw wobec przetwarzania ich danych do celów marketingu bezpośredniego. Jeśli znajdują się na takiej liście, wiadomości (komunikaty) marketingowe nie zostaną do nich skierowane.

Prawo dostępu do informacji o przetwarzaniu danych do celów marketingu bezpośredniego

106. Zgodnie z art. 15 RODO każda osoba, której dane dotyczą, ma prawo dostępu do informacji na temat przetwarzania jej danych osobowych przez określonego marketera. W kontekście działań marketingu bezpośredniego prawo to oznacza, że każdy może zadać dowolnemu marketerowi pytanie o to, czy ten marketer przetwarza jego dane osobowe do celów marketingu bezpośredniego i jeśli tak – jakie to są dane. Marketer ma obowiązek udzielić taką informację w każdym przypadku, z uwzględnieniem wszelkich reguł wynikających z RODO.

Prawo dostępu do danych w kontekście działań marketingu bezpośredniego oznacza również, że osoba, której dane podlegają przetwarzaniu do ww. celu ma prawo do tego, aby marketer podał jej również następujące informacje o przetwarzaniu danych:

a) komu dane były, są lub będą ujawniane przy przetwarzaniu do celów marketingu bezpośredniego, czyli informacje o odbiorcach lub kategoriach odbiorców, a zwłaszcza o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
b) jak długo dane będą przetwarzane do celów marketingu bezpośredniego;
c) jakie inne prawa przysługują w związku z przetwarzaniem danych do celów marketingu bezpośredniego
d) informację o prawie wniesienia skargi do organu nadzorczego na przetwarzanie danych do celów marketingu bezpośredniego;
e) jeżeli dane osobowe przetwarzane do celów marketingu bezpośredniego nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle (np. wskazanie publicznie dostępnych źródeł, z których dane te zostały zebrane);
f) o tym, czy w ramach marketingu bezpośredniego są podejmowane zautomatyzowane decyzje, w tym czy dochodzi do profilowania wywołującego skutki prawne lub w podobny sposób istotnie wpływającego na osobę, której dane dotyczą; jeśli dochodzi do takiego profilowania – na czym dokładnie ono polega i jakie może mieć znaczenie i konsekwencje dla osoby, której dane dotyczą.

Jeżeli marketer do celów marketingu bezpośredniego przekazuje dane osobowe do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z takim przekazaniem jej danych. Marketer ma obowiązek podać, na jakiej podstawie przekazuje dane osobowe do celów marketingowych do państwa trzeciego lub organizacji międzynarodowej.

107. Jeśli osoba, której dane dotyczą tego żąda, marketer ma obowiązek dostarczyć jej kopię danych osobowych podlegających przetwarzaniu do celów marketingu bezpośredniego. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, marketer może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której

dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.

108. 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 marketera na podstawie zebranych danych (np. stwierdzone przez marketera preferencje zakupowe).

Prawo do usunięcia danych przetwarzanych do celów marketingu bezpośredniego („prawo do bycia zapomnianym")

109. Osoba, której dane dotyczą, ma prawo zażądać od marketera, aby niezwłocznie usunął on dane osobowe, które dotyczą tej osoby i są przetwarzane do celów marketingu bezpośredniego, a marketer ma obowiązek do tego żądania się zastosować, jeżeli zachodzi choćby jedna z następujących okoliczności:

a) dane, których żądanie dotyczy nie są niezbędne do celów marketingu bezpośredniego;

> ***Przykład:***
> *Marketer przetwarza do celów marketingu bezpośredniego produktów dziecięcych informację o zainteresowaniach sportowych ojca dziecka. Tego rodzaju informacja może nie być konieczna do celów marketingu bezpośredniego produktów dziecięcych i wówczas marketer ma obowiązek ją usunąć, zwłaszcza jeśli żąda tego osoba, której dane dotyczą.*

b) osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie jej danych do celów marketingu bezpośredniego i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych do celów marketingu bezpośredniego;

d) dane osobowe były przetwarzane niezgodnie z prawem;

> ***Przykład:***
> *Marketer przetwarzał do celów marketingu bezpośredniego numery telefonów pozyskane w sposób nielegalny Nie miał z osobami ujętymi w bazie żadnych relacji prawnych ani faktycznych, a następnie realizował na pozyskane numery telefonów połączenia marketingowe, w których na drodze manipulacji emocjonalnej zachęcał rozmówców do nabywania jednostek uczestnictwa w systemie o charakterze piramidy finansowej.*

110. Jeśli marketer upublicznił dane dotyczące określonej osoby, a następnie ta osoba zażąda od marketera usunięcia jej danych, to jeśli to żądanie jest uzasadnione, wówczas taki marketer musi również podjąć działania, aby poinformować znanych mu innych administratorów przetwarzających dane tej osoby o tym, że żąda ona usunięcia jej danych. Wspomniani powyżej inni administratorzy mają wówczas obowiązek usunąć wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Marketer realizuje te czynności w rozsądnych granicach, biorąc pod uwagę dostępną technologię i koszt realizacji.

W szczególności, marketer powinien poinformować o takiej okoliczności wszystkie podmioty, którym w drodze umowy przekazał dane osobowe osoby, która zażądała ich usunięcia, o ile kontakt z nimi w danym czasie drogą elektroniczną jest możliwy, a także podmiotom, co do których stwierdził, że opublikowały one dane osobowe dotyczące ww. osoby w Internecie, 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.

111. Marketer może odmówić danej osobie prawa do bycia zapomnianym, o ile zachodzą przesłanki wyłączające prawo do żądania usunięcia danych osobowych. W kontekście działań marketingu bezpośredniego, których dotyczy niniejszy Kodeks, marketer zobowiązany jest zawsze zachować dane osobowe dla przypadków:

a) przetwarzania danych na potrzeby realizacji obowiązków prawnych nakładanych na organizatora w związku z akcjami promocyjnymi (np. rozliczenia podatkowe, obowiązki sprawozdawcze w zakresie gier hazardowych);
b) ustalenia, zaspokojenia oraz obrony roszczeń, w tym w ramach procesów sądowych.

112. Prawo do usunięcia danych („prawo do bycia zapomnianym") w kontekście działań marketingu bezpośredniego może wiązać się z istotnymi problemami praktycznymi. W ramach takich działań konieczne jest zapewnienie rozliczalności m. in. w zakresie źródeł danych oraz faktu uzyskania wymaganej prawem zgody na komunikację marketingową.

Jeżeli marketer realizujący marketing bezpośredni całkowicie usunie dane dotyczące określonej osoby („zapomni" taką osobę), to w przyszłości nie będzie w stanie wykazać zgodności z prawem wcześniejszych działań marketingu bezpośredniego. Może to narazić takiego marketera na istotne sankcje, w tym karę administracyjną.

W celu uniknięcia powyższej sytuacji, marketer jest uprawniony do stworzenia wewnętrznej listy osób, które skorzystały z prawa do bycia zapomnianym, do której dostęp będą mieli wyłącznie upoważnieni pracownicy, np. administrator systemów informatycznych oraz osoba odpowiedzialna w organizacji za dane osobowe (możliwie minimalny krąg osób). W ramach takiej listy mogą być przechowywane podstawowe dane osoby, która skorzystała z prawa do bycia zapomnianym oraz wszelkie dane oraz informacje pozwalające na zapewnienie rozliczalności działań marketera. Dostęp do tego rodzaju listy może być uzasadniony wyłącznie tym, że jest to niezbędne marketerowi do wykazania zgodności z prawem jego działań marketingu bezpośredniego, które realizował przed uwzględnieniem żądania usunięcia danych określonej osoby. Przykładem takiej sytuacji może być kontrola organu nadzorczego.

113. Inny ważny problem dostrzegany w praktyce marketingu bezpośredniego, to brak dostatecznego zrozumienia przez osoby, których dane dotyczą, na czym polega prawo do nieotrzymywania więcej komunikacji marketingowej, a na czym „prawo do bycia zapomnianym".

Pierwsza sytuacja wynika z wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego albo z wycofania zgody na takie przetwarzanie danych. Polega na tym, że marketer zaprzestaje przetwarzania danych, którego dotyczy sprzeciw albo którego dotyczyła zgoda. Z kolei druga sytuacja polega na całkowitym usunięciu danej osoby z systemów marketera, które wykorzystuje do działań marketingu bezpośredniego.

Zrealizowanie drugiego z ww. praw, czyli usunięcie danych osoby na jej żądanie, wiąże się z tym, że osoba ta może zostać ponownie wpisana do systemu marketera jako potencjalny nowy klient. Skoro marketer wcześniej ją „zapomniał" (usunął dotyczące jej dane), to stanowi ona dla marketera nową osobę. Tego rodzaju sytuacja może nierzadko przeczyć pierwotnym intencjom osoby, której dane dotyczą (zaprzestanie dalszego przetwarzania danych do celów marketingu bezpośredniego), choć czysto formalnie będzie zgodna z przepisami o ochronie danych osobowych.

W celu zapewnienia możliwie najlepszego i zgodnego z prawem uwzględnienia właściwych intencji osoby, która zgłasza żądanie usunięcia jej danych przetwarzanych do celów marketingu bezpośredniego, marketer w ramach najlepszej praktyki powinien w pierwszej kolejności zweryfikować, jaki dokładnie cel chce osiągnąć osoba zgłaszająca żądanie. W celu dokonania takiej weryfikacji marketer jest uprawniony nawiązać kontakt z taką osobą i zapytać o zakładany cel jej działania. Dalsze działania marketer powinien podejmować w zgodzie z poczynionymi ustaleniami.

114. Prawo do usunięcia danych („prawo do bycia zapomnianym") może być realizowane poprzez anonimizację danych.

Pozostałe prawa osób, których dane dotyczą

115. W związku z przetwarzaniem danych osobowych do celów marketingu bezpośredniego osobom, których dane dotyczą, przysługują również inne prawa: prawo do sprostowania danych, prawo do ograniczenia przetwarzania danych, a także prawo do przenoszenia danych. W praktyce działań marketingu bezpośredniego nie występują jednak żadne szczególnych aspekty wykonywania tych praw. Marketerzy mają obowiązek rzetelnie rozpatrywać i odpowiadać na żądania dotyczące ww. praw tak, jak tego wymagają ogólne przepisy RODO.

INFORMOWANIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH PRZY MARKETINGU BEZPOŚREDNIM

116. Marketerzy mają obowiązek spełniać wszystkie wymagania RODO w zakresie naruszeń ochrony danych osobowych przy działaniach marketingu bezpośredniego. Oznacza to, że mają w szczególności obowiązek:

a) przeciwdziałać potencjalnym naruszeniom ochrony danych osobowych,
b) wykrywać naruszenia, do których doszło.

Jeśli doszło do naruszenia ochrony danych osobowych przy działaniach marketingu bezpośredniego, marketer ma obowiązek wyczerpująco przeanalizować jego przyczyny, przebieg i skutki, a także opracować i wdrożyć środki mające na celu zaradzenie naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków. Marketer ma również obowiązek opracować środki mające na celu wyeliminowanie przyczyn naruszenia i uniknięcie takich samych lub podobnych naruszeń w przyszłości.

117. Każde stwierdzone naruszenie ochrony danych osobowych przy działaniach marketingu bezpośredniego musi być odpowiednio udokumentowane. Jeśli naruszenie ochrony danych osobowych stwierdził marketer-procesor, ma obowiązek niezwłocznie zgłosić to naruszenie marketerowi-administratorowi. Dalsze postępowanie wynikające ze stwierdzonego naruszenia ochrony danych osobowych jest zadaniem marketera-administratora.

118. Jeśli jest więcej niż mało prawdopodobne, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, marketer ma obowiązek zgłosić naruszenie organowi nadzorczemu zgodnie z wymogami RODO. Jeśli naruszenie ochrony danych osobowych przy działaniach marketingu bezpośredniego może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, marketer ma ponadto obowiązek zawiadomić o naruszenia osoby, których danych dotyczy naruszenie – tak, jak wymaga tego RODO.

119. Naruszeniem ochrony danych osobowych przy działaniach marketingu bezpośredniego są w szczególności następujące sytuacje:

a) uzyskanie dostępu do bazy marketingowej przez osobę nieuprawnioną;
b) udostępnienie adresów e-mail lub numerów telefonów odbiorców komunikacji marketingowej nieograniczonej liczbie osób, np. na stronie internetowej;
c) przesłanie komunikatu marketingowego zawierającego dane identyfikacyjne oraz historię zakupów określonego odbiorcy komunikacji marketingowej do innego odbiorcy komunikacji marketingowej;
d) przesłanie zbiorowej komunikacji marketingowej jednocześnie do wielu odbiorców w sposób ujawniający dane kontaktowe pozostałych odbiorców;
e) przypadkowa utrata dostępu do bazy marketingowej na skutek działania złośliwego oprogramowania szyfrującego dane zawarte w bazie;
f) nieautoryzowana zmiana adresów e-mail odbiorców komunikacji marketingowej.

120. Naruszenie ochrony danych osobowych przy działaniach marketingu bezpośredniego może powodować ryzyko naruszenia praw lub wolności osób fizycznych. Naruszenia praw lub wolności osób fizycznych mogą mieć różny charakter i zależeć od okoliczności naruszenia. Jako przykładowe naruszenia praw lub wolności osób fizycznych, do których mogą prowadzić naruszenia ochrony danych osobowych przy działaniach marketingu bezpośredniego można wskazać:
a) brak otrzymywania komunikacji marketingowej, na której zależy odbiorcom tej komunikacji (np. atrakcyjnych ofert, promocji itp.);
b) otrzymywanie uciążliwych telefonów lub wiadomości od innych podmiotów, które weszły w posiadanie danych kontaktowych odbiorców komunikacji marketingowej;
c) obawa o bezpieczeństwo swoich danych osobowych;
d) straty finansowe na skutek ujawnienia danych kontaktowych ułatwiających ataki phishingowe.

121. 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, marketer 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 marketer powinien wysłać do osób których dotyczy naruszenie bez zbędnej zwłoki, jak tylko finalnie określi pełen zakres naruszenia oraz występujących ryzyk.

Zawiadomienie powinno odbyć się z wykorzystaniem możliwie najszybszych środków komunikacji. W szczególności może się to odbyć poprzez przesłanie do osób, których dotyczy naruszenie stosownych wiadomości e-mail. Jeżeli marketer nie posiada adresów e-mail, może się to odbyć poprzez przesłanie SMS z linkiem do specjalnej strony internetowej zawierającej niezbędne informacje. Jeżeli marketer nie posiada ani adresu e-mail ani numeru telefonu, marketer powinien rozważyć wysłanie do wszystkich osób, których dane dotyczyło naruszenia, stosownych komunikatów pocztą tradycyjną. Jeśli marketer powiadomił już o naruszeniu osoby, których danych to naruszenie dotyczy i zgłosił naruszenie organowi nadzorczemu, może otrzymać od tego organu wskazanie przeprowadzenia dodatkowych działań informacyjnych. Takie wskazania marketer ma również obowiązek respektować.

8. Marketer może zrezygnować z ww. 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 marketer powinien wydać publiczny komunikat lub zastosować inny podobny środek, za pomocą którego osoby, których danych dotyczyło naruszenie, zostaną poinformowane w równie skuteczny sposób.

Aby zapewnić przejrzystość i możliwie najszersze dotarcie informacji o naruszeniu do ww. osób, marketer powinien wybrać takie środki publicznej komunikacji, jakimi standardowo i na co dzień

posługuje się w relacji z osobami, których danych dotyczyło naruszenie. Skoro marketer uznaje dany środek publicznej komunikacji jako skuteczny w codziennej komunikacji z tymi osobami (np. z swoimi klientami lub potencjalnymi klientami), to naturalne będzie użycie tego samego środka do zawiadomienia o naruszeniu.

Przykład:
Marketer prowadzi stronę internetową i jest to dla niego główny środek publicznej komunikacji. Doszło do naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Marketer nie ma możliwości, aby skontaktować się indywidualnie z osobami dotkniętymi naruszeniem lub wymagałoby to niewspółmiernie dużego wysiłku. Marketer ten publikuje na swojej stronie internetowej komunikat w formie pop-up lub „paska" informacyjnego, który pojawia się automatycznie po otwarciu strony internetowej.

STOSOWANIE KODEKSU I ADMINISTROWANIE

Monitorowanie przestrzegania Kodeksu

Z komentarzem [25]: Rozdział dotyczący stosowania i monitorowania został istotnie zmieniony z uwzględnieniem dotychczasowych uwag Urzędu.

122. Zgodnie z art. 41 RODO monitorowaniem przestrzegania Kodeksu zajmuje się podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy. Działania organu monitorującego pozostają bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego.

Organ monitorujący w swoich działaniach zobowiązany jest zapewnić zachowanie niezależności oraz brak konfliktu interesów.

123. Składając deklarację przystąpienia do stosowania niniejszego Kodeksu, deklarujący podmiot poddaje się przeglądowi przez organ monitorujący w odniesieniu do zgodności swojej działalności z regulacjami niniejszego Kodeksu. Obejmuje to:
a) udostępnianie do wglądu i/lub w celu przeprowadzenia audytu – procesów przetwarzania danych na żądanie organu monitorującego;
b) obowiązek udzielania odpowiedzi i informacji na wezwania organu monitorującego, w szczególności w odniesieniu do oceny faktycznej w skargach;
c) stosowanie się do ustaleń, wniosków i poleceń organu monitorującego.

124. Organ monitorujący w toku realizacji swoich działań może korzystać ze wsparcia organizacyjnego biura Polskiego Stowarzyszenia Marketingu SMB.

125. Każdy podmiot (w tym przedsiębiorca prowadzący jednoosobową działalność) realizujący marketing bezpośredni może przystąpić do Kodeksu.

126. W celu przystąpienia do Kodeksu i uzyskania rejestracji jako sygnatariusz Kodeksu aplikujący podmiot musi wypełnić i wnieść oświadczenie o przystąpieniu do Kodeksu, jak również wnieść wymaganą opłatę. Oświadczenie powinno zostać wypełnione przez aplikujący podmiot zgodnie ze stanem faktycznym i prawnym.

127. Podpisując oświadczenie o przystąpieniu do Kodeksu aplikujący zgadza się na związanie regulacjami Kodeksu oraz potwierdza, że jego organizacja na dzień podpisania oświadczenia spełnia wszystkie warunki przetwarzania danych osobowych stawiane przez Kodeks.

128. Po potwierdzeniu prawidłowości zgłoszenia audytorzy wyznaczeni przez organ monitorujący realizują audyt wstępny w celu weryfikacji zgodności działania podmiotu zgłaszającego z Kodeksem. W przypadku pozytywnej oceny z audytu, organ monitorujący podejmuje decyzję o przyjęciu danego podmiotu w poczet Sygnatariuszy. W przypadku negatywnej oceny z audytu organ monitorujący odmawia przyjęcia w poczet Sygnatariuszy. Wniesiona opłata nie podlega zwrotowi.

129. Organ monitorujący prowadzi publiczny rejestr sygnatariuszy Kodeksu. Sygnatariusze są uprawnieni do posługiwania się indywidualnym zaświadczeniem Sygnatariusza Kodeksu.

130. Postępowanie w sprawie przyjęcia sygnatariusza Kodeksu nie powinno trwać dłużej niż 30 dni roboczych od daty przyjęcie zgłoszenia. W przypadkach uzasadnionych okolicznościami (np. duża liczba aplikacji w jednym czasie, wielkość organizacji aplikującego) termin ten może ulec przesunięciu.

131. Każdy Sygnatariusz zobowiązany jest przejść audyt zgodności z niniejszym Kodeksem, realizowany przez organ monitorujący, co 3 (trzy) lata. Audyt przeprowadzany jest po uprzednim zawiadomieniu o tym fakcie Sygnatariusza z co najmniej 14-dniowym wyprzedzeniem.

132. Podmiot monitorujący może zwracać się do Sygnatariuszy z pytaniami lub prośbami o przedstawienie wyjaśnień, mającymi na celu weryfikację zgodności określonych procesów u Sygnatariuszy z niniejszym Kodeksem oraz RODO, w tym w ramach rozpatrywania skarg na Sygnatariusza. Jeżeli Sygnatariusz uchyla się od udzielenia pełnej odpowiedzi lub wyjaśnień, albo z ich treści wynika realne ryzyko naruszenia Kodeksu przez Sygnatariusza, podmiot monitorujący ma prawo zobowiązać Sygnatariusza do poddania się dodatkowemu audytowi podmiotu monitorującego. W przypadku realizowania audytu w tym trybie, Sygnatariusz może zostać obciążony dodatkowymi kosztami zaangażowania audytorów.

133. Przystąpienie i partycypacja w Kodeksie, jak również możliwość posługiwania się zaświadczeniem Sygnatariusza Kodeksu, są odpłatne.

Proces Skargowy

134. Każdy, kogo interes został naruszony w wyniku nieprzestrzegania postanowień niniejszego Kodeksu przez Sygnatariusza, może złożyć skargę na tego Sygnatariusza do podmiotu monitorującego. Skarga może zostać złożona poprzez formularz internetowy. Skarga powinna zawierać co najmniej:
   a) oznaczenie składającego skargę: imię, nazwisko lub nazwę firmy, adres korespondencyjny, adres e-mail lub telefon kontaktowy
   b) oznaczenie Sygnatariusza, którego działanie jest przedmiotem skargi
   c) opis okoliczności, w jakich doszło do naruszenia Kodeksu wraz z przedstawieniem ewentualnych dokumentów potwierdzających, że doszło do naruszenia
   d) ewentualnie – żądania wnoszącego skargę.

135. Skarga przyjmowana jest do rozpoznania przez Komisję Skargową powołaną przez podmiot monitorujący (dalej: **Komisja Skargowa**). Członkowie Komisji Skargowej powinni być powoływani spośród osób mających wiedzę i doświadczenie w zakresie reguł przetwarzania danych osobowych, w tym Kodeksu, oraz w zakresie marketingu bezpośredniego.

136. Komisja Skargowa działa na podstawie ustalonego przez siebie regulaminu, który udostępniany jest do wiadomości publicznej. Komisja Skargowa może kontaktować się

z wnoszącym skargę, jak również z Sygnatariuszem, przeciwko któremu została wniesiona skarga, w celu uzyskania pełnej informacji o zaistniałej sytuacji.

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

138. Od rozstrzygnięcia Komisji Skargowej nie przysługuje odwołanie.

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

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

Sankcje nakładane przez organ monitorujący

141. W przypadku stwierdzenia przez podmiot monitorujący, że Sygnatariusz narusza regulacje niniejszego Kodeksu, podmiot monitorujący może:
   a) wezwać Sygnatariusza do zaprzestania praktyk niezgodnych z Kodeksem;
   b) zawiesić Sygnatariusza w prawach Sygnatariusza Kodeksu;
   c) wykreślić dany podmiot z rejestru Sygnatariuszy Kodeksu;
   d) zakazać danemu podmiotowi ponownego przystąpienia do Kodeksu na okres do 3 lat w przypadku powtarzającego się, rażącego łamania Kodeksu.

Reguły dokonywania zmian w Kodeksie

142. W przypadku stwierdzenia, że Kodeks wymaga zmiany, Zarząd Polskiego Stowarzyszenia Marketingu SMB przygotowuje projekt zmian do Kodeksu wraz z uzasadnieniem. Po wypracowaniu projektu zmian Zarząd Stowarzyszenia kieruje wniosek o dokonanie zmian w Kodeksie pod obrady walnego zebrania członków Polskiego Stowarzyszenia Marketingu SMB. Projekt zmian wymaga przyjęcia przez walne zebranie członków Polskiego Stowarzyszenia Marketingu SMB uchwałą podjętą większością głosów. Po wypracowaniu projektu zmian Zarząd Stowarzyszenia kieruje wniosek o dokonanie zmian w Kodeksie pod obrady walnego zebrania członków Polskiego Stowarzyszenia Marketingu SMB. Projekt zmian wymaga przyjęcia przez walne zebranie członków Polskiego Stowarzyszenia Marketingu SMB uchwałą podjętą większością głosów.

143. W przypadku podjęcia uchwały o przyjęciu projektu zmian w Kodeksie, Polskie Stowarzyszenie Marketingu SMB poddaje projekt zmian w Kodeksie publicznym konsultacjom.

144. Prezes Urzędu Ochrony Danych Osobowych na wniosek Polskiego Stowarzyszenia Marketingu SMB opiniuje i zatwierdza zmiany i rozszerzenia Kodeksu w toku procedury.

145. Po uzyskaniu formalnego zatwierdzenia zmian Kodeksu przez Prezesa Urzędu Ochrony Danych Osobowych, Zarząd Polskiego Stowarzyszenia Marketingu SMB 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.

146. Sygnatariusze zobowiązani są dostosować się do zmian w Kodeksie, niezwłocznie po uzyskaniu informacji o dokonanych zmianach. Uchwała o zmianie treści Kodeksu może przewidywać stosowne vacatio legis, aby dać czas sygnatariuszom na dokonanie niezbędnych zmian.