Wstęp

Realizacja praw osób fizycznych stanowi coraz częściej pojawiające się wyzwanie w działalności podmiotów publicznych. Zwiększająca się świadomość prawna mieszkańców powoduje, że chętniej korzystają oni z przysługujących im na podstawie RODO uprawnień. Szczególnie istotnym jest więc, aby każdy pracownik potrafił rozpoznać żądanie realizacji praw, a także potrafił zareagować na nie w odpowiedni sposób.

Kolejną ważną sprawą jest świadome kształtowanie procesów przetwarzania danych osobowych w taki sposób, aby ochrona danych osobowych stanowiła jedno z kluczowych zagadnień na każdym etapie konstruowania nowych czynności przetwarzania danych.

Wreszcie, obecnym na co dzień problemem bywa ustalenie zakresu danych osobowych, do których są Państwo uprawnieni.

Odpowiedź na wskazane powyżej zagadnienia stanowić będą przedmiot tego szkolenia.

Privacy by design i *privacy by default*

Są to pojęcia wprowadzone przez RODO i oznaczają one kolejno – prywatność w fazie projektowania i prywatność domyślną. Jak to działa w praktyce?

Privacy by design to ochrona prywatności w fazie projektowania. Stosowanie się do tej zasady oznacza przewidywanie i wdrażanie środków ochrony danych osobowych na każdym etapie tworzenia procesu, począwszy od samego pomysłu.

Czym jest *privacy by design*? Tworząc nowe procesy przetwarzania danych, a więc mając pomysł na wprowadzenie rozwiązania, projektujemy je, nadajemy im ramy. Z punktu widzenia ochrony danych istotne jest, aby nie zapomnieć o konieczności ochrony tych danych już na tym etapie. Przewidywanie tego, w jaki sposób działać będzie nowy proces, a więc w jaki sposób dane będą gromadzone, w jakim zakresie, jak będą przechowywane, itp., pozwala na wcześniejsze wdrożenie odpowiednich rozwiązań, a to z kolei przełożyć się może na ich skuteczność, jak również oszczędność w przypadku ich aktualizacji.

Przykład

Dla przykładu, tworząc aplikację mobilną – powiedzmy – informator gminny, powinniśmy być świadomi tego, że będą w niej przetwarzane dane osobowe. Jakie? To już zależy od konkretnych ustawień, ale mogą być to choćby imię, nazwisko, adres e-mail czy lokalizacja. Prywatność w fazie projektowania oznacza, że zaplanowane zostaną środki zabezpieczeń, które – następnie wdrożone – zapewnią bezpieczeństwo tych danych.

Privacy by default to domyślna ochrona prywatności. Stosowanie się do tej zasady oznacza stosowanie takich rozwiązań, które automatycznie chronią prywatność osoby fizycznej, którą osoba ta może ograniczyć poprzez dobrowolne i świadome działanie.

Przejdźmy do *privacy by default* (prywatności domyślnej). Prywatność domyślna stanowi, że automatyczne ustawienia powinny zapewniać prywatność osobom, które korzystają z danego rozwiązania. Nie chodzi tu o ustawienia sztywne, które nie podlegają zmianie. Jeżeli osoba ta zechce ograniczyć z jakichś względów ochronę swojej prywatności, może ona tego dokonać. Musi to jednak nastąpić poprzez świadome i dobrowolne działanie z jej strony. W przeciwnym razie nie można mówić o prywatności domyślnej.

Przykład

Wracając do wcześniejszego przykładu: nasza aplikacja wymaga podania adresu e-mail oraz imienia i nazwiska – te dane są danymi wymaganymi do korzystania z aplikacji. Jest ona jednak wyposażona również w inne funkcje, jak choćby pobieranie danych o lokalizacji. Przesyłanie takich informacji może usprawnić działanie aplikacji, ale wiąże się z osłabieniem prywatności przez udzielenie informacji o tym, gdzie aktualnie znajduje się użytkownik.

Prywatność domyślna polega na tym, że domyślne ustawienia aplikacji nie pozwalają na zbieranie danych w szerszym zakresie niż niezbędny do działania, a więc ograniczając się jedynie do tych wymaganych. Nie oznacza to oczywiście, że aplikacja nie może uzyskać informacji o lokalizacji użytkownika. Jest to możliwe w przypadku wyrażenia na to zgody przez tego użytkownika, który działając dobrowolnie i świadomie rezygnuje z części zagwarantowanej mu automatycznie ochrony prywatności.

Oczywiście raz ustalone i wdrożone środki nie stanowią ostatecznego załatwienia sprawy. Nie wolno zapominać o tym, aby utrzymać dane rozwiązanie, jak przykładowa aplikacja, w stanie zapewniającym ochronę przez dalszy czas jej istnienia, ponieważ zabezpieczenia powinny być aktualizowane pod kątem nowych potrzeb.

Należy poruszyć jeszcze jedną kwestię, która dotyka administrację publiczną. Chodzi o zamówienia publiczne. Stosowanie się do reguł *privacy by design* i *privacy by default* pociąga za sobą konieczność uwzględniania tychże w specyfikacji istotnych warunków zamówienia. Należy bowiem przyjąć, że ochrona danych osobowych – także w przypadku zamówień, w ramach których będą one przetwarzane – stanowi pewien standard, a nie wartość dodatkową.

Ustalanie zakresu danych osobowych

Niejednokrotnie problematyczną kwestią wydaje się być ustalenie zakresu danych osobowych, jakie mogą być pozyskane, a następnie przetwarzane w inny sposób. Z zagadnieniem tym wiąże się pojęcie minimalizacji danych osobowych.

Wyrażona w RODO zasada minimalizacji danych osobowych oznacza, że uzyskując dane powinniśmy kierować się tym, czy rzeczywiście są one nam niezbędne. To zaś, czy są one niezbędne, jest zależne od celu, w jakim mają być one uzyskane.

Przykład

Jeżeli do realizacji celu, np. przeprowadzenia postępowania administracyjnego, przepisy wymagają podania jedynie imienia i nazwiska, to niepotrzebne będzie pozyskanie adresu e-mail czy numeru telefonu. W takim zakresie będą one nadmiarowe.

Jeżeli jednak dane te, tj. e-mail lub numer telefonu, będą one zebrane w jakimś innym celu, jak choćby przyśpieszenie załatwienia sprawy przez usprawnienie komunikacji, to również mogą one podlegać przetwarzaniu, jednakże będzie się to odbywać na innej podstawie przetwarzania (np. zgodzie).

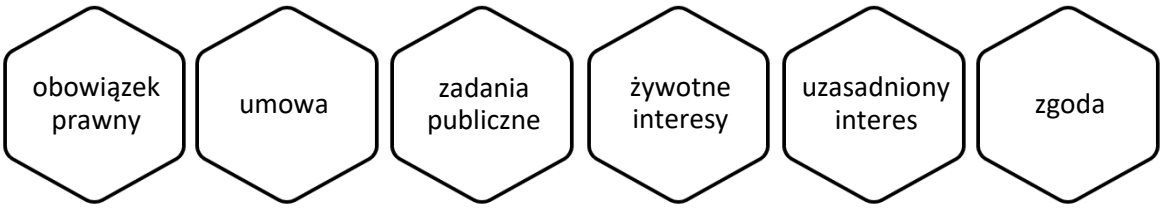
Ważne jest jednak, aby od początku było wiadomo, jakie dane są przetwarzane w jakim celu i aby były one niezbędne dla realizacji tego celu.

Zakres danych jest ściśle powiązany z podstawami przetwarzania.

Dla przypomnienia, zgodnie z RODO, podstawą przetwarzania danych zwykłych może być:

- zgoda (art. 6 ust. 1 lit. a RODO),
- umowa (art. 6 ust. 1 lit. b RODO),
- obowiązek prawny (art. 6 ust. 1 lit. c RODO),
- żywotne interesy (art. 6 ust. 1 lit. d RODO),
- zadania publiczne (art. 6 ust. 1 lit. e RODO),
- uzasadniony interes (art. 6 ust. 1 lit. f RODO).

Powyższa kolejność przedstawiona w RODO nie pokrywa się jednak z kolejnością, którą należy kierować się w praktyce. Szukając podstawy do przetwarzania powinno się stosować do następującej kolejności:



Powody, dla których zgoda powinna być zawsze na końcu owych poszukiwań podstawy przetwarzania, zostaną przedstawione w dalszej części szkolenia (możliwość cofnięcia zgody i skutki tego działania).

Ustalając podstawę przetwarzania danych, w pierwszej kolejności szukamy przepisu prawnego, z którego wynika obowiązek prawny wykonania jakiegoś działania, do którego konieczne jest przetwarzanie danych osobowych. Przepisy mogą określać jednoznacznie jaki zakres danych może zostać pozyskany dla realizacji celu.

Za przykład przepisów stanowiących podstawę przetwarzania posłużyć mogą przepisy:

- art. 22^1 Kodeksu pracy
- art. 150 Prawa oświatowego
- art. 6m ustawy o utrzymaniu czystości i porządku w gminach

Jeżeli nie istnieje przepis prawa, który mógłby stanowić podstawę przetwarzania, należy ustalić, czy dane osobowe nie będą przetwarzane na podstawie zawartej umowy lub w ramach działań zmierzających do jej zawarcia.

Kolejną potencjalną podstawą przetwarzania może być wykonywanie zadania w interesie publicznym lub w ramach powierzonej administratorowi władzy publicznej. W dużym uproszczeniu, działania podejmowane na tej podstawie obejmować będą ten obszar działalności podmiotów publicznych, który nie znajduje swojej bezpośredniej podstawy w przepisach obowiązującego prawa. Tytułem przykładu, opierać się na tej podstawie będą – zgodnie z wydanym przez MEN i UODO poradnikiem – cele oświatowe, wymienione w ustawie z dnia 14 grudnia 2016 r. – Prawo oświatowe, czy niewymienione wprost w ustawie z dnia 8 marca 1990 r. o samorządzie gminnym.

W braku powyższych przesłanek, podstawą przetwarzania może być żywotny interes osoby, której dane dotyczą, lub innej osoby. Żywotnym interesem może być np. przetwarzanie danych osób, które uległy wypadkowi, a które umożliwią ustalenie ich tożsamości i skontaktowanie się z bliskimi im osobami. Przesłanka ta znajdzie swoje zastosowanie w szczególności w sytuacjach awaryjnych, kryzysowych, wypadków i innych wymagających szybkiej interwencji.

Następną w kolejności szukania przesłanką jest prawnie uzasadniony interes administratora. W przypadku podmiotów publicznych należy jednak pamiętać, że RODO wyłącza co do zasady zastosowanie tej przesłanki do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Przykładem prawnie uzasadnionego interesu administratora będącego podmiotem publicznym może być ustalanie, dochodzenie lub obrona roszczeń, do których konieczne jest przetwarzanie danych osobowych.

Dopiero gdy stwierdzimy brak powyższych przesłanek, możemy odwołać się do zgody osoby, której dane dotyczą. Wbrew kolejności wskazanej w RODO, jak również panującemu przeświadczeniu, zgoda nie jest najbardziej uniwersalną podstawą przetwarzania, a wręcz nie powinna być ona odbierana, gdy zastosowanie mogą znaleźć pozostałe wskazane wyżej przesłanki. Jakie są tego powody?

Zgoda może być cofnięta w dowolnym momencie, a wiele działań w administracji publicznej wymaga choćby przechowywania dokumentacji przez określony czas. W takich wypadkach nie będzie więc możliwe pogodzenie tych dwóch kwestii, w związku z czym zgoda nie może być skutecznie cofnięta. Z tego względu należy uznać, że odebranie zgody na przetwarzanie danych osobowych w sytuacji, gdy dysponujemy inną podstawą przetwarzania, jest zbędne i może wprowadzać w błąd osobę, której dane dotyczą.

Przykład

Pracująca w ośrodku pomocy społecznej Janina Kowalska odebrała zgodę na przetwarzanie danych osobowych w celu przeprowadzenia postępowania o ustalenie prawa do świadczenia rodzinnego. Jakie skutki wywoła cofnięcie zgody przez stronę postępowania?

Cofnięcie zgody będzie w tym przypadku nieskuteczne w odniesieniu do danych niezbędnych do przeprowadzenia postępowania (są one przetwarzane na podstawie obowiązku prawnego), a skuteczne w odniesieniu do danych dodatkowych, tj. takich, które nie są niezbędne do przeprowadzenia postępowania (np. numeru telefonu przetwarzanego na podstawie zgody).

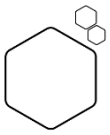
Skuteczne cofnięcie zgody nastąpi w odniesieniu do tych danych, które przetwarzane były na podstawie zgody osoby (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO w odniesieniu do danych „wrażliwych"). Należy pamiętać, że niezależnie od cofnięcia zgody, ośrodek pomocy społecznej związany jest przepisami prawa będącymi źródłem obowiązku prawnego, np. nakładającymi obowiązek przechowywania dokumentacji przez określony czas. Z tych powodów odebranie zgody na przetwarzanie danych osobowych jest nieprawidłowe, ponieważ dane są w tym przypadku przetwarzane na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c RODO). Podstawa ta może być jednak zastosowana do danych dodatkowych.

Poza przepisami prawa, wskazówką w ustalaniu zakresu danych mogą być również wzory dokumentów, zarówno wewnętrzne jak i zewnętrzne. Należy jednak pamiętać o tym, że mogą one nie być dostosowane do RODO, przez co określony w nich zakres może wykraczać poza ten minimalny.

Często wykorzystywanymi wzorami dokumentów są te utworzone w ramach podmiotu wiele lat temu, a więc opierającymi się na przepisach ustawy z dnia 27 sierpnia 1997 r. o ochronie danych osobowych. Wzór taki z pewnością powinien zostać prześwietlony pod kątem aktualności i zgodności z nowymi zasadami ochrony danych osobowych oraz zmodyfikowany, gdy zaistnieje taka potrzeba.

Z odwołaniem do ustawy z dnia 27 sierpnia 1997 r. spotkać się można również we wzorach określonych rozporządzeniami, które wciąż oczekują na dostosowanie ich do obecnych regulacji.

W najprostszych słowach, zasada minimalizacji oznacza: im mniej, tym lepiej!



Realizacja praw osób fizycznych

Na samym początku przypomnieć należy podstawową zasadę: nie należy oceniać pisma po nazwie, tak samo jak i książki po okładce. To treść pisma jest najważniejsza, w związku z czym niezależnie od tego, w jaki sposób zostało ono zatytułowane, jeżeli odnosi się ono do ochrony danych osobowych, prawdopodobnie będzie chodziło w nim właśnie o realizację praw.

Osobom fizycznym, których dane podlegają przetwarzaniu (a więc wszelkim czynnościom począwszy od ich zbierania, przez utrwalanie, kopiowanie, modyfikowanie, przenoszenie, jak również innym, aż do zniszczenia) przysługują następujące prawa:

- prawo do uzyskania informacji o przetwarzaniu ich danych osobowych,
- skarga do Prezesa Urzędu Ochrony Danych Osobowych,
- prawo dostępu do danych,
- prawo do sprostowania danych,
- prawo do bycia zapomnianym,
- prawo do ograniczenia przetwarzania danych,
- prawo do przenoszenia danych,
- prawo do sprzeciwu oraz do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu,
- prawo do wycofania zgody.

Zakres powyższych praw jest ściśle powiązany z podstawą przetwarzania. Oznacza to, że w zależności od podstawy na jakiej przetwarzane są dane, zastosowanie będą mieć konkretne prawa. Przykładowo, w przypadku przetwarzania na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c RODO) przysługiwać będzie prawo dostępu, do sprostowania czy ograniczenia przetwarzania, ale nie będzie przysługiwać prawo do usunięcia lub przeniesienia danych czy do sprzeciwu.

Z cofnięcia zgody, jak wspomniano wyżej, można skorzystać w przypadku przetwarzania na podstawie zgody, zaś skarga do Prezesa Urzędu Ochrony Danych Osobowych może być składana bez ograniczeń.

Poniżej prezentujemy omówienie poszczególnych praw przysługujących osobom fizycznym na podstawie przepisów RODO.

	PRAWO DOSTĘPU	PRAWO DO SPROSTOWANIA	PRAWO DO USUNIĘCIA	PRAWO DO OGRANICZENIA PRZETWARZANIA	PRAWO DO PRZENIESIENIA DANYCH	PRAWO DO SPRZECIWU
ZGODA (art. 6 ust. 1 lit. a)	TAK	TAK	TAK	TAK	TAK	TAK/NIE (wycofanie zgody)
UMOWA (art. 6 ust. 1 lit. b)	TAK	TAK	TAK	TAK	TAK	NIE
OBOWIĄZEK PRAWNY (art. 6 ust. 1 lit. c)	TAK	TAK	NIE	TAK	NIE	NIE
ŻYWOTNE INTERESY (art. 6 ust. 1 lit. d)	TAK	TAK	TAK	TAK	NIE	NIE
ZADANIA PUBLICZNE (art. 6 ust. 1 lit. e)	TAK	TAK	NIE	TAK	NIE	TAK
UZASADNIONY INTERES (art. 6 ust. 1 lit. f)	TAK	TAK	TAK	TAK	NIE	TAK

Obowiązek informacyjny

Z jednej strony, przekazanie informacji dotyczących przetwarzania stanowi obowiązek administratora, który jest najczęściej realizowany przez przekazanie klauzuli informacyjnej. W takim wypadku należy go rozumieć jako obowiązek ciążący na administratorze, który zobowiązany jest do przekazania informacji o przetwarzaniu danych osobowych tym osobom, których dane przetwarza.

Przypomnieć w tym miejscu należy, że zmiany w tym zakresie wymogła nowelizacja 167 ustaw, w tym przepisów Kodeksu postępowania administracyjnego, która weszła w życie 4 maja 2019 r. Doprecyzowały one formę w jakiej powinien być realizowany obowiązek informacyjny.

Z drugiej strony, przekazanie informacji o przetwarzaniu danych osobowych stanowi również realizację prawa osoby fizycznej, ponieważ każda osoba ma prawo uzyskać informacje na temat tego czy i w jaki sposób są przetwarzane jej dane.

Realizacja obowiązku informacyjnego jest niejako pierwszym etapem realizacji praw, ponieważ to właśnie wtedy przekazuje się informacje o przysługujących uprawnieniach, np. wymieniając je w klauzuli informacyjnej.

Skarga do Prezesa Urzędu Ochrony Danych Osobowych

Jeżeli jakaś osoba uzna, że jej prawa zostały w jakiś sposób naruszone, ma prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (PUODO). Nie musi ona zaskarżyć danego działania u samego administratora, ponieważ jest to postępowanie odrębne od administracyjnego trybu rozpatrywania skarg i jest oparte na przepisach RODO. Skargę do PUODO wnieść można bezpośrednio i bez przeprowadzenia uprzednio postępowania przez administratora, nie istnieje procedura odwoławcza, którą należałoby przed złożeniem skargi do PUODO wyczerpać. W wyniku skargi PUODO może wszcząć postępowanie administracyjne.

Warto zaznaczyć, że oprócz tak oczywistych przypadków jak zniszczenie czy zgubienie danych, naruszeniem, które skutkować może złożeniem skargi do PUODO, może być również brak odpowiedzi na żądanie realizacji któregoś z wymienionych wcześniej praw. Choćby z tego względu tak istotne jest, aby potrafić rozpoznać takie żądanie, a następnie w odpowiedni sposób się do niego odnieść.

Prawo dostępu do danych

Każda osoba posiada prawo do uzyskania od administratora informacji, czy przetwarza on jej dane, a także do dostępu do tych danych i informacji dotyczących ich przetwarzania. Każda osoba posiada również prawo uzyskania kopii przetwarzanych danych, która co do zasady powinna być bezpłatna. Realizując to prawo należy mieć na uwadze skuteczną identyfikację osoby, która chce z niego skorzystać, aby uniknąć ewentualnego udzielenia dostępu lub wydania kopii osobie do tego nieuprawnionej.

Prawo do sprostowania danych

Prowadzenie postępowań administracyjnych wiąże się z korzystaniem z różnych baz danych, jak również pracy na uzyskanych od ludzi informacjach. Istotne jest, aby dysponować w takim zakresie danymi z jednej strony prawdziwymi, z drugiej zaś kompletnymi.

Z punktu widzenia ochrony danych, każda osoba fizyczna ma prawo do sprostowania danych w przypadku, gdy administrator posiada dane nieprawidłowe. Każda osoba fizyczna ma również prawo do uzupełnienia danych, jeżeli administrator dysponuje danymi niekompletnymi.

Prawo do bycia zapomnianym

Prawo do bycia zapomnianym polega na możliwości żądania przez osobę fizyczną usunięcia dotyczących jej danych przez administratora.

Z uwagi na ostateczny charakter tego usunięcia wprowadzony został szereg ograniczeń tego prawa.

Prawo to przysługuje w sytuacji, gdy:

- dane osobowe nie są już niezbędne do realizacji celów, w jakich zostały zebrane lub w inny sposób przetwarzane,
- cofnięta została zgoda na przetwarzanie danych, a brak innej podstawy przetwarzania,
- wniesiony został sprzeciw, a nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub sprzeciw dotyczy marketingu bezpośredniego,
- dane osobowe były przetwarzane niezgodnie z prawem,
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego,
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Wokół prawa do bycia zapomnianym narosło wiele mitów, zgodnie z którymi prawo to miałoby być wykorzystywane w sytuacjach, gdy ono nie przysługuje, stanowiąc pole do nadużyć. Należy jednak pamiętać, że właśnie z tego względu prawo do bycia zapomnianym zostało obwarowane licznymi ograniczeniami.

Dla przykładu, nie będzie mógł skorzystać z tego prawa dłużnik, chcący w ten sposób uniknąć odpowiedzialności względem wierzyciela. Urząd gminy nie będzie mógł usunąć danych osoby, które zostały uzyskane w ramach postępowania administracyjnego na podstawie przepisu prawa, a co do której dokumentacji istnieje ustawowy obowiązek przechowywania jej przez określony czas.

Prawo do ograniczenia przetwarzania danych

Ograniczenie przetwarzania zmierza co do zasady do zawieszenia wszystkich czynności przetwarzania za wyjątkiem jednej – przechowywania, niezależnie czy będzie się to odbywało w archiwum czy bazie danych, choć w wyjątkowych wypadkach możliwe będzie podejmowanie innych działań na danych, których przetwarzanie podlega ograniczeniu.

Z uprawnienia tego można skorzystać w sytuacji, gdy:

- dane są potrzebne podmiotowi tych danych do ustalenia, dochodzenia lub obrony roszczeń,
- przetwarzanie jest niezgodne z prawem, ale podmiot nie chce ich usunięcia,
- kwestionowana jest prawidłowość danych, na czas sprawdzenia prawidłowości tych danych,
- w przypadku zgłoszenia sprzeciwu, na czas do rozpatrzenia sprzeciwu.

Ograniczenie praw ma na celu pozostawienie danych w niezmienionym kształcie na okres potrzebny do załatwienia sprawy.

Dla przypomnienia, przetwarzaniem jest każda operacja dokonywana na danych osobowych, taka jak utrwalanie, modyfikowanie, przenoszenie, kopiowanie, niszczenie, itd. Istotną kwestią dla zrozumienia tego pojęcia jest charakter tego przetwarzania – przetwarzaniem są nie tylko te czynności, które wymagają aktywności, ale również bierne oddziaływanie na dane, jak np. samo ich przechowywanie. Ograniczeniem przetwarzania danych, jak wspomniano wyżej, jest ograniczenie tych wszystkich czynności do jednej, którą jest przechowywanie danych.

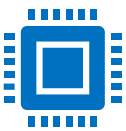
Prawo do przenoszenia danych

Prawo do przenoszenia danych obejmuje sytuacje, w których dane przetwarzane są na podstawie zgody lub w celu realizacji umowy, a przetwarzanie to odbywa się w sposób zautomatyzowany. Realizacją tego prawa jest przesłanie przez jednego administratora dostarczonych mu danych innemu administratorowi, w formacie możliwym do odczytania przez komputer. Przykładem zastosowania tego prawa może być przeniesienie rachunku bankowego, gdy klient banku może zlecić staremu bankowi przekazanie jego danych osobowych do nowego banku.

Prawo do sprzeciwu

Sprzeciw może zostać wyrażony w przypadku przetwarzania danych na podstawie działania w ramach interesu publicznego (art. 6 ust. 1 lit. e RODO) lub uzasadnionego interesu administratora (art. 6 ust. 1 lit. f RODO). Złożenie sprzeciwu ma na celu zatrzymanie przetwarzania danych przez administratora.

W przypadku zgłoszenia takiego sprzeciwu, powinien on zostać rozpatrzony na zasadach określonych w RODO. Rozpatrując sprzeciw, administrator powinien ocenić, czy jest on zasadny, a następnie odpowiedzieć osobie zgłaszającej sprzeciw, niezależnie od rodzaju rozstrzygnięcia. Odpowiedź, w szczególności nieuwzględniająca sprzeciwu, powinna być uzasadniona, a do czasu rozpatrzenia sprzeciwu przetwarzanie danych może podlegać ograniczeniu na żądanie osoby, która złożyła ten sprzeciw.



Prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu

Podstawowym założeniem jest prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu danych, co oznacza, że każdej osobie przysługuje prawo do tego, aby decyzja jej dotycząca podjęta została przy udziale człowieka, a nie

wyłącznie na podstawie automatycznych kalkulacji skonstruowanego do tego celu systemu informatycznego.

W niektórych przypadkach może się jednak zdarzyć, że nasze dane będą podlegać zautomatyzowanemu podejmowaniu decyzji. Może to wynikać z konieczności realizacji umowy, z przepisów prawa. Możemy także dobrowolnie poddać się ocenie systemu, który na podstawie ustalonych kryteriów wyda dotyczącą nas decyzję automatycznie. Przykładem zastosowania takich systemów może być budżet obywatelski, czy rozpatrywanie wniosków kredytowych. W miarę postępu cyfryzacji w grę wchodzą również systemy przeprowadzające rekrutacje do placówek oświatowych, decydujące o zakwalifikowaniu się kandydata na podstawie kryteriów ustalonych w ustawie i aktach prawa miejscowego, jak również w wydarzeniach o charakterze sportowym, gdzie system może zadecydować choćby o przydzieleniu uczestników do poszczególnych grup startowych.

Przykładowo, ze zautomatyzowanym podejmowaniem decyzji możemy mieć do czynienia w sytuacji, gdy w ramach rekrutacji do placówki oświatowej, przy pomocy udostępnionego w formie cyfrowej formularza odpowiadamy na pytania, stanowiące kolejne kryteria wynikające z ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe oraz uchwalonych miejscowo. Na tej podstawie system dokonuje automatycznych obliczeń, które – w zależności od uzyskanego wyniku – decydują o przyjęciu lub nie kandydata.

Dodatkowymi, związanymi z powyższym, prawami są prawo do uzyskania interwencji ludzkiej, do wyrażenia stanowiska i do zakwestionowania decyzji wydanej w sposób zautomatyzowany. Oznacza to, że w każdej sytuacji przysługuje nam prawo do wydania decyzji w sprawie przez człowieka.

Prawo do cofnięcia zgody

W przypadku przetwarzania danych na podstawie zgody wyrażonej przez osobę fizyczną, przysługuje tej osobie prawo do jej cofnięcia, w każdym momencie. Oznacza to, że dalsze przetwarzanie po cofnięciu zgody należy uznać za bezpodstawne, o ile oczywiście nie istnieją inne podstawy, które pozwalają na takie działania. Co do zasady więc, od momentu cofnięcia zgody nie można już przetwarzać danych. Należy pamiętać, że przetwarzanie dokonane do tego momentu było zgodne z prawem, o ile zgoda była uzyskana prawidłowo.

Jak wspomniano na wstępie, zgoda jako podstawa przetwarzania powinna być brana pod uwagę jako ostatnia. Wynika to właśnie z faktu możliwości cofnięcia jej w dowolnym momencie. Nie zawsze bowiem będzie możliwe skuteczne cofnięcie zgody.

Przykładowo, nie będzie skuteczne cofnięcie zgody na przetwarzanie danych osobowych w odniesieniu do danych, które zostały pozyskane na potrzeby przeprowadzenia postępowania administracyjnego i w granicach dozwolonych przepisami (bez danych nadmiarowych). Wynika to z tego, że organ może być związany odrębnymi przepisami dotyczącymi obowiązku przechowywania dokumentacji z postępowania przez pewien okres. Z tego względu nieprawidłową praktyką jest zbieranie zgód na przetwarzanie danych osobowych w celu przeprowadzenia postępowania administracyjnego (przy założeniu zasady minimalizacji danych osobowych), które to działanie może wprowadzać w błąd co do możliwości skorzystania z prawa do cofnięcia zgody, które przysługiwać może co najwyżej do danych podanych dodatkowo.

Należy pamiętać o tym, by zapewnić skuteczną identyfikację osoby, która chce skorzystać z któregoś z praw, aby zminimalizować ryzyko pomyłki lub uniemożliwić podszywanie się pod osobę uprawnioną. Brak weryfikacji tożsamości może prowadzić do naruszeń ochrony danych osobowych.

Ograniczenia praw osób fizycznych i ich przykłady

Przedstawione powyżej prawa posiadają swoje ograniczenia, które wprowadzane być mogą przepisami prawa krajowego. Ograniczenia te mogą wyłączać lub ograniczać stosowanie pewnych praw wynikających z RODO. Poniżej przedstawiamy kilka przykładów ustaw, zawierających takie ograniczenia:

- prawo prasowe (ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych),
- prawo zamówień publicznych (ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych),
- statystyka publiczna (ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej),
- planowanie i zagospodarowanie przestrzenne (ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym),
- archiwizacja (ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach).

Jak reagować na żądanie realizacji praw?

W przypadku uzyskania żądania realizacji praw, niezależnie od formy w jakiej to nastąpi, należy w pierwszej kolejności ustalić treść żądania. Jak już wspomniano na wstępie, istotna jest sama treść pisma, nie zaś jego tytuł. Jest to o tyle ważne, że postępowanie w sprawach realizacji praw podlega zasadom innym niż określone przez Kodeks postępowania administracyjnego, w związku z czym nieprawidłowa klasyfikacja może prowadzić do błędów natury proceduralnej.

Brak jest wymogów co do formy, w jakiej może być złożone żądanie. Przystępując do rozpatrywania sprawy należy zweryfikować tożsamość osoby, aby uniknąć błędu co do tego, czy w ogóle przysługuje jej dane prawo. Jest to również istotne, aby nie przekazać danych osobie do tego nieuprawnionej, co mogłoby stanowić naruszenie ochrony danych. W trakcie rozpatrywania żądania, administrator może żądać dodatkowych informacji służących identyfikacji.

W razie wątpliwości dotyczących zgłoszonych żądań rekomendowane jest przeprowadzenie konsultacji z wyznaczonym Inspektorem Ochrony Danych.

Administrator zobowiązany jest do udzielenia odpowiedzi, które może zostać dokonane w formie pisemnej lub innej formie, w tym elektronicznej (w zależności między innymi od tego w jakiej formie zostało złożone żądanie). Maksymalny czas na rozpatrzenie sprawy i przekazanie odpowiedzi wynosi miesiąc i w wyjątkowych sytuacjach może podlegać wydłużeniu. Jak już wspomniano, w szczególności w przypadku odmowy realizacji żądania, odpowiedź należy uzasadnić.

Kolejnym obowiązkiem administratora związanym z realizacją praw jest obowiązek powiadomienia odbiorców, a więc podmiotów uprawnionych do otrzymywania danych (np. podmiotów przetwarzających), danych o dokonaniu sprostowania, usunięciu lub ograniczeniu praw.

Poniżej prezentujemy infografikę przedstawiającą kolejność działań, jakie powinny zostać podjęte w sytuacji otrzymania żądania realizacji praw: