Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej

PROJEKT DO KONSULTACJI PUBLICZNYCH

Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej - PROJEKT DO KONSULTACJI PUBLICZNYCH

Opinie proszę kierować na adres: konsultacje@iab.org.pl do 31 sierpnia 2018

Spis treści

Wprowadzenie

Istota i zakres zastosowania Kodeksu

Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej (dalej: „Kodeks") stanowi zbiór zasad postępowania w zakresie ochrony danych osobowych w branży internetowej, ze szczególnym uwzględnieniem sektora reklamy internetowej.

Kodeks stanowi kodeks postępowania, o którym mowa w art. 40 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 (dalej: „Rozporządzenie", „RODO").

Stosowanie Kodeksu postępowania stanowi potwierdzenie wywiązywania się z obowiązków nałożonych w przepisach RODO na administratorów danych oraz podmioty przetwarzające, które działają w sektorze reklamy internetowej.

Niniejszy kodeks stosuje się zarówno do administratorów danych, jak i podmiotów przetwarzających dane osobowe zrzeszonych w Związku Pracodawców Branży Internetowej IAB Polska. Zasady przystąpienia do Kodeksu i jego funkcjonowania zostały szczegółowo określone w rozdziale VII.

Cel opracowania Kodeksu

Kodeks stanowi doprecyzowanie zasad przetwarzania i ochrony danych osobowych określonych w RODO.

Celem opracowania niniejszego Kodeksu jest pomoc we właściwym stosowaniu przepisów RODO, z uwzględnieniem specyfiki działania sektora reklamy internetowej. Służyć temu ma upowszechnienie i jednolite wdrażanie dobrych praktyk branżowych określonych w Kodeksie.

Niniejszy Kodeks koncentruje się na zastosowaniu przepisów Rozporządzenia przede wszystkim w odniesieniu do kwestii najważniejszych i specyficznych dla branży internetowej, wskutek czego część zagadnień uregulowanych w RODO, a wspólnych dla wszystkich branż (sektorów), została w Kodeksie pominięta.

I. Rozdział pierwszy: Dane osobowe na podstawie RODO

1.1. Dobre praktyki branżowe:

- w zależności od okoliczności konkretnego przetwarzania danych osobowych, ta sama kategoria informacji (np. adres IP, identyfikator pliku *cookie*) może stanowić dane osobowe w rozumieniu RODO lub też nie mieć takiego charakteru. Z ostrożności zalecane jest, aby w przypadkach braku pewności, czy określona kategoria danych stanowi daną osobową, także stosować do niej zasady ochrony określone w RODO,
- nie należy traktować pseudonimizacji równoważnie z anonimizacją. Anonimizacja jest nieodwracalna, a pseudonimizacja jest procesem możliwym do odwrócenia z wykorzystaniem dodatkowych informacji (np. tabeli przyporządkowań, kluczy szyfrujących, danych źródłowych itp.),
- dane osobowe spseudonimizowane, po usunięciu informacji pozwalającej na przyporządkowanie ich do osoby fizycznej (np. wiersza tabeli przyporządkowań, kluczy szyfrujących, danych źródłowych itp.), można traktować jako dane zanonimizowane,
- zalecane jest śledzenie standardów stosowanych technik anonimizacji i pseudonimizacji.

1.2. Definicja danych osobowych na gruncie RODO – kryteria oceny, czy dana informacja stanowi dane osobowe.

Przy stosowaniu kryteriów oceny, czy konkretna informacja stanowi dane osobowe, należy pamiętać o następujących zasadach:

- przepisy RODO nie dotyczą przetwarzania danych osobowych dotyczących osób prawnych oraz tzw. ułomnych osób prawnych, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (ułomnej osoby prawnej),
- dane zagregowane, które nie odnoszą się do jednej osoby, ale do całej grupy osób, nie stanowią danych osobowych, o ile nie można w takim agregacie danych zidentyfikować określonych osób fizycznych, których dane dotyczą. Przykładowo, informacja o lokalizacji

(nazwie miasta użytkownika) nie będzie stanowić danej osobowej, jeżeli administrator nie dysponuje dodatkowymi informacjami, które mógłby powiązać z tą informacją.

Zgodnie z art. 4 pkt 1) RODO:

> *„dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");*
>
> *możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;*

Na gruncie RODO dane osobowe stanowią zarówno informacje o zidentyfikowanej, jak i możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować. W branży internetowej szczególne znaczenie ma ocena, czy różnego rodzaju identyfikatory generowane przez urządzenia, aplikacje, narzędzia i protokoły stanowią dane osobowe. Należy w związku z tym podkreślić, że **identyfikatory internetowe „same w sobie" nie stanowią danych osobowych.** Identyfikatory te uzyskują taki charakter dopiero wówczas, gdy łączone są z innymi unikatowymi identyfikatorami (np. ID użytkownika z systemu autoryzacyjnego administratora danych) lub innymi informacjami pozwalającymi na identyfikację danej osoby fizycznej. Taką wykładnię potwierdza motyw 30 Preambuły RODO:

> *Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery, mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób.*

Przykładowo, pliki *cookies*, które dostosowują wygląd strony internetowej - począwszy od pierwszych jej odwiedzin przez użytkownika - i wygasają stosunkowo szybko, czy też są nośnikiem informacji o lokalizacji dla celów wyświetlania ceny w odpowiedniej walucie, przeważnie nie będą stanowić danych osobowych. Identyfikatory plików *cookies* będą natomiast stanowiły dane osobowe w sytuacji, w której administrator danych przetwarza dane w ramach dwóch odrębnych procesów biznesowych: w pierwszym zbierane są pliki *cookies*, a w drugim przetwarzane są informacje identyfikujące osobę fizyczną, takie jak adres *e-mail* czy imię i nazwisko użytkownika serwisu internetowego, a istnieje możliwość zestawienia informacji z tych dwóch procesów. Bez znaczenia

pozostaje okoliczność, że administrator danych osobowych nie podjął środków w celu identyfikacji osoby, której dotyczą przetwarzane przez niego informacje (nie zestawił tych danych), jeżeli tylko takie środki były dozwolone przez prawo, a ich podjęcie leżało w zakresie możliwości administratora danych. Podobnie, identyfikatory plików *cookies* będą stanowiły dane osobowe w razie połączenia tych danych z danymi transakcyjnymi umożliwiającymi identyfikację konkretnej osoby.

Aby ocenić, czy określone dane stanowią dane osobowe zalecane jest również przeprowadzenie testu przez administratora danych zgodnie z motywem 26 Preambuły RODO:

> *Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.*

Zgodnie z powyższym, do administratora należy obowiązek przeprowadzenia oceny, czy na podstawie dostępnych danych określona osoba fizyczna może zostać zidentyfikowana. Każda informacja, niezależnie od sposobu i formy jej wyrażenia, może zostać uznana za informację o charakterze osobowym, jeżeli pozwala na zidentyfikowanie określonej osoby fizycznej. Konkretna informacja nie musi być powszechnie zrozumiała – charakter prawny tej informacji będzie bowiem oceniany indywidualnie dla każdego jej dysponenta. Nie musi być również prawdziwa, co należy rozumieć w ten sposób, że może dotyczyć okoliczności w sposób obiektywny nieistniejących, pod warunkiem jednak, iż może prowadzić do zidentyfikowania konkretnej osoby fizycznej. Innymi słowy, **konkretna informacja stanowi dane osobowe określonej osoby, jeżeli administrator danych ma możliwość powiązania tej konkretnej informacji z konkretną osobą przy uwzględnieniu takich czynników jak koszt i czas potrzebny do zidentyfikowania danej osoby oraz technologia dostępna w momencie przetwarzania danych, jak i postęp technologiczny.**
Nadmierne koszty, czas, a także dostępna technologia, winny być czynnikami branymi pod uwagę przez administratora danych w przeprowadzonym teście determinującym, czy określony identyfikator (aplikacji, urządzenia, internetowy) w połączeniu z zestawionymi z nim danymi stanowi dane osobowe. Administrator danych nie jest zobowiązany do prowadzenia badań nad rozwojem technologii w środowiskach naukowych, inżynierii programistycznej, czy
nieadekwatnego dla przedmiotowego testu poszukiwania informacji o nowych technologiach. Wygórowane koszty, nadmierny czynnik czasu, dostępne technologie i postęp technologiczny powinny być uwzględnione obiektywnie, z zachowaniem racjonalności i adekwatności.

1.3. Anonimizacja danych osobowych.

Motyw 26 Preambuły RODO definiuje anonimizację w następujący sposób:

> *Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych. (…)*

Anonimizacja danych osobowych to **trwałe i nieodwracalne** przekształcenie danych osobowych, po którym nie można (w rozsądnym wymiarze czasowym) przyporządkować informacji określonej lub możliwej do zidentyfikowania osobie fizycznej za pomocą wszystkich możliwych środków, jakimi dysponuje administrator, podmiot przetwarzający lub osoba trzecia. Kluczową cechą anonimizacji jest jej nieodwracalność. Potwierdza to definicja z PN-ISO/IEC 29100: "*anonimizacja jest procesem, w którym informacje umożliwiające identyfikację osoby są nieodwracalnie zmienione w taki sposób, aby nie istniała już możliwość bezpośredniego lub pośredniego zidentyfikowania podmiotu informacji umożliwiających identyfikację osoby przez administratora informacji umożliwiających identyfikację osoby działającego samodzielnie lub we współpracy z jakąkolwiek inną stroną*."

1.3.1. Korzyści anonimizacji danych osobowych.

Główną korzyścią anonimizacji wynikającą z definicji i regulacji prawnych jest to, iż **dane osobowe po zastosowaniu anonimizacji przestają być „danymi osobowymi" i tym samym przestają podlegać wymogom RODO.** Takie dane mogą być dalej przetwarzane bez ograniczeń związanych z regulacjami o ochronie danych osobowych (np. w zakresie zmiany celu przetwarzania danych osobowych).

1.3.2. Ryzyka skuteczności anomimizacji danych osobowych.

Nie ma standardu pozwalającego na uznanie za najlepszą konkretnej techniki anonimizacji, stąd podczas dokonywania jej wyboru, mając na uwadze aktualny stan technologii, należy uwzględnić trzy czynniki ryzyka mogące wpłynąć na skuteczność procesu anonimizacji:

- możliwość wyodrębnienia (wydzielenia) informacji dotyczących zidentyfikowanej osoby fizycznej, które pozwalają na wydzielenie zapisów identyfikujących określoną osobę fizyczną w zbiorze,
- możliwość tworzenia powiązań, np. na podstawie analizy korelacji danych, prowadzących do przyporządkowania danych do określonej osoby fizycznej,

- możliwość wnioskowania ze znacznym prawdopodobieństwem o wartości danego atrybutu na podstawie innych atrybutów zbioru, prowadzącego do przyporządkowania danych do określonej osoby fizycznej.

1.3.3. Techniki anonimizacji.

Utworzenie prawdziwie anonimowego zbioru danych przy jednoczesnym zachowaniu odpowiedniej ilości podstawowych informacji, które są niezbędne do realizacji zadania, nie jest łatwe, dlatego istotnym problemem staje się dobór odpowiednich technik anonimizacji. Dla każdego przypadku anonimizacji danych należy podejść indywidualnie. W zależności od kategorii danych i celu, w jakim zanonimizowane dane mają być przetwarzane, powinno się dobrać odpowiednie techniki anonimizacji danych. Opierając się na wytycznych Grupy Roboczej Art. 29 zawartych w Opinii 05/2014 w sprawie technik anonimizacji, zaleca się stosowanie dwóch technik opartych na **randomizacji i uogólnieniu**:

- **randomizacja** zmienia prawdziwość danych w celu wyeliminowania ścisłego związku między danymi a konkretną osobą fizyczną. Dane charakteryzujące się wystarczającą nieprawidłowością nie pozwalają na określenie konkretnej jednej osoby. Jednak jeżeli dane dalej odnoszą się do jednej osoby, istnieje ryzyko wnioskowania, dlatego konieczne staje się skorzystanie z dodatkowych technik: a
    - **dodanie zakłóceń** polega na modyfikacji atrybutów, które mogą mieć niekorzystny skutek dla poszczególnych osób fizycznych, w taki sposób, aby były one mniej dokładne, przy jednoczesnym zachowaniu ogólnej atrybucji. Przykładowo, modyfikacja wieku pacjenta w przeprowadzanych badaniach klinicznych +/- 5 lat, skutecznie nie pozwoli osobie trzeciej na identyfikację osoby fizycznej;
    - **permutacja** polega na tasowaniu wartości atrybutów w tabelach, poprzez podstawianie wartości z jednego zapisu do innego zapisu – dane w zbiorze pozostają takie same, ale korelacja między wartościami i poszczególnymi osobami fizycznymi jest inna. Metodę tę stosuje się wtedy, gdy istotne jest zachowanie dokładnych atrybutów w zbiorze;
    - **prywatność różnicowa** jest stosowana w czasie rzeczywistym podczas generowania zanonimizowanego widoku danych, przy zachowaniu danych pierwotnych przez administratora. Korzyścią stosowania tej techniki jest fakt, że dane osobowe są udostępniane upoważnionym osobom trzecim w odpowiedzi na zapytanie, a nie przez udostępnianie całego zbioru;
- **uogólnienie lub osłabienie atrybutów** poprzez zmianę zakresu lub rzędu wielkości może skutecznie uniemożliwić wyodrębnianie, jednak nie zabezpiecza przed tworzeniem powiązań i wnioskowaniem. Dla silniejszej gwarancji prywatności łączy się dodatkowe techniki:
    - **agregacja i k-anonimizacja** ma na celu uniemożliwienie wyodrębnienia poprzez zgrupowanie danych osoby z co najmniej k innymi osobami fizycznymi;

- **l-dywersyfikacja** jest rozszerzeniem k-anonimizacji uniemożliwiającym ataki oparte na wnioskowaniu deterministycznym poprzez zadbanie, aby w każdej klasie równoważności każdy atrybut miał co najmniej l różnych wartości. Technika jest skuteczna, jeśli wartości atrybutów są równo rozmieszczone. W przeciwnym wypadku, lub gdy atrybuty należą do małego zakresu wartości, technika może nie zapobiec identyfikacji.

Poniższa przykładowa tabela wskazuje, jakie techniki anonimizacji danych stosować w kontekście przetwarzania danych pracowników, a które to techniki znajdują zastosowanie do anonimizacji danych osobowych również innych kategorii podmiotów danych (np. użytkowników Internetu).

Pole	Typ zmiany	Technika
ID Pracownika	Hashowanie	SHA-2 z solą
Data Urodzin	Wstawić losową datę z przedziału (1-2000)	Randomizacja
Nazwisko panieńskie matki	Usunąć	Usunięcie rzadkich atrybutów
Pesel/Nip	Usunąć	Usunięcie rzadkich atrybutów
Adres email	Zamienić na mail@iab.pl dla wszystkich	Uogólnienie
Telefon	Zamienić na losowy numer	Randomizacja
Ulica	Zamienić na jeden adres dla wszystkich pracowników	Uogólnienie
Numer Budynku Mieszkania	Zamienić na numer z zakresu 1-1000	Uogólnienie
Kod Pocztowy	Zamienić na kod miasta wojewódzkiego	Uogólnienie
Miasto	Zamienić na miasto wojewódzkie	Uogólnienie

1.4. Spseudonimizowane dane osobowe.

Zgodnie z art. 4 pkt 5) RODO:

> *„pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.*

Psuedonimizacja to **środek zwiększający bezpieczeństwo przetwarzania danych osobowych**. Zastosowanie tego zabezpieczenia powinno wynikać z analizy ryzyka dla systemu informatycznego uwzględniającej ryzyko naruszenia praw i wolności osoby fizycznej.

Pseudonimizacja to proces **odwracalny**, który polega na zastąpieniu jednego atrybutu innym atrybutem, co nadal umożliwia wyodrębnienie konkretnej osoby fizycznej i tworzenie w odniesieniu do tej osoby powiązań między różnymi zbiorami. Pseudonimizacja skutecznie podwyższa bezpieczeństwo przetwarzania danych, poprzez ograniczenie możliwości tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą. Nie jest to jednak równoznaczne z anonimizacją, w związku z czym te dane dalej podlegają przepisom o ochronie danych osobowych.

1.4.1. Korzyści pseudonimizacji danych osobowych.

RODO przewiduje następujące korzyści związane z pseudonimizacją:

- pseudonimizacja stanowi środek zwiększający bezpieczeństwo przetwarzania danych osobowych. Zastosowanie tego zabezpieczenia powinno wynikać z analizy ryzyka dla systemu informatycznego uwzględniającej ryzyko naruszenia praw i wolności osoby fizycznej (art. 32 ust. 1 lit. a)),
- pseudonimizacja stanowi techniczny środek ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 ust. 1 RODO),
- w razie wdrożenia odpowiednich zabezpieczeń, w tym ewentualnego szyfrowania lub pseudonimizacji oraz pod warunkiem spełnienia pozostałych wymogów przewidzianych przez art. 6 ust. 4 RODO, dane osobowe mogą być przetwarzane w celu innym niż cel, dla którego dane osobowe zostały zebrane,
- w razie naruszenia ochrony danych osobowych uprzednie wdrożenie pseudonimizacji może wiązać się z brakiem konieczności zawiadamiania osób, których dane dotyczą o takim naruszeniu (art. 34 RODO) ze względu na brak wysokiego ryzyka naruszenia ich praw lub wolności (np. w razie wycieku danych osobowych osoby nieuprawnione nie będą miały do

tych danych osobowych dostępu ze względu na pseudonimizację). Ponadto, w pewnych okolicznościach uprzednie wdrożenie pseudonimizacji może wiązać się nawet z brakiem konieczności zgłaszania naruszenia do organu nadzorczego (art. 33 RODO) ze względu na małe prawdopodobieństwo by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,

- pseudonimizacja jest istotnym zabezpieczeniem w razie przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (art. 89 ust. 1 RODO).

Jedną z głównych wartości pseudonimizacji jest możliwość bezpiecznego przekazania danych do systemów zewnętrznych przetwarzania danych osobowych. Po dokonaniu pseudonimizacji zewnętrzne systemy nie mają możliwości zidentyfikowania konkretnych osób na podstawie takich danych.

1.4.2. Techniki pseudonimizacji danych osobowych.

Przykładowe techniki pseudonimizacji to:

- szyfrowanie z kluczem tajnym – dobry klucz daje dużą gwarancję bezpieczeństwa, jednak administrator może odszyfrować dane,
- funkcja skrótu – dla każdej wartości dodaje się stałej wielkości wynik, którego nie można odwrócić (jest to technika często stosowana do przechowywania haseł),
- funkcja skrótu z dodaniem losowego ciągu znaków (ang. *salt*) – ogranicza prawdopodobieństwo uzyskania wartości treści lub odczytania zasobu,
- funkcja skrótu z dodanym kluczem, który jest przechowywany – zapewnia łatwiejsze odzyskanie treści lub odczytania zasobu dla administratora, co jednocześnie jest trudne dla atakującego,
- szyfrowanie deterministyczne lub funkcja skrótu z kluczem, bez przechowywania klucza – pozwala ograniczyć ryzyko tworzenia powiązań między zbiorami przy zastosowaniu innych kluczy,
- tokenizacja - często stosowana w sektorze finansowym, polega na przypisaniu wartości, które nie zostały w sposób matematyczny uzyskane z danych pierwotnych, np. dla numerów kart.

Wraz z postępem technologicznym i doświadczeniami administratorów danych oraz podmiotów przetwarzających powyższe techniki mogą ulec zmianie i udoskonaleniu.

1.5. Podatność poszczególnych technik anonimizacji i pseudnomizacji na ryzyka.

Poszczególne techniki anonimizacji i pseudonimizacji wykazują różne podatności względem trzech czynników ryzyka: wyodrębnienia, tworzenia powiązań oraz wnioskowania. W poniższej tabeli określono, czy przy zastosowaniu danej techniki ryzyka te istnieją. Należy je wziąć pod uwagę przy wyborze odpowiedniej techniki anomizacji i pseudonimizacji danych, uwzględniając również rodzaj przetwarzanych danych..

Technika	Wyodrębnianie	Tworzenie powiązań	Wnioskowanie
Pseudonimizacja	Tak	Tak	Tak
Dodawanie zakłóceń	Tak	Być może nie	Być może nie
Zastąpienie	Tak	Tak	Być może nie
Agregacja lub k-anonimizacja	Nie	Tak	Tak
L-dywersyfikacja	Nie	Tak	Być może nie
Prywatność różnicowa	Być może nie	Być może nie	Być może nie
Skracanie/Tokeniza-cja	Tak	Tak	Być może nie

II. Rozdział drugi: Określenie roli w procesie przetwarzania: administrator i podmiot przetwarzający

2.1. Dobre praktyki branżowe:

- planując nową operację przetwarzania danych osobowych należy określić swój status, w szczególności, czy jest się administratorem danych, czy podmiotem przetwarzającym;
- w sytuacji, w której dany podmiot określa cele i sposoby przetwarzania danych osobowych, jest on administratorem danych. W praktyce chodzi o decyzje dotyczące tego, jakie dane o użytkowniku mają być wykorzystywane (np. dane zbierane z urządzenia użytkownika), jak również o sposobie wykorzystywania tych danych (np. konfigurowanie spersonalizowanej reklamy dla tego użytkownika). Podmiot przetwarzający nie realizuje własnych celów przetwarzania danych, nie może wykorzystywać danych osobowych w inny sposób niż zgodnie z instrukcjami administratora. W reklamie internetowej powierzone mu przez administratora procesy przetwarzania danych związane są np. z dostarczaniem technologii służącej do kupowania i sprzedawania reklam, czy też realizacji instrukcji klienta lub strony trzeciej, dotyczących tego, jakie dane zbierać oraz jak personalizować reklamy dla tego użytkownika;
- przy ocenie, czy dany podmiot jest administratorem, czy podmiotem przetwarzającym należy stosować kryteria określone w niniejszym rozdziale.

2.2. Rodzaje podmiotów przetwarzających dane osobowe.

W myśl art. 4 pkt 7) RODO:

> „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Podstawowym kryterium odróżniającym administratora danych osobowych od innych podmiotów przetwarzających dane jest **sprawowanie faktycznej kontroli nad przetwarzaniem danych, a więc**

decydowanie o celach i sposobach przetwarzania, nie zaś faktyczne przetwarzanie, które może zostać powierzone innemu podmiotowi.

Administratorem jest podmiot, który spełnia dwa warunki: a) ustala cele przetwarzania danych osobowych oraz b) ustala sposoby przetwarzania danych. W sytuacji, gdy te czynności są wykonywane wspólnie przez dwa podmioty, są one współadministratorami danych. Okoliczność, że w ramach jednej kampanii reklamowej dane są przetwarzane w tym samym celu (np. marketingowym) przez więcej niż jeden podmiot, nie czyni ich jednak współadministratorami danych, konieczne jest bowiem jeszcze stwierdzenie elementu wspólności podejmowania decyzji przez te podmioty.

W myśl art. 4 pkt 7) RODO:

> „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Przetwarzanie danych osobowych przez podmiot przetwarzający zawsze odbywa się w imieniu administratora danych. Podmiot ten nie realizuje więc własnych celów przetwarzania danych. Nie może on wykorzystywać danych osobowych w inny sposób, niż zgodnie z instrukcjami administratora.

2.3. Dalszy podmiot przetwarzający (*podprocessor*).

Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego (tzw. dalszego podmiotu przetwarzającego lub podprocessora) tylko za zgodą administratora. Dalsze podmioty przetwarzające są obowiązane do spełnienia tych samych warunków przetwarzania danych, co podmioty przetwarzające. W sytuacji, gdy podmiot przetwarzający zleci część wykonywanych czynności przetwarzania (np. jeden obszar związany z przetwarzaniem danych osobowych) swojemu podwykonawcy, ten podwykonawca staje się podprocessorem. W przypadku branży reklamy internetowej z dalszym podpowierzeniem danych osobowych możemy mieć do czynienia w przypadku podmiotów realizujących kampanie reklamowe w modelu *programmatic.*

2.4. Kryteria ustalenia, czy dany podmiot w branży internetowej jest administratorem danych, czy podmiotem przetwarzającym.

W wielu przypadkach ustalenie, na podstawie wyżej przedstawionych definicji legalnych, który z podmiotów jest administratorem danych, a który podmiotem przetwarzającym, nastręcza trudności.

Z tych przyczyn, przy dokonywaniu oceny rekomenduje się uwzględnienie przez podmioty z branży internetowej **następujących, dodatkowych kryteriów.**

Tworzenie identyfikatora użytkownika (UID) - identyfikatora pliku cookie lub innego internetowego identyfikatora	
Czy podmiot tworzy identyfikator dla danego użytkownika w celu przetwarzania danych (identyfikatora oraz danych powiązanych z tym identyfikatorem) dla własnych celów?	Odpowiedź TAK wskazuje, że ten podmiot w typowych sytuacjach jest administratorem.
Czy podmiot tworzy identyfikator dla danego użytkownika w celu przetwarzania danych (identyfikatora oraz danych powiązanych z tym identyfikatorem) jedynie dla celów swojego klienta (zgodnie ze zleceniem klienta) np. reklamodawcy lub wydawcy?	Odpowiedź TAK wskazuje, że w typowych sytuacjach ten podmiot jest podmiotem przetwarzającym.
Czy ten sam identyfikator jest nadawany użytkownikowi w odniesieniu do wielu klientów? Dany podmiot łączy dane o użytkowniku od różnych klientów (tworzy jeden "data pool" w celach reklamowych).	Odpowiedź TAK wskazuje, że w typowych sytuacjach ten podmiot jest administratorem.
Czy użytkownik ma nadawany inny identyfikator w odniesieniu do różnych klientów np.UID123 dla reklamodawcyXYZ i UID456 dla reklamodawcyABC?	Odpowiedź TAK wskazuje, że w typowych sytuacjach ten podmiot jest podmiotem przetwarzającym.
Sposób korzystania z danych osobowych	
Czy dany podmiot określa, jakie dane o użytkowniku mają być zbierane z urządzenia użytkownika i konfiguruje spersonalizowane reklamy dla tego użytkownika?	Odpowiedź TAK wskazuje, że w typowych sytuacjach ten podmiot jest administratorem.
Czy dany podmiot dostarcza jedynie technologię kupowania i sprzedawania reklam, działając na podstawie instrukcji klienta lub strony trzeciej, dotyczących tego, jakie dane zbierać oraz jak personalizować reklamy dla tego użytkownika?	Odpowiedź TAK wskazuje, że w typowych sytuacjach ten podmiot jest podmiotem przetwarzającym.

2.5. Status podmiotów przetwarzających dane w ramach reklamy internetowej, w tym reklamy *programmatic*.

W łańcuchu podmiotów biorących udział w prowadzeniu reklamy internetowej wyróżnić można takie podmioty jak:

a) wydawcy,
b) sieci reklamowe,
c) domy mediowe,
d) agencje interaktywne,
e) reklamodawców.

W przypadku oferowania reklamy internetowej w technologii *programmatic*, a więc modelu polegającym na automatyzacji sprzedaży i zakupu reklamy internetowej, dodatkowo wyróżnić należy następujące podmioty:

a) operatorzy platform DMP (Data Management Platform) – platform do zbierania i zarządzania danymi o użytkownikach, które mogą być wykorzystywane przez wydawcę lub reklamodawcę,
b) operatorzy platform DSP (Demand-Side-Platform) – platform strony popytowej, których reklamodawca (lub agencja) używa do kupowania powierzchni reklamowej,
c) operatorzy platform SSP (Supply-Side-Platform) – platform strony podażowej, umożliwiających wydawcy udostępnienie powierzchni reklamowej do sprzedaży.

Na rynku reklamy internetowej, zarówno w modelu tradycyjnym, jak i w modelu *programmatic*, funkcjonują jeszcze podmioty świadczące usługi analityczne.

Poniższa tabela przedstawia poszczególne podmioty uczestniczące w łańcuchu reklamy internetowej, z określeniem danych przez nie przetwarzanych, a także ich typowego statusu, z uwagi na rodzaj i sposób przetwarzania danych osobowych.

PODMIOTY PRZETWARZAJĄCE DANE OSOBOWE W INTERNECIE

Podmiot	Rodzaje danych	Typowy status ze względu na sposób wykorzystania danych
Model tradycyjny		
WYDAWCA	Cookie ID, Advert ID, IP, inne	ADMINISTRATOR DANYCH
SIEĆ REKLAMOWA	Cookie ID, Advert ID, IP, inne	ADMINISTRATOR DANYCH
DOM MEDIOWY	Cookie ID, Advert ID, IP, inne	PODMIOT PRZETWARZAJĄCY
AGENCJA INTERAKTYWNA	IP, email	PODMIOT PRZETWARZAJĄCY
REKLAMODAWCA	IP – opcjonalnie	ADMINISTRATOR DANYCH
Model programmatic		
PLATFORMA DMP	Cookie ID, dane demograficzne dopisane do rekordu, inne	ADMINISTRATOR DANYCH (m.in. w zakresie danych third party użytkownika) PODMIOT PRZETWARZAJĄCY (w zakresie danych first party użytkownika)
PLATFORMA DSP	Cookie ID, Advert ID, IP	W zależności od operacji na danych - ADMINISTRATOR DANYCH/ PODMIOT PRZETWARZAJĄCY
PLATFORMA SSP	Cookie ID, Advert ID, IP	W zależności od operacji na danych - ADMINISTRATOR DANYCH/ PODMIOT PRZETWARZAJĄCY
Analityka		
FIRMA ANALITYCZNA	Cookie ID, Advert ID, IP, inne	PODMIOT PRZETWARZAJĄCY

III. Rozdział trzeci: Podstawy prawne przetwarzania danych osobowych

3.1. Dobre praktyki branżowe:

- planując nową operację przetwarzania danych osobowych niezbędne jest określenie odpowiedniej podstawy prawnej przetwarzania,
- w przypadku przetwarzania danych osobowych w celach marketingowych, to na administratorze danych (np. wydawcy) spoczywa obowiązek dokonania wyboru odpowiedniej podstawy prawnej, np. zgody podmiotu danych osobowych (*opt-in*) lub prawnie uzasadnionego interesu administratora (*opt-out*),
- w przypadku niektórych działań reklamowych w Internecie, legalność prowadzenia kampanii marketingowych wymaga spełnienia warunków określonych w innych – niż RODO – aktach prawnych, w szczególności ustawie o świadczeniu usług drogą elektroniczną oraz prawie telekomunikacyjnym.

3.2. Przesłanki legalności prowadzenia działalności marketingowej w Internecie.

W działalności podmiotów z branży internetowej szczególnego znaczenia nabiera wykorzystywanie informacji w celu marketingowym. Przykładowo, działalność ta może polegać na przesyłaniu za pomocą środków komunikacji elektronicznej, w tym za pomocą poczty elektronicznej, jakichkolwiek materiałów reklamowych, promocyjnych lub informacyjnych, w celu wywołania określonej reakcji osoby, której dane dotyczą, w szczególności w celu zachęcenia do nabywania określonych towarów, usług, a także promowania określonych postaw, zachowań lub wizerunku określonych podmiotów (*mailing*). Inną formą działalności marketingowej jest reklama *display* tzn. reklama graficzna emitowana na powierzchni witryny lub jako baner reklamowy, przy wykorzystaniu mechanizmów personalizacji reklamy do zainteresowań i potrzeb użytkownika.

W związku z powyższym należy podkreślić, że **prowadzenie aktywności marketingowej wskazanej powyżej wymaga zgodności nie tylko z przepisami RODO, ale również innymi regulacjami**

sektorowymi. W szczególności, podmiot wykorzystujący dane w celach marketingowych, w zależności od rodzaju prowadzonych działań, może być zobowiązany do wykazania, że:

- prawidłowo określił podstawę prawną przetwarzania danych osobowych dla celów marketingowych zgodnie z wymogami RODO,
- uzyskał skuteczną zgodę na przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego zgodnie z art. 173 prawa telekomunikacyjnego,
- uzyskał skuteczną zgodę na kierowanie treści marketingowych (informacji handlowych) zgodnie z art. 10 ust. 2 ustawy o świadczeniu usług drogą elektroniczną lub art. 172 prawa telekomunikacyjnego.

Powyższe rozróżnienie warunków legalności prowadzenia działalności marketingowej w Internecie może mieć **istotne znaczenie przy ocenie**:

- legalności korzystania z danych w celach marketingowych. Przykładowo, inne mogą być warunki dopuszczalności wyrażenia zgody na przetwarzanie informacji (danych osobowych) zawartych w plikach *cookies* od warunków wyrażenia zgody na instalowanie tego rodzaju plików w urządzeniach końcowych abonenta lub użytkownika końcowego,
- właściwego organu nadzorczego do weryfikacji, czy przesłanki te zostały spełnione. Przykładowo, do oceny zgodności przetwarzania danych osobowych z przepisami RODO właściwy będzie Prezes Urzędu Ochrony Danych Osobowych (PUODO,) a do oceny zgodności pozostałych wymogów zawartych w regulacjach sektorowych – właściwe będą inne organy nadzorcze.

3.3. Podstawy prawne przetwarzania danych osobowych przez podmioty z branży internetowej (art. 6 ust. 1 RODO).

Przetwarzanie danych osobowych, które nie należą do tzw. szczególnych kategorii danych (art. 9 i 10 RODO), jest dozwolone w razie spełnienia jednej z sześciu przesłanek, określonych w art. 6 ust. 1 RODO. Należy podkreślić, że wszystkie przesłanki przetwarzania danych są równoważne.

Wybór przez administratora najbardziej odpowiedniej podstawy prawnej przetwarzania danych osobowych będzie zależał od **celu** oraz **kontekstu przetwarzania danych**. Przykładowo, jeżeli celem przetwarzania jest świadczenie usługi, to nie ma konieczności zbierania zgody na przetwarzanie danych osobowych w tym celu, wystarczającą podstawą prawną jest bowiem w takim przypadku przepis art. 6 ust. 1 lit. b) RODO).

Poniżej przedstawione są warunki powoływania się administratora na podstawy prawne najczęściej spotykane w przypadku podmiotów z branży internetowej.

3.4. Niezbędność przetwarzania danych osobowych do zawarcia i wykonania umowy z podmiotem danych osobowych.

W art. 6 ust. 1 lit. b) RODO wskazane zostały dwie sytuacje związane z zawieraniem i wykonywaniem umowy, legalizujące przetwarzanie danych osobowych:

a) gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
b) gdy jest to niezbędne do wykonania umowy z podmiotem danych.

Przesłanka niezbędności przetwarzania danych osobowych w praktyce branży internetowej znajdzie zastosowanie w przypadku różnych umów *online*, zawieranych z podmiotami danych osobowych. Bez znaczenia jest przy tym, czy umowy te mają charakter odpłatny, czy nieodpłatny. Na podstawie art. 6 ust.1 lit. b) RODO mogą być przetwarzane zarówno dane przekazane przez podmiot danych, jak i dane eksploatacyjne zebrane przy okazji wykonania danej umowy.

Przesłanka niezbędności nie może - co do zasady - być podstawą przetwarzania danych w celach marketingowych, z drugiej jednak strony można się na nią powołać w przypadku, gdy przedmiotem usługi świadczonej użytkownikowi (podmiotowi danych) na jego żądanie jest przedstawianie ofert marketingowych (np. portale służące do prezentacji i porównywania towarów oferowanych przez sklepy internetowe).

3.5. Obowiązek prawny określony w przepisach prawa.

Zgodnie z art. 6 ust. 1 lit. c) RODO, przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. c) RODO jest dopuszczalne pod warunkiem łącznego spełnienia następujących przesłanek:

- gdy istnieje przepis prawa, który nakłada na administratora danych obowiązek prawny,
- gdy przetwarzanie danych jest niezbędne dla realizacji tego obowiązku prawnego.

W myśl motywu 45 Preambuły RODO:

> *Rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania.*

W świetle powyższego należy przyjąć, że dla spełnienia przesłanki z art. 6 ust.1 lit. c) RODO, nie jest konieczne, aby dany akt prawny zawierał wyraźne odniesienie do przetwarzania danych osobowych, wystarczy gdy określa on obowiązek, którego stroną jest np. dostawca usług internetowych. Przykładem takiej sytuacji mogą być przepisy podatkowe.

3.6. Zgoda jako podstawa prawna przetwarzania danych osobowych w celach marketingowych.

Jedną z dopuszczalnych podstaw prawnych przetwarzania danych osobowych w celach działań marketingowych jest zgoda podmiotu danych osobowych. Przesłanka ta w szczególności znajduje zastosowanie w przypadku, gdy administrator danych nie może oprzeć przetwarzania na przesłance uzasadnionego interesu (zob. uwagi poniżej – pkt 3.7).

Zgodnie z art. 4 pkt 11) RODO:

> *„zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;*

3.6.1. Sposób wyrażenia zgody.

W myśl art. 7 ust. 2 RODO:

> *Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.*

Z kolei, zgodnie z motywem 32 Preambuły RODO:

> *Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności (...). Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych.*

Zgodnie z konstrukcją zgody w RODO, powinna być ona wyrażona w formie oświadczenia woli lub wyraźnego działania potwierdzającego.

Oświadczenie woli może być wyrażone w dowolnej formie, w tym formie elektronicznej, np. poprzez zaznaczenie okienek wyboru na stronie internetowej, czy przesłanie oświadczenia o wyrażeniu zgody drogą elektroniczną (np. e-mailem). Oświadczenie o wyrażeniu zgody musi być odrębne od innych oświadczeń, a przed wyrażeniem zgody osoba ją wyrażająca musi mieć możliwość zapoznania się z informacjami dotyczącymi przetwarzania danych osobowych (obowiązek informacyjny – zob. pkt IV Kodeksu).

Zgodnie z powołanym przepisem art. 7 ust. 2 RODO samo zapytanie o zgodę lub oświadczenie o jej wyrażeniu powinno być czynnością odseparowaną, samodzielną od innych oświadczeń, umów lub regulaminu świadczenia usług. Jeżeli zatem na stronie internetowej, poza klauzulą zgody, znajdują się także inne *checkboxy* lub regulamin świadczenia usługi, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od innych zagadnień, tak by zgoda mogła być udzielona niezależnie.

Przy ocenie skuteczności wyrażenia zgody należy wziąć pod uwagę treść motywu 32 Preambuły RODO, zgodnie z którym:

> *Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody.*

Mając na uwadze powyższe, za niedozwoloną praktykę należy uznać stosowanie domyślnie zaznaczanych *checkboxów*. Użytkownik samodzielnie powinien kliknąć w okienko zgody (*opt-in*) w odpowiednim *checkboxie*, aby zgoda w postaci oświadczenia woli była skutecznie udzielona. Z drugiej jednak strony, nie ma przeszkód, aby stosować dodatkowy *checkbox* pod kilkoma zgodami np.: "[_] *Zaznacz wszystkie powyższe*."

Równolegle z możliwością udzielenia zgody poprzez złożenie oświadczenia woli, w przepisach RODO przewidziano również możliwość przyjęcia, że zgoda została skutecznie udzielona w razie podjęcia przez osobę, której dane dotyczą, różnego rodzaju działań potwierdzających w danym kontekście, że osoba ta zaakceptowała proponowane przetwarzanie jej danych osobowych (konkludentna zgoda). Takim zachowaniem może być przykładowo podanie danych opcjonalnych w formularzu służącym do rejestracji w serwisie lub też uzupełnienie swojego profilu utworzonego w serwisie społecznościowym o dodatkowe informacje (np. dodawanie zdjęcia, opisu zainteresowań itp. w celu jego uatrakcyjnienia). Użytkownik powinien być przy tym poinformowany, że dodanie/wpisanie danych stanowi jego zgodę na ich przetwarzanie oraz powinien być poinformowany o możliwości wycofania zgody. Informacja ta może zostać przekazana np. w formie komunikatu pojawiającego się w momencie najechania kursorem na pole, które należy wypełnić. Do innych występujących w branży internetowej przykładów skutecznego wyrażenia zgody zaliczyć należy: przesunięcie palca po ekranie, zamknięcie bannera informacyjnego lub okienka *pop-up* poprzez naciśnięcie narożnego znaku zamykania okien "x", naciśnięcie przycisku "rozumiem"/ "zgoda", *scrollowanie* strony, machnięcie przed „inteligentną kamerą", obrócenie *smartfona* zgodnie z ruchem wskazówek zegara, o ile równocześnie spełniony jest obowiązek informacyjny (zob. pkt IV Kodeksu), a podmiot danych ma świadomość, że np. dany ruch oznacza zgodę w odpowiedzi na konkretne zapytanie („jeżeli przesuniesz ten pasek w lewo, zgadzasz się na wykorzystanie informacji X w celu Y", „powtórz ruch w celu potwierdzenia" etc.).

3.6.2. Dobrowolność zgody.

W myśl RODO zgoda na przetwarzanie danych musi być dobrowolna. Ta zasada została szerzej opisana w art. 7 ust. 4 RODO:

> *Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.*

Podobnie, w myśl motywu 43 Preambuły RODO:

> *Zgody nie uważa się za dobrowolną, (…) jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.*

Mając na uwadze powyższe, niezbędne jest zapewnienie możliwości niewyrażenia zgody (np. zgody na przetwarzanie danych osobowych w celu marketingowym lub na udostępnienie danych), przy jednoczesnym zapewnieniu świadczenia usługi osobie, która takiej zgody nie chce wyrazić. Ten wymóg może przykładowo oznaczać konieczność zapewnienia osobie, której dane dotyczą, wyboru pomiędzy skorzystaniem z bezpłatnej usługi świadczonej drogą elektroniczną, przy jednoczesnym wyrażeniu zgody na przetwarzanie lub udostępnienie danych np. w celach marketingowych albo świadczeniem jej usługi w wersji odpłatnej, bez konieczności wyrażania zgody na cele marketingowe.

3.6.3. Zgoda na kilka celów przetwarzania danych osobowych.

W myśl motywu 32 Preambuły RODO:

> *Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.*

Co więcej, motyw 42 Preambuły RODO mówi:

> *"aby wyrażenie zgody było świadome, osoba której dane dotyczą, powinna znać przynajmniej tożsamość administratora."*

W świetle powyższych przepisów, za dopuszczalne należy uznać zebranie zgody w jednym oświadczeniu na przetwarzanie danych osobowych przez szereg podmiotów, pod warunkiem że każdy z tych podmiotów będzie przetwarzał dane osobowe w tym samym celu (np. celu marketingowym).

Podkreślenia wymaga, że w praktyce reklamy internetowej (np. przy zbieraniu danych osobowych za pomocą plików *cookies*) wymienienie wszystkich podmiotów, które będą przetwarzały dane osobowe na podstawie zgody – w przypadku wyboru tej przesłanki jako podstawy prawnej przetwarzania - może nastręczać licznych trudności, z jednej strony z uwagi na konieczność oznaczenia bardzo dużej liczby tych podmiotów, a drugiej strony z uwagi na częsty brak możliwości przewidzenia *a priori,* jakie podmioty będą przetwarzać dane osobowe na tej podstawie (np. reklamodawcy). Rozwiązaniem tych trudności może być **ujęcie wyrażenia zgody w dwóch warstwach, a także odpowiednie określenie odbiorców danych.** W warstwie podstawowej, dostępnej bezpośrednio np. na stronie internetowej, wystarczające jest sformułowanie zgody poprzez określenie kategorii podmiotów, które będą przetwarzały dane osobowe na podstawie zgody (np. "zaufani partnerzy"), natomiast w warstwie szczegółowej następuje szczegółowe wymienienie podmiotów, które będą przetwarzały dane osobowe na podstawie zgody, a w zakresie, w jakim brak jest możliwości oznaczenia tych podmiotów – podawana jest informacja o „kategorii odbiorców danych".

3.6.4. Prawo do wycofania zgody.

Zgodnie z art. 7 ust. 3 RODO:

> *Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.*

Ponadto, zgodnie z motywem 42 Preambuły RODO:

> *Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.*

Wycofanie zgody musi być równie łatwe, jak jej udzielenie (nie jest jednak konieczne zapewnienie identyczności sposobu udzielenia i wycofania zgody). Niedozwolone są praktyki utrudniania podmiotom danych składania oświadczeń o wycofaniu zgody. Zalecane jest udostępnienie w klauzuli informacyjnej, polityce prywatności lub w stopce maila: linku, formularza lub adresu mailowego umożliwiającego zgłoszenie prośby o wycofanie zgody. Administrator danych może wskazać

konkretny kanał do wycofywania zgód – np. wycofywanie zgody tylko przez wiadomość na podany adres. Istotne jest zapewnienie przez administratora rzeczywistej odwoływalności zgody, co w przypadku skorzystania z tego prawa przez podmiot danych ma w konsekwencji doprowadzić do zaprzestania przetwarzania danych przez administratora w celu objętym zgodą. W niektórych przypadkach wycofanie zgody może oznaczać zaoferowanie osobie, której dane dotyczą, świadczenia usługi w formie odpłatnej lub bez rabatu związanego z wyrażeniem zgody na przetwarzanie danych w celach marketingowych.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, musi być jednak o tym informowana, zanim wyrazi zgodę (np. w klauzuli zgody lub w klauzuli informacyjnej). Skutkiem odwołania zgody jest brak możliwości przetwarzania danych osobowych na podstawie zgody w przyszłości, chyba że osoba ta ponownie udzieli zgody.

3.7. Prawnie uzasadniony interes administratora jako podstawa prawna przetwarzania danych osobowych.

Ważną podstawą prawną przetwarzania danych osobowych jest tzw. uzasadniony interes administratora danych lub strony trzeciej (art. 6 ust. 1 lit. f) RODO):

> *przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.*

Prawnie uzasadniony interes administratora danych lub strony trzeciej będący podstawą przetwarzania danych osobowych należy rozumieć w sposób szeroki, gdyż w praktyce obejmuje on interesy gospodarcze, faktyczne oraz prawne. W branży reklamy internetowej szczególne znaczenie ma stosowanie tej przesłanki w przypadku prowadzenia działań marketingowych, w tym profilowania. Możliwość taką podkreślono w motywie 47 Preambuły RODO *in fine*:

> *Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego.*

Oparcie przetwarzania danych osobowych na przepisie art. 6 ust. 1 lit. f) RODO wymaga przeprowadzenia tzw. testu równowagi. Wymaga on z jednej strony weryfikacji przyjęcia, że

administrator danych ma **rzeczywiście uzasadniony interes** w przetwarzaniu danych osobowych np. na cele marketingowe, a drugiej strony **wpływu tego przetwarzania na podmiot danych osobowych** (zob. pkt 3.7.1 oraz 3.7.2 poniżej).

Warunkiem dopuszczalności przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu jest uznanie, w wyniku przeprowadzenia testu równowagi, że **interes administratora danych w przetwarzaniu danych osobowych jest co najmniej równoważny wobec praw, wolności i interesów podmiotów danych osobowych.**

3.7.1. Uzasadniony interes administratora danych.

Przy ocenie, czy zachodzi uzasadniony interes administratora danych, należy między innymi wziąć pod uwagę następujące kryteria:

- czy interes jest zgodny z prawem?
- czy jest wystarczająco konkretny, aby możliwe było przeprowadzenie testu równowagi?
- czy jest to rzeczywisty i aktualnie istniejący interes (tj. nie jest spekulatywny)?
- czy istnieją inne, mniej inwazyjne środki do osiągnięcia określonego celu przetwarzania oraz służące interesowi administratora danych, tj. środki niewymagające przetwarzania danych osobowych?

3.7.2. Wpływ przetwarzania na podmiot danych.

Istotną okolicznością, którą należy brać pod uwagę przy ocenie, czy istnieje uzasadniony interes administratora, nad którym nie przeważają prawa i wolności osoby, której dane dotyczą, jest odpowiedni rodzaj powiązania między osobą, której dane dotyczą a administratorem (np. łącząca ich umowa lub świadczona przez administratora usługa). W myśl motywu 47 Preambuły RODO:

> *Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania.*

Ocena, czy podmiot danych ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w określonym celu, ma znaczenie w szczególności przy działaniach z zakresu marketingu bezpośredniego. Ocenę tę należy prowadzić w sposób zobiektywizowany. Jeżeli zatem użytkownik skorzysta z określonej usługi, to może liczyć się z tym, że po jej zrealizowaniu zaczną się w serwisach internetowych wyświetlać przeznaczone dla niego propozycje innych podobnych usług/produktów, które będą dopasowane do usług/produktów poprzednio przez niego zamówionych (np. po obejrzeniu określonych filmów w serwisie VOD użytkownik może być namawiany do zakupu kolejnych filmów z tego serwisu o podobnej tematyce). Tak samo klienci sklepów internetowych mogą się spodziewać, że przedsiębiorca będzie chciał zaproponować im kolejne zakupy na podstawie historii ich zakupów. Co więcej, dopasowywanie treści serwisu internetowego do użytkownika także może być oparte o przesłankę uzasadnionego interesu administratora.

Niezależnie od wyżej określonego kryterium, przy ocenie wpływu przetwarzania na podmiot danych osobowych warto jeszcze wziąć pod uwagę następujące kryteria:

- w jaki sposób dane osobowe będą przetwarzane?
- racjonalne oczekiwania osoby, której dane dotyczą – czy osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu?
- jakie są podstawowe prawa, wolności lub interesy osoby, której dane dotyczą, na które może być wywarty wpływ poprzez przetwarzanie danych? Jaki może być wpływ przetwarzania na osobę, której dane dotyczą?

3.8. Podstawy prawne wykorzystywania technologii śledzących (w tym *cookies*).

Technologia *cookies* jest powszechnie wykorzystywana do celów reklamy internetowej. Z punktu widzenia dopuszczalności jej stosowania odróżnić należy dwie sytuacje:

- podstawę prawną przetwarzania informacji zawartych w plikach *cookies*, a mających często charakter danych osobowych w rozumieniu RODO,
- podstawę prawną stosowania technologii *cookies*.

W przypadku informacji (danych osobowych) zbieranych przy pomocy *cookies* do celów reklamowych, zastosowanie znajdą wyżej omówione podstawy prawne określone w RODO, w szczególności zgoda podmiotu danych osobowych (tzw. „zgoda RODO") lub prawnie uzasadniony interes administratora danych.

W przypadku natomiast stosowania technologii *cookies* właściwe będą przepisy prawa telekomunikacyjnego (PT). Należy przy tym podkreślić, że w pewnych sytuacjach instalowanie tych

plików nie będzie wymagało zgody abonenta lub użytkownika końcowego (art.173 ust. 3 PT). Będzie tak w szczególności, gdy korzystanie z nich jest konieczne do:

- wykonania transmisji komunikatu za pośrednictwem publicznej sieci telekomunikacyjnej,
- dostarczania usługi telekomunikacyjnej lub usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego.

Powyższe wyjątki z PT dotyczą przede wszystkim takich sytuacji wykorzystania *cookies,* jak:

- pliki *cookies* z danymi wprowadzanymi przez użytkownika (identyfikator sesji) na czas trwania sesji (*user input cookies*),
- uwierzytelniające pliki *cookies* wykorzystywane do usług wymagających uwierzytelniania na czas trwania sesji (*authentication cookies*),
- pliki *cookies* służące do zapewnienia bezpieczeństwa, np. wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania (*user centric security cookies*),
- sesyjne pliki *cookies* odtwarzaczy multimedialnych (np. pliki *cookies* odtwarzacza flash), na czas trwania sesji (*multimedia player session cookies*),
- trwałe pliki *cookies* służące do personalizacji interfejsu użytkownika, na czas trwania sesji lub nieco dłużej (*user interface customization cookies*),
- pliki *cookies* służące do monitorowania ruchu na stronie internetowej, tj. analityki danych.

W przypadku wykorzystania technologii *cookies* na cele marketingowe, konieczne będzie uzyskanie zgody (tzw. "zgoda na *cookies*"). Zgoda ta powinna zostać **wyrażona w sposób określony w art. 173 ust. 2 PT** (m.in. poprzez wybór ustawień technicznych do korzystania z usług społeczeństwa informacyjnego, pod warunkiem poinformowania użytkowników o tym, w jaki sposób zebrane informacje będą następnie wykorzystywane).

Wykorzystywanie plików *cookies* (oraz podobnej technologii) oraz przetwarzanie danych osobowych zapisanych w plikach *cookies* w celach reklamowych nabiera szczególnego znaczenia w ramach modelu *programmatic*. W przypadku internetowej reklamy *programmatic cookies* ID są przetwarzane przez wydawcę, ale także przez szereg operatorów sieci reklamowych (AdExchange, podmioty DSP, SSP) zaliczanych w Kodeksie do grupy: "zaufanych partnerów". Jak zostało już wskazane, w celu zapewnienia odpowiedniej podstawy do prowadzenia działań reklamowych, niezbędne jest zapewnienie zarówno podstawy prawnej z RODO (art. 6 ust. 1), ale także z PT (art. 173).

RODO (podstawa prawna przetwarzania danych osobowych)	Prawo telekomunikacyjne (zgoda na *cookies*)
Zgoda (art. 6 ust. 1 lit. a) RODO) albo Niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f) RODO.	Zgoda na przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (art. 173 ust. 1 pkt 2) prawa telekomunikacyjnego)

Niniejszy Kodeks nie przesądza, która podstawa prawna z RODO na przetwarzanie danych osobowych zapisanych w plikach *cookies* w celach reklamowych (pierwsza kolumna) jest właściwa. Ta kwestia zależy od indywidualnego przypadku administratora danych. Do administratora należy wybór odpowiedniej podstawy prawnej: zgody lub uzasadnionego interesu administratora (powinien on w szczególności uwzględnić, czy spełnione są warunki zachowania równowagi interesów).

IV. Rozdział czwarty: Profilowanie

4.1. Dobre praktyki branżowe:

- dokonując profilowania na cele marketingowe należy poinformować o tym podmiot danych, jak również zapewnić mu realizację innych praw określonych w RODO odnośnie profilowania, w tym prawo do sprzeciwu,
- w przypadku oparcia profilowania na podstawie prawnie uzasadnionego interesu, należy szczególnie uważnie wykonać test równowagi, w szczególności pod kątem ustalenia, czy interes administratora w przetwarzaniu danych jest co najmniej równoważny wobec praw, wolności i interesów osoby, której dane dotyczą.

4.2. Istota profilowania.

Zgodnie z definicją „profilowania" zawartą w art. 4 pkt 4 RODO:

> *„profilowanie" oznacza dowolną formę 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 efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.*

W świetle powyższej definicji, należy podkreślić, że nie każde automatyczne zestawienie informacji o osobach fizycznych stanowić będzie profilowanie określone w RODO, ale tylko takie, którego celem jest ocena niektórych czynników osobowych danej osoby.

4.3. Profilowanie na cele marketingowe na podstawie RODO.

W RODO uregulowane są **dwa rodzaje profilowania**. Pierwsze z nich, do którego odnosi się art. 21, dopuszcza profilowanie tak długo, jak podmiot danych nie wyrazi na to sprzeciwu *(opt-out)*. W przypadku profilowania „marketingowego", sprzeciw ten powinien być bezwzględnie respektowany (art. 21 ust.3).

Drugi z rodzajów profilowania uregulowany został w art. 22 RODO. Zgodnie z nim, zasadą jest niedopuszczalność podejmowania automatycznych decyzji, opartych między innymi na profilowaniu, chyba że zachodzą przesłanki legalizujące określone w tym przepisie (np. zgoda podmiotu danych osobowych).

W świetle wyżej wymienionych przepisów należy stwierdzić, że w **typowych sytuacjach prowadzenie reklamy internetowej opartej na przetwarzaniu danych osobowych mieści się w zakresie określonym w art. 21 RODO,** nie ma ono bowiem charakteru wywierania „istotnego wpływu„ w rozumieniu art. 22 ust.1 RODO.

4.4. Podstawy prawne i obowiązki w przypadku profilowania na cele marketingowe.

W przypadku profilowania na potrzeby marketingowe podstawą prawną przetwarzania będzie zgoda podmiotu danych osobowych (opt-in) lub prawnie uzasadniony interes podmiotu (opt-out). Obie te podstawy prawne opisane zostały w rozdziale III Kodeksu.

W przypadku oparcia profilowania marketingowego na przesłance prawnie uzasadnionego interesu szczególnego znaczenia nabiera odpowiednie wykonanie testu równowagi w sytuacji, gdy dochodzi do skomplikowanych czynności przetwarzania, np. gdy przetwarzana jest duża ilość informacji na temat wielu osób. W trakcie dokonywania tego testu administratorzy danych powinni szczególnie zważyć kryteria uzasadnionego interesu wskazane powyżej.

V. Rozdział piąty: Obowiązek informacyjny

5.1. Dobre praktyki branżowe:

- poza wyjątkami określonymi w RODO, należy spełnić obowiązek informacyjny wobec podmiotów danych, bez konieczności złożenia odrębnego żądania w tym zakresie przez podmiot danych,
- zakres informacji przekazywanej podmiotowi danych osobowych może być podzielony na dwie warstwy – informacje przekazywane bezpośrednio („warstwa podstawowa") oraz informacje przekazywane po przekierowaniu np. do polityki prywatności administratora danych („warstwa szczegółowa").

5.2. Sposób spełnienia obowiązku informacyjnego i zakres informacji podawanych podmiotowi danych osobowych.

Obowiązek informacyjny należy wypełnić z mocy prawa, bez konieczności składania dodatkowych wniosków przez osoby, których dane są przetwarzane.

Zakres informacji przekazywanych przez administratora danych osobowych obejmuje:

- informacje opisane w art. 13 RODO, w przypadku zbierania danych bezpośrednio od osoby,
- informacje opisane w art. 14 RODO, w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą.

W przypadku branży internetowej, w typowych sytuacjach należy spełnić obowiązek informacyjny, w pewnych jednak sytuacjach spełnione mogą zostać określone w RODO przesłanki wyłączające taki obowiązek. Administrator danych osobowych zwolniony będzie od obowiązku informacyjnego w szczególności, gdy:

- osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych jest wyraźnie przewidziane prawem (w odniesieniu do obowiązku z art. 13 i 14 RODO) lub
- poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub poinformowanie wymagałoby niewspółmiernie dużego wysiłku, w szczególności w sytuacji, gdy administrator co prawda dysponuje danymi umożliwiającymi kontakt z osobą, której dane są przetwarzane, ale weryfikacja aktualności danych wymagałaby podjęcia innych czynności weryfikujących i konieczności zbierania informacji dodatkowych, lub podjęcia innych nadmiernych czynności, a osiągnięcie celu przetwarzania nie wymaga gromadzenia dodatkowych informacji lub weryfikowania ich aktualności.

Administrator danych powinien przekazywać wymagane prawem informacje w sposób zrozumiały, wykorzystując, o ile jest to możliwe, prosty i zrozumiały sposób przekazu. Dobór kanału komunikacji winien uwzględniać obowiązek wykazania wypełnienia obowiązku informacyjnego wobec osoby, której dane są przetwarzane.

Wypełnienie obowiązku informacyjnego następować powinno w sposób adekwatny do sposobu zbierania danych, tj.:

- w przypadku zbierania danych za pośrednictwem strony www – należy zamieścić stosowne informacje w bezpośrednim sąsiedztwie formularza służącego do wprowadzania danych,
- w przypadku zbierania danych za pośrednictwem komunikacji e-mail lub podobnej – należy zamieścić stosowne informacje w bezpośrednim sąsiedztwie takiego oznaczenia adresu komunikacji (adres e-mail, nr komunikatora) lub w instrukcji nawiązania komunikacji.

W obu powyższych sytuacjach dopuszczalny jest podział przekazywanych informacji na dwie „warstwy" (podstawową i szczegółową). Zalecane jest przy tym, aby administrator zapewnił, żeby:

- informacje w warstwie podstawowej były zawsze widoczne dla osoby, której dane są zbierane,
- informacje w warstwie szczegółowej były komunikowane.

Przykładowo, w przypadku komunikatów dostępnych na stronach WWW, warstwa „podstawowa" może wyglądać w sposób następujący:

Administrator danych	XYZ Sp. z o.o., Sp.k „więcej"
Cel przetwarzania danych	Świadczenie usługi elektronicznej „więcej" Marketing bezpośredni
Podstawa prawna	Wykonanie umowy „więcej" prawnie uzasadniony interes administratora danych
Odbiorcy danych	Dane będą udostępniane „zaufanym partnerom"
Twoje prawa	Prawo dostępu, poprawiania lub żądania usunięcia danych, a także inne prawa których opis znajduje się „tutaj" (gdzie tutaj jest łączem alfanumerycznym)
Informacje dodatkowe	Więcej informacji o przetwarzaniu danych znajduje się w zakładce „Prywatność" dostępnej pod adresem www.abc.pl

Przekazanie informacji w warstwie „szczegółowej" może mieć charakter wskazany powyżej (*link*), a w przypadku innych – niż poprzez stronę internetową – form komunikacji, może się odbywać w następujący sposób:

- w formie wiadomości *e-mail* przesyłanej osobie, której dane są zbierane, przygotowane do pobrania pod unikalnym adresem URL,
- w formie komunikatu na stronie www dostępnego tylko dla osoby, której dane są zbierane (zakładka prywatność np. w panelu konta użytkownika),
- w formie komunikacji telefonicznej, informacja powinna być przesłana na adres e-mail podany podczas rozmowy telefonicznej niezwłocznie po jej zakończeniu.

VI. Rozdział szósty: Realizacja praw podmiotów danych osobowych

6.1. Dobre praktyki branżowe.

- w przypadku gdy administrator danych nie może zrealizować żądania podmiotów danych z uwagi na braku możliwości identyfikacji, powinien ich o tym – o ile jest to możliwe – poinformować,
- administrator danych powinien opracować procedurę realizacji praw podmiotów danych oraz – co najmniej – uruchomić adres elektroniczny, na który mogą być kierowane żądania przez te podmioty,
- administrator danych jest zobowiązany do weryfikacji tożsamości podmiotów danych i w tym celu może m.in. żądać złożenia przez nie odpowiednich oświadczeń,
- w określonych sytuacjach, administrator danych może zwrócić się do wnioskodawcy z wezwaniem o uzupełnienie wniosku, wraz z informacją, że jego nieuzupełnienie spowoduje odmowne rozpatrzenie wniosku (np. w sytuacji, gdy wniosek jest niejasny),
- realizując żądanie podmiotów danych, administrator powinien mieć na celu ochronę interesów podmiotów danych (np. w zakresie zabezpieczenia przekazywanych danych).

6.2. Wyjątki od obowiązku realizacji żądań osób, których dane dotyczą.

Większość podmiotów z branży internetowej zbiera i przetwarza informacje o charakterze identyfikatorów internetowych, np. identyfikatory plików *cookies,* a celem przetwarzania tych informacji nie jest bezpośrednia identyfikacja osoby fizycznej.

W powyższym kontekście należy wskazać na uregulowanie art. 11 ust. 1 RODO, zgodnie z którym jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, **administrator nie ma obowiązku**

zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO. Jeżeli więc administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, to nie znajdują do niego zastosowania przepisy art. 15–20 RODO, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować. Administrator, w miarę możliwości, powinien poinformować podmiot danych o braku możliwości identyfikacji.

6.3. Procedura realizacji żądań osób których dane dotyczą.

Zalecany sposób realizacji praw podmiotów danych opisać można w pięciu, następujących po sobie, krokach.

1) Krok pierwszy - stwórz procedurę oraz udostępnij adres poczty lub formularz elektroniczny do zgłaszania żądań.

Procedura realizacji praw podmiotów danych powinna określać zasady postępowania dotyczące rozpatrywania następujących rodzajów żądań podmiotów w zakresie realizacji ich uprawnień:

a) prawa dostępu do informacji, w tym prawa do kopii danych (art. 15),
b) prawa do sprostowania danych (art. 16),
c) prawa usunięcia danych osobowych (art. 17),
d) prawa do ograniczenia przetwarzania (art. 18),
e) prawa do przenoszenia danych (art. 20),
f) prawa do sprzeciwu (art. 21),
g) prawa do niepodlegania automatycznym rozstrzygnięciom indywidualnym (art. 22).

Procedura powinna zawierać co najmniej takie elementy, jak: zasady i tryb przyjmowania żądań (wniosków) podmiotów danych, termin i sposób ich rozpatrzenia, a także zasady postępowania w przypadku pozytywnego i negatywnego rozpoznania wniosku.

Administrator jest zobowiązany określić, w jaki sposób (sposoby) podmiot danych może złożyć wniosek. W przypadku firm z branży internetowej rekomendowane jest, aby co najmniej udostępnić w tym celu adres poczty elektronicznej, a także – w miarę możliwości – formularz elektroniczny dostępny na stronie internetowej.

2) Krok drugi – ustal swoją rolę: czy jesteś dla operacji na danych, których dotyczy żądanie, podmiotem przetwarzającym czy administratorem lub ewentualnie współadministratorem.

Jeżeli z analizy wynika, że podmiot, do którego skierowano wniosek, jest podmiotem przetwarzającym, niezbędne jest przekazanie tego żądania do właściwego administratora lub, jeżeli to przewiduje umowa z administratorem, rozpoznanie żądania zgodnie z instrukcjami administratora.

3) Krok trzeci – sprawdź, czy w danym stanie faktycznym stosuje się wyjątek od obowiązku realizacji żądania osoby, której dane dotyczą.

Administrator danych nie jest zobowiązany do realizacji praw podmiotów danych w sytuacji określonej w art. 11 ust. 1 (zob. wyjaśnienia – pkt 6.2 Kodeksu).

4) Krok czwarty – zweryfikuj tożsamość podmiotu danych.

Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO). Administratorzy mogą w szczególności domagać się od wnioskodawców, aby złożyli oświadczenie, że są jedynymi posiadaczami oraz użytkownikami przeglądarki lub urządzenia mobilnego, przy pomocy których przetwarzane były dane objęte żądaniem.

5) Krok piąty– zrealizuj żądanie użytkownika lub odmów realizacji, jeżeli istnieją do tego podstawy.

Rozpatrzenie wniosku następuje w terminie 30 dni od dnia otrzymania wniosku, co oznacza, że w tym terminie powinna zostać wysłana do wnioskodawcy informacja o sposobie rozpoznania wniosku. W razie potrzeby termin można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim przypadku informację o przedłużeniu terminu należy przekazać w ciągu 30 dni od otrzymania żądania, powiadamiając o tym wnioskodawcę z podaniem przyczyn opóźnienia.

Administrator danych może zwrócić się do wnioskodawcy z wezwaniem o uzupełnienie wniosku, wraz z informacją, że jego nieuzupełnienie spowoduje odmowne rozpatrzenie wniosku, w sytuacjach gdy:

a) podane we wniosku informacje nie umożliwiają przesłania odpowiedzi oraz kopii danych osobowych,
b) wniosek jest niejasny lub niezrozumiały,
c) wniosek dotyczy przekazania kopii danych lub przeniesienia danych, ale wnioskodawca nie określił zakresu danych do skopiowania lub przeniesienia,
d) wniosek dotyczy przeniesienia danych, ale wnioskodawca zażądał użycia formatu danych lub technologii, które nie są stosowane przez danego administratora,

e) wniosek dotyczy przeniesienia danych, ale wnioskodawca nie podał nazwy i adresu innego administratora lub podał błędny adres lub nazwę administratora, do którego zażądał przeniesienia danych.

W wezwaniu powinien zostać określony termin, w którym wnioskodawca powinien uzupełnić wniosek.

Administrator może negatywnie rozpatrzyć wniosek w sytuacji, gdy:

a) wniosek jest nieuzasadniony, w szczególności, gdy pozytywne załatwienie wniosku jest prawnie niedopuszczalne lub niewymagane,
b) wniosek jest nadmiarowy, w szczególności gdy jest składany ustawicznie, co oznacza wniosek składany częściej niż raz na 2 miesiące w tej samej kategorii sprawy,
c) brak możliwości technologicznych zrealizowania wniosku np. w sytuacji wniosku o przeniesienie danych,
d) wniosek nie został w terminie uzupełniony przez wnioskodawcę o informacje, pomimo wezwania wysłanego do wnioskodawcy.

W przypadku negatywnego rozpatrzenia wniosku skierowana do wnioskodawcy informacja powinna zawierać uzasadnienie negatywnej decyzji oraz pouczenie o możliwości wniesienia przez wnioskodawcę skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

W sytuacji pozytywnego rozpatrzenia wniosku podejmowane przez administratora działania powinny mieć na celu ochronię interesów podmiotów danych, np. w przypadku przekazywania kopii danych osobowych lub przeniesienia danych powinny być one dodatkowo zabezpieczane w zależności od formy ich przesyłania.

VII. Rozdział siódmy: Przystąpienie do Kodeksu i jego stosowanie

7.1. Postanowienia ogólne

Kodeks jest kodeksem postępowania, o którym mowa w art. 40 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) i został zatwierdzony w dn. _____ przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO).

Kodeks stanowi również kodeks dobrych praktyk w rozumieniu art. 2 pkt 5) ustawy z dn. 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym.

Kodeks posiada charakter komplementarny w stosunku do przepisów obowiązującego na terytorium Rzeczpospolitej Polskiej prawa.

Wykładnia, bieżący nadzór nad przestrzeganiem, orzekanie w sprawach stwierdzonych naruszeń oraz zmiany Kodeksu należą do wyłącznej kompetencji IAB Polska.

IAB Polska może wnioskować do PUODO o przedstawienie wyjaśnień dotyczących kwestii związanych z ochroną danych osobowych.

7.2. Przystąpienie do Kodeksu

Przystąpienie do Kodeksu jest dobrowolne. Każdy przedsiębiorca działający na terytorium Rzeczpospolitej Polskiej, będący członkiem IAB Polska, może przystąpić do Kodeksu, zobowiązując się w ten sposób do jego przestrzegania.

Aby przystąpić do Kodeksu, należy złożyć do IAB Polska oświadczenie o przystąpieniu do Kodeksu stanowiące załącznik nr … Oświadczenie powinno być podpisane zgodnie z zasadami reprezentacji podmiotu przystępującego.

Przystąpienie następuje z momentem doręczenia IAB Polska podpisanego oświadczenia o przystąpieniu.
Od momentu przystąpienia do Kodeksu, podmiot przystępujący zobowiązany jest do jego przestrzegania.

7.3. Zmiana Kodeksu

Zmiana Kodeksu następuje w drodze uchwały Zarządu IAB Polska. Zmiana poprzedzona będzie konsultacjami, prowadzonymi z udziałem _____.
Informacja o zmianie Kodeksu zostanie podana do wiadomości na stronie internetowej IAB Polska. Dodatkowo, IAB Polska powiadomi wszystkie podmioty, które przystąpiły do Kodeksu, o jego zmianie.
Zmiana wchodzi w życie nie wcześniej niż po upływie 14 dni od dnia podjęcia uchwały o zmianie, pod warunkiem jej zatwierdzenia przez Prezesa Urzędu Ochrony Danych Osobowych.

7.4. Wykluczenie z Kodeksu

Każdy podmiot, który przystąpił do Kodeksu, może powiadomić IAB Polska o podejrzeniu naruszenia postanowień Kodeksu przez inny podmiot.
W razie uzyskania informacji o nieprzestrzeganiu Kodeksu przez podmiot, który do niego przystąpił, IAB Polska, w drodze pisemnego wezwania, wyznaczy mu odpowiedni termin na usunięcie naruszenia, nie dłuższy jednak niż 14 dni.
W razie nieusunięcia naruszenia w przepisanym terminie, IAB Polska może, niezależnie od działań podmiotu monitorującego, podjąć uchwałę o zawieszeniu lub wykluczeniu takiego podmiotu z Kodeksu. Uchwała zostanie doręczona przesyłką pocztową na adres rejestrowy wykluczonego podmiotu.

7.5. Zawiadamianie o problemach z ochroną danych osobowych

Każdy podmiot, który przystąpił do Kodeksu, może zawiadomić IAB Polska o:

a) problemach w interpretacji postanowień Kodeksu,
b) zidentyfikowanych istotnych kwestiach związanych z ochroną danych osobowych, które powinny zostać uregulowane w Kodeksie,
c) zagadnieniach, w których IAB Polska, jako autor Kodeksu, powinno zająć stanowisko,
d) ……

Zawiadomienia mogą być składane drogą mailową na adres: _____poprzez formularz zgłoszeniowy dostępny na stronie internetowej _____.

7.6. Podmiot monitorujący

Podmiotem monitorującym Kodeks w rozumieniu art. 41 ust.1 RODO jest _____.