PARP Grupa PFR
Centrum Rozwoju MŚP

REALIZACJA PRAW PODMIOTÓW DANYCH W ŚWIETLE RODO

REALIZACJA PRAW PODMIOTÓW DANYCH W ŚWIETLE RODO

Warszawa 2022

REALIZACJA PRAW PODMIOTÓW DANYCH W ŚWIETLE RODO

Autor: adwokat Adrianna Michałowicz

Redakcja: Paweł Sikorski

Niniejsza publikacja została sfinansowana ze środków budżetu państwa w związku z realizacją działań w ramach Centrum Rozwoju Małych i Średnich Przedsiębiorstw.

Wydawca:
Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83
00-834 Warszawa
www.parp.gov.pl

ISBN: 978-83-7633-481-3

Opracowanie graficzno-techniczne:
www.ccpg.com.pl

Spis treści

Wprowadzenie

Jednym z wyzwań, a jednocześnie celów reformy prawa ochrony danych osobowych w Unii Europejskiej, było wzmocnienie uprawnień kontrolnych przysługujących osobom fizycznym w związku z przetwarzaniem ich danych osobowych. Globalizacja i intensywny rozwój gospodarki cyfrowej od początku XXI wieku, a w konsekwencji zwiększona wymiana danych osobowych pomiędzy różnymi podmiotami, w dodatku niezależnie od granic geograficznych, sprawiły, że kontrola ta przybrała charakter iluzoryczny. Problem ten został dostrzeżony przez unijnego prawodawcę i stał się jednym z kluczowych zagadnień podejmowanych w toku prac legislacyjnych nad pakietem reform w zakresie ochrony danych osobowych. Dostrzeżono, że w dynamicznie rozwijającym się środowisku internetowym osoby fizyczne nie tylko tracą kontrolę nad tym kto, w jaki sposób i w jakich celach przetwarza ich dane osobowe, ale również nie mają świadomości, iż przetwarzanie danych może wiązać się z istotnymi zagrożeniami ich praw i wolności.

Przyjęte w dniu 27 kwietnia 2016 r., a stosowane od 25 maja 2018 r., Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zawiera rozbudowany katalog praw przysługujących podmiotom danych w sytuacji, gdy dochodzi do przetwarzania ich danych osobowych. Możliwość realizacji tych praw ma sprzyjać podnoszeniu poziomu kontroli nad danymi osobowymi oraz wzmacniać pozycję osób fizycznych względem podmiotów, które są odpowiedzialne za procesy przetwarzania danych, tj. przede wszystkim względem administratorów, ale też podmiotów działających w ich imieniu, czyli podmiotów przetwarzających.

Niniejsze opracowanie zawiera omówienie problematyki realizacji praw podmiotów danych, w szczególności obowiązków nałożonych na administratorów w związku z wykonywaniem uprawnień przysługujących osobom fizycznym. Publikacja została wzbogacona o listę wybranych decyzji krajowych organów nadzorczych, wydanych w ramach postępowań prowadzonych w związku z naruszeniami podstawowych praw podmiotów danych.

1. Podstawowe pojęcia

1.1. Dane osobowe

Definicja pojęcia „dane osobowe” została wprowadzona na gruncie dwóch międzynarodowych aktów prawnych: Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[1] oraz w ogólnym rozporządzeniu o ochronie danych (RODO)[2]. W art. 2 lit. a) Konwencji nr 108 wskazano, że termin „dane osobowe” oznacza każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować. Zgodnie natomiast z art. 4 pkt 1 RODO „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Obydwie definicje w identyczny sposób kształtują zakres przedmiotowy pojęcia danych osobowych, aczkolwiek ta przyjęta przez unijnego prawodawcę jest bardziej szczegółowa, ponieważ dodatkowo precyzuje, że osoba fizyczna możliwa do zidentyfikowania to taka, 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.

Definicja wskazana w art. 4 pkt 1 RODO składa się z czterech elementów – przesłanek definicyjnych, które wymagają osobnego omówienia w celu dokładnego wyjaśnienia pojęcia „dane osobowe”. Elementami tymi są: „wszelkie informacje”, „dotyczące”, „zidentyfikowanej lub możliwej do zidentyfikowania”, „osoby fizycznej”[3]. Sformułowanie

[1] Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dn. 28.01.1981 r., Strasburg.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z dnia 4.05.2016 r., s. 1–88.

[3] Podział przyjęty w ślad za *Opinią 4/2007 w sprawie pojęcia danych osobowych* wydaną w dniu 20.06.2007 r. przez Grupę Roboczą Art. 29, WP 136. Opinia 4/2007 została wydana w odniesieniu do pojęcia danych osobowych zdefiniowanego w art. 2 lit. a) dyrektywy 95/46/WE, jednak ze względu na zbieżny przedmiotowo zakres tego pojęcia na gruncie uchylonej dyrektywy 95/46/WE, jak i RODO, zaprezentowany podział nadal znajduje zastosowanie.

„wszelkie informacje" sugeruje, że intencją unijnego prawodawcy było wprowadzenie szerokiej interpretacji terminu danych osobowych[4]. Takie założenie można poczynić biorąc pod uwagę również cel przyjęcia rozporządzenia 2016/679, wskazany w art. 1 RODO, jakim jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych[5]. Dla oceny osobowego wymiaru informacji bez znaczenia pozostaje to, czy informacja ma charakter obiektywny lub subiektywny, jak i to, w jaki sposób jest utrwalona[6]. Treść może odnosić się do różnego rodzaju informacji, np. dotyczących życia rodzinnego, prywatnego, zawodowego, społecznego, jakichkolwiek działań podejmowanych przez konkretną osobę, jej zachowań ekonomicznych, pozycji, stanowiska, funkcji itp.[7] Informacje mogą być też przechowywane w jakiejkolwiek formie, np. graficznej, fotograficznej, akustycznej, liczbowej, a także na jakimkolwiek nośniku, np. na papierze, w pamięci komputera, na dysku zewnętrznym, w chmurze itp.[8] **Niezależnie zatem od charakteru, treści, formatu czy sposobu przechowywania, każda informacja może stanowić daną osobową, jeśli spełnione są pozostałe przesłanki definicyjne.**

Drugi element wskazuje na konieczność powiązania określonej informacji z osobą fizyczną[9]. Jak przyjęła Grupa Robocza Art. 29, informacja dotyczy osoby, jeśli jest „na temat" tej osoby[10]. W praktyce ustalenie związku pomiędzy informacją a osobą bywa trudne, zwłaszcza wówczas, gdy informacja nie odnosi się wprost do konkretnej osoby, lecz do określonego

---

4 Grupa Robocza Art. 29, *Opinia 4/2007…,* s. 6. Warto zaznaczyć, że w polskiej wersji językowej RODO przymiotnik „wszelkie" – w odniesieniu do informacji – nie pojawia się w definicji danych osobowych zawartej w art. 4 pkt. 1 RODO. Pojawia się natomiast w innych wersjach językowych, np. w angielskiej („any information"), niemieckiej („alle Informationen"), francuskiej („toute information"), hiszpańskiej („toda información"). Niemniej jednak, zarówno w literaturze przedmiotu, jak i w motywie 26 RODO, akcentuje się, że dane osobowe obejmują „wszelkie informacje" dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Celem takiego podkreślenia jest objęcie jak największej ilości informacji zakresem pojęcia danych osobowych.

5 D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 165.

6 D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 165. Podkreślił to również Trybunał Sprawiedliwości (TS) w wyroku z dnia 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak przeciwko Data Protection Commissioner, ECLI:EU:C:2017:994, pkt 34.

7 Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 6.

8 Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 7.

9 W polskiej wersji językowej RODO w art. 4 pkt 1 nie pojawia się sformułowanie „dotycząca", lecz spójnik „o" – „informacja o osobie fizycznej". Sformułowanie to pojawia się natomiast w innych wersjach językowych RODO, np. ang. „any information relating to an (…) natural person", franc. „toute information se rapportant à une personne physique", niem. "alle Informationen, die sich auf eine (…) natürliche Person".

10 Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 9.

przedmiotu. Jednak w wielu przypadkach informacje o cechach, funkcjach czy sposobach używania przedmiotów mogą zawierać także dane odnoszące się do osoby. Przykładowo, wartość samochodu stanowi przede wszystkim informację o przedmiocie, aczkolwiek w odniesieniu do osoby fizycznej może stanowić daną osobową wskazującą na status majątkowy tej osoby, jej preferencje co do marki lub modelu samochodu; wartość pojazdu może być wyznacznikiem przy ocenie zdolności leasingowej lub przy ustalaniu zobowiązań podatkowych[11]. Informacja o położeniu geograficznym danego przedmiotu może zawierać jednocześnie informację o lokalizacji osoby, do której przedmiot ten należy. Informacje umożliwiające dostęp i korzystanie z urządzenia niewątpliwie będą informacjami na temat konkretnej osoby fizycznej, jeśli do uruchomienia urządzenia potrzebne są dane biometryczne użytkownika.

Trzecią przesłanką definicyjną pojęcia „dane osobowe" jest przesłanka identyfikowalności. Aby informacja była kwalifikowana jako dane osobowe, musi identyfikować lub przynajmniej pozwalać na identyfikację określonej osoby fizycznej. Zidentyfikowana osoba fizyczna to taka, której tożsamość można ustalić bezpośrednio i natychmiast. To też osoba, którą można odróżnić od pozostałych członków grupy, w jakiej się znajduje[12]. W takim przypadku administrator ma obiektywną możliwość powiązania konkretnych informacji z daną osobą bez potrzeby podejmowania dodatkowych aktywności.

Inaczej jest w odniesieniu do osób możliwych do zidentyfikowania. Prawodawca unijny w motywie 26 RODO wskazał, że przy ocenie, czy mamy do czynienia z osobą fizyczną możliwą do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Z kolei weryfikacja „uzasadnionego prawdopodobieństwa" wykorzystania „rozsądnie prawdopodobnych sposobów" winna następować przez pryzmat wszelkich obiektywnych czynników, takich jak koszt i czas potrzebny do zidentyfikowania osoby fizycznej, oraz uwzględniać technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Należy więc brać pod uwagę nie wszelkie dowolne sposoby aktywności administratora, lecz te, którymi faktycznie może się on posłużyć; uwzględnia się

[11] Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 9.

[12] Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 12; D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 175.

przy tym też osoby trzecie, do których administrator może racjonalnie się odwołać w celu uzyskania dodatkowych informacji potrzebnych do zidentyfikowania osoby fizycznej[13].

Nie wlicza się również sposobów identyfikacji, które w praktyce są niewykonalne, wiążą się z nadmiernym nakładem czasu, kosztów, pracy ludzkiej itp. Sam fakt, że administrator nie posiada wystarczających informacji pozwalających na identyfikację konkretnej osoby fizycznej nie oznacza, że informacje te nie mogą uzyskać przymiotu identyfikowalności. Wprost przeciwnie – będą to informacje identyfikowalne, jeśli administrator jest w stanie, z zastrzeżeniem obiektywnych czynników wskazanych w motywie 26 RODO, pozyskać dodatkowe dane od podmiotów trzecich, pozwalające na ustalenie tożsamości osoby fizycznej. Co więcej, udostępnianie przez administratora innym podmiotom informacji, na bazie których nie może dokonać samodzielnie identyfikacji osoby fizycznej, może być kwalifikowane jako udostępnianie danych osobowych, a tym samym jako operacja przetwarzania danych, w sytuacji, gdy odbiorca tych informacji mógłby dokonać takiej identyfikacji z wykorzystaniem dostępnych mu dodatkowych informacji[14].

Warto też zwrócić uwagę jeszcze na dwa aspekty wiążące się z przesłanką identyfikowalności. Po pierwsze, ustalenie tożsamości osoby fizycznej następuje w oparciu o tzw. identyfikatory, których przykładowy katalog został zawarty w art. 4 pkt 1 RODO[15]. Niemniej jednak, możliwość zidentyfikowania osoby fizycznej nie musi wcale oznaczać możliwości ustalenia jej danych personalnych, takich jak imię czy nazwisko; wystarczająca jest sama możliwość wyróżnienia określonej osoby na tle danej grupy[16]. Po drugie, jako informacje zezwalające na identyfikację osoby fizycznej mogą być traktowane dane osobowe spseudonimizowane, ponieważ w razie powiązania ich z dodatkowymi informacjami posiadanymi przez administratora lub osobę trzecią staną się one danymi osobowymi[17]. Identyfikacja osoby fizycznej nie będzie natomiast możliwa z wykorzystaniem danych osobowych zanonimizowanych w taki sposób, że na ich podstawie nie można już zidentyfikować osób, których dane dotyczą.

---

13 Wyrok TS z dnia 19.10.2016 r. w sprawie C-582/14 *Breyer*, ECLI:EU:C:2016:779, pkt 46.

14 D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 182.

15 W art. 4 pkt 1 RODO wskazano na takie identyfikatory jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

16 D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 183.

17 Motyw 26 RODO.

Wreszcie ostatnim kryterium definiującym dane osobowe jest wymóg, aby informacja odnosiła się do osoby fizycznej. Choć to pojęcie nie zostało na gruncie RODO wyjaśnione, pośrednio z samej nazwy aktu prawnego, a wprost z treści motywu 14 RODO wynika, że ochrona nie przysługuje osobom prawnym, w szczególności przedsiębiorstwom będącym osobami prawnymi. Ochroną przewidzianą przez RODO nie będą więc objęte dane o firmie i formie prawnej oraz dane kontaktowe osoby prawnej, z tym jednak zastrzeżeniem, że **ochrony nie są pozbawione** informacje o charakterze osobowym związane z danymi dotyczącymi osób prawnych, jak przykładowo dane osobowe wchodzące w skład firmy przedsiębiorstwa, dane osobowe członków organów spółki czy dane osobowe zamieszczone w adresie poczty elektronicznej wykorzystywanym przez osobę prawną do prowadzenia działalności gospodarczej[18]. Podobnie jest w przypadku przedsiębiorców będących osobami fizycznymi[19].

Niewątpliwie pojęcie osoby fizycznej w kontekście podmiotu danych osobowych powinno być definiowane przez pryzmat podmiotowości prawnej, a zatem zdolności prawnej osoby fizycznej. Z tego względu osobą fizyczną, a w konsekwencji podmiotem danych osobowych, nie będzie ani *nasciturus* ani osoba zmarła, aczkolwiek w przypadku tych drugich państwa członkowskie mogą przyjąć odpowiednie przepisy regulujące przetwarzanie ich danych osobowych[20]. W odniesieniu do *nasciturusa* dominuje natomiast pogląd, że jego dane do czasu urodzenia stanowią dane osobowe matki lub ojca[21].

Na koniec warto dodać, że dane poddane pseudonimizacji nadal traktowane są jako dane osobowe. Jak stanowi art. 4 pkt 5) RODO, pseudonimizacja oznacza takie przetworzenie danych osobowych, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, z tym zastrzeżeniem, że owe dodatkowe informacje muszą być przechowywane osobno i z uwzględnieniem środków technicznych i organizacyjnych uniemożliwiających ich przypisanie zidentyfikowanej lub możliwej

[18] D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 169–170; Grupa Robocza Art. 29, *Opinia 4/2007*…, s. 24. Zob. też wyrok TS z dnia 9.11.2010 r. w sprawach połączonych C-92/09 oraz C-93/09 *Volker und Markus Schecke i Eifert*, ECLI:EU:C:2010:662.

[19] Pojęcie przedsiębiorcy zostało na gruncie RODO zdefiniowane w art. 4 pkt 18. Oznacza ono „osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą".

[20] Zostało to wprost wyrażone w motywie 27 RODO. Przykładem regulacji odnoszących się do ochrony danych osobowych osób zmarłych mogą być przepisy dotyczące praw pacjenta. Dane te mogą być też pośrednio chronione, jeśli zawierają informacje o spokrewnionych osobach żyjących.

[21] D. Lubasz, *Artykuł 4 pkt 1* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 169.

do zidentyfikowania osobie fizycznej. Pseudonimizacja jest więc procesem odwracalnym, gdyż z wykorzystaniem wydzielonych, dodatkowych informacji, można zidentyfikować konkretną osobę fizyczną, której dane zostały poddane pseudonimizacji. Stąd konieczność, aby informacje te były przechowywane w innym miejscu niż dane spseudonimizowane.

1.2. Administrator

Pojęcie administratora zostało uregulowane w art. 4 pkt 7 RODO. Zgodnie z definicją legalną pojęcie to oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". Z definicji tej wynikają dwie podstawowe funkcje, jakie w procesie przetwarzania danych osobowych są przypisane administratorowi, tj. po pierwsze, określenie celów przetwarzania, a po drugie – określenie sposobów przetwarzania. Decyzję w zakresie celów i sposobów przetwarzania administrator może podjąć samodzielnie lub wspólnie z innym administratorem.

Zakwalifikowanie danego podmiotu jako administratora ma istotne konsekwencje. Podmiot ten ponosi odpowiedzialność za prawidłowe zorganizowanie procesów przetwarzania danych osobowych, jest zobligowany do wypełnienia wielu obowiązków wynikających z RODO, a w razie naruszeń przepisów dotyczących ochrony danych osobowych[22] organ nadzorczy[23] może na niego nałożyć administracyjną karę pieniężną. Dlatego tak ważne jest rzetelne zweryfikowanie roli i funkcji, jaką dany podmiot pełni w procesach przetwarzania danych osobowych, nie tylko w celu zapewnienia odpowiedniego poziomu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, ale również w celu dokładnego ustalenia zakresu obowiązków nałożonych na dany podmiot oraz zakresu odpowiedzialności za ewentualne naruszenia przepisów.

Zgodnie z zaprezentowaną wyżej definicją, administratorem może być „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot". Nie ma ograniczeń co do rodzaju

[22] Mowa nie tylko o RODO, ale też innych krajowych przepisach regulujących kwestie przetwarzania danych osobowych. W Polsce będą to przykładowo: Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781); Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2020 r. poz. 1320) – w zakresie w jakim dotyczy przetwarzania danych osobowych pracowników (zob. np. art. 221 tejże ustawy).

[23] W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych (PUODO). Zasady powoływania, właściwość, zadania i uprawnienia krajowych organów nadzorczych zostały uregulowane w rozdziale VI RODO.

i formy prawnej podmiotu, który może pełnić rolę administratora – może nim być przykładowo przedsiębiorca prowadzący działalność gospodarczą, spółka komandytowa, spółka z ograniczoną odpowiedzialnością, stowarzyszenie, fundacja itd. Zdarza się jednak, że faktyczne decyzje dotyczące przetwarzania danych osobowych w organizacji mogą być podejmowane przez konkretne osoby (np. osoby pełniące funkcję kierowniczą w danej strukturze albo osoby odpowiedzialne za wdrożenie i przestrzeganie przepisów dotyczących ochrony danych osobowych). Wówczas, w takich sytuacjach co do zasady rolę administratora pełni dany podmiot, a nie osoba działająca w imieniu tego podmiotu lub której powierzono określone obowiązki[24]. Zdarzają się też przypadki, w których rola administratora jest wyraźnie przypisana określonemu podmiotowi na mocy przepisów[25].

Administrator ustala cele i sposoby przetwarzania danych osobowych, co oznacza, że określa, dlaczego przetwarzanie ma miejsce (po co dane osobowe są przetwarzane?) oraz w jaki sposób chce osiągnąć rezultat przetwarzania (środki, jakie zostaną zastosowane, aby osiągnąć cel przetwarzania). Co do zasady decyzja w tym zakresie powinna być podejmowana wyłącznie przez administratora, aczkolwiek w sytuacji powierzenia przetwarzania dopuszczalne jest pozostawienie pewnej swobody decyzyjnej podmiotowi przetwarzającemu. Swoboda ta nie może jednak dotyczyć określenia celów przetwarzania, a jedynie sposobów przetwarzania, w dodatku sposobów „nieistotnych" (*non-essential means*), odnoszących się do bardziej praktycznych aspektów przetwarzania, takich jak rodzaj wykorzystywanego sprzętu lub oprogramowania, szczegółowe środki bezpieczeństwa itp.[26] Wystarczy więc, że administrator ogólnie określi sposoby osiągnięcia celu przetwarzania, a dookreślenie tych sposobów nastąpi przez procesora.

---

[24] EROD, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 2.0, przyjęte w dn. 7.07.2021 r., s. 10.

[25] Zob. przykładowo: art. 10 ust. 8 Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2021 r., poz. 666), w którym wskazano, że administratorem danych przetwarzanych w Systemie Informacji Medycznej jest minister właściwy do spraw zdrowia; rozdział 9 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 poz. 125), zawierający wykaz zmian w obowiązujących przepisach, w tym polegających na ustawowym wyznaczeniu konkretnych podmiotów pełniących rolę administratora w zakresie realizacji celów ww. ustawy (np. Komendant Główny Policji, Komendant Główny Straży Granicznej, Główny Inspektor Ochrony Środowiska).

[26] Zwraca na to uwagę m.in. EROD w swoich wytycznych, wskazując, że sposoby istotne (*essential means*) są ściśle związane z celem i zakresem przetwarzania. Ustalanie istotnych sposobów przetwarzania wiąże się więc z podjęciem decyzji co do rodzaju przetwarzanych danych osobowych, czasu przetwarzania, kategorii odbiorców danych oraz kategorii osób, których dane będą przetwarzane. Zob. EROD, *Guidelines 07/2020…,* s. 15.

Oprócz decydowania o celach i sposobach przetwarzania, administrator na mocy RODO jest zobowiązany do wypełniania szeregu obowiązków. Wśród nich można wymienić m.in. obowiązki:

- przestrzegania zasad przetwarzania danych osobowych wyszczególnionych w art. 5 RODO;
- przetwarzania danych osobowych w oparciu o właściwą przesłankę legalizującą przetwarzanie z art. 6 ust. 1 lub art. 9 ust. 2 RODO;
- poinformowania podmiotu danych o przetwarzaniu danych osobowych (art. 13 i 14 RODO);
- realizacji praw podmiotów danych (art. 15–22 RODO);
- wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodności przetwarzania z RODO oraz bezpieczeństwa przetwarzania adekwatnego do ryzyka naruszenia praw lub wolności osób fizycznych (art. 24 i 32 RODO);
- zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu (art. 33 RODO);
- przeprowadzenia oceny skutków dla ochrony danych, jeśli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 RODO).

Mając na uwadze to, że podstawowym celem przypisania danemu podmiotowi roli administratora jest zapewnienie rozliczalności oraz skutecznej i kompleksowej ochrony danych osobowych, pojęcie „administratora" powinno być interpretowane w sposób wystarczająco szeroki, tak by zapewnić pełną skuteczność prawa ochrony danych, uniknąć luk prawnych oraz zapobiec ewentualnemu obchodzeniu przepisów[27]. Z tego względu ocena, czy dany podmiot pełni funkcję administratora następuje obiektywnie i nie jest zależna od woli czy świadomości tego podmiotu. Kluczowe jest samo spełnienie kryteriów definicyjnych z art. 4 pkt 7 RODO; jeśli są one spełnione, podmiot pełniący funkcję administratora nie może zrzec się tej roli ani przenieść swoich obowiązków na inny podmiot, np. w drodze umowy.

Jak podkreśla Europejska Rada Ochrony Danych (EROD) w wytycznych, pojęcia administratora i podmiotu przetwarzającego powinny być traktowane funkcjonalnie, co oznacza, że status prawny danego podmiotu jako administratora lub procesora musi być określony z uwzględnieniem jego rzeczywistych działań w konkretnej sytuacji, a nie na podstawie formalnego określenia tego podmiotu jako „administratora" lub „podmiotu przetwarzającego"[28]. **Przypisanie obowiązków administratora lub procesora musi być więc zgodne z rzeczywistymi rolami stron**.

[27] EROD, *Guidelines 07/2020…*, s. 9.

[28] EROD, *Guidelines 07/2020…*, s. 9.

1.3. Współadministrator

W świetle RODO za współadministratorów uważa się podmioty, które wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Administrator w tym zakresie nie musi bowiem podejmować decyzji samodzielnie – o tym, w jakim celu i jakimi sposobami przetwarzać dane osobowe może decydować kilka podmiotów jednocześnie. Podobnie jak przy ocenie, który podmiot pełni rolę administratora, również przy weryfikacji, czy zachodzi relacja współadministrowania konieczna jest obiektywna analiza okoliczności faktycznych, tj. tego, które podmioty rzeczywiście wpływają na cele i sposoby przetwarzania, niezależnie od formalnych ustaleń poczynionych między stronami.

Współadministrowanie danymi zachodzi zarówno w przypadku, gdy co najmniej dwa podmioty podejmują jedną, wspólną decyzję co do celów i sposobów przetwarzania danych osobowych, jak i w przypadku, gdy podejmują osobne decyzje, które jednak są zbieżne i uzupełniają się w odniesieniu do celów i sposobów przetwarzania[29]. Jak podkreśla EROD, osobne decyzje muszą być ze sobą nierozerwalnie związane[30]. Warto przy tym zaznaczyć, że współadministrowanie danymi będzie odnosiło się wyłącznie do tych operacji przetwarzania, co do których administratorzy wspólnie decydują o celach i sposobach przetwarzania, czy to w drodze wspólnej decyzji, czy osobnych, uzupełniających się decyzji. Jeśli w ramach przetwarzania dokonywane są również operacje na danych, co do których administratorzy samodzielnie określają cele i sposoby przetwarzania, to w tym zakresie relacja współadministrowania nie zachodzi[31]. Dla zaistnienia relacji współadministrowania nie ma natomiast znaczenia to, że jeden ze współadministratorów nie ma dostępu do przetwarzanych danych osobowych; jeśli tylko bierze udział w decydowaniu o celach i sposobach przetwarzania, to może być uznany za współadministratora[32].

29 EROD, *Guidelines 07/2020…*, s. 19.

30 EROD, *Guidelines 07/2020…*, s. 20.

31 Wyrok TS z dn. 29 lipca 2019 r. w sprawie C-40/17 *Fashion ID*, pkt 74.

32 Wyrok TS z dn. 5 czerwca 2018 r. w sprawie C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, pkt 38; wyrok TS z dn. 10 lipca 2018 r. w sprawie C-25/17 *Jehovan todistajat*, pkt 75.

Współadministrowanie danymi powinno być odpowiednio uregulowane pomiędzy administratorami. Powinni oni, w drodze wspólnych uzgodnień[33], określić zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, zwłaszcza w odniesieniu do realizacji obowiązków informacyjnych oraz obowiązków związanych z wykonywaniem przez podmioty danych przysługujących im praw[34]. Współadministratorzy nie muszą uzgadniać tych kwestii, jeśli podział obowiązków i zakres ich odpowiedzialności wynika z przepisów unijnych lub krajowych[35]. Niezależnie od powyższego, każdy ze współadministratorów ma obowiązek zapewnić, że posiada podstawę prawną do przetwarzania danych oraz że dane nie są dalej przetwarzane w sposób niezgodny z celami, dla których zostały pierwotnie zebrane[36].

1.4. Podmiot przetwarzający

Podmiot przetwarzający, zwany też procesorem, to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora[37]. Zakres podmiotowy tego pojęcia jest, podobnie jak w przypadku administratora, tak samo szeroki – rolę procesora może pełnić każdy podmiot bez ograniczeń co do formy prawnej. Procesorem może być więc spółka, stowarzyszenie, fundacja, osoba fizyczna prowadząca działalność gospodarczą itp. Czynnikiem determinującym, czy dany podmiot pełni rolę procesora jest to, czy przetwarza on dane osobowe w imieniu administratora. Administrator nie musi bowiem przetwarzać danych osobowych samodzielnie, lecz może w ramach realizowanych działań powierzyć innemu podmiotowi wykonywanie wszystkich lub niektórych czynności przetwarzania. Powierzenie przetwarzania przyjmuje *de facto* formę delegacji zadań administratora na rzecz zewnętrznego podmiotu,

[33] RODO nie narzuca formy prawnej takiego porozumienia pomiędzy współadministratorami, jednak z uwagi na zasadę rozliczalności i w celu zapewnienia przejrzystości przetwarzania, dobrą praktyką jest zawarcie takiego porozumienia w formie pisemnej lub innej formie dokumentującej podział obowiązków pomiędzy współadministratorami. Jak stanowi art. 26 ust. 2 RODO, zasadnicza treść tych uzgodnień powinna być udostępniana podmiotom, których dane są przetwarzane przez współadministratorów.

[34] Zob. art. 26 ust. 1 RODO.

[35] Zob. przykładowo art. 24c Ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2021 r., poz. 2053); art. 10 Ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 2021 r., poz. 268).

[36] EROD, *Guidelines 07/2020…*, s. 4.

[37] Zob. definicję podmiotu przetwarzającego zawartą w art. 4 pkt. 8 RODO.

który ma działać „w jego imieniu", to znaczy ma w ten sposób realizować jego interesy związane z przetwarzaniem danych osobowych, wykonywać jego polecenia i działać zgodnie z wydawanymi przez administratora instrukcjami[38].

Administrator ma zasadniczo pełną dowolność w wyborze podmiotu przetwarzającego. Powinien jednak pamiętać, że podmiot, który wybierze i któremu powierzy przetwarzanie danych osobowych musi zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Na administratorze spoczywa więc obowiązek dochowania należytej staranności i rzetelnej weryfikacji podmiotu przetwarzającego. Ocena tego, czy gwarancje są wystarczające, jest formą oceny ryzyka i zależy od rodzaju przetwarzania powierzonego procesorowi[39]. Powinna być dokonywana indywidualnie dla każdego przypadku, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, ryzyka dla praw i wolności osób fizycznych, jak również powinna być dokonywana cyklicznie, a nie tylko jednorazowo przy wyborze podmiotu przetwarzającego[40]. W praktyce ocena ta może oznaczać konieczność zażądania od podmiotu przetwarzającego okazania odpowiednich dokumentów celem analizy, takich jak polityka prywatności, regulamin świadczenia usług przez procesora, polityka bezpieczeństwa informacji, sprawozdania z zewnętrznych audytów ochrony danych, odpowiednie certyfikaty potwierdzające spełnianie norm ISO dotyczących bezpieczeństwa informacji itp.[41] Administrator powinien też pamiętać, że zgodnie z zasadą rozliczalności, musi być w stanie udowodnić, iż przeprowadził prawidłową ocenę „wystarczających gwarancji" wdrożenia środków technicznych i organizacyjnych przez podmiot przetwarzający, o których mowa w przepisie.

Procesor dokonuje przetwarzania danych osobowych w imieniu administratora i z uwzględnieniem określonych przez niego celów i sposobów przetwarzania, z tym zastrzeżeniem, że podmiotowi przetwarzającemu może przysługiwać pewna swoboda w wyborze tzw. nieistotnych sposobów przetwarzania (zob. pkt 1.2 niniejszego opracowania). Podmiot przetwarzający nie może natomiast wykraczać poza cele i sposoby przetwarzania określone przez administratora. Jeśli samodzielnie zacznie przetwarzać powierzone mu

38 EROD, *Guidelines 07/2020…*, s. 26.

39 EROD, *Guidelines 07/2020…*, s. 31.

40 EROD, *Guidelines 07/2020…*, s. 31.

41 EROD, *Guidelines 07/2020…*, s. 31.

dane osobowe w innych celach lub w inny sposób, stanie się w odniesieniu do takiego przetwarzania odrębnym administratorem.

Relacja powierzenia przetwarzania danych osobowych powinna wynikać z zawartej między stronami umowy powierzenia lub innego instrumentu prawnego uregulowanego na mocy przepisów krajowych lub unijnych[42]. Taka umowa lub inny instrument prawny powinny mieć formę pisemną[43] oraz określać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj powierzanych danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora, a także inne postanowienia, wskazane w art. 28 ust. 3 RODO, jak przykładowo obowiązek przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora[44], obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania[45], zobowiązanie do wspierania administratora w udzielaniu odpowiedzi na żądania podmiotów danych oraz w wywiązywaniu się z obowiązków dotyczących zapewnienia bezpieczeństwa przetwarzania, zgłaszania naruszeń ochrony danych osobowych, zawiadamiania podmiotów danych o naruszeniu ochrony ich danych osobowych czy przeprowadzania oceny skutków dla ochrony[46] danych osobowych[47].

Strony powinny także uregulować kwestię korzystania przez procesora z usług innego podmiotu przetwarzającego, czyli subprocesora. Zgodnie z art. 28 ust. 2 RODO dalsze powierzenie przetwarzania danych osobowych wymaga szczegółowej lub przynajmniej ogólnej pisemnej zgody administratora. W przypadku ogólnej zgody na dalsze powierzenie procesor ma obowiązek powiadomić administratora o każdej planowanej zmianie w zakresie subprocesorów, z których usług korzysta; administrator może wówczas wyrazić sprzeciw wobec dalszego powierzenia przetwarzania konkretnemu podmiotowi. Co istotne, subprocesora obciążają również obowiązki ochrony danych nałożone na procesora, które wynikają z umowy lub innego instrumentu prawnego regulującego relację pomiędzy administratorem a pierwotnym podmiotem przetwarzającym. W razie uchybienia przez

42 Artykuł 28 ust. 3 RODO.

43 Dopuszczalna jest forma elektroniczna – zob. art. 28 ust. 9 RODO.

44 Chyba że obowiązek taki nałożony jest na procesora na mocy przepisów krajowych lub unijnych – zob. art. 28 ust. 3 lit. a) RODO.

45 Artykuł 28 ust. 3 lit. c) RODO.

46 Artykuł 28 ust. 2 RODO.

47 Artykuł 28 ust. 3 lit. f) RODO.

subprocesora tym obowiązkom, pełną odpowiedzialność wobec administratora za ich realizację ponosi procesor[48].

Przykładem powierzenia przetwarzania danych osobowych może być zawarcie przez przedsiębiorcę umowy z biurem księgowym, na mocy której ma ono prowadzić obsługę księgowo-rachunkową. Biuro będzie przetwarzać dane osobowe klientów, kontrahentów czy pracowników zatrudnionych przez przedsiębiorcę, jednak nie będzie dokonywać przetwarzania we własnym interesie, lecz realizując interesy administratora, czyli przedsiębiorcy. Podobnie będzie w przypadku agencji marketingowej, której przedsiębiorca powierzy przetwarzanie danych osobowych swoich klientów w celu przeprowadzenia kampanii reklamowej. Jeśli natomiast agencja wykorzysta przekazane dane osobowe we własnych celach, np. wysyłając oferty handlowe obejmujące własne usługi, to w odniesieniu do takiego przetwarzania danych osobowych stanie się odrębnym administratorem ze wszystkimi tego konsekwencjami.

1.5. Odbiorca i strona trzecia

Odbiorcą danych osobowych może być każda osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią[49]. Prawodawca unijny zaznaczył jednak, że za odbiorców nie uznaje się organów publicznych, które otrzymują dane osobowe w ramach prowadzonego postępowania na podstawie prawa krajowego lub unijnego.

Okolicznością kwalifikującą dany podmiot jako odbiorcę danych osobowych jest to, czy dane zostały mu ujawnione. Rozporządzenie nie zawiera definicji pojęcia „ujawnienie danych osobowych", jednak z pewnością operacja ta stanowi przetwarzanie danych osobowych. Zgodnie bowiem z art. 4 pkt 2 RODO przez przetwarzanie należy rozumieć m.in. operacje ujawniania danych osobowych „poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie". W celu wyjaśnienia tego pojęcia w literaturze przedmiotu pojawiają się odwołania do słownikowej definicji terminu „ujawnianie"[50]. Wskazuje się

48 Artykuł 28 ust. 4 RODO.

49 Artykuł 4 pkt 9 RODO.

50 K. Witkowska, *Artykuł 4 pkt 9* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO…, s. 230; W. Chomiczewski, *Odbiorca* [w:] D. Lubasz (red.), *Meritum Ochrona Danych Osobowych*, Warszawa, 2020 r., s. 93.

zatem, że ujawnianie polega na czynieniu jawnym lub podawaniu do wiadomości tego, co było trzymane w tajemnicy[51]. W kontekście danych osobowych ujawnianie oznacza, że dane osobowe są przekazywane podmiotowi, który nie miał do nich wcześniej dostępu, albo że są tworzone takie warunki, w których podmiot ten może zapoznać się z danymi osobowymi. Przykładowo, ujawnieniem danych osobowych będzie nadanie określonej osobie uprawnień dostępowych do bazy danych zawierającej dane osobowe klientów i kontrahentów przedsiębiorcy. Wówczas taka osoba stanie się odbiorcą danych osobowych. Odbiorcą danych osobowych może być też inny administrator lub podmiot przetwarzający, któremu dane są ujawniane w celu realizacji określonych zadań (np. zawarcia umowy, wykonania usługi). Z ujawnieniem nie będziemy mieli natomiast do czynienia w sytuacji, gdy przedsiębiorca, będący administratorem, przekaże dane osobowe swojego klienta organom ścigania lub organom podatkowym na potrzeby prowadzonych przez nie postępowań. Ponadto, wskazuje się, że za odbiorców danych nie powinno się traktować pracowników lub współpracowników administratora pozostających pod kontrolą administratora[52].

Właściwe ustalenie odbiorców lub kategorii odbiorców danych osobowych jest jedną z powinności administratora i wpływa na sposób realizacji niektórych obowiązków wynikających z przepisów, jak choćby na zakres obowiązków informacyjnych czy na konieczność poinformowania tychże odbiorców o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania. Administrator ma również obowiązek wskazać kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych, w prowadzonym rejestrze czynności przetwarzania.

Z kolei za stronę trzecią na gruncie RODO uznaje się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe[53]. Definicja strony trzeciej została skonstruowana w oparciu o dwie przesłanki – pozytywną i negatywną. Przesłanka pozytywna odnosi się do wymogu zakwalifikowania osoby trzeciej jako osoby fizycznej, osoby prawnej, organu publicznego, jednostki lub innego podmiotu. Przesłanka negatywna nawiązuje

[51] Zob. definicję pojęcia „ujawniać" dostępną na stronie: https://sjp.pwn.pl/szukaj/ujawnić.html (dostęp: 29.01.2022 r.).

[52] W. Chomiczewski, *Odbiorca* [w:] D. Lubasz (red.), *Meritum…*, s. 92.

[53] Artykuł 4 pkt 10 RODO.

natomiast do oceny, czy dany podmiot jest administratorem, podmiotem przetwarzającym, osobą, której dane dotyczą, lub osobą przetwarzającą dane osobowe z upoważnienia administratora lub procesora. Pojęcie osoby, której dane dotyczą, zostało wyjaśnione na gruncie definicji pojęcia „dane osobowe"; należy więc przyjąć, że odnosi się ono do podmiotu danych osobowych, czyli zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę przetwarzającą dane osobowe z upoważnienia administratora lub procesora należy zaś uznać osobę zaliczaną do personelu administratora lub podmiotu przetwarzającego, przy czym za personel należy uważać zarówno pracowników, jak i inne osoby wypełniające obowiązki o podobnym charakterze (np. w ramach tymczasowego zatrudnienia), choć wyłącznie w zakresie, w jakim są one upoważnione do przetwarzania danych osobowych[54]. Pracownik, który uzyskuje dostęp do danych osobowych przetwarzanych przez pracodawcę-administratora, poza zakresem udzielonego mu upoważnienia i w celach innych niż cele pracodawcy, nie należy do tej kategorii, przez co w konsekwencji powinien być traktowany jako strona trzecia[55]. **Jeśli pracownik zacznie przetwarzać dane osobowe we własnych celach, innych niż cele określone przez pracodawcę, stanie się w tym zakresie odrębnym administratorem.** Innym przykładem podmiotu, który zwykle staje się stroną trzecią w odniesieniu do danych osobowych przetwarzanych przez administratora lub procesora, może być podmiot świadczący usługi sprzątania w siedzibie administratora lub procesora – personel takiego podmiotu nie jest upoważniony do przetwarzania danych osobowych, jednak w trakcie świadczenia usług może mieć dostęp do danych osobowych, np. zgromadzonych w dokumentacji przechowywanej na biurku lub w szufladach.

1.6. Przetwarzanie

Przetwarzanie zostało zdefiniowane na gruncie RODO jako „operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie"[56]. Zakres tego pojęcia jest bardzo szeroki i w praktyce obejmuje każde

[54] W kwestii upoważnienia do przetwarzania zob. art. 29 RODO.

[55] EROD, *Guidelines 07/2020…*, s. 29.

[56] Artykuł 4 pkt 2) RODO.

działanie, które ma za przedmiot dane osobowe. Ocenę, czy dochodzi do przetwarzania, należy więc poprzedzić rzetelną weryfikacją, czy informacje, które mają być poddane różnego rodzaju operacjom, stanowią dane osobowe. Błędne uznanie, że informacje takie nie są kwalifikowane jako dane osobowe, może powodować brak świadomości po stronie administratora co do faktu, że przetwarza on dane osobowe, a w konsekwencji brak wiedzy o obowiązkach, jakie spoczywają na nim w świetle RODO. Ocena, czy ma miejsce przetwarzanie danych osobowych, czy nie, powinna mieć bowiem charakter obiektywny, to znaczy powinna być dokonywana w oparciu o analizę okoliczności faktycznych towarzyszących przetwarzaniu, nie zaś w oparciu o to, czy podmiot dokonujący różnych operacji na danych osobowych realizuje je świadomie lub z własnej woli.

Przykładem przetwarzania danych osobowych może być wprowadzanie danych osobowych klientów do programu płatniczego, tworzenie bazy danych w celu wysyłki newslettera, przechowywanie danych osobowych w chmurze, profilowanie użytkowników Internetu w celu dostarczania spersonalizowanych reklam, pozyskanie danych osobowych w celu zawarcia umowy, przekazanie dokumentacji zawierającej dane osobowe wyspecjalizowanemu podmiotowi w celu jej zniszczenia itp.

2. Realizacja praw podmiotów danych w kontekście zasady przejrzystości

2.1. Uwagi ogólne

Prawodawca unijny przyznał podmiotom danych osobowych na mocy RODO trzy kategorie uprawnień:

1. uprawnienia o charakterze informacyjnym,
2. uprawnienia korekcyjne,
3. uprawnienia o charakterze zakazowym.

Pierwsza kategoria, czyli uprawnienia o charakterze informacyjnym, obejmuje prawo dostępu do informacji związanych z przetwarzaniem danych osobowych, realizowane przez administratora poprzez spełnienie obowiązków informacyjnych z art. 13 lub 14 RODO, oraz prawo dostępu do danych osobowych, które są przetwarzane przez konkretnego administratora, realizowane przez podmiot danych na mocy art. 15 RODO. Druga kategoria uprawnień to uprawnienia korekcyjne, przejawiające się w prawie do sprostowania danych osobowych na podstawie art. 16 RODO, tj. do aktualizacji i poprawienia nieprawidłowych danych osobowych przetwarzanych przez administratora. Trzecia kategoria, czyli uprawnienia o charakterze zakazowym, jest najszerszą grupą praw przysługujących osobom, których dane dotyczą, obejmującą prawo do:

– usunięcia danych, zwane też prawem do bycia zapomnianym (art. 17 RODO),
– ograniczenia przetwarzania danych osobowych (art.18 RODO),
– przenoszenia danych osobowych (art. 20 RODO),
– sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO),
– niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu danych osobowych, która wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa (art. 22 RODO).

Uprawnienia informacyjne, w zakresie w jakim obejmują prawo dostępu do informacji związanych z przetwarzaniem danych osobowych na podstawie art. 13 i 14 RODO, powinny

być realizowane samodzielnie przez administratora. Przekazanie odpowiednich informacji na temat przetwarzania danych osobowych jest jednym z jego podstawowych obowiązków, który materializuje się już w chwili pozyskiwania danych osobowych. Natomiast w przypadku pozostałych uprawnień, czyli prawa dostępu do danych oraz uprawnień korekcyjnych i zakazowych, wymagane jest działanie po stronie podmiotu danych osobowych. Są one realizowane na skutek inicjatywy osoby, której dane dotyczą. Aktywność po stronie podmiotu danych jest więc przesłanką *sine qua non* dalszych działań administratora, przy czym nie jedyną – dla każdego z uprawnień prawodawca unijny przewidział również odrębne wymogi. Oznacza to, że każde zgłoszone przez podmiot danych żądanie podlega weryfikacji i ocenie administratora pod kątem spełnienia przesłanek wskazanych w art. 15–22 RODO. W razie braku spełnienia choćby jednej przesłanki, administrator może odmówić realizacji zgłoszonego żądania.

Zakres uprawnień przysługujących podmiotowi danych może być różny, w zależności od różnych okoliczności, w tym od podstawy prawnej, w oparciu o którą dane osobowe są przetwarzane, od spełnienia przez podmiot danych warunków skorzystania z danego prawa czy też od możliwości, np. technicznych lub finansowych, administratora. Przykładowo prawo do wyrażenia sprzeciwu wobec przetwarzania danych osobowych materializuje się tylko wtedy, kiedy dane są przetwarzane na podstawie art. 6 ust. 1 lit. e) RODO (tj. gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi) lub na podstawie art. 6 ust. 1 lit. f) RODO (tj. gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią). Jeśli dane osobowe są przetwarzane na potrzeby wykonania zawartej umowy lub w celu wykonania obowiązku prawnego (np. przechowywane w związku z realizacją obowiązków podatkowych), prawo do sprzeciwu nie będzie przysługiwało. Co więcej, oprócz odpowiedniej podstawy przetwarzania muszą być spełnione dodatkowe przesłanki, o których mowa w przepisie, w tym m.in. uzasadnienie wniesienia sprzeciwu przez podmiot danych przyczynami związanymi z jego szczególną sytuacją.

Prawa przysługujące osobom, których dane są przetwarzane, są skorelowane z różnymi obowiązkami po stronie administratora, ale też innych podmiotów, którym dane zostały ujawnione. W kolejnych punktach niniejszego rozdziału opisano ogólne obowiązki związane z realizacją praw podmiotów danych. Mają one charakter uniwersalny, co oznacza, że odnoszą się do wszystkich uprawnień podmiotów danych. Szczegółowe obowiązki

administratorów wynikające z realizacji konkretnych uprawnień podmiotów danych zostały omówione we fragmentach dotyczących wykonywania poszczególnych praw.

2.2. Przejrzystość jako kluczowa zasada w relacji pomiędzy administratorem a podmiotem danych

Na realizację praw podmiotów danych należy patrzeć przez pryzmat zasady przejrzystości, stanowiącej jedną z podstawowych zasad dotyczących przetwarzania danych osobowych na mocy RODO[57]. Prawodawca unijny, mając na względzie autonomię informacyjną jednostek z jednej strony, a z drugiej konieczność zapewnienia równowagi informacyjnej w relacji administrator-podmiot danych, nałożył na administratora szereg obowiązków, których celem jest dostarczenie podmiotowi danych wiedzy na temat okoliczności związanych z przetwarzaniem jego danych osobowych. Wiedza ta musi być przekazywana w sposób zrozumiały dla osoby, której dane są przetwarzane, czyli w sposób pozwalający na podjęcie świadomej decyzji w zakresie przetwarzania danych osobowych, np. decyzji co do udostępnienia swoich danych osobowych konkretnemu administratorowi, zakresu przekazywanych danych. Przejrzyste informowanie o przetwarzaniu danych osobowych ma też na celu podniesienie ogólnego poziomu świadomości społeczeństwa co do przetwarzania danych osobowych, a w konsekwencji również zwrócenie uwagi na zagrożenia, jakie wiążą się z przetwarzaniem danych osobowych oraz na sposoby ich mitygacji lub niwelowania potencjalnych skutków. Posiadanie odpowiedniej wiedzy przez osobę, której dane są przetwarzane, sprzyja wzmacnianiu jej pozycji względem administratora, choćby poprzez

[57] Zob. art. 5 ust. 1 lit. a) RODO. Przejrzystość, obok wymogu zgodnego z prawem i rzetelnego przetwarzania, jest nie tylko jedną z fundamentalnych zasad przetwarzania danych osobowych, ale również zasadą stanowiącą stały element prawa UE. Jak wskazała Grupa Robocza Art. 29 (organ zastąpiony na mocy RODO przez EROD) w wytycznych dotyczących przejrzystości, jej celem jest „zapewnienie zaufania do procesów, które mają wpływ na obywatela, dzięki umożliwieniu mu ich zrozumienia, a w razie konieczności również zgłoszenia wobec nich sprzeciwu" – zob. Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679*, WP260, s. 5. Warto w tym miejscu nadmienić, że wiele dokumentów wydanych przez Grupę Roboczą Art. 29, jeszcze pod rządami obowiązującej przed RODO Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, zostało przyjętych przez EROD i w niezbędnym zakresie zaktualizowanych pod kątem nowych przepisów.

ogólną orientację co do działań podejmowanych przez administratora oraz znajomość przysługujących jej praw. W rezultacie sprzyja to sprawowaniu bardziej efektywnej kontroli nad działalnością administratora i zmniejsza ryzyko nadużyć z jego strony.

Zasada przejrzystości powinna być realizowana na różnych etapach procesu przetwarzania danych osobowych, zarówno przed lub w chwili rozpoczęcia przetwarzania, czyli w chwili pozyskiwania danych osobowych, jak i w poszczególnych momentach cyklu przetwarzania, np. w trakcie informowania podmiotu danych o przetwarzaniu i przysługujących mu prawach, w trakcie realizacji żądań zgłoszonych przez podmiot danych, aktualizowania obowiązków informacyjnych itd.[58] Cały proces komunikacji pomiędzy administratorem a osobą, której dane dotyczą, powinien być zorganizowany z uwzględnieniem tej zasady i jej praktycznych wymogów opisanych szczegółowo w art. 12 RODO.

2.3. Przejrzystość w świetle art. 12 RODO – analiza wymogów w zakresie komunikacji pomiędzy administratorem a podmiotem danych

Zgodnie z art. 12 ust. 1 RODO administrator został zobowiązany do udzielania informacji wymienionych w art. 13 i 14 RODO oraz do prowadzenia wszelkiej komunikacji związanej z realizacją uprawnień przez osobę, której dane dotyczą, w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. W stosownych przypadkach przekazywane informacje mogą być dodatkowo wizualizowane, jeśli będzie to sprzyjać lepszemu lub łatwiejszemu zrozumieniu komunikatu. Administrator powinien komunikować się z podmiotem danych w sposób zwięzły, efektywny i tak, aby nie przytłoczyć go informacjami. Nadmiar informacji lub brak uporządkowania treści w różnych dokumentach, komunikatach czy oświadczeniach, z którymi podmiot danych ma się zapoznać, może działać zniechęcająco i wywoływać tzw. efekt zmęczenia informacyjnego. W rezultacie może to prowadzić do niezaznajomienia się podmiotu danych

[58] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 6.

z kierowanym do niego przekazem. Zaleca się zatem, zwłaszcza w środowisku internetowym, stosowanie warstwowych komunikatów umożliwiających przejście do konkretnej części informacji dotyczących przetwarzania danych osobowych, do której osoba zapoznająca się z komunikatem chce się natychmiast dostać, tj. w taki sposób, aby nie musiała przewijać długiego tekstu w poszukiwaniu konkretnych kwestii[59]. Poruszanie się po obszernych komunikatach kierowanych do osób, których dane są przetwarzane, np. po politykach prywatności zamieszczanych na stronach internetowych, z pewnością ułatwiają np. spisy treści zamieszczone na początku i stosowanie aktywnych linków odsyłających bezpośrednio do danej części komunikatu. Co więcej, informacje dotyczące przetwarzania danych osobowych powinny być wyraźnie oddzielone od innych treści, np. od regulaminów, postanowień umownych, ogólnych warunków korzystania z usług.

Wymóg „zrozumiałości" informacji jest ściśle powiązany z wymogiem stosowania jasnego i prostego języka. Administrator powinien dopasować język komunikatu do odbiorcy, co oznacza, że powinien posiadać wiedzę na temat osób, których dane osobowe przetwarza, i wykorzystać ją do sformułowania przekazu zrozumiałego dla docelowej grupy odbiorców. Przykładowo, inaczej mogą być sformułowane komunikaty kierowane do wysokiej klasy specjalistów z określonej branży, w przypadku których administrator może założyć wyższy stopień zrozumienia treści wśród odbiorców, niż komunikaty dedykowane dzieciom lub osobom niepełnosprawnym[60]. Jeśli administrator nie jest w stanie określić grupy odbiorców lub jeśli grupa ta jest różnorodna, powinien on formułować informacje w taki sposób, aby były one zrozumiałe dla przeciętnego odbiorcy, a zatem powinny być pozbawione skomplikowanych określeń (np. technicznych lub prawnych), pojęć abstrakcyjnych lub wieloznacznych, złożonych struktur zdaniowych. Informacje te powinny być zawsze jednoznaczne i sformułowane tak, aby nie pozostawiać dowolności interpretacji[61]. Z kolei łatwy dostęp do informacji oznacza, że podmiot danych nie powinien być zmuszony do wyszukiwania informacji dotyczących przetwarzania danych osobowych. Miejsce i sposób dostępu do takich informacji powinny być oczywiste czy wręcz intuicyjne. Łatwo dostępną informacją będzie więc taka, która jest bezpośrednio udzielana podmiotowi danych, wyraźnie oznaczona i odróżniona od innych przekazywanych informacji, podana w formie odpowiedzi na często zadawane pytania czy też dostępna po kliknięciu w stosowny link, przy czym

[59] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 7.

[60] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 7–8, 11–12.

[61] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 9.

zaznacza się, że informacja powinna być zawsze dostępna najwyżej po dwóch kliknięciach[62]. W odniesieniu do aplikacji lub innych programów pobieranych przez użytkowników Internetu informacje dotyczące ochrony prywatności powinny być dostępne zarówno z poziomu sklepu internetowego, jak i z poziomu samej aplikacji i programu.

Jak wskazano w art. 12 ust. 1 RODO, informacje przekazywane osobie, której dane dotyczą, powinny być udzielane na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Domyślną formą komunikacji jest forma pisemna[63]; sprzyja ona też realizacji zasady rozliczalności, gdyż przekazywanie informacji w formie pisemnej ułatwia administratorowi wykazanie, że spełnił swoje obowiązki, np. w odniesieniu do zakresu przekazywanych informacji czy co do spełnienia wymogu przejrzystości. RODO nie wyklucza jednak innych form komunikacji, w tym formy elektronicznej, ustnej czy obrazkowej. Forma ta powinna być dostosowana do sytuacji i do odbiorcy przekazu, np. w przypadku przetwarzania danych osobowych dzieci. Informacje o przetwarzaniu tych danych powinny być przekazywane w sposób bardzo prosty i przystępny dla dzieci, m.in. za pomocą komiksów, infografik, kreskówek, animacji itp. Przekazywanie informacji za pomocą pisemnych środków elektronicznych, np. na stronach internetowych, może następować w sposób warstwowy, tak aby osoby odwiedzające stronę mogły zapoznać się z najbardziej interesującymi dla nich fragmentami informacji. Jednocześnie, informacje te powinny być przekazywane w sposób uporządkowany, z zachowaniem odpowiedniej hierarchii wynikającej z treści, a przy tym powinny być łatwo dostępne, tj. zawarte w jednym miejscu na stronie (np. w zakładce na stronie w panelu klienta, gdzie można znaleźć wszystkie relewantne informacje z perspektywy ochrony danych osobowych, zmienić preferencje w tym zakresie) lub w jednym dokumencie poświęconym zagadnieniom ochrony prywatności (np. w polityce prywatności). Jak wskazuje Grupa Robocza Art. 29, informacje na temat przetwarzania danych osobowych przekazywane drogą elektroniczną nie muszą ograniczać się wyłącznie do stosowania warstwowych komunikatów i oświadczeń, ale mogą obejmować również inne mechanizmy dostarczania informacji, jak np. wyskakujące powiadomienia kontekstowe typu „just-in-time", powiadomienia za pomocą funkcji 3D Touch, powiadomienia wyświetlające się po najechaniu kursorem oraz pulpity nawigacyjne prywatności[64]. Administrator może dodatkowo skorzystać z niepisemnych środków elektronicznych, jak filmy wideo

[62] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 8–9.

[63] Tak też wskazuje Grupa Robocza Art. 29, zob. *Wytyczne w sprawie przejrzystości…*, s. 12.

[64] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 13.

lub powiadomienia głosowe; takie środki mogą stanowić dobre uzupełnienie przekazu kierowanego w formie pisemnej. Ponadto, zgodnie z art. 12 ust. 1 RODO, jeżeli osoba, której dane dotyczą, zgłosi takie żądanie, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość tej osoby. Sposób potwierdzenia tożsamości powinien prowadzić do uzyskania przez administratora wystarczającej pewności co do tożsamości danej osoby i nie powinien opierać się wyłącznie na przyjęciu zapewnienia, że jest ona osobą o danym imieniu i nazwisku[65]. Należy jednak podkreślić, że wymóg weryfikacji tożsamości aktualizuje się wyłącznie w kontekście realizacji praw podmiotów danych, o których mowa w art. 15–22 RODO, nie ma zaś zastosowania w przypadku wykonywania przez administratora obowiązków informacyjnych na mocy art. 13 lub art. 14 RODO. W ramach realizacji obowiązków informacyjnych administrator może więc udzielać informacji o przetwarzaniu danych osobowych w formie ustnej, np. poprzez bezpośredni kontakt lub w sposób zautomatyzowany. Grupa Robocza Art. 29 zaznacza przy tym, że gdy dochodzi do ustnego przekazywania informacji na podstawie art. 13 lub art. 14 RODO lub gdy podmiot danych zażąda prowadzenia ustnej komunikacji, administrator powinien umożliwić osobie, której dane dotyczą, ponowne odsłuchanie nagranych wiadomości[66]. Jest to niezbędne, zwłaszcza wtedy, kiedy żądanie takie zostało zgłoszone przez osobę słabowidzącą lub mającą problemy z dostępem do informacji w formie pisemnej lub z ich zrozumieniem. Jednocześnie, na potrzeby spełnienia wymogu rozliczalności, administrator powinien odpowiednio udokumentować okoliczności związane z przekazywaniem informacji i prowadzeniem komunikacji w formie ustnej, w tym okoliczności dotyczące zgłoszonego wniosku o ustne przekazanie informacji, metody wykorzystanej w celu weryfikacji tożsamości podmiotu danych oraz faktu przekazania informacji.

Na koniec warto podkreślić, że mimo zawarcia w art. 12 RODO konkretnych wymogów co do realizacji zasady przejrzystości w odniesieniu do informowania o przetwarzaniu danych osobowych i prowadzenia komunikacji z podmiotem danych, a także mimo wydania obszernych wyjaśnień i wytycznych w tym zakresie przez Grupę Roboczą Art. 29, faktyczny sposób realizacji tej zasady przez administratora zależy od kontekstu przetwarzania, a przede wszystkim od kategorii osób, których dane są przetwarzane, i w konsekwencji do których kierowany jest przekaz. **Administrator ma zatem swobodę wyboru co do sposobów realizacji zasady przejrzystości.** W szczególności może korzystać z różnych nowoczesnych

[65] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 14.

[66] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 15.

form przekazu, w tym bazujących na nowych technologiach, jeśli uzna, że taka forma spełnia wymóg przejrzystości komunikacji z podmiotem danych oraz ułatwia mu właściwe zrozumienie przekazu. Z uwagi na to, że zasada przejrzystości musi być realizowana przez cały czas trwania cyklu przetwarzania, administrator powinien też obserwować reakcje i zachowania podmiotów danych, które mogą dostarczać informacji o rzeczywistym stopniu zrozumienia przekazu. Przykładowo, otrzymywanie wielu pytań ze strony osób, których dane dotyczą, na temat szczegółowych celów przetwarzania lub dokładnego czasu trwania przetwarzania, może sugerować, że informacje na ten temat nie są wystarczająco jasno lub precyzyjnie zakomunikowane. Wówczas administrator powinien podjąć działania zmierzające do usunięcia tego rodzaju problemów, np. poprzez zamieszczenie dodatkowych wyjaśnień w polityce prywatności lub stworzenie listy najczęściej zadawanych pytań i jej opublikowanie wraz z odpowiedziami na stronie internetowej. Administrator musi też pamiętać, że każdą decyzję dotyczącą sposobu zapewnienia przejrzystości musi być w stanie umotywować i wykazać, dlaczego taki sposób w jego ocenie jest adekwatny – tego wymaga od niego zasada rozliczalności.

3. Realizacja praw podmiotów danych – zagadnienia ogólne

3.1. Adresat żądania

Wyłącznym adresatem żądań podmiotów danych jest administrator i to na nim spoczywa odpowiedzialność za prawidłową realizację praw podmiotów danych. Nie oznacza to jednak, że żądania te mogą być kierowane tylko do administratora – w praktyce może zdarzyć się, że osoba, której dane dotyczą, zwróci się z żądaniem realizacji praw do jednego ze współadministratorów lub do podmiotu przetwarzającego. W zależności od ukształtowania relacji współadministrowania lub powierzenia przetwarzania, różne obowiązki mogą spoczywać na podmiotach zaangażowanych w przetwarzanie danych osobowych.

Współadministratorzy zobowiązani są ustalić między sobą podział obowiązków wynikających z RODO, w tym związanych z wypełnianiem obowiązków informacyjnych na mocy art. 13 i art. 14 RODO oraz realizacją praw podmiotów danych[67]. Mogą więc uzgodnić, że jeden lub kilku współadministratorów odpowiedzialnych jest za komunikację z osobami, których dane dotyczą, poprzez przyjmowanie zgłaszanych przez nich żądań, udzielanie odpowiedzi oraz faktyczną realizację praw, czyli utworzenie punktu kontaktowego dla osób, których dane dotyczą. Podział obowiązków powinien być funkcjonalny i korelować z rodzajem działań i czynności przetwarzania podejmowanych przez poszczególnych współadministratorów, a przez to gwarantować skuteczną realizację żądań podmiotów danych. Przykładowo, powierzenie realizacji praw podmiotów danych współadministratorowi, który nie ma dostępu do przetwarzanych danych osobowych, gdyż jego rola ogranicza się do współdecydowania o celach i sposobach przetwarzania, raczej nie znajduje uzasadnienia. Nie oznacza to, że realizacja żądania zgłoszonego przez podmiot danych jest niemożliwa; współadministrator musi mieć wówczas zapewnioną realną możliwość pozyskania od pozostałych współadministratorów informacji dotyczących przetwarzania danych osobowych

[67] Artykuł 26 ust. 1 RODO. Współadministratorzy nie muszą ustalać podziału obowiązków, jeśli podział ten wynika z prawa unijnego lub prawa państwa członkowskiego, któremu administratorzy ci podlegają.

lub możliwość przekazania żądania podmiotu danych właściwemu współadministratorowi. Z organizacyjnego punktu widzenia nie jest to jednak dogodne rozwiązanie.

Podział obowiązków pomiędzy współadministratorami powinien być zakomunikowany osobom, których dane dotyczą, po to, aby miały one wiedzę, do kogo zwrócić się w celu skorzystania z przysługujących im praw. Mimo to, jak stanowi art. 26 ust. 3 RODO, niezależnie od poczynionych ustaleń, podmiot danych może wykonywać swoje prawa w odniesieniu do każdego ze współadministratorów i przeciwko każdemu z nich. Przyjęcie takiego rozwiązania ma na celu zapewnienie podmiotom danych skutecznej i pełnej realizacji ich praw, bez względu na stopień skomplikowania relacji pomiędzy współadministratorami. Nierzadko relacje współadministrowania danymi zachodzą pomiędzy podmiotami mającymi siedziby w różnych państwach, powiązanymi ze sobą gospodarczo lub kapitałowo czy prowadzącymi działalność na skalę międzynarodową – w takich sytuacjach trudno nakładać na podmiot danych obowiązek aktywnego poszukiwania właściwego adresata żądania, które chce zrealizować. Niezależnie od charakteru powiązań pomiędzy podmiotami, podmiot danych powinien móc łatwo ustalić, do którego z nich może się zwrócić w celu wykonania przysługujących mu praw. Na administratorze spoczywa bowiem ogólny obowiązek przyjęcia procedur ułatwiających podmiotom danych wykonywanie ich praw[68], co w kontekście relacji współadministrowania może być realizowane m.in. poprzez przejrzyste i zrozumiałe dla podmiotów danych ustalenie, do którego administratora może się zwrócić w celu najsprawniejszego wykonania żądania[69].

Administratorzy korzystający z usług podmiotu przetwarzającego również powinni uzgodnić z nim kwestie dotyczące realizacji praw podmiotów danych. Należy zwrócić uwagę, że obowiązek ten wynika wprost z przepisów rozporządzenia, a dokładnie z art. 28 ust. 3 lit. e) RODO, który stanowi, iż podmiot przetwarzający w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw. Pomoc w wywiązywaniu się z powyższych obowiązków może polegać

[68] Zob. motyw 59 i art. 12 ust. 2 RODO.

[69] Jeszcze raz warto podkreślić, że podmiot danych może zwrócić się do każdego ze współadministratorów ze swoim żądaniem. Jeśli jednak zwróci się do tego, który w świetle poczynionych ustaleń między współadministratorami nie odpowiada za realizację praw podmiotów danych, proces realizacji tego prawa w praktyce może się wydłużyć, chociażby z uwagi na konieczność przekazania żądania do innego współadministratora.

na przekazywaniu administratorom szczegółowych informacji na temat przetwarzania danych osobowych konkretnych osób fizycznych czy faktycznej realizacji tych praw, np. poprzez usunięcie lub sprostowanie danych osobowych objętych żądaniem podmiotu danych, jeśli ich przetwarzanie zostało powierzone procesorowi. Takie rozwiązanie jest zasadne, zwłaszcza gdy podmiot przetwarzający wchodzi w bezpośrednią interakcję z podmiotem danych w związku z realizacją usług na rzecz administratora.

Można to zobrazować na takim przykładzie: administrator prowadzący księgarnię internetową powierza agencji marketingowej przygotowywanie i wysyłkę miesięcznych newsletterów, prowadzenie kont w mediach społecznościowych, organizację konkursów, akcji promocyjnych itp. Agencja działa jako procesor, ponieważ przetwarza dane klientów administratora (aktualnych lub potencjalnych) w celu realizacji jego interesów – w tym przypadku w celu prowadzenia działań marketingowych. Na potrzeby prowadzonych działań agencja wyznaczyła osobę kontaktową, udzielającą odpowiedzi na różne pytania klientów. W takim przypadku ustanowienie tej osoby jako osoby upoważnionej do przyjmowania żądań podmiotów danych znajduje uzasadnienie – przede wszystkim z perspektywy organizacyjnej, ponieważ ułatwi to kontrolę nad wypływającymi żądaniami i nad ich realizacją. W umowie powierzenia przetwarzania danych zawartej pomiędzy administratorem a procesorem można ustalić, że procesor będzie odpowiedzialny nie tylko za przyjmowanie żądań podmiotów danych, ale również za ich realizację, np. gdy podmiot danych chce zrezygnować z udziału w konkursie lub z otrzymywania newsletterów i w tym celu zgłasza sprzeciw wobec przetwarzania jego danych osobowych. Jeśli umowa powierzenia przewiduje wyraźne upoważnienie dla procesora do realizacji żądań praw podmiotów danych, to procesor, po uprzedniej weryfikacji zasadności konkretnego żądania, powinien je wykonać[70]. Jeśli umowa powierzenia nie zawiera postanowień w tym zakresie, procesor nie jest zobowiązany, ani nawet uprawniony do wchodzenia w interakcję z podmiotem danych, udzielania odpowiedzi na żądanie czy do jego realizacji. Wówczas żądanie podmiotu danych, które do niego wpłynęło, powinien niezwłocznie przekazać do administratora, jednocześnie informując podmiot danych o przyjęciu zgłoszenia i przekazaniu go do podmiotu odpowiedzialnego za jego realizację, czyli do administratora[71].

[70] W takiej sytuacji podmiot przetwarzający działa jako pełnomocnik administratora, o czym powinien poinformować podmiot danych, udzielając odpowiedzi na żądanie.

[71] Jest to wskazane z punktu widzenia zasady przejrzystości. Podmiot danych powinien mieć świadomość, że jego żądanie wpłynęło do procesora, a nie bezpośrednio do administratora.

Jak widać, kluczowe są szczegółowe postanowienia zawartej umowy powierzenia, ponieważ strony mogą różnie uzgodnić zakres swoich obowiązków. Niemniej jednak należy pamiętać, że nawet wtedy, kiedy podmiot przetwarzający ma w imieniu administratora realizować żądania podmiotów danych, to i tak nie zwalnia to samego administratora z odpowiedzialności za ich prawidłowe wykonywanie. Administrator musi mieć więc zapewnione skuteczne narzędzia kontroli nad procesorem i powinien tę kontrolę systematycznie sprawować, np. poprzez regularne sprawdzanie, czy procesor prowadzi rejestr praw podmiotów danych, w jaki sposób udziela odpowiedzi na zgłaszane żądania, czy terminowo realizuje prawa podmiotów danych.

3.2. Weryfikacja tożsamości

Realizacja żądania prawa podmiotu danych musi być poprzedzona identyfikacją osoby występującej z żądaniem. Jest to konieczne z kilku przyczyn – przede wszystkim w celu ustalenia, czy administrator przetwarza dane osoby fizycznej, której dotyczy żądanie, a jeśli tak – w celu prawidłowego powiązania danych znajdujących się w zasobach administratora z osobą występującą z żądaniem. Ponadto prawidłowa weryfikacja tożsamości podmiotu danych jest niezbędna w celu zapewnienia zasady poufności, a w niektórych przypadkach również zasady integralności. Wdrożone przez administratora środki bezpieczeństwa muszą bowiem zapewniać właściwą ochronę przed nieuprawnionym dostępem do przetwarzanych przez niego danych osobowych, w tym przed błędnym ujawnieniem danych osobowych w toku realizacji praw podmiotów danych na skutek błędnej identyfikacji osoby występującej z żądaniem. Podobnie jest w odniesieniu do integralności danych – administrator nie może dopuścić przykładowo do tego, aby na skutek nieprawidłowej identyfikacji podmiotu danych usunąć czy ograniczyć przetwarzanie danych osoby, która w rzeczywistości nie wystąpiła z tego rodzaju żądaniem. W takich sytuacjach może dojść nie tylko do przypadkowej utraty danych osobowych, ale także mogą zaistnieć negatywne konsekwencje dla osoby, której dane są przetwarzane (np. ograniczenie dostępu do świadczonej usługi, wykreślenie z listy subskrybentów itp.).

Wybór sposobu identyfikacji osób realizujących prawa wynikające z RODO należy do administratora. RODO nie narzuca w tym zakresie żadnych konkretnych rozwiązań; jedynie w motywie 64 RODO prawodawca unijny zawarł ogólne zalecenie, aby administrator korzystał z „wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby,

której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych". Sposób weryfikacji tożsamości powinien być zatem dostosowany do kontekstu i charakteru przetwarzania. Wśród przykładowych metod identyfikacji podmiotu danych można wymienić:

– zalogowanie się do konta użytkownika w serwisie administratora[72];
– zadanie pytań kontrolnych w oparciu o dane osobowe, do których administrator ma dostęp;
– żądanie podania dodatkowych informacji w celu identyfikacji;
– żądanie podania jednorazowego kodu weryfikacyjnego wysłanego przez administratora na adres e-mail lub numer telefonu podany wcześniej przez podmiot danych;
– autoryzacja żądania za pośrednictwem powiadomienia push w aplikacji dostarczanej przez administratora.

Z pewnością administrator, wybierając metodę identyfikacji, powinien mieć na uwadze kategorie danych osobowych, jakie przetwarza, a w konsekwencji to, czy zgłoszone żądanie może dotyczyć danych osobowych o podwyższonym stopniu ochrony. Administrator zawsze musi dochować staranności przy uwierzytelnianiu podmiotu zgłaszającego żądanie, ale szczególnej staranności powinien dochować, jeśli przetwarza dane wrażliwe. Może wtedy skorzystać z bardziej rozbudowanych metod weryfikacji (np. kilkuetapowych sposobów uwierzytelniania), uzasadniając to istnieniem większego ryzyka dla ochrony praw i wolności osób, których dane są przetwarzane[73]. Jest to zgodne z przyjętym na gruncie RODO podejściem opartym na ryzyku – im większe ryzyko dla podmiotu danych, tym wyższy poziom zabezpieczeń powinien być wdrożony przez administratora. Analogicznie jest więc przy realizacji praw podmiotów danych

[72] Często zalogowanie się do swojego konta umożliwia bezpośrednie zarządzanie danymi osobowymi przetwarzanymi w serwisie, np. poprzez zmianę danych niepoprawnych, wprowadzenie nowych danych, zgłoszenie żądania dostępu do danych, zgłoszenie sprzeciwu wobec przetwarzania itp. Opcje te są zwykle dostępne z poziomu konta użytkownika w zakładce dedykowanej zasadom prywatności i ochrony danych osobowych.

[73] Zob. przykładowo decyzję PUODO z dn. 10.12.2018 r. (ZSPR.440.783.2018), gdzie organ uznał, że podwójna weryfikacja za pomocą numeru PESEL oraz serii i numeru dowodu osobistego przed przekazaniem dostępu do danych chronionych tajemnicą bankową, a zatem danych wrażliwych, jest zasadna, ponieważ pozwala ustalić w sposób niebudzący wątpliwości tożsamość osoby wnioskodawcy. Stanowisko to jest częściowo krytykowane – zob. P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, komentarz do art. 15 RODO, gdzie autorzy wskazują, że proces weryfikacji danych osób wnioskujących o dostęp do treści swoich danych powinien wykluczać dublowanie danych weryfikacyjnych.

– im większe ryzyko dla podmiotu danych związane z ewentualną błędną realizacją żądania, tym bardziej zasadne wprowadzenie rozbudowanych metod identyfikacji podmiotu danych, nawet powiązanych z żądaniem podania dodatkowych informacji. Na możliwość żądania podania dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą, wskazuje wprost art. 12 ust. 6 RODO, przy czym warto zaznaczyć, że żądanie dodatkowych informacji może nastąpić wówczas, gdy administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie. Zakres dodatkowych informacji wymaganych przez administratora powinien być ograniczony do niezbędnego minimum – zgodnie z zasadą minimalizacji danych, a informacje pozyskane w ten sposób powinny być usunięte po osiągnięciu celu przetwarzania – zgodnie z zasadą ograniczenia celu[74]. Należy przy tym pamiętać, że dobór metody weryfikacji tożsamości powinien z jednej strony zapewniać skuteczną i co do zasady pozbawioną ryzyka błędu identyfikację osoby występującej z żądaniem, a z drugiej – nie powinien działać odstraszająco i zniechęcająco na podmiot danych. Zbyt skomplikowane metody weryfikacji, połączone z gromadzeniem nadmiarowych danych, lub nieadekwatne względem ryzyka związanego z przetwarzaniem, nie powinny być stosowane. Przykładowo, sklep internetowy prowadzący sprzedaż ubrań nie powinien żądać na potrzeby identyfikacji przesłania skanu dokumentu potwierdzającego tożsamość osoby występującej z żądaniem.

W praktyce często zdarza się, że podmiot danych występuje z kilkoma żądaniami jednocześnie lub w krótkich odstępach czasowych, np. najpierw żąda dostępu do danych, a następnie zgłasza sprzeciw wobec przetwarzania lub żąda usunięcia jego danych. W takich sytuacjach weryfikacja tożsamości może co do zasady być przeprowadzona jednorazowo

[74] Dane te mogą być przechowywane przykładowo do zakończenia procesu realizacji żądania zgłoszonego przez podmiot danych. Mogą być też przetwarzane po zakończeniu tego procesu, ale tylko przez czas niezbędny do wykazania prawidłowości identyfikacji podmiotu danych i sposobu realizacji zgłoszonego żądania, w tym na potrzeby uzasadnienia braku realizacji żądania podmiotu danych (np. w razie wniesienia przez osobę występującą z żądaniem skargi do organu nadzorczego). W żadnym wypadku administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania, o czym stanowi wyraźnie motyw 64 RODO.

przed realizacją pierwszego żądania[75]. Zdarza się również, że administrator nie jest w stanie zidentyfikować osoby zgłaszającej żądanie, np. gdy przetwarza wyłącznie dane zanonimizowane. Stanowi o tym art. 11 ust. 1 RODO, wskazując, że jeśli cele, w których administrator przetwarza dane osobowe, nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, nie ma on obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zrealizować jej żądanie. W takim przypadku administrator powinien poinformować osobę, od której wpłynęło żądanie, o braku możliwości identyfikacji. W konsekwencji administrator nie jest zobowiązany do realizacji praw podmiotów danych wymienionych w art. 15–20 RODO, za jednym wyjątkiem – gdy podmiot danych w celu wykonania przysługujących mu praw dostarczy administratorowi dodatkowych informacji pozwalających na identyfikację[76]. Jednakże nawet w takiej sytuacji administrator może odmówić przyjęcia dodatkowych informacji, jeśli jest w stanie wykazać, że przetwarzane przez niego dane nie mają już charakteru danych osobowych, gdyż nie pozwalają na jednoznaczną identyfikację osoby fizycznej; gromadzenie takich informacji wykraczałoby bowiem poza cel przetwarzania, naruszając zasadę minimalizacji danych, ponieważ i tak nie pozwoliłoby na weryfikację tożsamości podmiotu danych i realizację jego żądania.

3.3. Sposób i termin realizacji żądania

Podmiot danych może zgłosić swoje żądanie w dowolnej formie: ustnie, na piśmie, elektronicznie itp. Nie jest związany sposobem określonym przez administratora – nawet jeśli administrator udostępnia specjalny formularz w celu realizacji praw przez podmiot danych lub umożliwia zarządzanie danymi po zalogowaniu do konta użytkownika, podmiot danych nie musi korzystać ze sposobów przewidzianych w tym celu przez administratora. Sposoby te mogą mieć jedynie na celu ułatwienie podmiotowi danych realizacji jego praw. W żadnym

[75] W celu usprawnienia procesu realizacji praw podmiotów danych warto każdemu zgłoszeniu przypisywać numer identyfikacyjny. Wówczas podmiot danych może powoływać się na ten numer, a administrator może odstąpić od ponownej weryfikacji tożsamości w razie zgłoszenia kolejnego żądania przez podmiot danych w ramach tej samej komunikacji. Niemniej jednak administrator nie powinien odstępować od ponownej weryfikacji tożsamości podmiotu danych w razie zmiany przez podmiot danych kanału komunikacji – zob. M. Susałko, *Identyfikacja podmiotu danych* [w:] D. Lubasz (red.), *Meritum…,* s. 161.

[76] Artykuł 12 ust. 2 RODO.

wypadku wybór innego sposobu przez podmiot danych nie może uzasadniać odmowy podjęcia działań przez administratora.

Przepisy rozporządzenia nie narzucają też administratorowi konkretnego sposobu wykonywania zgłaszanych żądań ani udzielania odpowiedzi podmiotom danych. Nie ulega natomiast wątpliwości, że wszelka komunikacja w tym zakresie musi być prowadzona z poszanowaniem zasady przejrzystości, a zatem w sposób zwięzły, zrozumiały dla podmiotu danych, w łatwo dostępnej formie i za pomocą jasnego i prostego języka. Zasadniczo sposób skierowania żądania przez podmiot danych determinuje sposób udzielenia odpowiedzi przez administratora. Przykładowo na zgłoszenie dokonane w formie elektronicznej administrator powinien odpowiedzieć również za pomocą środków komunikacji elektronicznej, chyba że osoba, której dane dotyczą, wyraźnie zażąda innej formy[77].

Zgodnie z art. 12 ust. 3 RODO administrator zobowiązany jest do niezwłocznego poinformowania podmiotu danych o działaniach podjętych na skutek zgłoszonego przez niego żądania. Informacja taka powinna być przekazana najpóźniej w ciągu miesiąca od otrzymania żądania. W wyjątkowych przypadkach, z uwagi na skomplikowany charakter żądania lub dużą liczbę żądań, administrator może przedłużyć o dwa miesiące termin na udzielenie odpowiedzi. W ciągu miesiąca od otrzymania żądania powinien jednak o tym poinformować podmiot danych. Jeśli administrator nie podejmuje działań w związku ze zgłoszonym żądaniem – np. gdy niemożliwa jest identyfikacja osoby zgłaszającej bądź żądanie jest niezasadne – powinien o tym poinformować również w ciągu miesiąca od otrzymania żądania, wyjaśniając powody niepodjęcia działań oraz informując o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem[78].

Miesięczny, a w niektórych przypadkach trzymiesięczny, termin na poinformowanie o podjętych działaniach może tylko z pozoru wydawać się długim terminem na realizację żądania. Administrator powinien brać pod uwagę, że w ramach rozpatrywania żądania powinien podjąć szereg działań, m.in. zarejestrować w wewnętrznym systemie wpływ żądania i w razie potrzeby przekazać zgłoszenie do dedykowanej jednostki/osoby zajmującej się ochroną danych osobowych w organizacji, zidentyfikować osobę występującą z żądaniem,

[77] Artykuł 12 ust. 3 RODO.

[78] Artykuł 12 ust. 4 RODO.

zweryfikować, czy na pewno posiada on względem tej osoby status administratora, przeanalizować zgłoszenie i ustalić treść żądania[79], ocenić zasadność zgłoszenia i możliwość jego realizacji, w razie konieczności skontaktować się z podmiotami przetwarzającymi lub współadministratorami, wreszcie udzielić odpowiedzi podmiotowi danych co do sposobu wykonania jego żądania. Gdy dane osobowe są przetwarzane w różnych systemach lub gdy administrator, pod względem organizacyjnym, jest podmiotem o rozbudowanej strukturze, wypełnienie wszystkich obowiązków, w tym wymiana informacji pomiędzy poszczególnymi działami/jednostkami wyodrębnionymi organizacyjnie w strukturze administratora, może okazać się czasochłonne.

3.4. Pobieranie opłat

Spełnienie obowiązków informacyjnych oraz realizacja praw zgłaszanych przez podmioty danych zasadniczo nie uprawniają administratora do pobrania opłat za podjęte przez niego działania, i to bez względu na to, ile razy wobec podmiotu danych spełniany jest obowiązek informacyjny lub dochodzi do realizacji zgłaszanego przez niego żądania[80]. Artykuł 12 ust. 5 RODO wprowadza jednak wyjątek – administrator może pobrać opłatę, a nawet odmówić podjęcia działań w związku z żądaniem, jeśli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Pobrana przez administratora opłata powinna być „rozsądna", tzn. powinna odzwierciedlać administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań. Opłata taka nie może być traktowana przez administratora jako dodatkowe źródło dochodu, a jej wysokość nie powinna działać odstraszająco na podmioty danych, powodując rezygnację z realizacji przysługujących im praw. Jej celem jest wyłącznie rekompensata adekwatnych kosztów poniesionych w związku z przekazywaniem informacji lub prowadzeniem komunikacji z podmiotem danych.

[79] Rolą administratora jest poprawne zdekodowanie treści żądania podmiotu danych tak, aby następnie móc zrealizować prawo podmiotu danych zgodnie z jego oczekiwaniami. Administrator powinien więc wykazać się pewnego rodzaju dociekliwością w ustalaniu, jaka jest faktyczna treść i zakres zgłoszonego żądania, zwłaszcza gdy budzi ono wątpliwości lub może być różnie interpretowane. Przykładowo administrator powinien mieć pewność, że podmiot danych chce usunięcia jego danych osobowych, a nie tylko zaprzestania ich przetwarzania w celach marketingowych.

[80] Wyjątek przewidziano jedynie w odniesieniu do realizacji prawa dostępu do danych osobowych – w art. 15 ust. 3 RODO wskazano, że za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

Wykazanie, że żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, obciąża administratora.

Administrator może też zastrzec, że opłata zostanie pobrana w razie wystąpienia przez podmiot danych z takim samym żądaniem przed upływem określonego czasu od daty realizacji tożsamego żądania przez administratora. Wyznaczony przez administratora czas musi znajdować uzasadnienie w okolicznościach przetwarzania, np. w tym, jak często dochodzi do zmiany kontekstu przetwarzania, zakresu przetwarzanych danych. Ponadto administrator nie może uzależniać przekazania informacji udzielanych podmiotowi danych od dokonania transakcji finansowej, np. zapłaty za usługi lub towary bądź ich zakupu[81].

3.5. Obowiązek poinformowania odbiorców o realizacji żądania podmiotu danych

Zgodnie z art. 19 RODO administrator musi pamiętać o poinformowaniu wszystkich odbiorców, którym ujawniono dane osobowe, o dokonanym sprostowaniu, usunięciu danych lub ograniczeniu przetwarzania. Obowiązek ten jest podyktowany potrzebą usunięcia rozbieżności pomiędzy danymi przetwarzanymi przez administratora (lub których przetwarzania zaprzestał) – w następstwie skorzystania przez podmiot danych z prawa do sprostowania, usunięcia danych lub ograniczenia przetwarzania – a danymi przetwarzanymi przez odbiorców, tj. podmioty, którym wcześniej udostępnił dane[82].

Krąg odbiorców danych może być szeroki. Obejmuje on nie tylko innych administratorów lub podmioty przetwarzające, którym administrator samodzielnie ujawnił przedmiotowe dane, ale również dalsze podmioty, które mogą mieć dostęp do tych danych, jak np. subprocesor. Warto więc, przy wchodzeniu w różne relacje w zakresie przetwarzania danych osobowych, mieć na uwadze uregulowanie tej kwestii. Przykładowo, zawierając umowę powierzenia można zobowiązać podmiot przetwarzający do prowadzenia i stałej aktualizacji listy podmiotów, którym przekazuje on dane osobowe w celu dalszego przetwarzania. W razie realizacji jednego z ww. praw przez podmiot danych, administrator

[81] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 15.

[82] Więcej na temat pojęcia „odbiorca” – zob. pkt 1.5 niniejszego opracowania.

będzie wtedy wyposażony w kompletną listę odbiorców danych, do których powinien skierować stosowną informację. Obowiązek ten można scedować w drodze umowy powierzenia na podmiot przetwarzający. Należy jednak pamiętać, że za jego prawidłową realizację ostateczną odpowiedzialność ponosi zawsze administrator. Administrator musi mieć więc zapewnione narzędzia kontroli nad procesorem i weryfikować faktyczne spełnienie tego obowiązku[83].

Obowiązek poinformowania odbiorców nie ma charakteru bezwzględnego. Zgodnie z przepisem, obowiązek ten nie ma zastosowania, jeśli poinformowanie odbiorców okaże się niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku ze strony administratora. Pierwsza przesłanka – niemożność poinformowania odbiorców – jest przesłanką obiektywną i może wynikać np. z przyczyn technicznych. W praktyce będą to rzadkie sytuacje, jak np. likwidacja podmiotu, któremu ujawniono dane osobowe[84]. W momencie, gdy przesłanka ta ustanie, administrator powinien wykonać swój obowiązek[85].

Druga przesłanka – niewspółmiernie duży wysiłek – jest natomiast przesłanką subiektywną, wymagającą oceny przez administratora. Może ona zajść wówczas, gdy zaistnieje istotna dysproporcja pomiędzy wysiłkiem administratora włożonym w informowanie odbiorców a założonym celem, jakim jest zabezpieczenie interesów podmiotu danych korzystającego z przysługujących mu praw[86]. Jeśli administrator odstępuje od poinformowania odbiorców o sprostowaniu, usunięciu danych lub ograniczeniu przetwarzania z powodu niewspółmiernie dużego wysiłku, musi być w stanie udowodnić ów „niewspółmiernie duży wysiłek" zachodzący w konkretnym stanie faktycznym oraz wskazać, dlaczego ta okoliczność uzasadnia odstąpienie od realizacji obowiązku.

---

83 Jest to ważne chociażby z punktu widzenia zasady rozliczalności – administrator musi posiadać narzędzia do wykazania, że (1) obwiązek poinformowania dalszych procesorów o sprostowaniu, usunięciu danych lub ograniczeniu przetwarzania został przeniesiony na podmiot przetwarzający oraz (2) że obowiązek ten został, w ramach wykonywania prawa przez podmiot danych, faktycznie zrealizowany przez procesora. Na dowód jego realizacji administrator może zażądać np. przekazania protokołu z wykonania danej czynności wraz z listą wszystkich odbiorców, do których została przekazana informacja.

84 M. Czerniawski, *Artykuł 19* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 541.

85 Zob. Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 33. Co prawda, Grupa Robocza Art. 29 przedstawia taki pogląd w odniesieniu do realizacji obowiązku informacyjnego z art. 14 RODO, jednak wobec tożsamego brzmienia przesłanek, *per analogiam,* należy go stosować również w kontekście art. 19 RODO.

86 M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, komentarz do art. 19.

Niezależnie od powyższego, jeśli osoba wykonująca przysługujące jej prawo tego zażąda, administrator powinien ją poinformować o wszystkich odbiorcach, do których przekazał informację w oparciu o omawiany przepis[87]. W literaturze wskazuje się, że administrator powinien przekazać także informację o odbiorcach, do których z różnych przyczyn nie udało mu się dotrzeć[88].

3.6. Prowadzenie rejestru realizacji praw podmiotów danych

Zasada rozliczalności, ujęta w art. 5 ust. 2 RODO, zobowiązuje administratora do przestrzegania pozostałych podstawowych zasad przetwarzania danych osobowych[89], jak i do tego, aby był on w stanie wykazać ich prawidłową realizację. Administrator powinien więc wdrożyć odpowiednie środki zapewniające przestrzeganie przepisów rozporządzenia oraz udokumentować swoje działania w taki sposób, aby mógł wykazać, jakie rozwiązania zastosował.

Realizacja zasady rozliczalności w kontekście wykonywania praw podmiotów danych może nastąpić nie tylko przez dokumentowanie prowadzonej z podmiotem danych komunikacji oraz podejmowanych na jego żądanie działań, ale również przez prowadzenie rejestru realizacji praw podmiotów danych. Do rejestru administrator powinien wpisywać najważniejsze informacje związane z realizacją żądań podmiotów danych, dzięki którym będzie w stanie wykazać, jak rozpoznał zgłoszone żądanie oraz dlaczego podjął określone działania w związku z jego realizacją. Do rejestru warto więc wpisywać informacje takie jak:

– data wpłynięcia żądania,
– przedmiot wniosku, w tym zakres danych objętych żądaniem,
– informacje o osobie występującej z żądaniem,
– sposób rozpoznania żądania,

87 Artykuł 19 RODO.

88 M. Czerniawski, *Artykuł 19* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 540.

89 Zasad, o których mowa w art. 5 ust. 1 RODO, a zatem zasad: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności.

– forma komunikacji,
– informacja, czy odbiorcy danych lub inni administratorzy zostali poinformowani o realizacji żądania,
– jeśli została pobrana opłata – w jakiej wysokości i na jakiej podstawie,
– jeśli żądanie nie zostało uwzględnione – przyczyny odmowy,
– data realizacji żądania.

3.7. Sankcje za naruszenia przepisów

Zgodnie z art. 83 ust. 5 lit. b) RODO naruszenia przepisów dotyczących praw osób, których dane dotyczą, o których mowa w art. 12–22 RODO, podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Należy przy tym zwrócić uwagę, że karze podlegają nie tylko naruszenia związane z realizacją żądań podmiotów danych *sensu stricto*, zgłaszane w oparciu o art. 15–22 RODO, ale również naruszenia pojawiające się na tle wykonywania tych praw, a związane z przestrzeganiem wymogów zasady przejrzystości.

Wysokość kar pieniężnych nakładanych przez organ jest miarkowana w zależności od okoliczności konkretnego stanu faktycznego. W ramach wymiaru kary organ bierze pod uwagę m.in.:
– charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody;
– umyślny lub nieumyślny charakter naruszenia;
– działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
– stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO;
– wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
– stopień współpracy z organem nadzorczym;
– kategorie danych osobowych, których dotyczyło naruszenie;

– sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
– inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty[90].

[90] Artykuł 83 ust. 2 RODO.

4. Prawa informacyjne – art. 13 i 14 RODO

4.1. Cele praw informacyjnych

Prawo do informacji o przetwarzaniu danych osobowych jest jednym z podstawowych praw przysługujących podmiotom danych na gruncie RODO, mającym na celu dostarczenie osobie, której dane dotyczą, wiedzy na temat przetwarzania jej danych osobowych przez konkretnego administratora, a przez to sprawowanie faktycznej kontroli nad tym, jakie informacje są w posiadaniu innych podmiotów, oraz weryfikację, czy przetwarzanie to odbywa się zgodnie z prawem. „Bycie poinformowanym" o fakcie i okolicznościach przetwarzania danych osobowych ma również na celu urzeczywistnienie idei autonomii informacyjnej jednostki poprzez umożliwienie samodzielnego decydowania o zakresie udostępnianych informacji, zwłaszcza w sytuacjach, gdy udostępnienie danych nie jest obowiązkiem wynikającym z przepisów, lecz następuje z inicjatywy osoby, której dane dotyczą. Prawo do informacji warunkuje też skorzystanie z innych uprawnień przewidzianych w RODO – bez świadomości, że dane są lub będą przetwarzane, podmiot danych nie ma realnej możliwości skorzystania z innych praw. Z tych przyczyn prawa do bycia poinformowanym nie można się skutecznie zrzec, ograniczyć ani przenieść na inną osobę.

Prawa informacyjne realizowane są przez administratora poprzez wypełnienie obowiązków informacyjnych, o których mowa w art. 13 i 14 RODO. Przepisy te nakładają na każdego administratora obowiązek przekazania odpowiednich informacji osobie, której dane dotyczą. Zakres tych informacji zależy od sposobu pozyskiwania danych. Jeśli dane osobowe pozyskiwane są bezpośrednio od podmiotu danych, zastosowanie znajdzie art. 13 RODO, natomiast gdy są pozyskiwane z innych źródeł – zastosowanie ma art. 14 RODO. Zarówno w jednym, jak i w drugim przypadku, zakres przekazywanych informacji jest bardzo podobny, ale zachodzą pewne różnice, o których administrator musi pamiętać, aby nie narazić się na zarzut niedopełnienia obowiązków.

Istotne jest to, że na mocy ww. przepisów administrator został zobowiązany do „aktywnego informowania", co oznacza, że realizacja obowiązków informacyjnych powinna następować

z inicjatywy samego administratora. Nie jest w tym przypadku, w przeciwieństwie do innych praw przysługujących podmiotom danych, potrzebny wniosek, prośba czy jakiekolwiek działanie ze strony osoby, której dane dotyczą. Administrator nie musi też osobiście spełniać obowiązków informacyjnych. Mogą to czynić w jego imieniu inne podmioty, np. pracownicy, osoby współpracujące czy podmioty przetwarzające. Ważne jest jednak to, aby administrator udzielił w tym zakresie wyraźnego upoważnienia, np. umieszczając stosowne postanowienia w umowie powierzenia. W niektórych sytuacjach realizowanie obowiązku informacyjnego przez inny podmiot działający z upoważnienia administratora jest bardziej celowe i efektywne, np. wówczas, gdy podmiot przetwarzający zajmuje się gromadzeniem danych dla administratora i przez to ma bezpośredni kontakt z osobami, których dane są pozyskiwane. W przypadku, gdy zachodzi relacja współadministrowania współadministratorzy muszą ustalić między sobą to, który z nich odpowiedzialny jest za wykonywanie obowiązków informacyjnych wobec podmiotów danych.

Warto też zaznaczyć, że obowiązek informacyjny z art. 13 RODO aktualizuje się nie tylko w sytuacji, gdy dane osobowe są podawane przez podmiot danych (np. przy wypełnianiu formularza, bezpośredniej rozmowy), ale również, gdy dane te są zaobserwowane przez administratora (np. utrwalone na nagraniu z monitoringu lub pozyskane dzięki internetowym narzędziom analitycznym). Natomiast obowiązek informacyjny z art. 14 RODO przykładowo aktualizuje się, gdy administrator pozyskuje dane osobowe od innego administratora, z publicznie dostępnych źródeł, jak publiczne rejestry, Internet, portale społecznościowe, czy od podmiotów zajmujących się profesjonalną sprzedażą baz danych.

4.2. Zakres obowiązków informacyjnych

Prawodawca unijny w art. 13 i 14 RODO zawarł szczegółowy katalog informacji, jakie mają być przekazywane osobie, której dane dotyczą. Katalog ten ma charakter wyczerpujący, co oznacza, że administrator nie musi podawać innych, nieuwzględnionych w ww. przepisach informacji dotyczących przetwarzania danych osobowych. Jeśli jednak ma taką wolę, może przekazać podmiotowi danych dodatkowe informacje, np. dotyczące sposobu prowadzenia przez niego działalności i związanych z tym metod przetwarzania danych osobowych, szczegółowych sposobów wykonywania praw przewidzianych w RODO itp. Warto jednak pamiętać, że obowiązki informacyjne i sposób ich wykonywania przez administratora podlegają ocenie z perspektywy zasady przejrzystości. Zasada ta stanowi m.in., że informacje

przewidziane w art. 13 i 14 RODO powinny być przekazywane w sposób zwięzły, przejrzysty i zrozumiały. Podmiot danych nie powinien doświadczać tzw. przytłoczenia informacyjnego na skutek podawania zbyt dużej ilości informacji jednocześnie. Biorąc zaś pod uwagę to, że na mocy art. 13 i 14 RODO administrator i tak jest już zobowiązany do przekazywania znacznego zakresu informacji, wydaje się, że wzbogacanie klauzul informacyjnych o dodatkowe treści, niewynikające wprost z ww. przepisów, może prowadzić właśnie do nadmiernego rozbudowania tych klauzul, a tym samym do uchybienia wymogom przejrzystości. Praktyka pokazuje bowiem, że na skutek zwiększenia zakresu obowiązków informacyjnych na gruncie RODO[91], wielu administratorów stosuje obszerne i zawiłe klauzule informacyjne, niespełniające kryterium zwięzłości, które zamiast zachęcać – zniechęcają podmioty danych do zapoznania się z informacjami na temat przetwarzania ich danych osobowych[92]. Efekt jest zatem odwrotny do zamierzonego, a sama realizacja obowiązków informacyjnych nie przyczynia się do podniesienia poziomu świadomości w zakresie ochrony danych osobowych ani do poprawy sytuacji osób, których dane są przetwarzane. Jeśli więc administrator chce przekazać podmiotowi danych dodatkowe informacje na temat przetwarzania, dobrym rozwiązaniem będzie wyodrębnienie tych informacji od treści samej klauzuli informacyjnej i umożliwienie dostępu do nich np. poprzez odesłanie do innego dokumentu lub dedykowanej zakładki na stronie internetowej, jak również stosowanie warstwowych komunikatów, w których w pierwszej warstwie administrator przekazuje kluczowe informacje dotyczące przetwarzania, a dopiero w kolejnych warstwach je precyzuje i uzupełnia.

Administrator, realizując prawa informacyjne osób, których dane dotyczą, powinien przekazać następujące informacje:

– tożsamość i dane kontaktowe administratora oraz – gdy ma to zastosowanie – przedstawiciela administratora spoza Unii Europejskiej [art. 13 ust. 1 lit. a) i art. 14 ust. 1 lit. a) RODO];
– dane kontaktowe inspektora ochrony danych – jeśli został on powołany [art. 13 ust. 1 lit. b) i art. 14 ust. 1 lit. b) RODO];

[91] Zwiększenie względem przepisów poprzedzających RODO, tj. dyrektywy 95/46 WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE L 281 z dn. 23.11.1995 r., s. 31—50.

[92] P. Fajgielski, „Obowiązek informacyjny z perspektywy dwóch lat stosowania nowych przepisów o ochronie danych osobowych", *Monitor prawniczy* (dodatek), nr 23/2020.

- cele przetwarzania i podstawa prawna przetwarzania [art. 13 ust. 1 lit. c) i art. 14 ust. 1 lit. c) RODO];
- informację o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią – jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO [art. 13 ust. 1 lit. d) i art. 14 ust. 2 lit. b) RODO];
- informację o odbiorcach danych osobowych lub o kategoriach odbiorców – jeżeli istnieją [art. 13 ust. 1 lit. e) i art. 14 ust. 1 lit. e) RODO];
- informacje o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – jeżeli ma to zastosowanie [art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO];
- okres, przez który dane osobowe będą przechowywane, albo kryteria ustalania tego okresu [art. 13 ust. 2 lit. a) i art. 14 ust. 2 lit. a) RODO];
- informacje o prawach przysługujących podmiotom danych [art. 13 ust. 2 lit. b)–d) i art. 14 ust. 2 lit. c)–e) RODO];
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych [art. 13 ust. 2 lit. e) RODO];
- informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą [art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) RODO];
- kategorie przetwarzanych danych osobowych [art. 14 ust. 1 lit. d) RODO];
- informacje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – również informację, czy pochodzą one ze źródeł publicznie dostępnych [art. 14 ust. 2 lit. f) RODO].

Przekazanie informacji o tożsamości i danych kontaktowych administratora ma celu zidentyfikowanie podmiotu odpowiedzialnego za proces przetwarzania danych osobowych oraz umożliwienie nawiązania łatwego, szybkiego i bezpośredniego kontaktu z nim. Podobnie jest w przypadku podmiotów niemających jednostki organizacyjnej w UE, zobowiązanych na mocy art. 27 ust. 1 RODO do ustanowienia swojego przedstawiciela. W klauzuli informacyjnej konieczne jest wskazanie, jaki podmiot został powołany do pełnienia tej roli oraz jakie są jego dane kontaktowe. Dane kontaktowe powinny obejmować takie informacje jak: dokładna nazwa podmiotu[93], adres siedziby lub adres do doręczeń, telefon kontaktowy

[93] W przypadku osób fizycznych – imię i nazwisko, firma.

lub adres elektroniczny – w zależności od tego, jaką formę kontaktu administrator przewiduje. Jeśli administrator powołał inspektora ochrony danych, winien wskazać również jego dane kontaktowe[94].

Wyjaśnienie, w jakim celu zbierane i przetwarzane są dane osobowe, jest powiązane z realizacją zasady ograniczenia celu, wynikającą z art. 5 ust. 1 lit. b) RODO. Informacja ta ma ułatwiać podmiotowi danych zorientowanie się, dlaczego administrator gromadzi jego dane, jak zamierza je wykorzystywać i czy zakres gromadzonych danych jest adekwatny względem celu ich przetwarzania. Cele powinny być sformułowane w sposób jasny i konkretny (np. dane zbierane w celu zawarcia i realizacji umowy, przygotowania oferty handlowej, przeprowadzenia rekrutacji na określone stanowisko, konkursu i wyboru laureata); mogą być też sformułowane zbiorczo (np. w celach marketingowych, w celu realizacji ustawowych obowiązków pracodawcy, takich jak obowiązki z zakresu ubezpieczeń społecznych, podatkowe, sprawozdawcze). Administrator powinien podać cele, które są aktualne, tzn. takie, które faktycznie będzie realizować. **Nie należy podawać celów, które administrator dopiero planuje i nie ma jeszcze pewności, czy rzeczywiście zacznie je realizować**. Taka sytuacja mogłaby bowiem prowadzić do gromadzenia danych „na zapas" i naruszenia zasady minimalizacji danych. Jeśli po rozpoczęciu procesu przetwarzania dojdzie do zmiany celu przetwarzania, administrator ma obowiązek poinformować o tym osobę, której dane dotyczą.

Zamieszczenie w klauzuli informacji o podstawach prawnych przetwarzania danych osobowych jest konieczne z punktu widzenia zasady zgodności z prawem, o której mowa w art. 5 ust. 1 lit. a) RODO. Wymaga to określenia właściwej przesłanki legalizującej przetwarzanie – w zależności od tego, czy administrator przetwarza dane zwykłe lub wrażliwe, przesłanki tej należy szukać odpowiednio w art. 6 ust. 1 lub art. 9 ust. 2 RODO. Jeśli podstawa przetwarzania wynika z przepisów prawa krajowego, to również należy ją wskazać. W literaturze podkreśla się nadto, że nie wystarczy samo podanie

[94] Kwestie związane z wyznaczaniem inspektora ochrony danych, jego statusem i zadaniami zostały uregulowane w art. 37–39 RODO. Warto na marginesie dodać, że w przypadku danych kontaktowych inspektora ochrony danych RODO nie zobowiązuje do wskazywania go z imienia i nazwiska – zob. Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych („DPO")* z 13.12.2016 r., zmienione i przyjęte 5.04.2017 r., WP243 rev.01, s. 16.

numeru przepisu, ale należy przytoczyć jego treść[95]. Jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO, administrator zobowiązany jest do wyjaśnienia, co stanowi prawnie uzasadniony interes realizowany przez niego lub przez stronę trzecią (np. bezpośredni kontakt z podmiotem danych w celu przedstawienia spersonalizowanej oferty handlowej). Wymagane jest precyzyjne opisanie tego interesu po to, aby podmiot danych mógł zweryfikować prawidłowość przeprowadzonego przez administratora testu równowagi[96] oraz ewentualne podstawy do zgłoszenia sprzeciwu wobec przetwarzania na mocy art. 21 RODO.

Administrator powinien też poinformować osobę, której dane dotyczą, o odbiorcach lub kategoriach odbiorców, przy czym wybór w tym zakresie został pozostawiony administratorowi. Należy pamiętać, że na mocy RODO za odbiorcę uważany jest także podmiot przetwarzający; nie ma natomiast w tym kontekście obowiązku informowania o podmiotach publicznych, które mogą uzyskiwać dane na podstawie przepisów w ramach prowadzonych postępowań (np. organy administracji publicznej, organy ścigania, sądy). Jeśli administrator zdecyduje się podać jedynie informacje o kategoriach odbiorców, musi być w stanie ją odpowiednio uzasadnić – zgodnie z zasadą rozliczalności z art. 5 ust. 2 RODO. Wówczas podawane przez niego informacje powinny być maksymalnie szczegółowe, tzn. powinien wskazać rodzaj odbiorcy (np. poprzez odniesienie do działalności, którą prowadzi), branżę, sektor, podsektor oraz lokalizację odbiorcy[97].

---

95 M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 13. Por. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych*, Warszawa 2018, s. 241, który wskazuje, co prawda w kontekście informowania podmiotu danych o tym, czy podanie danych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy, że jeżeli obowiązek podania danych wynika z przepisu prawa, to „należy wskazać ten przepis, natomiast nie jest konieczne przywołanie pełnej treści tego przepisu".

96 Aby móc przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. f) RODO, administrator powinien przeprowadzić tzw. test równowagi. W ramach tego testu powinien ocenić, czy (i) występują prawnie uzasadnione interesy realizowane przez niego lub stronę trzecią, (ii) czy do realizacji celów wynikających z tych interesów jest konieczne przetwarzanie danych osobowych oraz czy (iii) w analizowanym stanie faktycznym nie zachodzi przesłanka negatywna, tzn. nie występują interesy lub podstawowe prawa i wolności podmiotu danych, które mają charakter nadrzędny względem prawnie uzasadnionych interesów administratora lub strony trzeciej. Jeśli spełniona jest ostatnia z przesłanek, administrator nie może zalegalizować przetwarzania w oparciu o art. 6 ust. 1 lit. f) RODO.

97 Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, załącznik.

Jeśli administrator zamierza przekazywać dane osobowe poza Europejski Obszar Gospodarczy, również powinien o tym poinformować podmiot danych, wskazując jednocześnie, czy państwo lub organizacja międzynarodowa, do których ma być realizowany transfer danych, zostały uznane przez Komisję Europejską za zapewniające odpowiedni stopień ochrony danych na mocy art. 45 RODO. Administrator powinien więc skonkretyzować, do jakich państw trzecich lub organizacji następuje transfer oraz podać jego podstawę prawną, tj.:

– decyzję KE stwierdzającą odpowiedni stopień ochrony,
– przekazywanie danych z zastrzeżeniem odpowiednich zabezpieczeń (art. 46 RODO),
– przekazywanie danych na podstawie wiążących reguł korporacyjnych (art. 47 RODO),
– przekazywanie na podstawie jednej z przesłanek wymienionych w art. 49 ust. 1 RODO lub
– na podstawie art. 49 RODO ust. 1 akapit drugi RODO[98].

We wszystkich powyższych przypadkach, za wyjątkiem pkt 4), administrator zobowiązany jest nadto zamieścić wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych[99]. Nawet jeśli administrator nie ma zamiaru przekazywać danych osobowych poza EOG, w myśl zasady przejrzystości przetwarzania, powinien wyraźnie poinformować o braku takiego zamiaru[100].

W celu zapewnienia rzetelności i przejrzystości przetwarzania administrator powinien przekazać także szereg dodatkowych informacji, jak choćby okresy retencji danych czy prawa przysługujące podmiotom danych. W odniesieniu do okresów retencji zauważyć należy, że okresy te nierzadko wynikają wprost z przepisów (np. z kodeksu pracy, przepisów z zakresu ubezpieczeń społecznych, rachunkowości, podatkowych). W takich przypadkach administrator powinien przestrzegać ustanowionych przez krajowego ustawodawcę

98 Przepis ten stanowi: „[…] jeżeli przekazanie nie może się opierać na art. 45 ani 46, w tym na przepisach dotyczących wiążących reguł korporacyjnych, i nie ma zastosowania żaden z wyjątków mających zastosowanie w szczególnych sytuacjach zgodnie z akapitem pierwszym niniejszego ustępu, przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą, a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator informuje organ nadzorczy o przekazaniu. Poza informacjami, o których mowa w art. 13 i 14, administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego”.

99 Artykuł 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO.

100 Zob. też M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 13.

czasowych ram przechowywania danych osobowych. Jeśli natomiast okresy retencji nie wynikają z przepisów, administrator powinien określić je samodzielnie, uwzględniając cele przetwarzania. Zgodnie bowiem z zasadą ograniczenia przechowywania dane osobowe nie powinny być przechowywane dłużej niż jest to niezbędne do celów, w których dane te są przetwarzane[101]. Podjęta przez administratora decyzja co do przyjętych okresów retencji jest dla niego wiążąca, a same okresy powinny być, co do zasady[102], dostatecznie precyzyjnie ustalone poprzez wskazanie dni, tygodni, miesięcy lub lat przechowywania danych, lub też podanie konkretnej daty granicznej, lub okoliczności warunkujących koniec przechowywania danych (np. do czasu zakończenia procesu reklamacyjnego, do zakończenia procesu rekrutacji, do wyboru laureata konkursu). Z pewnością nie wystarczy ogólne stwierdzenie, że dane osobowe będą przechowywane tak długo, jak jest to niezbędne dla prawnie uzasadnionych celów przetwarzania, ponieważ na podstawie takiej informacji podmiot danych nie jest w stanie zorientować się, jak długo w rzeczywistości jego dane będą przechowywane przez administratora. Co więcej, jeśli w zależności od celu przetwarzania lub kategorii danych osobowych okresy retencji są różne, administrator powinien wskazać je odrębnie.

Obowiązkiem administratora jest też poinformowanie o prawach osoby, której dane dotyczą. Administrator powinien więc zawrzeć w klauzuli informacje o prawie do żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, o prawie do przenoszenia danych, wniesienia sprzeciwu wobec przetwarzania, cofnięcia w dowolnym momencie zgody na przetwarzanie danych, jeśli przetwarzanie odbywa się na podstawie zgody, oraz o prawie wniesienia skargi do organu nadzorczego. Mimo że nie zawsze wszystkie ww. prawa będą przysługiwały podmiotowi danych, RODO nie przewiduje wprost żadnych wyłączeń w tym zakresie. Uważam jednak, że administrator nie powinien wprowadzać w błąd osoby, której dane dotyczą, informując ją o prawach, które z uwagi na okoliczności przetwarzania, nie będą jej *de facto* przysługiwać. W celu zapewnienia rzetelności i przejrzystości przetwarzania administrator powinien więc za każdym razem weryfikować

[101] Wyjątkowo, o czym stanowi art. 5 ust. 1 lit. e) RODO, administrator może przechowywać dane osobowe ponad określone okresy retencji, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą.

[102] W sytuacji, gdy administrator nie jest w stanie precyzyjnie wskazać okresu retencji, powinien poinformować o kryteriach jego ustalania.

zakres faktycznych uprawnień podmiotu danych i wprost wskazać w klauzuli informacyjnej prawa, które w konkretnym przypadku nie będą przysługiwać po to, aby podmiot danych miał wiedzę, z jakich uprawnień może korzystać, a z jakich nie[103]. Podkreśla się, że administrator powinien zawrzeć dodatkowe informacje o tym, co dane prawo obejmuje i w jaki sposób podmiot danych może je zrealizować[104]. Warto też zaznaczyć, że informacja o przysługującym prawie do wniesienia sprzeciwu wobec przetwarzania powinna być wyodrębniona i odpowiednio wyeksponowana, co wynika wprost z treści art. 21 ust. 4 RODO, stanowiącego, że administrator wyraźnie informuje podmiot danych o prawie do sprzeciwu przy okazji pierwszej komunikacji oraz przedstawia tę informację „jasno i odrębnie od wszelkich innych informacji".

Do obowiązków administratora należy także poinformowanie o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, z zastrzeżeniem, że w odniesieniu do profilowania obowiązek ten aktualizuje się jedynie w przypadku profilowania wykorzystywanego w związku ze zautomatyzowanym podejmowaniem decyzji, a nie w przypadku każdego profilowania, z którego korzysta administrator[105]. Administrator nie musi podawać szczegółowych informacji technicznych czy nazw programów i technologii, które wykorzystuje, ale powinien za to wskazać podstawowe elementy procesu decyzyjnego, źródła informacji branych pod uwagę i ich znaczenie dla podmiotu danych, aby mógł on zrozumieć konsekwencje takiego przetwarzania[106].

Wszystkie wyżej omówione kategorie informacji administrator powinien przekazać podmiotowi danych niezależnie od sposobu, w jaki jego dane pozyskał – bezpośrednio od niego czy z innego źródła. Inaczej jest w przypadku trzech kategorii danych. Informację o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych, administrator przekazuje wyłącznie w przypadku bezpośredniego zbierania danych od podmiotu danych.

[103] Zgodnie z literalnym brzmieniem art. 13 ust. 2 lit. b) i art. 14 ust. 2 lit. c) RODO administrator ma przekazać „informacje o prawie", a nie „informacje o przysługującym prawie". Można więc wywodzić z tych przepisów obowiązek administratora poinformowania o wszystkich prawach podmiotów danych przewidzianych w RODO, z jednoczesnym wskazaniem, które z nich w konkretnym przypadku będą przysługiwać. Zob. też M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 13.

[104] D. Lubasz, *Prawa informacyjne* [w:] D. Lubasz (red.), *Meritum…*, s. 292.

[105] J. Łuczak, Artykuł 13 [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 484.

[106] Za: M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 13.

Praktycznie nie ma możliwości przekazania tej informacji, jeśli dane są pozyskiwane z innego źródła. Z kolei informację o kategoriach przetwarzanych danych osobowych administrator podaje wyłącznie, gdy realizuje obowiązek na podstawie art. 14 RODO. Jest to podyktowane potrzebą dostarczenia podmiotowi danych informacji o zakresie zebranych i przetwarzanych przez administratora danych osobowych. Podobnie jest w odniesieniu do informacji o źródle pochodzenia danych – tę również administrator podaje w przypadku realizowania obowiązku z art. 14 RODO. Ważne jest podanie tej informacji w sposób skonkretyzowany, aby identyfikacja podmiotów, od których zostały pozyskane dane, nie budziła wątpliwości. Nie wystarczy samo wskazanie, że informacje pochodzą np. ze źródeł publicznych. W motywie 61 RODO dopuszczono jeden wyjątek w tym zakresie – niemożność podania pochodzenia danych osobowych ze względu na ich pochodzenie z różnych źródeł. Okoliczność ta musi mieć jednak charakter obiektywny, tzn. musi zachodzić faktyczny brak możliwości podania źródeł, a nie trudność w ich wskazaniu.

4.3. Sposób i termin realizacji obowiązków informacyjnych

Prawodawca unijny nie zawarł w RODO wskazówek co do samej formy wypełniania przez administratora obowiązków informacyjnych. Należy jednak zwrócić uwagę na przyjęte w art. 13 i 14 RODO sformułowanie, że administrator „podaje informacje", co oznacza, iż zobowiązany jest do podjęcia aktywnych działań w celu przekazania osobie, której dane dotyczą, informacji wymienionych w tych artykułach, tj. przekazania wprost tych informacji lub skierowania podmiotu danych do miejsca, w którym się znajdują[107]. W żadnym wypadku nie może przerzucać na podmiot danych ciężaru poszukiwania tych informacji, np. poprzez wyszukiwanie informacji na temat przetwarzania danych osobowych w różnych dokumentach udostępnianych przez administratora, jak choćby regulamin świadczenia usług, korzystania ze strony internetowej itp. Należy bowiem pamiętać, że u podstaw obowiązków informacyjnych leży zasada przejrzystości, uregulowana w art. 5 ust. 1 lit. a) i art. 12 RODO, która zobowiązuje administratora do przekazywania podmiotom danych informacji w sposób przejrzysty, zwięzły, zrozumiały i w łatwo dostępnej formie. Konieczne jest zatem

[107] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 21.

spełnienie nie tylko wymogów co do jakości przekazu kierowanego do osoby, której dane są przetwarzane, ale również co do formy, w jakiej jest on kierowany.

Jednocześnie Grupa Robocza Art. 29 w swoich wytycznych sama zauważa, że na gruncie RODO istnieje kontrast pomiędzy wymogiem przekazania wyczerpujących informacji na mocy art. 13 i 14 RODO a wymogiem przekazania ich z poszanowaniem zasady przejrzystości. Jak wskazuje, „[…] mając na uwadze fundamentalne zasady rozliczalności i rzetelności, administratorzy muszą samodzielnie przeanalizować charakter, okoliczności, zakres i kontekst prowadzonego przez nich przetwarzania danych osobowych oraz postanowić […] które z wymaganych informacji potraktować priorytetowo oraz jakie są właściwe poziomy szczegółowości i metody przekazywania informacji". Z tego względu Grupa Robocza Art. 29 zaleca, aby obowiązki informacyjne były realizowane w sposób warstwowy poprzez odsyłanie do różnych kategorii informacji, które należy podać osobie, której dane dotyczą, zamiast wyświetlania na ekranie wszystkich tych informacji w formie ciągłego tekstu[108]. Stosowanie warstwowych komunikatów ma też przeciwdziałać tzw. zjawisku zmęczenia informacyjnego (ang. *information overload*), powodowanemu przekazywaniem dużej ilości informacji jednocześnie, które może prowadzić do zniechęcenia i niezaznajomienia się przez odbiorcę z kierowanym do niego komunikatem.

Obowiązki informacyjne mogą być realizowane warstwowo zarówno w środowisku cyfrowym, jak i poza nim. W otoczeniu cyfrowym warstwowe komunikaty mogą umożliwiać bezpośrednie przejście do tej sekcji komunikatu, z którą podmiot danych chce się zapoznać, np. poprzez zastosowanie aktywnych linków odsyłających w ramach jednego dokumentu, takiego jak polityka ochrony prywatności, oświadczenie o ochronie prywatności. Jak podkreśla Grupa Robocza Art. 29, warstwowe komunikaty nie muszą zawierać wbudowanych podstron, wymagających kilku kliknięć, aby dotrzeć do danej informacji[109]. Natomiast struktura i wygląd pierwszej warstwy komunikatu powinny dawać podmiotowi danych jasny obraz, jakie informacje są dostępne na temat przetwarzania jego danych osobowych, oraz gdzie, w jaki sposób i w których warstwach może je znaleźć. Zakres informacji, jakie przekaże administrator w pierwszej warstwie komunikatu, zależy zasadniczo od jego decyzji, niemniej jednak w wytycznych wskazano, że **powinny być to co najmniej informacje na temat celów przetwarzania, tożsamości administratora oraz praw osoby, której dane dotyczą**. Mogą

[108] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 21. Na temat warstwowego przekazywania informacji zob. też pkt. 2.3 niniejszego opracowania.

[109] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 22.

to być też informacje na temat przetwarzania, które ma największy wpływ na osobę, której dane dotyczą, oraz przetwarzania, które może zaskoczyć taką osobę[110]. Administrator musi – zgodnie z zasadą rozliczalności – być w stanie wykazać i uzasadnić, dlaczego określone informacje uznał za priorytetowe. W środowisku cyfrowym administrator może ponadto korzystać z innych form przekazywania podmiotom danych informacji dotyczących przetwarzania ich danych osobowych, zwłaszcza takich, które są specjalnie dostosowane do ich sytuacji lub do rodzaju towarów i usług, z których korzystają, np. przez stosowanie znaków graficznych czy symboli, powiadomień typu „push" i „pull"[111], kodów QR czy filmów wideo.

W środowisku innym niż cyfrowe również możliwe jest przekazywanie informacji w sposób warstwowy. Metody będą się różnić w zależności od formy komunikacji. Jeśli pierwszy kontakt z podmiotem danych ma miejsce drogą telefoniczną, obowiązek informacyjny z art. 13 lub 14 RODO może być spełniony poprzez przekazanie najważniejszych informacji bezpośrednio podmiotowi danych w trakcie rozmowy telefonicznej oraz dostarczenie pozostałych informacji wymaganych na podstawie ww. przepisów poprzez przesłanie kopii polityki ochrony prywatności w wiadomości e-mail, przesłanie linku do strony internetowej, na której są opublikowane informacje z zakresu przetwarzania danych osobowych, czy zapewnienie możliwości odtworzenia nagranego wcześniej komunikatu zawierającego te informacje. Obowiązki informacyjne mogą być też spełnione w tradycyjnej formie papierowej poprzez przekazanie ulotek, broszur informacyjnych, infografik lub innego rodzaju dokumentów prezentujących stosowne informacje, jak również poprzez kontakt bezpośredni i ustne wyjaśnienia przekazane podmiotowi danych.

Warto też wspomnieć, że obowiązek informacyjny nie musi być realizowany przez administratora osobiście (w znaczeniu „bezpośrednio"). Może on być wykonywany przez podmiot przetwarzający w imieniu administratora w ramach istniejącego stosunku

[110] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 22.

[111] Powiadomienia typu „push" polegają na wysyłaniu *ad hoc* informacji dotyczących przetwarzania danych osobowych w najodpowiedniejszym czasie dla osoby, której dane są przetwarzane. Pozwala to przykładowo na różnicowanie informacji i przekazywanie stosownych treści na różnych etapach przetwarzania. Powiadomienia typu „pull" pozwalają na dostęp do informacji o przetwarzaniu danych osobowych za pomocą takich narzędzi jak pulpity nawigacyjne, samouczki. Więcej na ten temat w: Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 23–24. Grupa Robocza Art. 29 nie wyłącza przy tym innych, bardziej nowoczesnych metod spełniania obowiązków informacyjnych, pod warunkiem, że metody te realizują jednocześnie zasadę przejrzystości przewarzania.

powierzenia przetwarzania. Jest to zasadne zwłaszcza w sytuacjach, kiedy to procesor zbiera dane osobowe od osób fizycznych.

Przekazanie osobie, której dane dotyczą, informacji na temat przetwarzania jej danych osobowych, musi nastąpić we właściwych terminach określonych w RODO. Jeśli dane osobowe zbierane są bezpośrednio od podmiotu danych, **informacje wskazane w art. 13 RODO powinny być przekazane w momencie pozyskiwania danych osobowych**. Przekazanie to powinno nastąpić na najwcześniejszym możliwym etapie, zwłaszcza jeśli przetwarzanie danych jest dobrowolne i zależy od woli podmiotu danych. Celem jest bowiem umożliwienie osobie, której dane dotyczą, jak najszybszego zorientowania się w okolicznościach przetwarzania oraz – tam, gdzie to możliwe – zaakceptowanie warunków przetwarzania.

Inaczej jest w przypadku gromadzenia danych w inny sposób niż od podmiotu danych – obowiązek informacyjny z art. 14 RODO powinien być wówczas spełniony w rozsądnym terminie po pozyskaniu danych osobowych, ale **nie później niż w ciągu miesiąca**. Jeżeli jednak dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – obowiązek informacyjny powinien być spełniony najpóźniej przy pierwszej takiej komunikacji, natomiast jeśli administrator planuje ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu powinien przekazać podmiotowi danych wymagane informacje.

Obowiązek informacyjny powinien być realizowany w sposób zindywidualizowany wobec konkretnej osoby, której dane administrator przetwarza lub zamierza przetwarzać. Zamieszczenie klauzul informacyjnych zawierających informacje wymagane zgodnie z art. 13 lub 14 RODO w polityce ochronie prywatności, regulaminie czy na stronie internetowej ma charakter ogólnoinformacyjny i dodatkowy. Tego rodzaju komunikaty są kierowane do ogółu, a nie do konkretnej osoby. Niemniej jednak uważam, że na zindywidualizowany charakter informowania nie wpływa negatywnie przyjęcie podejścia warstwowego w spełnianiu obowiązku informacyjnego. W takiej sytuacji wymóg zindywidualizowanego przekazania informacji byłby spełniony poprzez przekazanie najważniejszych informacji o przetwarzaniu danych osobowych w pierwszej warstwie komunikatu kierowanego do podmiotu danych, a następnie odesłanie do szczegółowych informacji zawartych w innym dokumencie, kierowanym do ogółu.

4.4. Zmiana celu przetwarzania i aktualizacja przekazanych informacji

Artykuł 13 ust. 3 i art. 14 ust. 4 RODO stanowią, że administrator, który planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, powinien poinformować podmiot danych o tym innym celu przed rozpoczęciem dalszego przetwarzania oraz udzielić mu wszelkich innych stosownych informacji, o których mowa w art. 13 ust. 2 lub art. 14 ust. 2 RODO. Jest to jedna sytuacja, wyraźnie i wprost wskazana przez prawodawcę unijnego, w której na administratora nałożony jest czynny obowiązek zaktualizowania klauzuli informacyjnej, jeśli zebrane dane osobowe mają być przetwarzane w celu innym niż pierwotnie planowany i zakomunikowany podmiotowi danych. Jednak z zasady przejrzystości, rzetelności i rozliczalności wywodzony jest także ogólny obowiązek administratora informowania o wszelkich istotnych lub dużych zmianach w zakresie przetwarzania, przy czym za „istotne lub duże zmiany" Grupa Robocza Art. 29 uznaje takie zmiany, które mogą mieć wpływ na osoby, których dane dotyczą (w tym ich zdolność do wykonywania swoich praw), mogą okazać się niespodziewane lub zaskakujące dla osób, których dane dotyczą[112]. W każdym wypadku podmiot danych powinien być poinformowany o zmianie tożsamości administratora, zmianie sposobu, w jaki może wykonywać swoje prawa w związku z przetwarzaniem danych osobowych, oraz – co zostało już wspomniane – o zmianie celu przetwarzania. Powinien być także informowany o innych kluczowych zmianach, jak np. rozszerzenie kategorii odbiorców lub rozpoczęcie przekazywania danych do państw trzecich.

Informowanie o zmianach ważnych okoliczności dotyczących przetwarzania danych osobowych ma istotne znaczenie, gdyż pozwala podmiotowi danych na zachowanie kontroli nad całym procesem przetwarzania jego danych osobowych, a nie tylko w momencie podejmowania decyzji o przekazaniu danych. Jeśli w ocenie podmiotu danych zmiana okoliczności przetwarzania jest istotna na tyle, że może oddziaływać na jego sytuację, podmiot ten może chcieć skorzystać z przysługujących mu praw, np. prawa do usunięcia danych, ograniczenia przetwarzania lub prawa sprzeciwu. Jeśli nie będzie mieć świadomości zachodzących zmian w obszarze przetwarzania, nie będzie w stanie podjąć jakichkolwiek kroków, a zatem jego kontrola nad przetwarzaniem danych może stać się iluzoryczna.

[112] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 19.

W tym kontekście warto zauważyć, że administrator nie może przenieść na podmiot danych obowiązku regularnego sprawdzania, czy doszło do zmiany okoliczności związanych z przetwarzaniem, czyli do zmiany treści dokumentów zawierających informacje, o których mowa w art. 13 i 14 RODO. To rolą administratora jest aktywne spełnianie obowiązków informacyjnych wobec osób, których dane przetwarza. Jak wskazuje Grupa Robocza Art. 29, „zamieszczenie w oświadczeniu o ochronie prywatności/informacji o polityce prywatności zalecenia dla osoby, której dane dotyczą, aby regularnie sprawdzała oświadczenie o ochronie prywatności/informację o polityce prywatności pod kątem zmian lub aktualizacji, uznaje się nie tylko za niewystarczające, ale również za nierzetelne w kontekście art. 5 ust.1 lit. a) [RODO – przyp. aut.]".

W przepisach rozporządzenia nie ma też sformułowanych wprost wymogów czasowych ani metod, które miałyby zastosowanie do powiadamiania o zmianach okoliczności dotyczących przetwarzania. Jedynie we wspomnianym wcześniej art. 13 ust. 3 i art. 14 ust. 4 RODO mowa jest o poinformowaniu podmiotu danych „przed takim dalszym przetwarzaniem", czyli przed rozpoczęciem przetwarzania danych osobowych w innym celu niż pierwotny. Powiadomienie o zmianach powinno jednak nastąpić z dużym wyprzedzeniem czasowym w stosunku do wejścia zmiany w życie, a metoda zastosowana do zawiadomienia o tych zmianach powinna zapewniać zasadę przejrzystości[113]. Zagwarantowanie odpowiedniej ilości czasu jest konieczne, aby podmiot danych mógł zorientować się, co się zmienia, jak ta zamiana może wpływać na jego sytuację oraz czy chce w związku z tym skorzystać z przysługujących mu uprawnień. Co więcej, aby ułatwić podmiotowi danych zrozumienie sensu wprowadzanych zmian w procesie przetwarzania, dobrą praktyką jest, aby administrator dodatkowo wyjaśnił, jaki będzie prawdopodobny wpływ tych zmian na osoby, których dane dotyczą[114].

W przypadku stałego i długotrwałego przetwarzania danych osobowych może dojść do sytuacji, w której podmiot danych nie będzie pamiętać, jakich informacji udzielił mu administrator na samym początku procesu przetwarzania. Wówczas powiadomienie o zmianach w treści klauzul informacyjnych może okazać się nieefektywne. Aby tego uniknąć, administrator może systematycznie przypominać o treści obowiązku informacyjnego osobom, których dane przetwarza[115]. Może to robić poprzez wysyłanie, w stosownych odstępach czasu, powiadomień o istnieniu polityki ochrony prywatności, panelu do zarządzania danymi

[113] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 19.

[114] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 20.

[115] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 20.

udostępnianego na stronie internetowej itp. Warto też, informując o zmianach, w pierwszej warstwie komunikatu zamieścić informację o tym, czego dotyczą zmiany w przetwarzaniu danych osobowych i jednocześnie odesłać podmiot danych do kolejnej, drugiej warstwy komunikatu, zawierającej pełną treść obowiązku informacyjnego, aby zapewnić w ten sposób podmiotowi danych kompletny obraz okoliczności związanych z przetwarzaniem jego danych osobowych.

4.5. Ograniczenia w realizacji obowiązków informacyjnych

Prawodawca unijny przewidział kilka wyjątków od obowiązku przekazywania osobom, których dane są przetwarzane, informacji dotyczących przetwarzania danych osobowych. W przypadku pozyskiwania danych osobowych bezpośrednio od podmiotu danych i realizowania obowiązku informacyjnego na podstawie art. 13 RODO, administrator nie jest zobowiązany do przekazywania informacji, jeśli **podmiot danych już tymi informacjami dysponuje**[116]. Może to mieć miejsce przykładowo, gdy podmiot danych, będący klientem administratora, nabywa od niego towary w różnych odstępach czasu. Nawet jeśli przy okazji każdego zamówienia podaje swoje dane osobowe, to administrator nie musi za każdym razem spełniać wobec niego na nowo obowiązku informacyjnego, chyba że zmianie uległa jego treść. Ważne jest jednak to, aby administrator – zgodnie z zasadą rozliczalności – był w stanie wykazać właściwe spełnienie obowiązku informacyjnego w momencie pozyskiwania danych osobowych za pierwszym razem.

Więcej wyjątków wprowadzono w odniesieniu do spełniania obowiązku informacyjnego z art. 14 RODO. Zgodnie z art. 14 ust. 5 RODO administrator nie musi przekazywać wymaganych informacji na temat przetwarzania danych osobowych, jeśli – podobnie jak w przypadku art. 13 ust. 4 RODO – osoba, której dane dotyczą, dysponuje już tymi informacjami, a także gdy:

– udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, lub gdy wykonanie obowiązku informacyjnego może uniemożliwić, lub poważnie utrudnić realizację celów przetwarzania (art. 14 ust. 5 lit. b) RODO);

[116] Artykuł 13 ust. 4 RODO.

– pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem unijnym lub krajowym, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą (art. 14 ust. 5 lit. c) RODO), lub
– dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, w tym ustawowym obowiązkiem zachowania tajemnicy (art. 14 ust. 5 lit. d) RODO).

Brak możliwości udzielenia informacji powinien mieć charakter obiektywny – jest to sytuacja zero-jedynkowa, w której administrator może powołać się na czynniki faktycznie uniemożliwiające mu wykonanie obowiązku informacyjnego. Jako przykład Grupa Robocza Art. 29 wskazuje pozyskanie od innego administratora danych osobowych niezawierających jakichkolwiek danych umożliwiających nawiązanie kontaktu z podmiotem danych i przekazanie mu informacji na temat przetwarzania jego danych osobowych (np. brak adresu e-mail, adresu korespondencyjnego, numeru telefonu)[117].

Natomiast więcej wątpliwości rysuje się na tle przesłanki „niewspółmiernie dużego wysiłku". W art. 14 ust. 5 lit. b) RODO wskazano, że okoliczność ta może zaistnieć zwłaszcza w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO[118]. Motyw 62 RODO precyzuje, że należy przy tym uwzględnić liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia. Stosowanie tego wyjątku powinno być jednak ograniczone wyłącznie do sytuacji przetwarzania danych w celach archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych – nie zaś do innych celów[119]. Ponadto, administrator powinien przeprowadzić test równowagi, w którym porówna z jednej strony wysiłek, jaki musi włożyć w udzielenie informacji podmiotowi danych, a z drugiej – potencjalne konsekwencje i skutki dla podmiotu danych w razie nieprzekazania tych informacji. Fakt przeprowadzenia testu i jego wynik, na potrzeby zasady rozliczalności, powinny być odpowiednio udokumentowane.

[117] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 33.

[118] W art. 89 ust. 1 RODO mowa o odpowiednich zabezpieczeniach dla praw i wolności osób, których dane dotyczą. Mają one polegać na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych; mogą też obejmować pseudonimizację danych.

[119] Grupa Robocza Art. 29, *Wytyczne w sprawie przejrzystości…*, s. 35.

Jako przykład zastosowania w praktyce tego wyjątku Grupa Robocza Art. 29 podaje odstąpienie przez szpital od wykonywania obowiązku informacyjnego z art. 14 RODO wobec wszystkich osób wskazywanych w formularzach rejestracyjnych przez pacjentów jako ich osoby bliskie. Biorąc pod uwagę liczbę osób korzystających z usług szpitala, realizowanie obowiązku informacyjnego mogłoby wymagać niewspółmiernie dużego wysiłku. Natomiast okoliczności uzasadniającej odstąpienie od realizacji obowiązku informacyjnego nie stanowi wysokie obciążenie administratora pod względem organizacyjnym lub finansowym – takie stanowisko zaprezentował PUODO w decyzji z dn. 15.03.2019 r. (ZSPR.421.3.2018)[120]. Decyzja ta została co prawda częściowo uchylona przez WSA w Warszawie (sygn. akt: II SA/Wa 1030/19), jednak w odniesieniu do interpretacji przesłanki z art. 14 ust. 5 lit. b) RODO sąd zgodził się z argumentacją organu, wskazując, że na gruncie RODO przez niewspółmiernie duży wysiłek nie można rozumieć kosztu (tak organizacyjnego, który stanowi w istocie o sposobie zorganizowania przez administratora w ramach prowadzonej działalności, wykonania tego zadania, jak i finansowego) dopełnienia obowiązku z art. 14 ust. 1 i 2 RODO[121].

W oparciu o art. 14 ust. 5 lit. b) RODO administrator może także odstąpić od realizacji obowiązku informacyjnego, powołując się na to, że jego wykonanie mogłoby spowodować poważne utrudnienie realizacji celów przetwarzania. Sytuacja taka może mieć miejsce, gdy dane osobowe są przekazywane innym podmiotom lub organom publicznym na potrzeby prowadzonych czynności. Najczęściej jednak takie przekazanie znajduje odrębną podstawę prawną wynikającą z przepisów (np. z regulacji z zakresu przeciwdziałania praniu pieniędzy).

Należy pamiętać, że jeśli administrator zamierza powoływać się na jedną z okoliczności wymienionych w art. 14 ust. 5 lit. b) RODO, powinien zgodnie z tym przepisem podjąć odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą. Takim środkiem może być udostępnienie informacji publicznie, np. na stronie internetowej administratora. Praktyka taka jest aprobowana przez

[120] W sprawie PUODO nałożył na spółkę, która pozyskiwała dane przedsiębiorców z publicznie dostępnych źródeł, karę w wysokości 943 470,00 złotych. W bazie danych spółki znajdowały się dane około 3,59 mln osób fizycznych, przy czym informację o przetwarzaniu danych osobowych spółka wysłała od około 900 000 osób. W pozostałym zakresie odstąpiła od spełniania zindywidualizowanego obowiązku informacyjnego, zamieszczając w zamian stosowną informację na swojej stronie internetowej.

[121] Orzeczenie dostępne na stronie: https://orzeczenia.nsa.gov.pl/doc/30EDD316DA (dostęp: 3.03.2022 r.).

przedstawicieli doktryny[122] oraz, jak się wydaje, przez PUODO, aczkolwiek organ do tej pory wydał sprzeczne decyzje w tym zakresie. W przywołanej wcześniej decyzji organ nie uznał argumentu ukaranej spółki, że wymagane informacje zostały opublikowane na jej stronie internetowej, podczas gdy w decyzji z dn. 30.01.2019 r. (ZSPU.440.574.2018) stwierdził, że forma ta stanowiła przedsięwzięcie odpowiednich i wystarczających środków w kontekście ochrony praw i wolności podmiotu danych.

Wymóg spełnienia obowiązku informacyjnego z art. 14 RODO jest zniesiony także, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w prawie unijnym lub krajowym, któremu podlega administrator, pod warunkiem, że regulacje te ustanawiają jednocześnie odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą. Administrator musi być w stanie wykazać, że pozyskuje dane osobowe w oparciu o takie przepisy, a dokładnie, że przepisy te mają zastosowanie do jego działalności oraz zobowiązują go do pozyskania lub ujawnienia danych osobowych[123].

Poza tym administrator może odstąpić od realizacji obowiązku informacyjnego ze względu na konieczność zachowania tajemnicy zawodowej. W tym przypadku administrator również musi być w stanie wykazać, że obowiązek zachowania tajemnicy wiąże go bezpośrednio i uniemożliwia przekazanie podmiotowi danych wszystkich wymaganych informacji. Administrator, zgodnie z polskim porządkiem prawnym, może więc powoływać się na wiążącą go tajemnicę dziennikarską, lekarską, pielęgniarki i położnej, psychologa, adwokacką, radcowską, notarialną, komorniczą, biegłego rewidenta czy doradcy podatkowego. W literaturze wskazuje się, że w ramach omawianego wyjątku należy też dopuścić możliwość powoływania się na inne tajemnice uregulowane ustawowo, jak tajemnica bankowa, skarbowa lub ubezpieczeniowa[124].

Zakres obowiązków informacyjnych może być ograniczony przez prawodawcę krajowego na mocy normy kompetencyjnej przewidzianej w art. 23 RODO. Z możliwości tej skorzystał

[122] Zob. J. Byrski, H. Hoser, *Nałożenie administracyjnej kary pieniężnej za niezrealizowanie obowiązku informacyjnego przy pozyskiwaniu danych z publicznie dostępnych źródeł – glosa do ostatecznej decyzji Prezesa Urzędu Ochrony Danych Osobowych z 15.03.2019 r. (ZSPR.421.3.2018)*, „Palestra", nr 5/2019, oraz przywołana tam literatura.

[123] Wyjątek ten może mieć zastosowanie przykładowo wobec niektórych organów publicznych, jak organy podatkowe lub administracji z zakresu ubezpieczeń społecznych, które są na mocy przepisów upoważnione do pozyskiwania określonych danych osobowych od przedsiębiorców, pracodawców itp.

[124] J. Łuczak, *Artykuł 14* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 505.

polski ustawodawca, wprowadzając różne zwolnienia z obowiązków informacyjnych Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych)[125]. Przykładowo, zwolnienia wprowadzone zostały w art. 4a ust. 2 i 3 Ustawy z dnia 30 maja 2014 r. o prawach konsumenta[126] czy w art. 13 § 7 Ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze[127].

[125] Dz. U. z 2019 r. poz. 730.

[126] Dz. U. z 2020 r. poz. 287.

[127] Dz. U. z 2021 r. poz. 66.

5. Prawo dostępu – art. 15 RODO

5.1. Zakres prawa

Zapewnienie osobom, których dane dotyczą, prawa dostępu do tych danych osobowych ma realizować dwie podstawowe funkcje w kontekście procesu przetwarzania danych osobowych. Po pierwsze, prawo to ma charakter gwarancyjny i kontrolny, ponieważ umożliwia podmiotowi danych zwrócenie się do dowolnego administratora i zweryfikowanie, czy przetwarza on jego dane osobowe, a jeśli tak, to w jakim zakresie. Po drugie, prawo to ma ułatwiać realizację innych uprawnień przewidzianych na gruncie RODO, a tym samym urzeczywistniać wspomniany aspekt kontrolny. Prawo dostępu do danych jest więc określane mianem uprawnienia o charakterze pierwotnym względem pozostałych, wtórnych uprawnień[128]. Nie oznacza to, że skorzystanie z prawa dostępu jest warunkiem koniecznym do skorzystania z innych praw przez podmiot danych. Wszystkie prawa wynikające z art. 15 – 22 RODO mogą być realizowane niezależnie. Praktyka jednak pokazuje, że wykonanie prawa dostępu często poprzedza skorzystanie z innych praw, ponieważ daje podmiotowi danych konkretną wiedzę w zakresie przetwarzania jego danych osobowych przez administratora, a tym samym podstawy do realizacji pozostałych uprawnień.

Na mocy art. 15 ust. 1 i 2 RODO osoba, której dane dotyczą, ma prawo zażądać od administratora przede wszystkim informacji, czy przetwarza on jej dane osobowe. Jeśli tak, to osoba ta może domagać się dostępu do tych danych oraz podania dodatkowych informacji, takich jak:

– cele przetwarzania;
– kategorie przetwarzanych danych osobowych;
– informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
– planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

[128] P. Fajgielski, *Ogólne rozporządzenie…*, s. 256.

– informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, prawie do wniesienia sprzeciwu wobec przetwarzania oraz informacje o prawie wniesienia skargi do organu nadzorczego;
– jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle[129];
– informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
– jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej – informacje o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Prawo dostępu do danych obejmuje również prawo otrzymania kopii przetwarzanych danych[130].

Przewidziany w art. 15 RODO katalog uprawnień przyznanych podmiotowi danych w ramach prawa dostępu ma charakter zamknięty, aczkolwiek administrator – jeśli uzna to za stosowne lub konieczne ze względu na okoliczności przetwarzania – może przekazać dodatkowe informacje, niewymagane ww. przepisem, które mogą okazać się istotne dla osoby, której dane są przetwarzane[131]. Przekazanie takich dodatkowych informacji będzie zgodne z zasadą rzetelności i przejrzystości przetwarzania.

Prawo dostępu realizowane w oparciu o art. 15 RODO należy odróżnić od podobnych praw przewidzianych w odrębnych przepisach, mających odmienne założenia, np. od prawa dostępu do dokumentów publicznych, którego celem jest zagwarantowanie przejrzystości w procesie podejmowania decyzji przez władze publiczne oraz dobrych praktyk administracyjnych. Przykładowo, art. 15 RODO nie daje podstaw do tego, by realizację określonych w nim uprawnień zrównywać z wynikającym z kodeksu postępowania administracyjnego prawem żądania wydania zaświadczenia na podstawie art. 217 Ustawy

[129] Jeśli administrator pozyskał dane z wielu źródeł lub gdy nie jest w stanie wskazać konkretnego źródła pochodzenia danych, powinien to zrobić w sposób ogólny i opisowy, podając przykładowo, że dane osobowe zostały pozyskane z ogólnodostępnych źródeł, takich jak: portale społecznościowe, strony internetowe, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowy Rejestr Sądowy.

[130] Artykuł 15 ust. 3 RODO.

[131] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 15.

z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (KPA)[132], czy też z prawem żądania dostępu do akt postępowania przez osobę będącą jego stroną[133]. Są to odrębne prawa, które powinny być wykonywane osobno według właściwych procedur.

Prawo dostępu do danych swoim charakterem jest zbliżone do praw informacyjnych wynikających z art. 13 i 14 RODO. Różnica pomiędzy tymi prawami przejawia się w kilku aspektach. Przede wszystkim prawa informacyjne realizowane są z inicjatywy administratora, podczas gdy prawo dostępu co do zasady wymaga aktywnego działania osoby, której dane dotyczą. Nic nie stoi jednak na przeszkodzie, aby to administrator realizował prawo dostępu z własnej inicjatywy, a przynajmniej, aby dostarczał takie rozwiązania, które znacząco ułatwią podmiotowi danych skorzystanie z tego prawa, jak np. zapewnienie dostępu do przetwarzanych danych za pośrednictwem dedykowanego panelu do zarządzania danymi osobowymi, linku umożliwiającego pobranie pliku zawierającego wykaz wszystkich zgromadzonych przez administratora danych osobowych dotyczących podmiotu danych czy poprzez cykliczne wysyłanie wiadomości e-mail z informacjami na temat przetwarzania danych osobowych, w tym z linkiem odsyłającym do wykazu przetwarzanych danych. Takie proaktywne podejście z pewnością jest dobrą praktyką i może być traktowane jako spełnienie ogólnego obowiązku ułatwiania osobie, której dane dotyczą, wykonywania przysługujących jej praw, o którym mowa w art. 12 ust. 2 i motywie 59 RODO.

Wykonywanie praw informacyjnych i prawa dostępu do danych następuje ponadto na różnych etapach procesu przetwarzania. W odniesieniu do praw informacyjnych termin ich realizacji jest z góry określony przez RODO. Jak wcześniej wspomniano, jeśli dane osobowe pozyskiwane są bezpośrednio od podmiotu danych, obowiązek informacyjny z art. 13 RODO powinien być zrealizowany w momencie ich pozyskiwania, natomiast jeśli dane pochodzą z innego źródła – obowiązek informacyjny z art. 14 RODO powinien być zrealizowany najpóźniej przy pierwszej komunikacji z podmiotem danych lub przy pierwszym ujawnieniu danych innemu odbiorcy, a w każdym razie najpóźniej w ciągu miesiąca od ich

[132] Dz. U. z 2021 r., poz. 735, t.j. z dnia 21.04.2021 r. Artykuł 217 § 1 KPA stanowi, że organ administracji publicznej wydaje zaświadczenie na żądanie osoby ubiegającej się o zaświadczenie. Zgodnie z art. 217 § 2 KPA zaświadczenie wydaje się, jeżeli (1) urzędowego potwierdzenia określonych faktów lub stanu prawnego wymaga przepis prawa lub (2) osoba ubiega się o zaświadczenie ze względu na swój interes prawny w urzędowym potwierdzeniu określonych faktów lub stanu prawnego.

[133] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 15; P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017, s. 392–393.

pozyskania. Prawo dostępu do danych – jako co do zasady inicjowane przez podmiot danych – może być wykonane na dalszych etapach przetwarzania, już po zgromadzeniu danych przez administratora. Na tym tle również widać gwarancyjny i kontrolny wymiar prawa dostępu, **jeśli** bowiem **administrator nie dopełni obowiązków informacyjnych przy zbieraniu danych osobowych, lub gdy jest z nich na mocy przepisów zwolniony, podmiot danych mimo to zachowuje swoje prawo do uzyskania informacji na temat przetwarzania jego danych osobowych** w późniejszym terminie, realizując swoje uprawnienia dostępowe[134].

Prawo dostępu do danych, w porównaniu do praw informacyjnych, jest też bardziej zindywidualizowane w tym znaczeniu, że informacje przekazywane w tym przypadku podmiotowi danych muszą odzwierciedlać jego faktyczną sytuację na tle procesu przetwarzania jego danych osobowych. Administrator nie powinien w odpowiedzi na zgłoszony wniosek o prawo dostępu do danych ograniczyć się jedynie do ponownego przekazania takich samych informacji, jak na gruncie art. 13 lub 14 RODO – w zależności od sposobu pozyskania danych, ale powinien, przed udzieleniem odpowiedzi, dokładnie przeanalizować okoliczności towarzyszące przetwarzaniu danych osobowych osoby występującej z wnioskiem i przekazać takie informacje, które dotyczą tej konkretnej osoby i sytuacji. Przykładowo, jeśli administrator pozyskał dane w celu realizacji umowy, a obecnie przechowuje je jedynie dla celów podatkowych, powinien przekazać podmiotowi danych jedynie informacje o aktualnie realizowanych celach. Jeśli administrator nie przetwarza danych na podstawie art. 6 ust. 1 lit. e) lub f) RODO, tj. w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej albo w oparciu o przesłankę uzasadnionego interesu administratora lub strony trzeciej, nie powinien w ramach prawa dostępu przekazywać informacji o prawie do sprzeciwu wobec przetwarzania danych osobowych, ponieważ prawo to nie będzie faktycznie przysługiwać.

Wreszcie, prawo dostępu różni się od praw informacyjnych zakresem przedmiotowym, ponieważ na mocy art. 15 RODO administrator nie musi przekazywać danych identyfikacyjnych administratora i inspektora danych osobowych. Takie ograniczenie nie budzi wątpliwości, gdyż podmiot danych, który realizuje swoje prawo dostępu do danych wobec administratora, nie potrzebuje dostępu do tych informacji. Zastrzeżenia natomiast może budzić fakt, że w ramach prawa dostępu administrator nie jest zobowiązany do informowania o podstawie prawnej przetwarzania danych osobowych. Bez znajomości

[134] P. Fajgielski, *Ogólne rozporządzenie…*, s. 256.

podstawy prawnej przetwarzania weryfikacja poprawności przetwarzania, chociażby pod kątem zasady minimalizacji, ograniczenia celu czy ograniczenia przechowywania, jest utrudniona.

5.2. Sposób skorzystania z prawa dostępu

Podmiot danych może skorzystać z prawa dostępu poprzez skierowanie do administratora stosownego wniosku w tej sprawie, przy czym nie musi on być tak nazwany. Wystarczy, aby z kontekstu i jego treści wynikało, że zamiarem podmiotu danych jest uzyskanie wiedzy, czy administrator przetwarza jego dane osobowe, a także skorzystanie z uprawnienia w postaci dostępu do danych, o ile przetwarzanie faktycznie ma miejsce. **Nie jest wymagane spełnienie jakichkolwiek wymagań przed skierowaniem takiego wniosku**, w szczególności podmiot danych nie musi go w żaden sposób uzasadniać istnieniem interesu faktycznego lub prawnego. Tym samym administrator nie jest uprawniony, aby żądać od podmiotu danych podania przyczyn korzystania z prawa dostępu. Na mocy RODO nie jest także wymagane dopełnienie jakichkolwiek formalności przez osobę korzystającą z prawa dostępu do danych, tak w zakresie formy żądania, jak i jego treści. Podmiot danych może zgłosić swój wniosek w każdej formie, np. ustnej, pisemnej, telefonicznie, mailowo. Niezależnie od wybranej przez podmiot danych formy zgłoszenia, administrator ma obowiązek zgłoszenie przyjąć i odpowiednio na nie zareagować (sposoby realizacji prawa dostępu zostały opisane w pkt 3).

Zdarza się natomiast, że administrator, w celu ułatwienia podmiotom danych korzystania z przysługujących im praw, wdraża w swojej organizacji procedurę realizacji praw podmiotów danych, zawierającą szczegółowe informacje na temat przyjmowania zgłoszeń, sposobów ich rozpatrywania, sposobów prowadzenia komunikacji z osobami korzystającymi ze swoich uprawnień itp. Procedura ta powinna być wyraźnie zakomunikowana podmiotowi danych, najlepiej podczas pozyskiwania danych osobowych (np. przy okazji realizowania obowiązku informacyjnego z art. 13 lub 14 RODO). Jeśli jednak podmiot danych nie skorzysta z ustalonej przez administratora procedury, lecz zgłosi swoje żądanie dostępu w inny sposób, to nie daje to administratorowi podstaw do odmowy rozpoznania wniosku podmiotu danych wyłącznie z przyczyny niedostosowania się do wymogów proceduralnych. W takiej sytuacji administrator powinien przyjąć żądanie (w taki sam sposób, jak w sytuacji, gdyby podmiot danych skorzystał z ustalonej procedury) i rozpocząć procedurę jego rozpatrywania. Może

ewentualnie dodatkowo przekazać informację[135], że w organizacji obowiązuje procedura realizacji praw podmiotów danych, wedle której rozpatrywane są zgłoszenia. Tego typu działanie może być podjęte z myślą o ponownym korzystaniu przez podmiot danych z prawa dostępu lub z innego prawa przewidzianego w RODO – administrator bowiem może zarekomendować skorzystanie z ustalonej procedury w celu szybszego rozpoznania zgłoszenia.

Warto jeszcze dodać, że prawo dostępu do danych może być realizowane w każdym czasie, ponieważ nie ulega przedawnieniu. Podmiot danych nie może zrzec się swojego prawa dostępu do danych, aczkolwiek kwestią otwartą pozostaje to, czy może on zobowiązać się umownie do niewykonywania tego prawa. Z uwagi na bezwzględny charakter praw przysługujących na gruncie RODO, w literaturze wskazuje się, że prawa tego nie można przenieść na inną osobę ani skutecznie go wyłączyć lub ograniczyć wolą stron[136]. Mając jednak na względzie to, jak ewoluuje praktyka w zakresie ochrony danych osobowych na skutek dynamicznego rozwoju technologicznego i wykorzystywania zaawansowanych metod przetwarzania danych osobowych, jak również wzrost wartości danych osobowych i korzyści, jakie wynikają z ich przetwarzania – głównie dla administratorów, ale także podmiotów danych – uważam, że kategoryczny zakaz ograniczania uprawnień przysługujących podmiotom danych nie zawsze znajduje uzasadnienie. Wydaje się, że przy spełnieniu kryterium dobrowolności, należy uznać za dopuszczalne zobowiązanie się do niewykonywania prawa dostępu do danych lub zaakceptowanie ograniczenia tego prawa, jeśli takie zobowiązanie czy akceptacja wynikają z woli podmiotu danych. Warto przy tym poczynić zastrzeżenie, że w takiej sytuacji podmiot danych powinien mieć zagwarantowaną możliwość odwołania złożonego wcześniej oświadczenia woli, a takie odwołanie nie może powodować negatywnych konsekwencji dla podmiotu danych.

Prawo dostępu do danych może być też wykonane przez pełnomocnika w oparciu o pełnomocnictwo udzielone przez osobę, której dane dotyczą. Może być też wykonywane przez przedstawiciela ustawowego.

---

[135] Informację taką można podać wraz z informacją o przyjęciu zgłoszenia, terminem jego rozpoznania itd. Więcej – zob. pkt 5.3.

[136] Zob. P. Fajgielski, *Ogólne rozporządzenie…*, s. 256, i przywołana tamże literatura; J. Łuczak, Artykuł 15 [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 514.

5.3. Sposób realizacji prawa dostępu

Podobnie jak w przypadku każdego prawa przewidzianego w art. 15 – 22 RODO, administrator przede wszystkim powinien ustalić faktyczną treść żądania zgłoszonego przez podmiot danych. Jeśli treść żądania budzi wątpliwości (np. nie wiadomo, czy podmiot danych chce skorzystać z prawa dostępu do danych i uzyskać kopię danych na własne potrzeby, czy może z prawa do przenoszenia danych i uzyskać kopię danych w specjalnym formacie pozwalającym na przeniesienie danych osobowych do zasobów innego administratora), należy ją doprecyzować, zadając osobie występującej z żądaniem dodatkowe pytania zmierzające do ustalenia rzeczywistego zamiaru i oczekiwań podmiotu danych. W kontekście prawa dostępu do danych w niektórych przypadkach zasadne jest doprecyzowanie treści żądania poprzez ustalenie, czy podmiot danych chce uzyskać wszystkie informacje na temat przetwarzania jego danych osobowych, wymienione w art. 15 ust. 1 i 2 RODO, czy tylko niektóre. Może to mieć znaczenie w sytuacji, gdy administrator przetwarza duże ilości danych osobowych, rozproszone w różnych zbiorach. Taka próba doprecyzowania zakresu informacji, które chce otrzymać podmiot danych, jest dopuszczalna na gruncie RODO, gdyż może przyczynić się do szybszej realizacji prawa[137].

Jednocześnie administrator w pierwszych krokach powinien zbadać, czy skierowane do niego żądanie jest ważne, tzn. czy osoba, która je wniosła, jest uprawniona do skorzystania z prawa dostępu oraz czy zgłoszony przez nią zakres żądania odpowiada zakresowi informacji wynikającemu z art. 15 RODO. Ustalenie, czy żądanie zostało wniesione przez osobę uprawnioną, sprowadza się do weryfikacji tożsamości tej osoby[138] i sprawdzenia, czy jej dane osobowe są przetwarzane przez administratora[139]. Natomiast weryfikacja zakresu żądania ma na celu ustalenie, czy zgłoszone żądanie nie wykracza poza prawo dostępu (np. czy podmiot danych nie żąda dostępu do informacji niestanowiących danych osobowych).

Sposób realizacji prawa dostępu zależy od tego, czego dokładnie domaga się podmiot danych. Prawo dostępu przewidziane w art. 15 RODO składa się *de facto* z trzech uprawnień:

1. prawa do informacji, czy administrator przetwarza dane osobowe konkretnej osoby, a jeśli tak, to prawa dostępu do tych danych;

[137] Zob. motyw 63 RODO.

[138] Ewentualnie działającego w jej imieniu pełnomocnika lub przedstawiciela ustawowego.

[139] Szerzej na temat weryfikacji osoby występującej z żądaniem – zob. pkt 3.2 niniejszego opracowania.

2. prawa do informacji związanych z przetwarzaniem danych osobowych, wymienionych w art. 15 ust. 1 i 2 RODO;
3. prawa do otrzymania kopii danych osobowych przetwarzanych przez administratora[140].

W pierwszym przypadku, pod warunkiem potwierdzenia, że administrator przetwarza dane osoby występującej z żądaniem, osoba ta jest uprawniona do otrzymania dostępu do swoich danych. Oznacza to, że administrator powinien umożliwić jej wgląd do treści danych, które przetwarza. Może to zrobić na różne sposoby, np. poprzez odczytanie treści danych, pokazanie na ekranie monitora czy przekazanie wydruku zawierającego dane[141] W motywie 63 RODO wskazano, że „[…] w miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych […]". Podkreśla się przy tym, że zapewnienie możliwości dostępu do danych nie jest jednoznaczne z żądaniem przekazania kopii danych osobowych[142] – są to dwa osobne uprawnienia, choć w praktyce często realizowane łącznie. Warto natomiast zaznaczyć, że **w ramach dostępu do danych podmiot danych ma prawo uzyskać dostęp wyłącznie do informacji o swoich danych osobowych**, a nie do informacji dotyczących innych osób, nawet jeśli informacje te są ze sobą ściśle powiązane lub nie są poufne.

Podmiot danych jest ponadto uprawniony do otrzymania kopii jego danych osobowych przetwarzanych przez administratora. Na tle wykonywania tego uprawnienia powstało kilka wątpliwości praktycznych. Podstawowe pytanie dotyczy tego, czy administrator powinien przekazać kopię danych z własnej inicjatywy, czy tylko w razie sformułowania przez podmiot danych wyraźnego żądania w tym zakresie. Brzmienie art. 15 ust. 3 RODO sugeruje[143], że przekazanie kopii danych powinno nastąpić z inicjatywy administratora, ale w literaturze podnosi się, że przepisu tego nie należy interpretować literalnie, a uprawnienie to stanowi

[140] EROD w swoich wytycznych 01/2022 dotyczących prawa dostępu wyróżnia trzy podstawowe uprawnienia w ramach prawa dostępu, tj. prawo do informacji, czy w ogóle administrator przetwarza dane osobowe konkretnej osoby, prawo dostępu do tych danych oraz prawo dostępu do określonych w przepisie informacji na temat przetwarzania. EROD pomija w tym zakresie prawo do otrzymania kopii przetwarzanych danych osobowych, traktując je jako sposób realizacji prawa dostępu. Zob. EROD, *Guidelines 01/2022 on data subject rights – Right of access*, przyjętych w dn. 18 stycznia 2022, ver. 1 (wersja do publicznych konsultacji), s. 2.

[141] P. Fajgielski, *Ogólne rozporządzenie…*, s. 259.

[142] P. Fajgielski, *Ogólne rozporządzenie…*, s. 259.

[143] Artykuł 15 ust. 3 RODO stanowi, że administrator „dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu".

element prawa dostępu do danych realizowanego na żądanie osoby, której dane dotyczą[144]. Podmiot danych może swobodnie kształtować zakres swojego żądania, a zatem może chcieć skorzystać wyłącznie z prawa dostępu do danych, a nie z prawa do uzyskania kopii tych danych. Mimo to podkreśla się też, że w pewnych przypadkach administrator może uznać za bardziej wygodne lub praktyczne przekazanie podmiotowi danych kopii zawierającej komplet jego danych osobowych, realizując właśnie w taki sposób żądanie pomiotu danych w zakresie dostępu do danych, i to niezależnie od wyrażonych przez podmiot danych preferencji[145]. Wskazuje się też, że niezależnie od zakresu zgłoszonego żądania, administrator ma prawo przyjąć takie rozwiązania techniczne i organizacyjne, na skutek których podmiot uprawniony uzyska zawsze kopię całości jego danych lub wgląd do wszystkich danych, które go dotyczą[146]. Jednak wówczas administrator powinien rozważyć, czy taki sposób realizacji żądania jest zgodny z ogólnym wymogiem ułatwiania podmiotom danych wykonywania przysługujących im praw. Może bowiem okazać się, że przekazana kopia danych jest na tyle obszerna, że podmiot danych z trudem odnajdzie w niej określone informacje objęte żądaniem dostępu.

Odnosząc się do sposobu i formy przekazania kopii danych, wskazać należy, że zasadą jest, iż udzielenie odpowiedzi na żądanie dostępu do danych, w tym przekazanie kopii danych, następuje w sposób odformalizowany, gdyż RODO nie przewiduje w tym zakresie żadnych szczególnych wymagań. Prawo dostępu może być zrealizowane taką samą drogą, którą przekazane było żądanie, co wynika z art. 15 ust. 3 RODO. Przepis ten wskazuje, że jeśli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Jeśli wskaże inny sposób realizacji prawa, administrator powinien wykonać żądanie z uwzględnieniem tego sposobu. Wątpliwość jaka powstała na tym tle dotyczyła natomiast tego, czy administrator powinien przekazać jedynie kopię przetwarzanych danych, czyli samą treść danych, czy może kopię dokumentów zawierających dane osoby występującej z żądaniem. Rozstrzygające w tym zakresie wydaje się stanowisko PUODO, który stwierdził, że „udostępnienie kopii danych zawartych w dokumentach (np. w pismach urzędowych), zgodnie z art. 15 ust. 3 RODO, nie jest równoznaczne z obowiązkiem udostępnienia kopii dokumentów. Administrator nie ma bowiem obowiązku udostępniania osobie zainteresowanej nośnika, na którym przetwarzane są dane osobowe oraz danych, które nie stanowią danych osobowych

144 P. Fajgielski, *Ogólne rozporządzenie…*, s. 261.

145 M. Susałko, *Prawo dostępu* [w:] D. Lubasz (red.), *Meritum…*, s. 174.

146 J. Łuczak, Artykuł 15 [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 511.

w rozumieniu art. 4 pkt 1 RODO i nie dotyczą wnioskującego. Realizując obowiązek wynikający z art. 15 ust. 3 RODO, administrator może poprzestać na wskazaniu treści danych dotyczących osoby, z wyłączeniem pozostałych informacji zawartych na nośniku. Wykonanie obowiązku określonego w art. 15 ust. 3 RODO może być zatem realizowane zarówno poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe oraz inne dane, jak i poprzez podanie uprawnionemu treści jego danych osobowych, z pominięciem informacji znajdujących się w nośniku, które nie są danymi osobowymi w rozumieniu art. 4 pkt 1 RODO”[147].

Otrzymanie pierwszej kopii danych jest bezpłatne. Za każdą kolejną kopię administrator może pobrać opłatę „w rozsądnej wysokości wynikającej z kosztów administracyjnych”[148]. Oznacza to, że administrator może przenieść na podmiot danych ciężar poniesienia kosztów związanych z przygotowaniem takiej kopii. Do kosztów tych można zaliczyć przykładowo koszt opłat pocztowych czy koszt czasu pracy pracownika przygotowującego kopię danych. Ustanowienie opłaty jest fakultatywne i zależy od decyzji administratora, przy czym opłata ta nie może być traktowana przez administratora jako dodatkowe źródło dochodów – jej wprowadzenie ma na celu wyłącznie rekompensatę kosztów przygotowania i przekazania kopii danych, a także ewentualne ograniczenie uciążliwości realizacji tego obowiązku oraz potencjalnego nadużywania prawa przez osoby, których dane dotyczą. W razie ustalenia opłaty, która w ocenie podmiotu danych stanowi nadmierne obciążenie i nie wynika z kosztów administracyjnych, ma on możliwość zakwestionowania jej wysokości, składając skargę do organu nadzorczego na podstawie art. 77 ust. 1 RODO.

W kontekście pobierania opłaty warto zwrócić uwagę na co najmniej dwie sytuacje generujące praktyczne wątpliwości. Po pierwsze, jeśli administrator przekazuje osobie uprawnionej kopię jej danych osobowych, mimo że osoba ta nie sformułowała wyraźnie żądania w tym zakresie, lecz domagała się jedynie dostępu do danych, to można mieć wątpliwość, czy żądanie opłaty za kopię danych jest umotywowane w przypadku, gdy osoba ta po pewnym czasie zwróci się z takim żądaniem do administratora. Takie żądanie będzie przecież pierwszym tego rodzaju żądaniem pochodzącym od podmiotu danych, niemniej

147 Decyzja PUODO z dn. 22.03.2019 r. (ZSZZS.440.660.2018). W swoim stanowisku PUODO zaznaczył również, że w przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie; może dokonać wyboru, czy udostępnia kopię dokumentów, czy kopię danych zawartych w tych dokumentach.

148 Artykuł 15 ust. 3 RODO.

jednak w razie jego realizacji podmiot danych uzyska *de facto* kolejną kopię danych, a nie pierwszą. Wydaje się zatem, mając przy tym na względzie brzmienie przepisu[149], że w takiej sytuacji administrator mógłby pobrać opłatę za przygotowanie i przekazanie kopii danych, jeśli kopia ta zawiera te same dane osobowe co kopia uprzednio przekazana podmiotowi danych[150]. Należy bowiem pamiętać, że jedną z funkcji wprowadzenia opłat za kolejne kopie jest przeciwdziałanie nadużywaniu tego prawa przez osoby, których dane dotyczą. W opisanym powyżej przykładzie funkcja ta byłaby realizowana, aczkolwiek można sobie również wyobrazić sytuacje, w których pobranie opłaty za kopię – zażądaną po raz pierwszy przez podmiot danych, choć *de facto* kolejną – może działać ograniczająco na prawo dostępu do danych.

Po drugie, RODO nie tylko nie definiuje samego pojęcia „kopia danych"[151], ale też nie zawiera żadnych wskazówek odnośnie do odstępów czasowych żądania owych kopii, co w pewnych przypadkach może powodować trudności w ustaleniu, czy mamy do czynienia z kolejną kopią, a w konsekwencji wiązać się z wątpliwym nakładaniem opłat zgodnie z art. 15 ust. 3 RODO. Uważam, że nie należy na przykład pobierać opłaty za kolejną kopię danych, jeśli żądanie w tym zakresie zostało zgłoszone przez podmiot danych po upływie znacznego okresu czasu od pierwszego żądania, np. kilku lat. Nawet jeśli zawartość merytoryczna kolejnej kopii danych jest tożsama z zawartością wcześniej przekazanej kopii, to ze względu na upływ czasu podmiot danych nie zawsze jest w stanie antycypować, że zakres przetwarzanych danych nie uległ zmianie. Wprost przeciwnie – w takim przypadku skorzystanie z prawa

[149] W art. 15 ust. 3 RODO wskazane jest, że administrator może pobrać opłatę „za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą". Akcent położony jest więc na „kolejne kopie", a nie kolejne żądania zgłoszone przez podmiot danych. W kontekście omawianej sytuacji może to być argument uzasadniający pobranie opłaty.

[150] Analogicznie wskazuje M. Susałko, podając następujący przykład: „[..] biorąc pod uwagę, że podmiot danych może żądać, zamiast wydania kopii wszystkich danych zgromadzonych przez administratora, wyłącznie określonych danych, np. wyników badań medycznych dotyczących diagnozowania konkretnego schorzenia lub informacji o liczbie wizyt w fitness clubie w określonym okresie, należy uznać, że odpłatność za kolejne kopie może dotyczyć wyłącznie sytuacji, kiedy podmiot danych żąda wydania kopii tych samych danych, które już raz uzyskał". Zob. M. Susałko, *Prawo dostępu* [w:] D. Lubasz (red.), *Meritum…*, s. 175.

[151] Szerzej opisuje ten problem M. Sakowska-Baryła, wskazując m.in. że nie wiadomo, czy w danym przypadku administrator powinien udostępniać kopię wszystkich danych osobowych dotyczących konkretnej osoby, czy też prawo do kopii danych może odnosić się do poszczególnych zbiorów, których te dane są częścią, bądź też do poszczególnych czynności przetwarzania danych, ujętych w rejestrze czynności przetwarzania danych prowadzonym na podstawie w art. 30 RODO". Zob. M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 15.

dostępu do danych spełnia funkcję gwarancyjną i kontrolną, umożliwiając osobie, której dane dotyczą, weryfikację poprawności przetwarzania jej danych osobowych, choćby w kontekście zasady ograniczenia celu przetwarzania lub ograniczenia przechowywania. Niemniej jednak warto poczynić zastrzeżenie, że nawet w takiej sytuacji podmiot danych może skorzystać w pierwszej kolejności z uprawnienia dostępu do danych osobowych, zamiast od razu z uprawnienia żądania wydania kopii tych danych.

Na koniec, odnosząc się do terminu realizacji prawa dostępu, wskazać należy, że w razie uznania przez administratora, iż zachodzą przesłanki do uwzględnienia żądania podmiotu danych, prawo to powinno być wykonane zgodnie z ogólnymi terminami wynikającymi z art. 12 ust. 3 lub 4 RODO, tj. zasadniczo w ciągu miesiąca od otrzymania zgłoszenia. Ewentualnie z uwagi na skomplikowany charakter żądania lub liczbę żądań termin ten może być wydłużony o kolejne dwa miesiące. Jeśli administrator zamierza wydłużyć termin udzielenia odpowiedzi, powinien o tym poinformować podmiot danych.

Ważne jest odnotowanie przez administratora dokładnej daty wpływu żądania, aby móc w przyszłości wykazać, że żądanie zostało zrealizowane terminowo. Wspomniane terminy, wbrew pozorom, w niektórych przypadkach mogą okazać się niewystarczające, zwłaszcza jeśli administrator przetwarza duże ilości danych lub korzysta w tym zakresie z usług różnych podmiotów przetwarzających. Rolą administratora jest więc takie zorganizowanie procesu przetwarzania, aby mógł tych terminów dochować, m.in. poprzez sprawowanie realnej kontroli nad sposobami przetwarzania danych osobowych. Administrator musi orientować się w tym, jakie posiada zasoby danych, jak są one tworzone i przechowywane, kto ma do nich dostęp itd. Pomocne w tym zakresie może być ustanowienie wewnętrznych procedur, w tym procedur realizacji praw podmiotów danych. W ramach takiej procedury administrator może określić poszczególne etapy realizacji zgłoszonych żądań, metody weryfikacji tożsamości osoby występującej z żądaniem, sposoby prowadzenia komunikacji z podmiotem danych, ustalając przy tym ramy czasowe konkretnych działań podejmowanych zgodnie z procedurą rozpatrywania zgłoszenia. Warto też pamiętać, że podmiot danych może skierować żądanie nie bezpośrednio do administratora, lecz do podmiotu przetwarzającego. Wówczas procesor powinien odnotować datę wpływu żądania i niezwłocznie przekazać je do administratora celem podjęcia dalszych kroków, chyba że co innego wynika z postanowień umowy

powierzenia przetwarzania[152]. Kwestie rozpoznawania żądań podmiotów danych powinny być też przedmiotem uzgodnień poczynionych pomiędzy współadministratorami, przy czym niezależnie od tych ustaleń podmiot danych i tak zachowuje prawo do wniesienia żądania do któregokolwiek ze współadministratorów.

5.4. Wyłączenia

Prawodawca unijny przewidział jeden wyjątek, kiedy administrator ma prawo odmówić realizacji żądania podmiotu danych. Mowa o sytuacji, w której wydanie kopii przetwarzanych przez administratora danych mogłoby niekorzystnie wpływać na prawa i wolności innych osób[153], przy czym za negatywny wpływ na prawa i wolności innych osób uważa się nie tylko prawa i wolności w sferze ochrony danych osobowych i prywatności, ale także inne, w tym prawo do ochrony tajemnicy handlowej, praw własności intelektualnej, praw autorskich itd.[154] Wymaga zaakcentowania, że – posiłkując się literalną wykładnią przepisu – wyłączenie to odnosi się tylko do jednego z uprawnień przysługujących podmiotowi danych w ramach prawa dostępu, a mianowicie prawa do posiadania kopii danych. Ryzyko niekorzystnego wpływu na prawa i wolności innych nie powinno więc stanowić uzasadnienia odmowy wykonania pozostałych uprawnień, tj. prawa do informacji, czy administrator w ogóle przetwarza dane konkretnej osoby, prawa dostępu do tych danych oraz prawa uzyskania dodatkowych informacji dotyczących ich przetwarzania, wymienionych w art. 15 ust. 1 i 2 RODO. Wydaje się jednak, że taka interpretacja nie jest właściwa, zwłaszcza w kontekście wyjaśnień prezentowanych w motywie 63 RODO. W motywie tym wskazano, że „prawo to", tj. w odniesieniu do prawa dostępu do danych w ogóle, a nie tylko do prawa do kopii danych nie powinno negatywnie wpływać na prawa lub wolności innych osób. W dostępnej

[152] Przykładowo, na mocy umowy powierzenia procesor może być też zobowiązany do przeprowadzenia procesu weryfikacji tożsamości osoby występującej z żądaniem. Jest to zasadne, zwłaszcza w przypadkach, gdy to procesor ma faktyczny dostęp do przetwarzanych danych i może taki proces przeprowadzić skuteczniej. Niemniej jednak nie zwalnia to administratora z odpowiedzialności za ewentualny błąd po stronie procesora i umożliwienie dostępu do danych osobie nieuprawnionej lub bezpodstawną odmowę takiego dostępu na skutek błędnie przeprowadzonej weryfikacji. W takich sytuacjach dobrym rozwiązaniem może być zobowiązanie procesora do skonsultowania się z administratorem przed udzieleniem odpowiedzi osobie zgłaszającej żądanie.

[153] Artykuł 15 ust. 4 RODO.

[154] Motyw 63 RODO.

literaturze przedmiotu wątek ten nie jest jednak szerzej przeanalizowany[155]. Na zagadnienie to również zwraca uwagę EROD w swoich wytycznych dotyczących prawa dostępu, w wersji przekazanej do publicznych konsultacji, wskazując, że w tym kontekście interpretacja wyjątku z art. 15 ust. 4 RODO nie powinna być zawężana wyłącznie do kopii danych[156].

Ocena, czy sporządzenie i przekazanie kopii danych może negatywnie wpływać na prawa i wolności innych, powinna stanowić stały element procedury rozpoznawania żądania podmiotu danych. Administrator powinien tę okoliczność weryfikować za każdym razem, jej istnienie lub brak zależy bowiem od charakteru i kontekstu przetwarzania danych osobowych. Niezależnie jednak od tego, że wyjątek w realizacji prawa dostępu literalnie dotyczy tylko uprawnienia do uzyskania kopii danych, administrator powinien być też przygotowany, aby w każdym przypadku realizować prawo dostępu w taki sposób, aby zakres udostępnianych informacji nie obejmował danych osobowych innych podmiotów – jeśli to w danym przypadku nie jest konieczne. Przedmiotem żądania realizowanego przez podmiot danych jest bowiem dostęp do jego danych osobowych, a nie do danych osobowych innych osób[157]. Jeśli administrator nie jest w stanie zrealizować prawa dostępu bez negatywnego wpływu na prawa lub wolności innych podmiotów, powinien o tym zawiadomić podmiot występujący z żądaniem. Okoliczność ta nie powinna jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji[158]. Administrator powinien więc zrealizować prawo dostępu w możliwym dopuszczalnym zakresie. Warto też w tym miejscu podkreślić, że zgodnie z art. 24 ust. 1 RODO jednym z podstawowych obowiązków administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodności przetwarzania z rozporządzeniem, a więc w kontekście analizowanego wyjątku administrator zasadniczo powinien przyjąć takie rozwiązania, które umożliwią mu realizację prawa dostępu do danych, w tym przekazanie kopii danych. Przykładowo, jeśli administrator stosuje monitoring wizyjny, powinien dysponować technologią umożliwiającą rozmycie wizerunku osób innych niż podmiot danych.

---

155 M. Sakowska w komentarzu do art. 15 RODO odnosi omawiany wyjątek jedynie do uprawnienia dotyczącego kopii danych – zob. M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 15. Podobnie P. Fajgielski – zob. P. Fajgielski, *Ogólne rozporządzenie…*, s. 261, a także J. Łuczak – zob. J. Łuczak, Artykuł 15 [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 513. Inaczej M. Susałko, która odnosi wyłączenie z art. 15 ust. 4 RODO do prawa dostępu jako takiego, a nie tylko do jednego z elementów tego prawa, jakim jest uprawnienie do kopii danych – zob. M. Susałko, *Prawo dostępu* [w:] D. Lubasz (red.), *Meritum…*, s. 175.

156 Zob. EROD, *Guidelines 01/2022…*, s. 4.

157 Por. uwagi w pkt. 5.5. niniejszego opracowania.

158 Motyw 63 RODO.

Dodatkowe ograniczenia w realizacji prawa dostępu zostały wprowadzone do polskiego porządku prawnego na mocy normy kompetencyjnej przewidzianej w art. 23 RODO. Ograniczenia te wprowadzono m.in. do:

- prawa o adwokaturze[159],
- ustawy o radcach prawnych[160],
- prawa o notariacie[161],
- prawa o prokuraturze[162],
- prawa o ustroju sądów powszechnych[163],
- prawa budowlanego[164].

5.5. Prawo dostępu w świetle wytycznych EROD

18 stycznia 2022 r. EROD wydała wytyczne dotyczące prawa dostępu, o którym mowa w art. 15 RODO. Wytyczne obecnie znajdują się w fazie publicznych konsultacji, w związku z czym opublikowanej wersji nie należy traktować jako ostatecznej, ponieważ treść poszczególnych zaleceń może jeszcze ulec modyfikacjom, choć zapewne nieznacznym. Mimo to, warto odnieść się do kilku najistotniejszych kwestii, które EROD podkreśla w dokumencie.

[159] Zob. art. 16a ust. 1 Ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2020 r., poz. 1651, t.j. z dnia 25.09.2020 r.), stanowiący że przepisy art. 15 ust. 1 i 3 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez adwokata tajemnicy zawodowej.

[160] Zob. art. 5a ust. 1 Ustawy z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. z 2020 r., poz. 75, t.j. z dnia 16.01.2020 r.), stanowiący że przepisy art. 15 ust. 1 i 3 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez radcę prawnego tajemnicy zawodowej.

[161] Zob. art. 78b § 1 Ustawy z dnia 14 lutego 1991 r. Prawo o notariacie (Dz. U. z 2020 r., poz. 1192, t.j. z dnia 3.07.2020 r.), stanowiący że przepisy art. 15 ust. 1 i 3 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez notariusza tajemnicy zawodowej.

[162] Zob. art. 13 § 7 ustawy Prawo o prokuraturze stanowiący, że o przetwarzania danych osobowych w postępowaniach lub systemach teleinformatycznych w ramach realizacji zadań, o których mowa w art. 2 ustawy, art. 15 RODO nie stosuje się.

[163] Zob. art. 175dc § 1 Ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2020 r., poz. 2072, t.j. z dnia 24.11.2020 r.), stanowiący że do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych nie stosuje się przepisów art. 15 RODO.

[164] Zob. art. 84aa ust. 1 Ustawa z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 2021 r., poz. 2351, t.j. z dnia 20.12.2021 r.), stanowiący że w związku z przetwarzaniem przez organy administracji architektoniczno-budowlanej i organy nadzoru budowlanego danych osobowych w toku realizacji zadań określonych w ustawie prawo, o którym mowa w art. 15 ust. 1 lit. g) RODO, przysługuje w zakresie, w jakim nie ma wpływu na ochronę praw i wolności osoby, od której dane pozyskano.

EROD zwraca uwagę, że zakres prawa dostępu jest określony przez zakres pojęcia danych osobowych zdefiniowany w art. 4 pkt 1 RODO. Zakres ten może być szeroki i obejmować podstawowe dane, jak imię i nazwisko, adres, numer telefonu itp., ale też – w zależności od rodzaju działalności administratora – np. dane medyczne, historię zakupów, wskaźniki zdolności kredytowej, dzienniki aktywności internetowej czy działania związane z wyszukiwaniem; zakres ten obejmuje też dane osobowe, które zostały poddane pseudonimizacji, ponieważ są one nadal danymi osobowymi. Co więcej, dane, które mogą być nieprawidłowe lub przetwarzane niezgodnie z prawem, również powinny być udostępnione przez administratora. Wyjątek dotyczy jedynie danych usuniętych zgodnie z przyjętą polityką retencji – oczywistym jest, że takich danych administrator nie musi przekazywać[165].

Prawo dostępu, choć odnosi się do danych osobowych dotyczących osoby składającej wniosek, w pewnych przypadkach nie powinno być ograniczane wyłącznie do tych danych, gdyż w zależności od sytuacji może ono obejmować także dane dotyczące innych osób, np. historię komunikacji obejmującą wiadomości przychodzące i wychodzące czy historię interakcji z innymi osobami w social mediach[166]

Administrator powinien mieć też możliwość spełnienia prawa dostępu w sposób warstwowy. Takie rozwiązanie byłoby optymalne, zwłaszcza gdy przetwarza on dużą ilość danych, przez co osobie, której dane dotyczą, trudno byłoby zrozumieć wszystkie udostępniane informacje, gdyby administrator przekazał je jednocześnie. Dostarczanie informacji w różnych warstwach może ułatwić osobie, której dane dotyczą, zrozumienie tych informacji oraz odszukanie interesujących ją danych, które są przetwarzane. Administrator musi jednak być w stanie wykazać, że podejście warstwowe ma wartość dodaną dla podmiotu danych, a wszystkie warstwy powinny być udostępniane jednocześnie, jeśli osoba, której dane dotyczą, tego zażąda[167].

W odniesieniu do terminu realizacji prawa dostępu EROD podkreśla, że mimo miesięcznego terminu na udzielenie odpowiedzi, a nawet możliwości wydłużenia tego terminu o kolejne dwa miesiące, administrator musi mieć na uwadze ogólne terminy usunięcia danych. Jeżeli dane są przechowywane tylko przez bardzo krótki okres, administrator musi wdrożyć środki

165 EROD, *Guidelines 01/2022…*, s. 4.

166 EROD, *Guidelines 01/2022…*, s. 3.

167 EROD, *Guidelines 01/2022…*, s. 3.

gwarantujące, że wniosek o dostęp będzie zrealizowany bez usuwania danych w trakcie jego rozpatrywania[168].

EROD akcentuje też, że oprócz wyjątku przewidzianego w art. 15 ust. 4 RODO, administrator może odmówić realizacji żądania na podstawie art. 12 ust. 5 RODO, jeśli żądanie jest wyraźnie nieuzasadnione lub nadmierne[169]. Przepisu tego jednak nie należy interpretować rozszerzająco. EROD zauważa, że w przypadku prawa dostępu administrator rzadko w praktyce będzie mógł się powołać na to, że żądanie jest nieuzasadnione, ponieważ realizacja prawa dostępu nie jest warunkowana spełnieniem wielu przesłanek. Natomiast powoływanie się na nadmierną liczbę wniosków zależy od specyfiki sektora, w którym działa administrator danych – im częściej zachodzą zmiany w bazie danych administratora, tym częściej podmiot danych może mieć prawo do składania wniosków o dostęp, i wnioski te nie będą uznawane za nadmierne[170]. Należy przy tym pamiętać, że administrator zawsze musi być w stanie wykazać, iż wniosek jest w sposób oczywisty nieuzasadniony lub nadmierny.

168 EROD, *Guidelines 01/2022…*, s. 4.

169 EROD, *Guidelines 01/2022…*, s. 4, 53.

170 EROD, *Guidelines 01/2022…*, s. 4, 53–56.

6. Prawo do sprostowania danych – art. 16 RODO

6.1. Zakres prawa

Osoba, której dane dotyczą, może żądać od administratora sprostowania jej danych osobowych, co oznacza, iż ma prawo żądać usunięcia danych nieprawidłowych lub ich aktualizacji poprzez wprowadzenie odpowiednich zmian mających na celu doprowadzenie do zgodności przetwarzanych danych ze stanem faktycznym[171]. Uprawnienie to jest ściśle związane z jedną z podstawowych zasad przetwarzania danych osobowych, jaką jest zasada prawidłowości, zobowiązująca administratora do podejmowania wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane[172]. Prawo do sprostowania danych jest więc kolejnym uprawnieniem kontrolnym przysługującym podmiotowi danych, dzięki któremu może on skutecznie egzekwować od administratora przestrzeganie zasad przetwarzania.

Prawodawca unijny w motywie 65 RODO wskazał, że każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących, jeżeli zatrzymywanie takich danych narusza rozporządzenie, prawo unijne lub prawo krajowe, któremu podlega administrator. Przetwarzanie danych nieprawidłowych niewątpliwie stanowi naruszenie przepisów o ochronie danych osobowych, i to niezależnie od tego, czy takie przetwarzanie zagraża prawom lub wolnościom podmiotu danych, czy nie.

W ramach prawa do sprostowania danych osoba, której dane dotyczą, może również żądać uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia, jeśli jest to uzasadnione z perspektywy celów przetwarzania danych osobowych.

Podmiot danych może dokonać sprostowania dotyczących go danych osobowych, rozumianych – zgodnie z art. 4 pkt 1 RODO – jako informacje o zidentyfikowanej lub możliwej

171 Art. 16 RODO.

172 Art. 5 ust. 1 lit. d) RODO.

do zidentyfikowania osobie fizycznej. W praktyce każda informacja pozwalająca na pośrednią lub bezpośrednią identyfikację konkretnej osoby fizycznej może być traktowana jako dana osobowa. Chodzi zarówno o informacje o charakterze obiektywnym, jak np. imię i nazwisko, numer identyfikacyjny czy adres zamieszkania, jak i o informacje subiektywne, wywnioskowane przez administratora na podstawie zachowania podmiotu danych czy inne posiadane informacje na jego temat. Jako dane osobowe możemy traktować więc dane zaobserwowane lub wydedukowane przez administratora, dotyczące np. preferencji zakupowych, zainteresowań, sposobu spędzania wolnego czasu, światopoglądu czy przynależności religijnej. Do danych osobowych należą także opinie administratora dotyczące podmiotu danych, np. opinie pracodawcy o sposobie wykonywania pracy przez pracownika. Takie dane również podlegają sprostowaniu, tj. zarówno dane będące podstawą wnioskowania (np. dane medyczne zgromadzone w dokumentacji lekarskiej), jak i dane stanowiące jego efekt (np. postawiona diagnoza i rodzaj przyjętego leczenia). Podmiot danych ma bowiem prawo do sprostowania wszelkich nieprawidłowych lub niekompletnych danych osobowych, których przetwarzanie doprowadziło administratora do błędnych wyników. Jeśli administrator stosuje zautomatyzowane podejmowanie decyzji, w tym profilowanie, podmiot danych ma prawo domagać się sprostowania danych wykorzystywanych w tym procesie i branych pod uwagę przy podejmowaniu decyzji czy przy profilowaniu. Wynika to z tego, że przetwarzanie nieprawidłowych lub niekompletnych danych może mieć negatywny wpływ na sytuację podmiotu danych i może powodować ryzyko naruszenia jego praw lub wolności. Zwraca na to uwagę Grupa Robocza Art. 29 w wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania. Wskazuje, że art. 16 RODO może mieć zastosowanie na przykład w sytuacji, gdy osoba fizyczna zostaje zakwalifikowana do kategorii, która określa jej zdolność do wykonania danego zadania, przy czym profil ten opiera się na nieprawidłowych informacjach. Wtedy osoba ta może zakwestionować prawidłowość wykorzystanych danych oraz słuszność zakwalifikowania ich do danej grupy lub kategorii[173].

[173] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, z 3.10.2017 r., zmienione i przyjęte 6.02.2018 r., WP251rev.01, s. 20.

6.2. Sposób skorzystania z prawa do sprostowania

Podmiot danych może zwrócić się do administratora z prośbą o realizację prawa do sprostowania jego danych osobowych, prawa do uzupełnienia jego danych osobowych lub też może zażądać realizacji obydwu uprawnień jednocześnie. Kierując swoje żądanie, podmiot danych powinien wykazać, że przetwarzane przez administratora dane osobowe są nieprawidłowe lub wymagają uzupełnienia – ciężar dowodu w tym przypadku spoczywa na osobie, która występuje z żądaniem. Jak stanowi art. 16 zd. 2 RODO, może w tym celu posłużyć się dodatkowym oświadczeniem. Przepis nie precyzuje, czy oświadczenie to musi pochodzić od podmiotu danych, czy nie, wobec czego można przyjąć, że może być ono wydane przez inny podmiot, np. pracodawcę czy organ publiczny. Z jego treści powinno jasno wynikać, jakie dane uległy zmianie.

Jeśli żądanie sprostowania lub uzupełnienia danych jest w ocenie administratora wątpliwe, może on zażądać przedstawienia dodatkowych dowodów, dokumentów lub oświadczeń potwierdzających prawdziwość prostowanych lub uzupełnianych danych. Administrator nie jest przy tym związany żądaniem podmiotu danych. Za każdym razem, uwzględniając okoliczności przetwarzania odnoszące się do konkretnego indywidualnego przypadku, musi ocenić, czy zgłoszone żądanie zasługuje na uwzględnienie, czy nie. Ocena ta powinna być oczywiście odpowiednio udokumentowana w celu spełnienia zasady rozliczalności.

6.3. Sposób realizacji prawa do sprostowania

Sprostowanie danych osobowych zwykle ma miejsce w następstwie zgłoszenia przez podmiot danych odpowiedniego żądania. Niemniej jednak sprostowanie może też nastąpić z inicjatywy administratora, jeśli stwierdzi on, że dane przez niego przetwarzane są nieprawidłowe.

Sposób realizacji prawa do sprostowania zależy od zakresu żądania zgłoszonego przez podmiot danych. Jeśli podmiot danych wnioskuje o sprostowanie jego danych osobowych, które są nieprawidłowe, administrator musi zweryfikować, czy faktycznie przesłanka nieprawidłowości danych jest spełniona, np. na podstawie oświadczenia lub dokumentu

złożonego przez podmiot danych. Jeśli osoba, której dane dotyczą, wnioskuje o uzupełnienie jej danych osobowych, administrator powinien przede wszystkim ocenić, czy uzupełniane dane są niezbędne z perspektywy celów przetwarzania. Ewentualne uwzględnienie żądania podmiotu danych nie może prowadzić do przetwarzania danych nadmiarowych i nieprzydatnych dla celów przetwarzania, powodując tym samym naruszenie zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c) RODO. Administrator nie jest więc zobowiązany do uzupełnienia danych – w ocenie podmiotu danych – niekompletnych, jeśli jego zdaniem dane te są wystarczające dla celów przetwarzania. W sytuacji, gdy administrator zdecyduje się uzupełnić dane zgodnie z żądaniem, powinien je jeszcze ocenić pod kątem ich prawidłowości. Oprócz wymogów zasady minimalizacji danych, administrator musi też pamiętać o spełnieniu zasady prawidłowości wynikającej z art. 5 ust. 1 lit. d) RODO, a zatem jeśli ma uzasadnione wątpliwości co do prawdziwości uzupełnianych danych, powinien odmówić realizacji żądania. Zaleca się, aby analiza adekwatności i prawidłowości danych w ramach realizacji prawa do sprostowania była tym bardziej wnikliwa, im większe jest ryzyko naruszenia praw i wolności podmiotu danych zgłaszającego żądanie[174].

Dane nieprawidłowe, które administrator na skutek żądania zastępuje nowymi, prawidłowymi danymi, nie muszą być przez niego usuwane. Administrator może je zatrzymać w swoich zasobach i usunąć zgodnie z terminami określonymi w polityce retencji, zwłaszcza jeśli dane te mogą być w przyszłości przydatne. Mowa tu o takich sytuacjach, jak przykładowo sprostowanie danych dotyczących zdrowia[175] czy danych finansowych[176]. Jeśli nie zachodzi potrzeba przechowywania danych objętych sprostowaniem, administrator powinien je usunąć[177].

[174] M. Susałko, *Prawo do sprostowania* [w:] D. Lubasz (red.), *Meritum…*, s. 180.

[175] Przykładowo poprzez dołączenie do dokumentacji medycznej nowych wyników badań, na skutek czego zmianie ulega diagnoza medyczna. W takim przypadku zasadne wydaje się pozostawienie danych dotyczących starej diagnozy.

[176] Przykładowo podmiot danych żąda sprostowania danych dotyczących jego zadłużenia, przedstawiając dokumenty potwierdzające spłatę istniejących długów. Administrator może uwzględnić żądanie i usunąć podmiot danych z rejestru aktualnych dłużników, jednak może być zobowiązany przechowywać dane dotyczące zadłużeń w celu wypełnienia obowiązków prawnych na nim ciążących.

[177] Przykładowo, gdy podmiot danych żąda sprostowania nazwiska, numeru telefonu czy adresu zamieszkania. Wówczas przechowywanie nieaktualnych danych może okazać się niecelowe, aczkolwiek ocena w tym zakresie zawsze należy do administratora.

Należy ponadto pamiętać, że przystąpienie przez administratora do realizacji zgłoszonego żądania musi być poprzedzone prawidłowym ustaleniem tożsamości podmiotu danych. Z kolei proces realizacji żądania powinien czasowo mieścić się w ogólnych terminach wynikających z art. 12 ust. 3 RODO, tj. administrator powinien wykonać prawo zasadniczo niezwłocznie, nie później niż w ciągu miesiąca od otrzymania żądania. W wyjątkowych przypadkach, z uwagi na skomplikowany charakter żądania lub liczbę żądań, administrator może ten termin wydłużyć o kolejne dwa miesiące. W razie uwzględnienia żądania i dokonania sprostowania danych osobowych administrator musi też pamiętać o wynikającym z art. 19 RODO obowiązku poinformowania o dokonanym sprostowaniu danych każdego odbiorcę, któremu ujawnił dane osobowe. Administrator może uchylić się od tego obowiązku, jeśli okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Poza tym administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda. Szerzej na ten temat – zob. pkt 3.5 niniejszego opracowania.

6.4. Wyłączenia

Przepisy ogólnego rozporządzenia nie przewidują wyjątków od prawa do sprostowania danych osobowych. Administrator zachowuje natomiast prawo do odmowy uwzględnienia żądania, jeśli nie są spełnione jego przesłanki opisane wcześniej. Na mocy art. 12 ust. 5 RODO administrator ma także prawo odmówić spełnienia żądania, jeśli w jego ocenie jest ono ewidentnie nieuzasadnione lub nadmierne, przy czym obowiązek wykazania tych okoliczności obciąża administratora. W odniesieniu do omawianego prawa wydaje się, że za ewidentnie nieuzasadnione żądanie sprostowania danych osobowych można uznać żądanie osoby, której dane nie są w ogóle lub już nie są przetwarzane przez administratora, a za nadmierne – żądanie, na podstawie którego podmiot domaga się uzupełnienia dotyczących go danych osobowych w sposób znacząco wykraczający poza to, co niezbędne z perspektywy celów przetwarzania. W tym drugim przypadku administrator, odmawiając uwzględnienia żądania, może jednak powołać się nie tyle na jego nadmierny charakter, co przede wszystkim na brak spełnienia przesłanki realizacji prawa.

W kontekście wyłączeń prawa do sprostowania warto zaznaczyć, że niektóre przepisy krajowe, zwłaszcza proceduralne, zawierają szczegółowe uregulowania w zakresie sprostowania przetwarzanych danych. Przykładowo, na podstawie art. 113 § 1 KPA

organ administracji publicznej może z urzędu lub na żądanie strony prostować w drodze postanowienia błędy pisarskie i rachunkowe oraz inne oczywiste omyłki w wydanych decyzjach. Jeśli więc w decyzji administracyjnej znajduje się literówka w oznaczeniu strony lub inny błąd dotyczący danych osobowych strony postępowania, strona ta powinna domagać się sprostowania w ramach przewidzianej w KPA procedury, nie zaś na podstawie art. 16 RODO. Analogiczna sytuacja będzie mieć miejsce na gruncie postępowania cywilnego i prostowania błędów pisarskich lub innych oczywistych omyłek w treści wydanego przez sąd wyroku[178].

[178] Zob. art. 350 § 1 Ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, Dz. U. z 2021 r., poz. 1805 t.j. z dn. 4.10.2021 r.

7. Prawo do usunięcia danych („prawo do bycia zapomnianym") – art. 17 RODO

7.1. Zakres prawa

Jednym z celów reformy prawa ochrony danych osobowych w UE było wzmocnienie ochrony użytkowników Internetu poprzez zapewnienie skutecznego prawa do bycia zapomnianym, zwłaszcza w środowisku internetowym[179]. Prawo do usunięcia danych osobowych, zwane również prawem do bycia zapomnianym[180], jest więc kolejnym uprawnieniem o charakterze kontrolnym przysługującym osobie, której dane dotyczą, na gruncie RODO, pozwalającym na żądanie usunięcia danych osoby fizycznej z zasobów administratora, jeśli ich przetwarzanie narusza RODO, inne przepisy unijne lub krajowe.

Na podstawie art. 17 ust. 1 RODO podmiot danych ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jego danych osobowych, a administrator

[179] Zob. motyw 65 i 66 RODO; KE, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku"*, COM(2012) 9 final, Bruksela, dn. 25.01.2012 r., s. 6.

[180] W literaturze wyrażony został pogląd, że prawo do usunięcia danych dotyczy uprawnienia przewidzianego w art. 17 ust. 1 RODO, czyli prawa żądania usunięcia danych osobowych przez administratora *sensu stricto*, podczas gdy prawo do bycia zapomnianym odnosi się do obowiązku powiadomienia przez administratora, który upublicznił te dane, o usunięciu danych innych administratorów, wynikającym z art. 17 ust. 2 RODO – zob. M. Czerniawski, *Artykuł 17* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 524; M. Susałko, *Prawo do usunięcia danych (prawo do bycia zapomnianym)* [w:] D. Lubasz (red.), *Meritum…*, s. 184. Uważam jednak, że czynienie takiego rozróżnienia jest niezasadne, biorąc choćby pod uwagę motyw 65 RODO, w którym prawodawca unijny nawiązuje do prawa do usunięcia danych (art. 17 ust. 1 RODO), nazywając je prawem do bycia zapomnianym. Podobnie w motywie 66 RODO, akcentując, że „należy rozszerzyć prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów […]", przy czym ma to nastąpić po to, aby „aby wzmocnić prawo do *bycia zapomnianym* w internecie". Wydaje się zatem, że nazwa art. 17 RODO [Prawo do usunięcia danych („prawo do bycia zapomnianym")] zawiera dwa określenia tego samego uprawnienia, które mogą być używane zamiennie (podobnie zob. P. Fajgielski, *Ogólne rozporządzenie…*, s. 268. Ponadto wydaje się, że niezależnie od tego, jak swoje żądanie formułowane na podstawie art. 17 RODO zatytułuje podmiot danych, administrator powinien je i tak wykonać – przy założeniu, że spełnione są przesłanki wynikające z przepisu.

ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeśli spełniona jest przynajmniej jedna z przesłanek wskazanych w przepisie, a jednocześnie nie zachodzi żaden z wyjątków uprawniających administratora do odmowy realizacji żądania[181]. Jeśli administrator stwierdzi, że zachodzą podstawy do uwzględnienia żądania i usunięcia danych, zgodnie z art. 17 ust. 2 RODO ma obowiązek powiadomienia innych administratorów przetwarzających te dane osobowe, iż osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Obowiązek ten aktualizuje się, jeśli administrator wcześniej upublicznił dane osobowe, które usuwa na skutek żądania podmiotu danych. Obowiązek ten nie ma jednak charakteru bezwzględnego, administrator bowiem w tym zakresie zobligowany jest do podjęcia „rozsądnych działań”, mając na uwadze dostępną technologię i koszt realizacji.

Osoba, której dane dotyczą, może żądać usunięcia jej danych osobowych, jeśli:

– dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane [art. 17 ust. 1 lit. a) RODO];
– osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania [art. 17 ust. 1 lit. b) RODO];
– osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania [art. 17 ust. 1 lit. c) RODO];
– dane osobowe były przetwarzane niezgodnie z prawem [art. 17 ust. 1 lit. d) RODO];
– dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator [art. 17 ust. 1 lit. e) RODO];
– dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO [art. 17 ust. 1 lit. f) RODO].

Pierwsza przesłanka nawiązuje do zasady ograniczenia celu (art. 5 ust. 1 lit. b) RODO) i zasady ograniczenia przechowywania (art. 5 ust. 1 lit. e) RODO). Dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób

[181] Wyjątki zostały wskazane w art. 17 ust. 3 RODO. Szerzej na ten temat – zob. pkt 7.4. niniejszego opracowania.

niezgodny z tymi celami oraz przechowywane przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia tych celów. Jeśli administrator osiągnie cele przetwarzania, to powinien usunąć dane osobowe, nie zaś czekać na stosowne żądanie ze strony podmiotu danych. Ważną rolę w tym aspekcie odgrywa wcześniejsze ustalenie okresów retencji danych, o których *nota bene* administrator powinien poinformować podmiot danych, wykonując obowiązek informacyjny zgodnie z art. 13 lub 14 RODO. W literaturze wskazuje się, że dokonanie oceny, czy dane osobowe są przetwarzane zgodnie z celami, dla których były gromadzone, oraz sprawdzenie, czy dane te nie są już niezbędne do realizacji celów przetwarzania, w praktyce może okazać się trudne z co najmniej dwóch powodów[182]. Po pierwsze, ocena wspomnianych okoliczności może być inna z perspektywy administratora niż z perspektywy podmiotu danych. Po drugie, należy brać pod uwagę nie tylko cele, które były wskazane przy zbieraniu danych, ale też inne cele przetwarzania, zgodne z pierwotnymi celami. Niemniej jednak, mając na względzie, że administrator i tak zobowiązany jest do przetwarzania danych osobowych zgodnie z zasadami ujętymi w art. 5 RODO, wydaje się, iż skuteczne skorzystanie z prawa do usunięcia danych będzie miało miejsce wówczas, gdy administrator uchybi nałożonym na niego obowiązkom co do realizacji zasady ograniczenia celu lub zasady ograniczenia przechowywania.

Opierając się na przesłance z art. 17 ust. 1 lit. a) RODO, podmiot danych może żądać od dostawcy wyszukiwarki internetowej usunięcia z listy wyników wyszukiwania określonych treści, jeżeli jego dane osobowe wyświetlane na skutek tego wyszukiwania nie są już niezbędne do celów przetwarzania przez wyszukiwarkę internetową. Jak zauważa EROD, w takim przypadku operator wyszukiwarki internetowej powinien rozpoznać zgłoszenie, wyważając z jednej strony prawo do ochrony prywatności podmiotu danych, a z drugiej – interes internautów w dostępie do informacji, a także biorąc pod uwagę to, czy dane objęte żądaniem usunięcia są aktualne czy uległy zmianie[183]. EROD przykładowo wskazuje, że podmiot danych mógłby skorzystać z prawa do usunięcia jego danych z listy wyników wyszukiwania, gdy:

– informacje o nim posiadane przez przedsiębiorstwo zostały usunięte z publicznego rejestru;
– link do strony internetowej firmy zawiera dane kontaktowe podmiotu danych, mimo że nie pracuje on już w tej firmie;
– informacje muszą być opublikowane w Internecie w celu spełnienia obowiązku prawnego, lecz pozostały dostępne online dłużej niż przewidziano w przepisach.

[182] P. Fajgielski, *Ogólne rozporządzenie…*, s. 270.

[183] EROD, *Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO (część 1)*, wersja 2.0., przyjęte 7.07.2020 r., s. 9.

Druga przesłanka odnosi się do przetwarzania danych osobowych – zwykłych lub szczególnych kategorii danych – w oparciu o zgodę wyrażoną przez podmiot danych. Jeśli przetwarzanie odbywa się na podstawie zgody, podmiot danych może w dowolnym momencie wycofać zgodę, co nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem[184]. W takim przypadku administrator, jeśli nie dysponuje inną podstawą prawną legalizującą przetwarzanie danych osobowych, powinien je usunąć lub przynajmniej zanonimizować. Nie może bowiem przetwarzać danych osobowych bez podstawy prawnej. Podobnie jak przy przesłance pierwszej, administrator nie musi czekać na złożenie przez osobę, której dane dotyczą, żądania usunięcia jej danych osobowych, lecz powinien usunąć przetwarzane dane osobowe niezwłocznie, gdy traci podstawę legalizującą ich przetwarzanie – w tym przypadku zgodę podmiotu danych. Analogicznie więc, skuteczna realizacja prawa do usunięcia danych osobowych w oparciu o art. 17 ust. 1 lit. b) RODO może mieć miejsce, gdy administrator sam nie dopełni swojego obowiązku[185].

Trzecia przesłanka związana jest z realizacją prawa do sprzeciwu wobec przetwarzania danych osobowych. Prawodawca unijny w art. 21 ust. 1 i 2 RODO przewidział dwa rodzaje sprzeciwu wobec przetwarzania danych osobowych:

1. sprzeciw wobec przetwarzania opartego na art. 6 ust. 1 lit. e) lub f) RODO[186], w tym profilowania na podstawie tych przepisów, który podmiot danych może wnieść z przyczyn związanych z jego szczególną sytuacją;
2. sprzeciw wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego.

---

184 Artykuł 7 ust. 3 RODO.

185 Na marginesie można dodać, że w kontekście przetwarzania danych osobowych w wyszukiwarkach internetowych omawiana przesłanka raczej nie może stanowić podstawy żądania usunięcia danych kierowanego wobec operatora wyszukiwarki, ponieważ nie jest on administratorem, wobec którego osoba ta mogłaby wyrazić zgodę na przetwarzanie danych osobowych. Takim administratorem może być natomiast operator konkretnej witryny internetowej, który przetwarza dane osobowe podmiotu danych. Zob. wyrok TS z dn. 24.09.2019 r. w sprawie C-136/17 Commission nationale de l'informatique et des libertés (CNIL) przeciwko Google LLC; EROD, *Wytyczne 5/2019…*, s. 10.

186 Administrator może przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. e) RODO w zakresie, w jakim jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Na podstawie art. 6 ust. 1 lit. f) RODO administrator może przetwarzać dane osobowe, jeśli jest to 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 pierwszym przypadku administrator może próbować wykazać istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności podmiotu danych, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Wówczas nie jest zobligowany uwzględnieniem sprzeciwu zgłoszonego przez podmiot danych. Jeśli jednak administrator nie jest w stanie wykazać powyższych okoliczności, nie może on dalej przetwarzać danych osobowych i powinien zaprzestać ich przetwarzania w zakresie objętym sprzeciwem. W drugim przypadku zakres swobody administratora jest zdecydowanie ograniczony, ponieważ wniesienie sprzeciwu wobec przetwarzania danych osobowych na potrzeby działań marketingowych pociąga za sobą konieczność zaprzestania ich przetwarzania w tym celu. W obydwu sytuacjach osoba, której dane dotyczą, może więc żądać od administratora niezwłocznego usunięcia jej danych osobowych, przy czym należy zwrócić uwagę na dodatkową przesłankę wynikającą z art. 17 ust. 1 lit. c) RODO. Przepis ten stanowi, że administrator ma obowiązek niezwłocznie usunąć dane osobowe, jeśli podmiot danych wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i „nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania". Sugeruje to, że rozpatrując żądanie usunięcia danych osobowych administrator powinien ponownie przeprowadzić test równowagi, analogiczny do tego, który przeprowadził wcześniej, rozpatrując sprzeciw podmiotu danych wobec przetwarzania[187]. Mimo że przesłanki z art. 17 ust. 1 lit. c) RODO i art. 21 ust. 1 RODO są sformułowane nieco odmiennie, nie upatrywałabym w tym różnic o znaczeniu praktycznym[188]. Trudno bowiem wyobrazić sobie sytuację, w której podmiot danych zgłasza sprzeciw wobec przetwarzania, który zostaje uwzględniony, a następnie nie może skutecznie wykonać prawa usunięcia danych objętych sprzeciwem. W praktyce uwzględnienie sprzeciwu wobec przetwarzania – przy założeniu, że nie ma innej podstawy prawnej wobec tego przetwarzania – powinno skutkować usunięciem danych przez administratora. Zatem nieuwzględnienie żądania usunięcia danych na podstawie art. 17 ust. 1 lit. c) RODO może nastąpić jedynie w sytuacji, gdy przetwarzanie danych objętych

[187] O teście równowagi wspomina również EROD, wskazując że „żądania usunięcia z listy wyników wyszukiwania wiążą się z sugestią osiągnięcia równowagi między powodami związanymi ze szczególną sytuacją osoby, której dane dotyczą, a ważnymi prawnie uzasadnionymi podstawami ze strony dostawcy wyszukiwarki internetowej". Zob. EROD, *Wytyczne 5/2019…*, s. 11.

[188] W art. 17 ust. 1 lit. c) RODO mowa o nadrzędnych prawnie uzasadnionych podstawach przetwarzania (ang. *overriding legitimate grounds for the processing*), natomiast w art. 21 ust. 1 RODO o ważnych prawnie uzasadnionych podstawach do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń (ang. *compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims*).

sprzeciwem może być realizowane w oparciu o inną podstawę prawną i ma służyć osiągnięciu innego celu przetwarzania[189].

Czwarta przesłanka dotyczy sytuacji, gdy dane osobowe są przetwarzane niezgodnie z prawem. Jeśli podmiot danych uważa, że jego dane osobowe są przetwarzane z naruszeniem prawa, przy czym pojęcie „prawo" należy w tym kontekście interpretować szeroko jako wszystkie przepisy odnoszące się do przetwarzania danych osobowych, zarówno RODO, jak i inne przepisy unijne i krajowe, ma prawo zgłosić żądanie usunięcia jego danych osobowych. Administrator powinien przeprowadzić wówczas ocenę legalności przetwarzania, niezależną od ogólnej oceny, do której zobowiązany jest choćby w ramach realizacji zasady legalności przetwarzania i w ramach wykonywania obowiązku zapewnienia zgodności przetwarzania z przepisami rozporządzenia[190]. Jeśli w ocenie administratora przesłanka niezgodności przetwarzania z prawem nie jest spełniona, powinien o tym poinformować podmiot danych, jednocześnie pouczając o możliwości wniesienia skargi do PUODO. W literaturze wskazuje się na wątpliwości, kogo powinien w praktyce obciążać dowód wykazania, że dane są przetwarzane niezgodnie z prawem – podmiot danych czy administratora?[191] Wydaje się, że to raczej od administratora należałoby wymagać wykazania zgodności z prawem przetwarzania[192], jednak można równocześnie oczekiwać, iż podmiot danych, zgłaszając żądanie usunięcia jego danych osobowych, wyjaśni lub przynajmniej wskaże okoliczności, które jego zdaniem mogą podważać zgodność przetwarzania z prawem. Inaczej rozpoznanie żądania może okazać się trudne lub niemożliwe w praktyce.

Zgodnie z piątą przesłanką wynikającą z art. 17 ust. 1 lit. e) RODO podmiot danych może żądać usunięcia jego danych osobowych, jeśli jest to konieczne dla wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator. Przesłanka ta jest podobna do przesłanki omówionej powyżej, jednak w tym przypadku wymaga się od podmiotu danych wskazania konkretnego przepisu prawa unijnego lub krajowego, który zobowiązuje administratora do usunięcia przetwarzanych danych osobowych. Na tle art. 17 ust. 1 lit. e) RODO również podnoszone są wątpliwości, dlaczego administrator miałby czekać na otrzymanie żądania podmiotu danych co do usunięcia jego danych osobowych, skoro obowiązek usunięcia wynika wprost

189 Podobnie zob. P. Fajgielski, *Ogólne rozporządzenie…*, s. 272.

190 Zob. art. 5 ust. 1 lit. b) RODO oraz art. 24 ust. 1 RODO.

191 P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

192 P. Fajgielski, *Ogólne rozporządzenie…*, s. 272.

z przepisów[193]. Oczywistym jest, że administrator nie powinien czekać na aktywność w tym zakresie ze strony osoby, której dane dotyczą. Jeśli jednak uchybi prawnemu obowiązkowi usunięcia danych, niezależnie od przyczyny (np. na skutek niewiedzy o istnieniu określonego przepisu, braku regularnego przeglądu czynności przetwarzania lub braku kontroli nad upływem okresu przechowywania danych), podmiot danych może mu o tym „przypomnieć", zgłaszając swoje żądanie usunięcia danych. Na tle tej przesłanki po raz kolejny ujawnia się zatem kontrolny charakter prawa przewidzianego w art. 17 RODO.

Szósta, ostatnia przesłanka wskazana w art. 17 ust. 1 lit. f) RODO, uprawnia podmiot danych do żądania usunięcia danych osobowych, jeśli dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO, tj. w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku oraz oparciem przetwarzania danych osobowych w tym celu na zgodzie [art. 6 ust. 1 lit. a) RODO] wyrażonej przez dziecko lub przedstawiciela prawnego. Usunięcia danych osobowych może więc żądać osoba, która wyraziła zgodę na przetwarzanie danych osobowych przed osiągnięciem pełnoletności lub za którą przedstawiciel wyraził taką zgodę w związku z realizacją usługi społeczeństwa informacyjnego[194]. Prawodawca unijny w motywie 65 RODO podkreślił, że „[…]prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z Internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem". Na tle stosowania tego przepisu mogą jednak powstawać wątpliwości, czy uprawnienie usunięcia danych dotyczy wyłącznie danych zwykłych, skoro w art. 8 ust. 1 RODO mowa jest o zgodzie wyrażonej na podstawie art. 6 ust. 1 lit. a) RODO, czy również danych szczególnej kategorii. Wówczas dane musiałyby być przetwarzane w oparciu o zgodę z art. 9 ust. 2 lit. a) RODO. Mając na względzie cele przepisu, dodatkowo zaakcentowane w motywie 65 RODO, należy przyjąć szerszą interpretację i opowiedzieć się za możliwością

[193] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

[194] Pojęcie usługi społeczeństwa informacyjnego zostało zdefiniowane w art. 4 pkt 25 RODO jako usługa w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535, tj. usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług Zob. Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, Dz. Urz. UE L 241 z 17.9.2015, s. 1–15 .

żądania usunięcia danych zgromadzonych w związku ze świadczeniem usług społeczeństwa informacyjnego również na podstawie art. 9 ust. 2 lit. a) RODO[195].

Oprócz wskazanych powyżej przesłanek, prawo do usunięcia danych obejmuje jeszcze opisany w art. 17 ust. 2 RODO obowiązek podjęcia przez administratora rozsądnych działań, aby poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Szerzej na ten temat – zob. pkt 3.5 niniejszego opracowania.

W literaturze przedmiotu słusznie wskazuje się, że w większości przypadków przewidzianych w art. 17 ust. 1 RODO prawo do usunięcia danych stanowi *superfluum* legislacyjne, ponieważ poza przesłanką opisaną w art. 17 ust. 1 lit. f) RODO, czyli przetwarzaniem danych osobowych w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku, nie wprowadza nowych podstaw do usunięcia danych ponad te, które wynikają z innych przepisów RODO[196]. Realizacja prawa do usunięcia danych sprowadza się więc *de facto* do wyegzekwowania od administratora obowiązku usunięcia danych, któremu uchybił. Zauważa się też, że prawo do usunięcia danych nie spełnia oczekiwań, jakie wobec niego były formułowane[197]. W praktyce jego zastosowanie jest ograniczone i najczęściej wiąże się z przetwarzaniem danych w celach marketingowych.

7.2 Sposób skorzystania z prawa do usunięcia danych

Podobnie jak w przypadku innych praw podmiotów danych, RODO nie zawiera szczegółowych wymogów ani wytycznych co do sposobu wykonania prawa do usunięcia danych osobowych. Podmiot danych może zgłosić takie żądanie w każdej chwili, przez cały cykl przetwarzania jego danych osobowych. Prawo to nie ulega przedawnieniu. Nie ma też formalnego wymogu, aby podmiot danych w jakikolwiek sposób uzasadniał swój wniosek o usunięcie danych,

[195] Podobnie zob. M. Susałko, *Prawo do usunięcia danych (prawo do bycia zapomnianym)* [w:] D. Lubasz (red.), *Meritum…*, s. 186.

[196] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

[197] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

aczkolwiek biorąc pod uwagę to, że art. 17 ust. 1 RODO precyzuje sytuacje, w których może on wystąpić z tego rodzaju żądaniem, można oczekiwać od podmiotu danych co najmniej wskazania jednej z przesłanek wymienionych w tym przepisie. Jeśli podmiot danych nie wskaże żadnej przesłanki, na której opiera swoje żądanie, uważam że administrator ma prawo zwrócić się z prośbą o doprecyzowanie żądania, zwłaszcza jeśli miałoby to na celu ułatwienie i przyspieszenie rozpoznania żądania. Jednocześnie należy zaznaczyć, że brak wskazania przez podmiot danych podstawy żądania usunięcia danych osobowych nie powinien stanowić samoistnej przyczyny odmowy uwzględnienia żądania.

Podmiot danych może żądać usunięcia wszystkich danych osobowych lub tylko wskazanych. Zakres żądania powinien w sposób niebudzący wątpliwości wynikać z treści zgłoszenia. Jeśli administrator ma wątpliwości, powinien skontaktować się z podmiotem danych i poprosić o wyjaśnienie. Podobnie może być w przypadku realizacji przez administratora obowiązku poinformowania innych administratorów na mocy art. 17 ust. 2 RODO o realizacji prawa do usunięcia danych. Obowiązek ten aktualizuje się w sposób automatyczny w razie uwzględnienia żądania usunięcia danych na podstawie art. 17 ust. 1 RODO. Jeśli więc intencją podmiotu danych jest wyłącznie usunięcie danych przetwarzanych przez konkretnego administratora, powinien to wyraźnie zaznaczyć w treści swojego zgłoszenia, żądając niewykonywania obowiązku, o którym mowa w art. 17 ust. 2 RODO. Uważam, że dobrą praktyką w tym zakresie powinno być poinformowanie podmiotu danych o tym, że w razie stwierdzenia przesłanek do usunięcia danych osobowych, administrator podejmie działania zmierzające do poinformowania innych administratorów o wykonaniu prawa do usunięcia danych osobowych oraz o tym, żeby usunęli oni wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Taka informacja mogłaby być zawarta np. w pierwszej odpowiedzi administratora na zgłoszone żądanie, w której administrator potwierdza wpłynięcie zgłoszenia. Jeśli zachodzi taka potrzeba, administrator może wówczas poprosić również o doprecyzowanie zakresu żądania, podstawy żądania lub dopytać o inne kwestie, niezbędne do rozpoznania wniosku.

Żądanie usunięcia danych osobowych może być zgłoszone w dowolny sposób, np. pisemnie, ustnie, elektronicznie. Administrator może ustalić specjalną procedurę lub wdrożyć dedykowane rozwiązania techniczne ułatwiające skorzystanie z tego prawa. Decydując się na takie rozwiązanie, administrator może, np. w formularzu służącym do wniesienia żądania usunięcia danych, poprosić podmiot danych o wskazanie jednej z podstaw wymienionych w art. 17 ust. 1 RODO, stanowiących podstawę zgłoszenia. Należy przy tym pamiętać,

że przyjęcie tego rodzaju procedury lub rozwiązań technicznych nie jest wiążące dla podmiotu danych – może on wnieść swoje żądanie również w inny sposób.

7.3. Sposób realizacji prawa do usunięcia danych

W przypadku prawa do usunięcia danych schemat realizacji żądania jest analogiczny jak w przypadku innych praw wykonywanych przez podmiot danych na gruncie RODO. Nieodzownym krokiem jest prawidłowe zidentyfikowanie osoby występującej z żądaniem, a w razie potwierdzenia, że adresat żądania przetwarza je jako ich administrator – weryfikacja, czy spełnione są pozytywne przesłanki, o których mowa w art. 17 ust. 1 RODO. W kolejnym kroku administrator powinien ocenić, czy nie zachodzi jakakolwiek z przesłanek negatywnych, tj. wyjątków opisanych w art. 17 ust. 3 RODO, które uprawniają administratora do odmowy realizacji żądania usunięcia danych osobowych[198]. Jeśli jednak w ocenie administratora żądanie nie może być uwzględnione, powinien on o tym poinformować podmiot danych, pouczając jednocześnie o przyczynach niemożności zrealizowania żądania oraz o możliwości wniesienia skargi do PUODO. Jeśli zachodzą przesłanki do uwzględniania żądania jedynie w części, administrator powinien je zrealizować w dopuszczalnym zakresie; w pozostałym zakresie może odmówić jego wykonania, przekazując podmiotowi danych stosowną informację.

Administrator powinien upewnić się, czy żądanie usunięcia danych dotyczy wszystkich przetwarzanych przez niego danych osobowych, czy tylko określonych. Jeśli zakres żądania nie jest sprecyzowany w jego treści, administrator ma prawo dopytać o to podmiot danych. Wydaje się to zasadne m.in. w sytuacji, gdy administrator przetwarza dane w różnych celach i na potrzeby różnych czynności przetwarzania, co ma przełożenie na ostateczną ocenę spełnienia przesłanek z art. 17 ust. 1 RODO. Przykładowo, administrator może przetwarzać dane osobowe podmiotu danych w celu przeprowadzenia rekrutacji na określone stanowisko, a ponadto w celu wysyłki newslettera. Przy założeniu, że proces rekrutacji został zakończony, a dane osobowe jego uczestnika, mimo braku zgody na ich przetwarzanie na potrzeby przyszłych rekrutacji, nie zostały usunięte, zgłoszenie żądania usunięcia danych w oparciu o art. 17 ust. 1 lit. a) RODO jest zasadne. Cel przetwarzania już ustał, ponieważ rekrutacja została zakończona. Natomiast w odniesieniu do danych osobowych przetwarzanych

[198] Szerzej na temat wyjątków – zob. pkt 7.4 niniejszego opracowania.

na potrzeby wysyłki newslettera cel przetwarzania nadal istnieje, przez co administrator może ocenić, że w tym kontekście ta sama przesłanka nie została spełniona. W takiej sytuacji warto więc dopytać podmiot danych o faktyczny zakres jego żądania, aby upewnić się, czy jego intencją jest usunięcie również danych służących do realizacji celów marketingowych.

Sama realizacja prawa może nastąpić przez całkowite usunięcie danych objętych żądaniem lub taką ich modyfikację, która spowoduje, że dane te stracą przymiot danych osobowych, np. poprzez zastosowanie anonimizacji[199]. Ważne, aby administrator doprowadził do usunięcia wszelkich danych objętych żądaniem, nawet jeśli dane te są przetwarzane w sposób rozproszony, np. w systemach informatycznych, bazach danych, kopiach zapasowych, plikach tworzonych przez osoby upoważnione przez administratora lub dokumentacji papierowej. Aby zrealizować skutecznie prawo do usunięcia danych, administrator musi więc orientować się, w jakich zestawieniach przetwarza te dane. Ułatwieniem w tym zakresie może być stworzenie odpowiedniej procedury realizacji żądania usunięcia danych, zawierającej m.in. listę kontrolną z wykazem zestawień, w których mogą być przetwarzane dane. W odniesieniu do przetwarzania danych przez operatora wyszukiwarki internetowej należy wspomnieć, że realizacja tego prawa następuje przez usunięcie linków prowadzących do strony internetowej, wyświetlanych na liście wyników wyszukiwania w następstwie wpisania imienia i nazwiska podmiotu danych do wyszukiwarki internetowej. Co do zakresu terytorialnego prawa do usunięcia danych przez operatora wyszukiwarki internetowej wypowiedział się TS w wyroku w sprawie C-507/17 *Google*, uznając że operator ten jest zobowiązany do usunięcia linków nie ze wszystkich wersji swojej wyszukiwarki, ale z tych wersji wyszukiwarki, które odpowiadają wszystkim państwom członkowskim UE[200].

[199] Zob. przykł. wyrok Naczelnego Sądu Administracyjnego z dnia 11 kwietnia 2017 r., sygn. akt: I OSK 2170/15, w którym sąd ten wskazał, że „anonimizacja (zaczernienie) danych osobowych jest równoznaczna z ich usunięciem. Usunięcie może następować za pomocą różnych działań, ważne jest natomiast, aby przyniosły one jeden efekt, tj. wykluczyły możliwość identyfikacji określonej osoby".

[200] Wyrok TS z dn. 24.09.2019 r. w sprawie C-507/17 Google LLC przeciwko Commission nationale de l'informatique et des libertés (CNIL).

W kontekście realizacji prawa do usunięcia danych należy zwrócić uwagę na regulację art. 17 ust. 2 RODO, nakładającą na administratora, który upublicznił[201] dane osobowe podlegające usunięciu na skutek realizacji żądania podmiotu danych, do podjęcia rozsądnych działań, by poinformować administratorów przetwarzających te dane osobowe o żądaniu podmiotu danych oraz o tym, że żąda on również usunięcia wszelkich łączy do tych danych, ich kopii lub replikacji. Jest to obowiązek, który aktualizuje się automatycznie w momencie, gdy administrator zobligowany jest do usunięcia danych na mocy art. 17 ust. 1 RODO, chyba że podmiot danych wyraźnie zażąda w swoim zgłoszeniu, aby administrator nie informował innych administratorów o usunięciu danych. Przepis nie ma przy tym charakteru bezwzględnego, ponieważ administrator zobowiązany jest do podjęcia „rozsądnych działań", biorąc pod uwagę dostępną technologię i koszt ich realizacji. Jeśli administrator jest w stanie wykazać, że nie dysponuje adekwatnymi możliwościami technicznymi lub że wypełnienie obowiązku wiązałoby się z wysokimi kosztami, może powstrzymać się od jego wykonania. Wskazane w przepisie przesłanki, uprawniające administratora *de facto* do odstąpienia od wykonania obowiązku, nie powinny być interpretowane szeroko, aczkolwiek mogą być one oceniane subiektywnie – z perspektywy konkretnego administratora. Można wnioskować, że im administrator jest większym podmiotem, tj. o rozbudowanej strukturze organizacyjnej lub większych możliwościach finansowych, tym w większym zakresie jest zobowiązany do realizacji obowiązku z art. 17 ust. 2 RODO[202]. Wydaje się ponadto, że niezależnie od tego, czy administrator przekaże innym administratorom żądanie usunięcia danych, czy też nie, powinien o tym poinformować podmiot danych, np. w końcowej wiadomości na temat sposobu i zakresu spełnienia żądania. Ponadto, niezależnie od realizacji art. 17 ust. 2 RODO, na administratorze spoczywa również ogólny obowiązek poinformowania o usunięciu danych każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku[203].

---

[201] Słusznie wskazuje P. Litwiński, że administrator może mieć wątpliwości, jakich innych administratorów powinien poinformować, realizując dyspozycję art. 17 ust. 2 RODO; zob. P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO. Pojęcie upublicznienia danych osobowych nie zostało wyjaśnione w RODO, ale samo pojęcie „upublicznić", zgodnie z definicją Słownika Języka Polskiego, oznacza „podać do publicznej wiadomości, ujawnić"; zob. https://sjp.pl/upublicznić (dostęp: 31.03.2022 r.). Administrator ma więc obowiązek poinformować o usunięciu danych przynajmniej tych administratorów, co do których wie, że przetwarzają dane objęte żądaniem.

[202] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

[203] Artykuł 19 RODO.

Jak wskazuje EROD, obowiązek z art. 17 ust. 2 RODO nie dotyczy dostawców wyszukiwarek internetowych w zakresie, w jakim znajdują informacje zawierające dane osobowe opublikowane lub zamieszczone w Internecie przez osoby trzecie, indeksując je w sposób automatyczny, czasowo przechowując i udostępniając internautom w sposób uporządkowany zgodnie z określonymi preferencjami[204]. Ponadto, jeśli operator wyszukiwarki internetowej otrzymuje od podmiotu danych żądanie usunięcia z listy wyników wyszukiwania jego danych osobowych, nie ma też obowiązku poinformowania o zgłoszonym żądaniu osoby trzeciej, która upubliczniła te informacje w Internecie. EROD powołała się w tym zakresie na jeden ze swoich wcześniejszych komunikatów, w którym stwierdziła, że „dostawcy wyszukiwarek internetowych nie powinni co do zasady informować webmasterów stron, których dotyczy usunięcie z listy wyników wyszukiwania, o tym, że dostęp do niektórych stron internetowych za pośrednictwem wyszukiwarki internetowej po wpisaniu konkretnych zapytań nie jest możliwy", ponieważ obowiązujące przepisy nie dają podstaw do wywodzenia takiego obowiązku[205].

Realizacja żądania powinna nastąpić zgodnie z ogólnymi terminami wynikającymi z art. 12 ust. 3 RODO, czyli zasadniczo niezwłocznie, najpóźniej w ciągu miesiąca od otrzymania żądania. Ewentualnie z uwagi na skomplikowany charakter żądania lub liczbę żądań termin ten można przedłużyć o kolejne dwa miesiące. Co do zasady administrator nie powinien pobierać opłaty za działania podejmowane w celu wykonania prawa do usunięcia danych, za wyjątkiem sytuacji, w których żądanie podmiotu danych jest ewidentnie nieuzasadnione lub nadmierne[206].

Warto też przypomnieć, że informację o wpłynięciu żądania usunięcia danych oraz sposobie jego rozpoznania należy odnotować w rejestrze realizacji praw podmiotów danych. Jest to ważne z perspektywy zasady rozliczalności, aby móc w przyszłości wykazać, że prawo zostało zrealizowane prawidłowo i terminowo, a w przypadku, gdy administrator odmówił jego wykonania – że miał ku temu odpowiednie podstawy. Udzielając końcowej odpowiedzi podmiotowi danych o sposobie realizacji jego żądania, warto pouczyć o tym, że na potrzeby realizacji zasady rozliczalności oraz w celu ochrony przed ewentualnymi roszczeniami

[204] EROD, *Wytyczne 5/2019 …*, s. 7.

[205] Grupa Robocza Art. 29, „Wytyczne w sprawie wykonania wyroku TSUE w sprawie *Google Spain i Inc przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi C-131/12*" z 26.11.2014 r., WP 225, s. 23.

[206] Artykuł 12 ust. 5 RODO.

związanymi z prawem do usunięcia danych, administrator będzie przez określony okres przetwarzał dane osobowe zawarte we wniosku. Okres ten powinien być ustalony z uwzględnieniem potrzeb administratora, rodzaju prowadzonej działalności czy okoliczności przetwarzania[207].

7.4. Wyłączenia

W art. 17 ust. 3 RODO przewidziano kilka wyjątków od obowiązku realizacji prawa do usunięcia danych osobowych. Administrator może odstąpić od tego obowiązku, jeśli przetwarzanie danych osobowych jest niezbędne do:

- korzystania z prawa do wolności wypowiedzi i informacji;
- wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- realizacji interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) i lit. i) oraz art. 9 ust. 3 RODO;
- celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że realizacja prawa do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

Niektóre wyjątki zawierają przesłanki o charakterze ocennym, co powoduje, że ich praktyczne wykorzystanie budzi niekiedy wątpliwości lub prowadzi do sporu pomiędzy podmiotem danych a administratorem. Najwięcej pytań o zakres wyłączenia prawa do usunięcia danych pojawia się w związku z korzystaniem z prawa do wolności wypowiedzi i informacji. Wolność wypowiedzi i informacji jest jednym z praw podstawowych, ujętych w art. 11 Karty Praw Podstawowych (KPP)[208], i obejmuje „wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych

[207] Okres retencji może korespondować z okresami przedawnienia roszczeń lub być krótszy, np. może wynosić rok od końca roku kalendarzowego, w którym wpłynęło żądanie. Zob. A. Sagan-Jeżowska, „Wniosek o usunięcie danych", *Informacja w Administracji Publicznej*, 2019/4, s. 35.

[208] Dz. Urz. UE C 326 z dn. 26.10.2012, s. 391–407.

i bez względu na granice państwowe". Prawo do ochrony danych osobowych jest również jednym z praw podstawowych, zagwarantowanych na mocy art. 8 KPP. Administrator, który odmawia usunięcia danych osobowych, powołując się na wyjątek w postaci konieczności ich przetwarzania w związku z prawem do wolności wypowiedzi i informacji, powinien więc dokonać wyważenia dwóch praw podstawowych, biorąc pod uwagę różne czynniki dotyczące samego procesu przetwarzania, takie jak kategoria przetwarzanych danych, okoliczności, charakter i kontekst przetwarzania, prawdziwość i aktualność przetwarzanych danych, ale też czynniki obejmujące szerszy kontekst, jak choćby status społeczny podmiotu danych wynikający z pełnionej funkcji społecznej, zajmowanego stanowiska czy roli odgrywanej w życiu publicznym[209]. Regulacja art. 17 ust. 3 lit. a) RODO ma zapobiegać swoistej cenzurze informacyjnej i w ten sposób zapewniać społeczeństwu dostęp do informacji. Ogólny charakter tego wyjątku może jednak sprzyjać jego nadużywaniu przez administratorów, zwłaszcza w przypadku informacji dostępnych w środowisku internetowym.

Administrator może odmówić usunięcia danych, jeśli ich przetwarzanie jest konieczne dla wykonania obowiązków wynikających z przepisów unijnych lub krajowych, lub zadań realizowanych w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi [art. 17 ust. 3 lit. b) RODO]. Wyjątek ten ma zastosowanie zarówno w przypadku administratorów z sektora publicznego, jak i podmiotów prywatnych, zobowiązanych do przetwarzania danych osobowych w określonych celach, np. podatkowych, archiwalnych. Usunięcie danych osobowych zgodnie z żądaniem podmiotu danych rodzi wówczas ryzyko niemożności realizacji zadań publicznych lub naraża administratora na zarzut działania wbrew jego prawnym obowiązkom. Podobnie jest w sytuacji, gdy dane osobowe są przetwarzane w celach archiwalnych, do celów badań naukowych lub historycznych lub do celów statystycznych [art. 17 ust. 3 lit. d) RODO]. Administrator w takich przypadkach również może odmówić wykonania prawa do usunięcia danych, z tym zastrzeżeniem, że obciąża go wówczas obowiązek uprawdopodobnienia, że ewentualne usunięcie danych mogłoby uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania.

[209] Na okoliczności te zwrócił uwagę TS w wyroku z dn. 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi oraz w wyroku z dn. 24.09.2019 r. w sprawie C-136/17 Commission nationale de l'informatique et des libertés (CNIL) przeciwko Google LLC, zaznaczając jednocześnie, że „co do zasady prawa osób, których dane dotyczą, będą przewyższały interes internautów w dostępie do informacji za pośrednictwem dostawców wyszukiwarek internetowych" – zob. wyrok w sprawie C-131/12, pkt 99; wyrok w sprawie C-136/17, pkt 53.

Odmowa uwzględnienia prawa do usunięcia danych osobowych może też nastąpić, gdy wymagają tego względy interesu publicznego w dziedzinie zdrowia publicznego. Wyłączenie to dotyczy przetwarzania danych szczególnej kategorii, za które zgodnie z definicją z art. 9 ust. 1 RODO uznaje się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej. W literaturze wskazuje się, że w praktyce wyłączenie to będzie miało zastosowanie głównie do trzech kategorii danych, tj. danych dotyczących stanu zdrowia, danych genetycznych oraz danych biometrycznych[210]. Zgodnie z dyspozycją art. 17 ust. 3 lit. c) RODO na wyłączenie to administrator może się powołać w sytuacji, gdy:

– przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 RODO[211] [zob. art. 9 ust. 2 lit. h) RODO];
– przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową [zob. art. 9 ust. 2 lit. i) RODO].

Ostatnim wyjątkiem, na który może powołać się administrator, jest konieczność przetwarzania danych dla ustalenia, dochodzenia lub obrony roszczeń [art. 17 ust. 3 lit.

[210] P. Fajgielski, *Ogólne rozporządzenie…*, s. 276.

[211] Artykuł 9 ust. 3 RODO stanowi, że dane osobowe mogą być przetwarzane na podstawie art. 9 ust. 2 lit. h) RODO, jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

e) RODO]. Wyjątek ten spełnia funkcję gwarancyjną, zapewniając innym podmiotom możliwość realizacji ich uprawnień, dla których konieczne jest przetwarzanie danych osobowych (np. dla wierzycieli). Usunięcie danych zgodnie z żądaniem podmiotu danych mogłoby w takiej sytuacji stanowić nadużycie prawa do ochrony danych[212]. Jak podnosi się w literaturze przedmiotu, wyjątek ten nie powinien być interpretowany zawężająco, tj. jedynie w odniesieniu do roszczeń aktualnie dochodzonych w trakcie wykonywania prawa do bycia zapomnianym, ponieważ taka interpretacja stawiałaby administratora w sytuacji nieporównywalnie mniej korzystnej niż podmiot danych[213].

[212] P. Fajgielski, *Ogólne rozporządzenie…*, s. 278.

[213] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 17 RODO.

8. Prawo do ograniczenia przetwarzania – art. 18 RODO

8.1. Zakres prawa

Artykuł 18 RODO statuuje prawo do ograniczenia przetwarzania danych osobowych, na mocy którego osoba, której dane dotyczą, może żądać od administratora czasowego zablokowania przetwarzania jej danych osobowych z uwagi na istnienie wymienionych w przepisie okoliczności. Pojęcie ograniczenia przetwarzania należy rozumieć, zgodnie z definicją z art. 4 pkt 3 RODO, jako „oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania". Podmiot danych ma więc prawo domagać się, aby administrator przez pewien czas wyłącznie przechowywał jego dane osobowe, nie dokonując na nich innych operacji przetwarzania, w szczególności takich, które mogłyby prowadzić do modyfikacji tych danych, negatywnie wpłynąć na możliwość wykonania innych praw podmiotu danych lub spowodować inne niekorzystne skutki dla sytuacji prawnej podmiotu danych, np. zniweczyć możliwość dochodzenia przez niego roszczeń. W literaturze przedmiotu prawo to jest uznawane za szczególnie restrykcyjne uprawnienie kontrolne podmiotu danych, ponieważ jego realizacja oznacza, że administrator nie może *de facto* wykorzystywać danych dotyczących konkretnej osoby fizycznej w ustalonych przez siebie celach, a jedynie zobowiązany jest do ich przechowywania[214]. W art. 18 ust. 2 RODO przewidziane są co prawda wyjątki, w których administrator może dokonywać innych operacji na danych, niemniej jednak nie zmienia to faktu, że skorzystanie z prawa do ograniczenia przetwarzania jest z reguły niekorzystną sytuacją dla administratora, ponieważ powoduje, że zgromadzone dane, przynajmniej przez określony czas, stają się dla niego bezużyteczne.

Można żądać ograniczenia przetwarzania danych osobowych, jeśli:

– podmiot danych kwestionuje prawidłowość jego danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych [art. 18 ust. 1 lit. a) RODO];

[214] M. Czerniawski, *Artykuł 18* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 531.

– przetwarzanie jest niezgodne z prawem, a podmiot danych sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania [art. 18 ust. 1 lit. b) RODO];
– administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne podmiotowi danych do ustalenia, dochodzenia lub obrony roszczeń [art. 18 ust. 1 lit. c) RODO];
– podmiot danych wniósł sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą [art. 18 ust. 1 lit. d) RODO].

Katalog przesłanek umożliwiających żądanie ograniczenia przetwarzania ma charakter zamknięty, co oznacza, że podmiot danych nie może domagać się realizacji tego uprawnienia w innych okolicznościach. Jednocześnie wystarczy zaistnienie jednej z wyżej wymienionych przesłanek, aby podmiot danych mógł skierować do administratora stosowne żądanie. Ograniczenie przetwarzania ma pełnić pewnego rodzaju funkcję gwarancyjną i zabezpieczyć sytuację prawną podmiotu danych. Przykładowo, jeśli administrator przetwarza dane osobowe niezgodnie z prawem, podmiot danych może skorzystać z prawa ograniczenia przetwarzania po to, aby zachować możliwość dochodzenia swoich praw i wykazania, np. w ramach skargi skierowanej do PUODO, niezgodności z prawem przetwarzania[215]. Podobnie będzie w przypadku, gdy administrator mógłby usunąć przetwarzane dane osobowe z uwagi na osiągnięcie celów przetwarzania, jednak wówczas ich usunięcie mogłoby uniemożliwić podmiotowi danych ustalenie, dochodzenie lub obronę przed roszczeniami[216]. W takiej sytuacji zachodzą istotne względy uzasadniające dalsze przechowywanie danych osobowych, nawet jeśli prowadzi ono do wykroczenia poza ustalone przez administratora okresy retencji danych.

[215] Za przetwarzanie niezgodnie z prawem uznaje się przetwarzanie danych osobowych bez ważnej podstawy prawnej z art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO, przetwarzanie w celach niezgodnych z prawem lub przetwarzanie wbrew zgłoszonym przez podmiot danych żądaniom dotyczącym, np. sprostowania danych lub ich usunięcia. Zob. M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 18.

[216] Należy zaznaczyć, że art. 18 ust. 1 lit. c) RODO odnosi się do roszczeń podmiotu danych, a nie innych osób, a nadto do roszczeń prawnych. Zob. M. Czerniawski, *Artykuł 18* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…*, s. 534.

Mimo ograniczenia przetwarzania, administrator może dokonywać innych operacji na danych – poza przechowywaniem – wyłącznie:
– za zgodą podmiotu danych,
– w celu ustalenia, dochodzenia lub obrony roszczeń,
– w celu ochrony praw innej osoby fizycznej lub prawnej,
– z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego[217].

Zgoda podmiotu danych musi spełniać wszystkie przesłanki ważności zgody, tj. powinna stanowić dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym podmiot danych – w formie oświadczenia lub wyraźnego działania potwierdzającego – przyzwala na dokonywanie innych operacji na jego danych osobowych, poza przechowywaniem. Zgoda powinna być zbierana w formie odrębnego oświadczenia, niepowiązanego z innymi oświadczeniami odbieranymi od podmiotu danych[218]. Ponadto, podmiot danych musi mieć zagwarantowaną możliwość wycofania w każdym czasie zgody na dokonywanie innych operacji na danych osobowych, mimo ograniczenia ich przetwarzania[219]. W doktrynie prezentowany jest pogląd, że zgoda wyrażona na gruncie art. 18 ust. 2 RODO powinna mieć charakter wyjątkowy i odnosić się tylko do sytuacji, gdy administrator przekona podmiot danych o konieczności wykorzystania danych, mimo ograniczenia ich przetwarzania[220]. Można jednak mieć wątpliwości, czy w takim przypadku zgoda będzie spełniać wymóg dobrowolności, skoro będzie wyrażona w następstwie „przekonania" podmiotu danych przez administratora co do konieczności przetwarzania. Wydaje się, że ostateczna ocena zależy od okoliczności przetwarzania i przyczyn, dla których administrator miałby dokonywać dalszego przetwarzania danych.

Administrator może przetwarzać dane osobowe również, gdy jest to konieczne w celu ustalenia, dochodzenia lub obrony roszczeń, ochrony praw lub z uwagi na ważne względy interesu publicznego. Przepis w tym zakresie odnosi się zarówno do roszczeń administratora, jak i do roszczeń, które mogą być zgłoszone przez inne osoby lub podmioty. Omawiany wyjątek może mieć więc zastosowanie w sytuacji, gdy administrator mimo ograniczenia przetwarzania, zostanie wezwany przez odpowiednie organy publiczne

217 Artykuł 18 ust. 2 RODO.
218 Artykuł 7 ust. 2 RODO.
219 Artykuł 7 ust. 3 RODO.
220 P. Fajgielski, *Ogólne rozporządzenie…*, s. 282.

do podjęcia określonych działań w związku z prowadzonymi przez nie postępowaniami, np. do zabezpieczenia dowodów, przekazania dokumentów.

8.2. Sposób skorzystania z prawa do ograniczenia przetwarzania

Podmiot danych może w każdej chwili wystąpić z żądaniem ograniczenia przetwarzania jego danych osobowych – przepisy nie wprowadzają żadnego czasowego ograniczenia w tym zakresie. Niemniej jednak ograniczenie przetwarzania może nastąpić wyłącznie z przyczyn określonych w art. 18 ust. 1 RODO, w związku z czym należy przyjąć, że podmiot danych w swoim zgłoszeniu powinien wskazać powód, dla którego domaga się ograniczenia przetwarzania oraz przedstawić uzasadnienie. Jeśli we wniosku o ograniczenie przetwarzania brakuje niezbędnych informacji wskazujących na istnienie przesłanek takiego ograniczenia, administrator ma prawo poprosić podmiot danych o przedstawienie dodatkowych wyjaśnień. Podobnie, gdy nie jest jasny zakres żądania – podmiot danych może bowiem żądać ograniczenia przetwarzania wszystkich jego danych osobowych przetwarzanych przez administratora lub tylko niektórych. Jeśli administrator poweźmie wątpliwości na tym tle, ma prawo dopytać podmiot danych o faktyczny zakres jego żądania.

Zgłoszenie żądania ograniczenia przetwarzania danych osobowych może nastąpić w dowolnej formie, dogodnej dla podmiotu danych, np. w formie elektronicznej, pisemnej lub ustnej. Podmiot danych może też w dowolnym momencie zrezygnować z żądania ograniczenia przetwarzania, wysyłając administratorowi stosowne powiadomienie.

8.3. Sposób realizacji prawa do ograniczenia przetwarzania

Administrator nie jest związany żądaniem podmiotu danych co do ograniczenia przetwarzania jego danych osobowych. Podobnie jak inne prawa przysługujące na gruncie RODO, prawo to nie ma charakteru bezwzględnego, lecz jego wykonanie wymaga uprzedniej oceny, czy w konkretnym przypadku zachodzą przesłanki wskazane w przepisie. Ocena ta polega

na weryfikacji zarówno przesłanek pozytywnych, tj. przesłanek z art. 18 ust. 1 RODO, jak i przesłanek uprawniających administratora do podejmowania innych operacji na danych osobowych mimo ograniczenia ich przetwarzania, opisanych w art. 18 ust. 2 RODO.

Jeśli zdaniem administratora ograniczenie przetwarzania jest zasadne, powinien on wdrożyć odpowiednie środki, za pomocą których przetwarzanie zestawu danych objętego żądaniem zostanie faktycznie ograniczone. Przede wszystkim administrator powinien wyraźnie odróżnić i wyodrębnić dane osobowe podlegające ograniczeniu od innych przetwarzanych danych. Zgodnie z motywem 67 RODO administrator może przykładowo czasowo przenieść wybrane dane osobowe do innego systemu przetwarzania, uniemożliwić użytkownikom dostęp do wybranych danych lub czasowo usunąć je ze strony internetowej. Jeśli dane przetwarzane są w formie papierowej ograniczenie przetwarzania może być zrealizowane poprzez wydzielenie ich z dokumentacji i przechowywanie w osobnym miejscu do czasu zakończenia ograniczenia przetwarzania. W zautomatyzowanych zbiorach danych administrator powinien zastosować takie środki techniczne, które nie tylko zabezpieczą dane przed dalszym przetwarzaniem, ale też uniemożliwią ich ewentualną modyfikację lub usunięcie. Innymi słowy, oprócz ograniczenia przetwarzania danych wyłącznie do ich przechowywania, administrator musi dodatkowo zapewnić nienaruszalność tak przechowywanych danych. Jeśli natomiast w przekonaniu administratora żądanie nie zasługuje na uwzględnienie, powinien o tym poinformować podmiot danych, podając przyczyny odmowy realizacji żądania i pouczając o możliwości wniesienia skargi do PUODO. Podobnie w przypadku, gdy administrator najpierw uwzględni żądanie i ograniczy przetwarzanie danych, po czym w trakcie trwania ograniczenia, uzna że odpadły przesłanki z art. 18 ust. 1 RODO lub zaistniała jedna z przesłanek z art. 18 ust. 2 RODO. Obowiązek poinformowania podmiotu danych w takiej sytuacji wynika wprost z art. 18 ust. 3 RODO.

Realizacja żądania podmiotu danych powinna nastąpić w sposób zgodny z wymogami zasady przejrzystości, o których mowa w art. 12 RODO. Administrator powinien udzielić odpowiedzi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Odpowiedzi można udzielić na piśmie, elektronicznie lub w inny sposób – najczęściej w sposób analogiczny do tego, jaki został wykorzystany przez podmiot danych w celu zgłoszenia żądania ograniczenia przetwarzania. Udzielenie odpowiedzi powinno nastąpić w terminach określonych w art. 12 ust. 3 RODO, tj. bez zbędnej zwłoki, co do zasady w terminie miesiąca od daty wpływu żądania; z uwagi na skomplikowany charakter żądania lub liczbę żądań administrator może przedłużyć ten termin o kolejne dwa miesiące.

Czas trwania ograniczenia przetwarzania może być różny w zależności od sytuacji i przyczyny ograniczenia. Jeśli podmiot danych kwestionuje prawidłowość jego danych osobowych, przetwarzanie może być ograniczone na okres pozwalający administratorowi sprawdzić prawidłowość tych danych, czyli w praktyce tak długo, dopóki administrator nie zweryfikuje ich poprawności [art. 18 ust. 1 lit. a) RODO]. Należy jednak pamiętać, że jeśli żądanie ograniczenia przetwarzania jest połączone z żądaniem sprostowania danych, administratora obowiązują ogólne terminy realizacji żądania wynikające z art. 12 ust. 3 RODO, a zatem czas trwania ograniczenia przetwarzania może być w tym przypadku skorelowany z czasem rozpoznawania żądania sprostowania danych. Jeśli ograniczenie przetwarzania następuje w związku ze zgłoszeniem przez podmiot danych sprzeciwu na mocy art. 21 ust. 1 RODO, ograniczenie może trwać przez czas niezbędny do stwierdzenia przez administratora, czy zachodzące po jego stronie prawnie uzasadnione podstawy przetwarzania danych są nadrzędne wobec podstaw sprzeciwu podmiotu danych [art. 18 ust. 1 lit. d) RODO]. W praktyce będzie to czas niezbędny do oceny zasadności sprzeciwu wobec przetwarzania danych osobowych. W obydwu opisanych wyżej sytuacjach, mimo że zasadniczo czas trwania ograniczenia przetwarzania zależy od decyzji administratora, musi on pamiętać o obowiązku dochowania ogólnych terminów wskazanych w art. 12 ust. 3 RODO.

Inaczej będzie w przypadku, gdy podmiot danych żąda ograniczenia przetwarzania, ponieważ w jego ocenie przetwarzanie jest niezgodne z prawem [art. 18 ust. 1 lit. b) RODO] lub gdy przetwarzane przez administratora dane są potrzebne podmiotowi danych do ustalenia, dochodzenia lub obrony roszczeń [art. 18 ust. 1 lit. c) RODO]. Wówczas ograniczenie przetwarzania może trwać przez dowolnie długi okres, nawet bezterminowo, ponieważ okres ten jest *de facto* zależny od decyzji podmiotu danych lub od decyzji organu (np. decyzji PUODO stwierdzającej niezgodność przetwarzania z prawem i nakazującej usunięcie danych).

Fakt ograniczenia przetwarzania danych osobowych administrator powinien wyraźnie odnotować w systemie. Niezależnie natomiast od sposobu rozpoznania żądania, powinien również dokonać odpowiedniego wpisu do rejestru realizacji praw podmiotów danych, wskazując m.in. datę wpłynięcia żądania, datę jego rozpoznania, sposób jego realizacji lub przyczyny odmowy wykonania prawa. Jest to ważne z perspektywy spełnienia zasady rozliczalności. Należy też pamiętać, że w razie uwzględnienia żądania ograniczenia przetwarzania administrator, zgodnie z art. 19 RODO, informuje o takim ograniczeniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Poza tym, na mocy tego przepisu administrator

ma obowiązek poinformowania podmiotu danych o tych odbiorcach, jeżeli zgłosi on takie zażądanie.

8.4. Wyłączenia

Polski ustawodawca skorzystał z możliwości ograniczenia prawa przewidzianego w art. 18 RODO, wprowadzając do szeregu ustaw stosowne przepisy. Przykładowo ograniczenia takie zostały wprowadzone w:

– KPA[221],
– prawie o ustroju sądów powszechnych[222],
– prawie o prokuraturze[223],
– prawie o adwokaturze[224],
– ustawie o radcach prawnych[225],
– prawie o notariacie[226],
– prawie budowlanym[227],
– ustawie o transporcie drogowym[228],

[221] Zob. art. 2a § 3 KPA stanowiący, że „[…] wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie wpływa na tok i wynik postępowania".

[222] Zob. 175dc § 1 ustawy Prawo o ustroju sądów powszechnych stanowiący, że do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych nie stosuje się art. 18 i art. 19 RODO.

[223] Zob. art. 13 § 7 ustawy Prawo o prokuraturze stanowiący, że do przetwarzania danych osobowych w postępowaniach lub systemach teleinformatycznych w ramach realizacji zadań, o których mowa w art. 2 ustawy, art. 18 RODO nie stosuje się.

[224] Zob. art. 16a ust. 1 ustawy Prawo o adwokaturze stanowiący, że art. 18 i 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez adwokata tajemnicy zawodowej.

[225] Zob. art. 5a ust. 1 ustawy o radcach prawnych stanowiący, że art. 18 i art. 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez radcę prawnego tajemnicy zawodowej.

[226] Zob. art. 78b § 2 ustawy Prawo o notariacie stanowiący, że art. 18 i art. 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez notariusza tajemnicy zawodowej.

[227] Zob. art. 84ab ustawy Prawo budowlane stanowiący, że wystąpienie z żądaniem ograniczenia przetwarzania danych osobowych nie wpływa na wykonywanie wymienionych szczegółowo w tym przepisie zadań ustawowych przez organy administracji architektoniczno-budowlanej i organy nadzoru budowlanego, jak przykładowo prowadzenie rejestrów i ewidencji czy prowadzenie czynności związanych z kontrolą przestrzegania i stosowania przepisów prawa budowlanego.

[228] Zob. art. 55a ust. 13 Ustawy z dnia 6 września 2001 r. o transporcie drogowym, Dz. U. z 2022 r., poz. 180, t.j. z dnia 26.01.2022 r., stanowiący, że wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO nie wpływa na wykonywanie przez Inspekcję Transportu Drogowego zadań, o których mowa w art. 50 tej ustawy.

9. Prawo do przenoszenia danych – art. 20 RODO

9.1. Zakres prawa

Uregulowane w art. 20 ust. 1 RODO prawo do przenoszenia danych uprawnia osobę, której dane są przetwarzane, do otrzymania od administratora wszystkich danych, które zostały mu wcześniej przekazane. Dane te powinny być dostarczone przez administratora w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, po to aby podmiot danych, jeśli taka jest jego intencja, mógł je następnie przekazać innemu administratorowi. Ewentualnie podmiot danych może zażądać od administratora, aby ten przesłał je bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Tak ukształtowane prawo do przenoszenia danych stanowi uzupełnienie przewidzianych w RODO innych uprawnień podmiotu danych, zwłaszcza prawa dostępu do danych, na mocy którego podmiot danych ma prawo otrzymać od administratora kopię jego danych osobowych, jednak z tą różnicą, że na podstawie art. 20 RODO administrator ma obowiązek wydać kopię danych w odpowiednim formacie, umożliwiającym przeniesienie danych do innego środowiska informatycznego. Prawo do przenoszenia danych wzmacnia pozycję podmiotu danych w ten sposób, że ułatwia mu np. zmianę dostawcy usług, w ramach której przetwarzane są dane osobowe. Zgodnie z założeniami regulacji, w ten sposób podmiot danych zyskuje większą kontrolę nad swoimi danymi w ramach zautomatyzowanego przetwarzania danych osobowych, ponieważ może swobodnie przenosić swoje dane między różnymi systemami, należącymi do różnych administratorów, wybierając ten, który w danym momencie jest dla niego najkorzystniejszy, oferuje najlepsze zabezpieczenia, lepiej chroni prywatność użytkowników itp. Podmiot danych może też chcieć udostępnić swoje dane osobowe innemu administratorowi, realizującemu inne cele przetwarzania i świadczącemu inne usługi. W takim przypadku prawo do przenoszenia danych również może mieć zastosowanie, dając – zgodnie z życzeniem podmiotu danych – nowemu administratorowi dostęp do gotowego zestawu danych, który w innej sytuacji musiałby zgromadzić samodzielnie. Pośrednio więc prawo do przenoszenia danych podnosi konkurencyjność pomiędzy administratorami – dostawcami różnych usług oferowanych podmiotom danych, wspiera swobodny przepływ danych w UE oraz sprzyja rozwojowi

nowych usług, o czym wspomina Grupa Robocza Art. 29 w wytycznych dotyczących prawa do przenoszenia danych[229].

Możliwość skorzystania z prawa do przenoszenia danych jest ograniczona tylko do określonych przypadków, a mianowicie podmiotowi danych przysługuje takie prawo jedynie, gdy:

– przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO [art. 20 ust. 1 lit. a) RODO];
– przetwarzanie odbywa się w sposób zautomatyzowany [art. 20 ust. 1 lit. b) RODO].

Podstawowym warunkiem skorzystania z prawa do przenoszenia danych osobowych jest to, aby dane te były przetwarzane w oparciu o odpowiednią podstawę prawną, tj. zgodę podmiotu danych lub umowę, której stroną jest podmiot danych i do wykonania której konieczne jest przetwarzanie jego danych osobowych. Prawo do przenoszenia danych nie ma zastosowania, jeżeli przetwarzanie opiera się na innej przesłance legalizującej przetwarzanie z art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO. Jak wskazano w motywie 68 RODO, prawa tego – z uwagi na jego charakter – **nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych**; z tego względu nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi[230]. W braku spełnienia tego warunku, administrator nie ma obowiązku spełnienia żądania.

Należy pamiętać, że przeniesieniu podlegają wyłącznie dane przetwarzane w sposób zautomatyzowany, tzn. przy wykorzystaniu narzędzi informatycznych. Jeśli określone czynności przetwarzania wykonywane są w sposób mieszany (częściowo zautomatyzowany, a częściowo w sposób niezautomatyzowany), to prawo do przeniesienia danych może być zrealizowane tylko w odniesieniu do tych danych, które są przetwarzane w sposób zautomatyzowany. Z tego względu podmiot danych nie może skutecznie żądać przeniesienia danych przetwarzanych w formie papierowej.

[229] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia danych*, zmienione i przyjęte w dniu 5.04.2017 r., WP 242 rev.01.

[230] Zob. art. 20 ust. 3 zd. drugie RODO.

W kontekście realizacji prawa do przenoszenia danych warto zwrócić uwagę, że art. 20 ust. 1 RODO uprawnia podmiot danych do otrzymania danych osobowych, które sam dostarczył administratorowi. Zgodnie z wytycznymi Grupy Roboczej Art. 29 za dane takie należy uważać nie tylko dane aktywnie i świadomie dostarczone przez podmiot danych (np. dane podane w formularzu lub na potrzeby zawarcia umowy), ale również dane zaobserwowane przez administratora podczas korzystania przez podmiot z określonej usługi lub urządzenia (np. historia wyszukiwania, dane o ruchu, dane dotyczące lokalizacji, tętno czy ciśnienie)[231]. Z kolei dane wywnioskowane przez administratora na podstawie danych dostarczonych przez podmiot danych nie mieszczą się w zakresie art. 20 ust. 1 RODO. Do takich danych mogą należeć przykładowo dane wytworzone na skutek personalizacji czy profilowania.

9.2. Sposób skorzystania z prawa do przenoszenia danych

Zgłoszenie żądania może nastąpić w dowolnej formie wybranej przez podmiot danych oraz w dowolnym momencie cyklu przetwarzania danych. Podmiot danych nie musi podawać przyczyn swojego żądania ani wykazywać jakiegokolwiek interesu prawnego lub faktycznego uzasadniającego jego realizację. Ważne natomiast, aby z treści żądania jasno wynikało, czy podmiot danych chce skorzystać tylko z prawa do otrzymania danych osobowych przetwarzanych przez administratora, do którego kieruje żądanie (art. 18 ust. 1 RODO), czy również z prawa do przesłania jego danych osobowych w odpowiednim formacie bezpośrednio do innego, wskazanego administratora (art. 18 ust. 2 RODO). W drugim przypadku, podmiot danych powinien wskazać dokładne dane administratora, do którego dane mają być przesłane. Należy jednak pamiętać, że obowiązek ten będzie zrealizowany przez administratora, jeśli operacja taka okaże się możliwa do przeprowadzenia pod kątem technicznym.

W swoim żądaniu podmiot danych powinien doprecyzować, czy chce wykonać prawo do przenoszenia danych w odniesieniu do wszystkich jego danych osobowych przetwarzanych przez administratora, czy tylko niektórych danych. Wyraźnie oznaczony zakres danych, których przeniesienia domaga się podmiot danych, pozostaje bez wpływu na ocenę przez administratora, czy spełnione są przesłanki z art. 20 ust. 1 RODO. Przykładowo, jeśli

[231] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 12.

administrator przetwarza dane konkretnej osoby fizycznej w oparciu o różne podstawy prawne, np. niektóre kategorie danych są przetwarzane w oparciu o zgodę podmiotu danych, a inne w celu realizacji obowiązku prawnego, a podmiot danych chce wykonać prawo do przenoszenia danych w odniesieniu do tych kategorii danych, które są przetwarzane w związku z realizacją obowiązku prawnego, to **administrator powinien odmówić realizacji żądania**. Powinien przy tym poinformować podmiot danych o przyczynach odmowy uwzględnienia żądania. Dodatkowo dobrą praktyką w takim przypadku będzie pouczenie o tym, kiedy przysługuje prawo do przenoszenia danych, oraz czy może mieć zastosowanie w odniesieniu do innych danych przetwarzanych przez administratora.

Podmiot danych może żądać przeniesienia wyłącznie swoich danych osobowych, co oznacza, że jeśli z jego danymi są powiązane dane osobowe innych osób, to dane osób trzecich, o ile to możliwe, nie powinny podlegać przeniesieniu. Aczkolwiek w praktyce mogą zdarzać się sytuacje, w których nie da się oddzielić danych dotyczących osoby zgłaszającej żądanie od danych dotyczących innych osób. Wówczas administrator, zanim zrealizuje prawo do przenoszenia danych, powinien rozważyć, czy nie zachodzi negatywna przesłanka, o której mowa w art. 20 ust. 4 RODO, to znaczy czy ewentualne uwzględnienie wniosku nie wpłynie niekorzystnie na prawa i wolności innych podmiotów[232]. Co więcej, przeniesieniu podlegają wyłącznie dane spełniające kryteria definicyjne danych osobowych, wskazane w art. 4 pkt 1 RODO. W ramach omawianego prawa przeniesieniu będą przykładowo podlegać dane poddane pseudonimizacji, podczas gdy dane zanonimizowane nie będą objęte zakresem zastosowania prawa.

Ze względu na wymóg przetwarzania danych w sposób zautomatyzowany, będący przesłanką warunkującą wykonanie prawa do przenoszenia danych, podmiot danych nie może domagać się przeniesienia danych przetwarzanych w formie papierowej. Jeśli zgłosi takie żądanie, administrator może odmówić jego wykonania, informując o tym podmiot danych, wraz z podaniem przyczyn odmowy.

Jednocześnie z żądaniem przeniesienia danych, podmiot danych może zgłosić żądanie usunięcia jego danych osobowych przetwarzanych przez dotychczasowego administratora. Wskazuje na to art. 20 ust. 3 RODO, stanowiąc, że wykonanie prawa do przeniesienia danych osobowych pozostaje bez uszczerbku dla art. 17 RODO.

[232] Taka sytuacja może mieć przykładowo miejsce, gdy przeniesieniu mają podlegać dane zgromadzone na portalu społecznościowym, takie jak zdjęcia czy filmy, na których oprócz podmiotu danych znajdują się również inne osoby.

9.3. Sposób realizacji prawa do przenoszenia danych

W ramach realizacji prawa do przenoszenia danych jednym z kluczowych obowiązków administratora, poza właściwą identyfikacją podmiotu danych i weryfikacją spełniania przesłanek prawa do przenoszenia danych, jest odpowiednie zorganizowanie przetwarzania pod kątem technicznym, aby wykonanie żądania było możliwe. Jak wynika z art. 20 ust. 1 RODO, realizując prawo do przenoszenia danych administrator ma obowiązek dostarczyć dane „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego". Wymóg ten jest nawiązaniem do przyjętej na gruncie RODO zasady neutralności technicznej, tj. zasady stanowiącej, że ochrona osób fizycznych powinna być zawsze taka sama, bez względu na to, jakie techniki przetwarzania stosuje administrator – mniej lub bardziej zaawansowane[233]. Niezależnie od sposobu i wykorzystywanej przez administratora technologii przetwarzania danych osobowych, powinien on dostarczyć osobie, której dane dotyczą, dane w standardowym, interoperacyjnym formacie, umożliwiającym ich dalsze wykorzystanie. Standardowy format przekazywanych danych może być różny w zależności od sektora, w którym działa administrator (np. XML, JSON, CSV)[234]. Wskazuje się też, że przekazywane dane osobowe powinny obejmować metadane potrzebne do prawidłowego opisania przenoszonych danych osobowych[235]. Jednocześnie RODO nie nakłada na administratorów obowiązku stosowania kompatybilnych technicznie systemów przetwarzania, czyli takich, które mogą ze sobą bezpośrednio się łączyć, współpracować i w ten sposób przekazywać dane osobowe[236]. Niemniej jednak administrator w ramach projektowania systemu informatycznego, uwzględniając zasadę *privacy by design*, może przyjąć takie środki techniczne, które ułatwią współpracę i wymianę danych z różnymi systemami IT; nie jest natomiast zobowiązany do wprowadzania takich systemów i rozwiązań technicznych, które zapewnią automatyczną migrację danych pomiędzy różnymi systemami

[233] Zob. motyw 15 RODO.

[234] Więcej na temat właściwego formatu danych oraz pojęć „interoperacyjność" i „nadający się do odczytu maszynowego" – zob. Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 20.

[235] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 21.

[236] Motyw 68 RODO.

– jest to tylko jego uprawnienie, którego realizacja powinna być poczytywana jako ułatwienie podmiotom danych wykonywania prawa do przenoszenia danych[237].

W tym kontekście warto też zwrócić uwagę, że zgodnie z art. 20 ust. 1 RODO podmiot danych ma prawo przesłać otrzymane dane osobowe innemu administratorowi „bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe". Grupa Robocza Art. 29 wskazuje, że takimi przeszkodami mogą być bariery prawne, techniczne lub finansowe ustanowione przez administratora w celu powstrzymania lub spowolnienia dostępu, przesyłania lub ponownego wykorzystania danych podlegających przeniesieniu przez podmiot danych lub innego administratora[238]. Do takich przeszkód mogą należeć przykładowo żądanie wniesienia opłaty z tytułu przekazania danych, brak interoperacyjności lub dostępu do formatu danych, interfejsu programowania aplikacyjnego lub dostarczonego formatu itp.[239] W praktyce administratorzy mogą powoływać się na różne przeszkody uniemożliwiające przeniesienie danych, zwłaszcza na przesłanki z art. 20 ust. 3 lub 4 RODO, aby zatrzymać podmiot danych i w ten sposób utrudnić mu łatwe rozpoczęcie przetwarzania jego danych osobowych przez innego administratora, a tym samym np. zmianę dostawcy usługi.

Wykonując prawo do przenoszenia danych, podmiot danych może jednocześnie wystąpić z wnioskiem o usunięcie danych, które zostaną przeniesione. Administrator nie jest jednak tym wnioskiem związany. Za każdym razem administrator musi ocenić, czy zachodzą odpowiednie przesłanki umożliwiające realizację prawa do usunięcia danych. W niektórych przypadkach administrator powinien odmówić, np. gdy przetwarzanie danych podlegających przeniesieniu jest konieczne w związku z zawartą umową, z tym zastrzeżeniem, że administrator powinien zbadać, które dane są niezbędne do wykonania umowy[240]. Wówczas administrator ma prawo dalej przetwarzać dane np. w celu dalszego

[237] Grupa Robocza Art. 29 w wytycznych podkreśla, że „[…] w ramach dobrej praktyki administratorzy danych powinni rozpocząć prace nad środkami, które będą pomocne przy udzielaniu odpowiedzi na żądania o przeniesienie danych, takimi jak narzędzia do pobierania i interfejsy programowania aplikacyjnego", przypominając jednocześnie, iż RODO nie nakłada obowiązku wprowadzenia kompatybilnych technicznie systemów przetwarzania, ani też nie zakazuje administratorom tworzenia barier utrudniających przesyłanie danych – zob. Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 3, 5–6.

[238] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 18.

[239] Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 18.

[240] Tak wskazano w motywie 68 RODO: „Prawo do […] nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, których osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy".

wykonywania umowy lub w celach rozliczeniowych. Niezależnie od sposobu rozpoznania takiego żądania, administrator ma obowiązek poinformować podmiot danych, czy zrealizuje wniosek dotyczący usunięcia danych, czy nie. W razie odmowy, powinien również pouczyć o możliwości wniesienia skargi do PUODO.

W przypadku prawa do przenoszenia danych administratora obowiązują ogólne terminy realizacji tego prawa wynikające z art. 12 ust. 3 RODO, a zatem administrator zobligowany jest udzielić podmiotowi danych odpowiedzi niezwłocznie, nie później niż w ciągu miesiąca od dnia otrzymania żądania. Termin ten może być przez administratora wydłużony o dodatkowe dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Realizacja prawa do przenoszenia danych następuje co do zasady bezpłatnie, chyba że żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne – wówczas administrator ma prawo pobrać rozsądną opłatę, skalkulowaną w oparciu o administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo odmówić podjęcia działań w związku z żądaniem[241]. Poza tym administrator powinien pamiętać o dokonaniu stosownego wpisu do rejestru realizacji praw podmiotów danych, zawierającego przynajmniej informacje o dacie wpływu żądania, dacie udzielenia odpowiedzi, sposobie realizacji prawa, w tym o danych podlegających przeniesieniu, przyczynach odmowy wykonania żądania, oraz jeśli ma to zastosowanie – informacje o administratorze, na rzecz którego nastąpiło przeniesienie danych. Prowadzenie tego rodzaju rejestru sprzyja realizacji zasady rozliczalności oraz umożliwia administratorowi wykazanie w przyszłości, że zgłoszone żądanie zostało prawidłowo rozpoznane.

9.4. Wyłączenia

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[242]. Wyłączenie to uzasadnione jest specyfiką przetwarzania danych osobowych w związku z realizacją zadań publicznych i oznacza, że nawet jeśli przetwarzanie danych przez administratora spełnia kryteria wymienione

[241] Artykuł 12 ust. 5 RODO.

[242] Artykuł 20 ust. 3 RODO.

w art. 20 ust. 1 RODO, podmiot danych nie może skutecznie żądać od niego wykonania prawa do przenoszenia danych[243].

Realizacja prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych[244]. Jak wskazuje Grupa Robocza Art. 29, niekorzystny wpływ może mieć miejsce, gdy przesyłanie danych przez jednego administratora danych innemu administratorowi uniemożliwia osobom trzecim wykonywanie uprawnień przysługujących im jako osobom, których dane dotyczą, na mocy RODO (np. prawa do informacji, prawa dostępu itd.)[245]. Przesłanka ta może zajść przykładowo, gdy wraz z danymi osoby składającej żądanie przenoszone są dane osobowe innych osób, ponieważ nie da się ich oddzielić[246]. Dobrą praktyką może być wdrażanie przez administratorów narzędzi umożliwiających podmiotom danych wybór tych danych, które chcą otrzymać i przesłać w ramach prawa do przenoszenia danych, oraz wyłączenie – w stosownych przypadkach – możliwości przekazywania danych innych osób fizycznych[247]. Innym sposobem może być – tam, gdzie to możliwe – odbieranie zgód od osób trzecich na przesyłanie ich danych osobowych do innego administratora[248]. Praktyki te mogą przyczynić się do ograniczenia potencjalnych zagrożeń dla osób trzecich, choć nie eliminują zupełnie związanego z tym ryzyka.

Przy dokonywaniu oceny, czy realizacja prawa do przenoszenia danych może niekorzystnie wpływać na prawa i wolności innych, należy brać pod uwagę również ryzyko naruszenia

---

243 P. Fajgielski, *Ogólne rozporządzenie…*, s. 292. W literaturze przedmiotu podnosi się ponadto, że skoro wobec podmiotów realizujących zadania w interesie publicznym lub w ramach sprawowania władzy publicznej nie powinno się wykonywać prawa do przenoszenia danych, to również podmioty te nie powinny otrzymywać takich danych na skutek przekazania ich, w ramach art. 20 ust. 1 RODO, przez innego administratora. – zob. M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 20.

244 Artykuł 20 ust. 4 RODO.

245 Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 13.

246 Przykładowo, przy zmianie operatora poczty mailowej i przeniesieniu do nowego administratora wszystkich danych pocztowych, w tym odbiorców i nadawców wiadomości, listy kontaktów itp.; przy zmianie dostawy usług bankowych i przeniesieniu do nowego administratora danych dotyczących transakcji dokonywanych przez posiadacza rachunku i inne osoby fizyczne. W tych przypadkach może dojść do naruszenia praw i wolności osób trzecich, jeśli nowy administrator wykorzysta dane osobowe do innych celów, np. do celów marketingowych i kierowania ofert handlowych. Dopuszczalne jest natomiast przetwarzanie tych danych w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą podmiotu danych występującego z żądaniem i są zarządzane wyłącznie w celu zaspokojenia jego potrzeb o osobistym lub domowym charakterze. Zob. Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 14.

247 Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 14.

248 Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia…*, s. 14. Przykładowo, przy przenoszeniu danych osobowych między portalami społecznościowymi.

tajemnic handlowych lub praw własności intelektualnej, w tym praw autorskich chroniących oprogramowanie. Mimo to, względy te nie powinny skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji[249].

Na koniec warto też zauważyć, że administrator przekazujący dane osobowe bezpośrednio innemu administratorowi wskazanemu przez podmiot danych, nie ponosi odpowiedzialności za sposób przetwarzania danych osobowych stosowany przez administratora otrzymującego dane. Zwłaszcza nie ponosi odpowiedzialności za obniżenie stopnia bezpieczeństwa tych danych. To podmiot danych ponosi ryzyko związane z przenoszeniem jego danych osobowych, ponieważ operacja ta odbywa się na jego żądanie. Można jednak zastanawiać się, czy administrator realizujący prawo do przenoszenia danych nie powinien w takim przypadku ocenić przekazania danych z perspektywy przesłanki, o której mowa w art. 20 ust. 4 RODO. Kwestia ta budzi wątpliwości w literaturze przedmiotu[250].

[249] Motyw 68 RODO. W tym kontekście w literaturze przedmiotu zwraca się uwagę, że administrator, który umożliwia samodzielne pobranie danych przez podmiot danych, powinien zweryfikować, czy czynność ta (czyli samodzielny dostęp do programu przez użytkownika) nie narusza postanowień licencji posiadanej przez administratora. Więcej zob. M. Sakowska-Baryła (red.), *Ogólne rozporządzenie…*, komentarz do art. 20.

[250] Zob. przykł. M. Susałko, *Prawo do przenoszenia* [w:] D. Lubasz (red.), *Meritum…*, s. 201.

10. Prawo do sprzeciwu – art. 21 RODO

10.1. Zakres prawa

Osoba, której dane dotyczą, ma prawo sprzeciwić się przetwarzaniu jej danych osobowych przez administratora, nawet jeśli jej dane są przetwarzane zgodnie z prawem. Jest to szczególne uprawnienie podmiotu danych, przysługujące mu w określonych w art. 21 RODO przypadkach. Jego istoty upatruje się w potrzebie zapewnienia równowagi między prawami osoby, której dane dotyczą, a uprawnieniami administratora[251].

Sprzeciw może być zgłoszony, jeśli dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. e) RODO, tj. gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub na podstawie art. 6 ust. 1 lit. f) RODO, tj. gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią[252]. Wnosząc sprzeciw wobec przetwarzania, podmiot danych powinien go uzasadnić swoją szczególną sytuacją. Wówczas administrator zobowiązany jest zaprzestać przetwarzać dane osobowe podmiotu danych, chyba że jest w stanie wykazać istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

---

[251] Wniosek taki można wyciągnąć na podstawie analizy przesłanek dopuszczalności skorzystania z prawa do sprzeciwu, a dokładnie przesłanek odnoszących się do podstaw prawnych przetwarzania danych osobowych. Jak wskazuje się w literaturze przedmiotu, podmiot danych nie ma możliwości wniesienia sprzeciwu wobec przetwarzania jego danych osobowych, jeśli dopuszczalność przetwarzania wynika z jego woli [art. 6 ust. 1 lit. a) i b) RODO]), z woli prawodawcy [art. 6 ust. 1 lit. c) RODO] lub z potrzeby ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej [art. 6 ust. 1 lit. d) RODO], w tych przypadkach zachowana jest bowiem równowaga między prawami podmiotu danych a prawami administratora. W pozostałych przypadkach, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej [art. 6 ust. 1 lit. e) RODO] lub gdy przetwarzanie jest niezbędne w celach wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią [art. 6 ust. 1 lit. f) RODO], pozycja podmiotu danych jest słabsza i wymaga większej ochrony. Zob. więcej – P. Fajgielski, *Ogólne rozporządzenie…*, s. 296.

[252] Artykuł 21 ust. 1 RODO.

Zgodnie z art. 21 ust. 2 RODO, podmiot danych może też zgłosić sprzeciw wobec przetwarzania, jeśli jego dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, w tym profilowania[253]. Taki sprzeciw nie musi być uzasadniony szczególną sytuacją podmiotu danych. Inne są też konsekwencje jego wniesienia – jeżeli okaże się zasadny, administratorowi nie wolno już przetwarzać danych do takich celów[254]. Prawodawca unijny nie pozostawił w tym przypadku administratorowi możliwości dalszego przetwarzania danych w zakresie, w jakim były przetwarzane w związku z marketingiem bezpośrednim.

Wreszcie podmiot danych może zgłosić sprzeciw wobec przetwarzania, jeśli przetwarzanie jego danych osobowych następuje w celu realizacji badań naukowych, badań historycznych lub do celów statystycznych na podstawie art. 89 ust. 1 RODO (art. 21 ust. 5 RODO). Podobnie jak w przypadku przetwarzania na podstawie art. 6 ust. 1 lit. e) lub f) RODO, sprzeciw musi być umotywowany szczególną sytuacją podmiotu danych. Mimo wniesionego sprzeciwu administrator może dalej przetwarzać dane osobowe, jeśli ich przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

W zależności od okoliczności i przyczyn sprzeciwu wobec przetwarzania, procedura jego rozpoznawania może się różnić. Sprzeciw zgłoszony na podstawie art. 21 ust. 1 RODO wymaga w pierwszej kolejności oceny i porównania interesów podmiotu danych i administratora, przemawiających za uwzględnieniem sprzeciwu albo za dopuszczalnością dalszego przetwarzania, podczas gdy sprzeciw wyrażony w oparciu o art. 21 ust. 2 RODO powinien skutkować od razu zaprzestaniem przetwarzania. Odmienne mogą być też skutki wniesionego sprzeciwu, gdyż w niektórych sytuacjach administrator będzie musiał usunąć przetwarzane dane, a w innych – mimo zasadności sprzeciwu – będzie mógł je dalej przetwarzać z uwagi na inną przesłankę legalizującą przetwarzanie. Zdarza się bowiem, że dane osobowe przetwarzane są w różnych celach i w oparciu o różne podstawy prawne. Tak może być, gdy te same dane przetwarzane są w celu wykonania umowy [art. 6 ust. 1 lit. b) RODO] i jednocześnie w celu realizacji prawnie uzasadnionego interesu administratora polegającego na wysyłaniu ofert handlowych [art. 6 ust. 1 lit. f) RODO]. Wniesienie przez

[253] Pojęcie „profilowanie” zostało zdefiniowane w art. 4 pkt 4 RODO. Zgodnie z definicją oznacza ono „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”.

[254] Artykuł 21 ust. 3 RODO.

podmiot danych sprzeciwu wobec przetwarzania powinno w takiej sytuacji poskutkować zaprzestaniem przetwarzania danych, ale wyłącznie w zakresie objętym sprzeciwem, tj. w zakresie, w jakim dane osobowe służą realizacji prawnie uzasadnionych interesów administratora[255]. Zaprzestanie przetwarzania danych w szerszym zakresie aniżeli wynika to ze sprzeciwu może unicestwić realizację innych celów przetwarzania.

10.2. Sposób skorzystania z prawa do sprzeciwu

Sprzeciw wobec przetwarzania może być zgłoszony w dowolnym momencie; podmiot danych nie jest w tym zakresie zobligowany jakimkolwiek terminem czy warunkiem. Z treści dokonywanego zgłoszenia powinno jasno wynikać, że intencją podmiotu danych jest wyrażenie sprzeciwu wobec przetwarzania jego danych osobowych przez konkretnego administratora. Jeśli treść lub zakres żądania budzą wątpliwości, administrator ma prawo poprosić o doprecyzowanie żądania[256]. Prawidłowo ustalony zakres żądania determinuje dalsze kroki administratora, dlatego tak ważne jest jego dookreślenie.

W przypadku realizacji prawa do sprzeciwu podmiot danych powinien umotywować swoje żądanie istnieniem przyczyn związanych z jego szczególną sytuacją. Wynika to wprost z art. 21 ust. 1 i ust. 6 RODO. Podmiot danych powinien zatem wskazać na okoliczności, które jego zdaniem przemawiają za tym, że znajduje się on w szczególnej sytuacji, która to sytuacja uzasadnia zaprzestanie przetwarzania jego danych osobowych. Pojęcie szczególnej sytuacji podmiotu danych nie zostało wyjaśnione w przepisach rozporządzenia. W literaturze przedmiotu wskazuje się, że za sytuację szczególną należy uznać „każdy stan faktyczny, który – po pierwsze – nie istniał w chwili zbierania danych osobowych, jeżeli dane były zbierane bezpośrednio od osoby, której dotyczą, lub który co prawda istniał w chwili zbierania danych, lecz nie był wiadomy administratorowi danych, jeżeli dane osobowe były zbierane nie

[255] P. Fajgielski, *Ogólne rozporządzenie…*, s. 298; M. Susałko, *Prawo do sprzeciwu* [w:] D. Lubasz (red.), *Meritum…*, s. 205.

[256] Przykładowo, gdy administrator przetwarza duże ilości danych osobowych w oparciu o art. 6 ust. 1 lit. f) RODO, w tym część z nich w celach marketingu bezpośredniego, a z treści żądania nie wynika, czy podmiot danych chce wyrazić sprzeciw w odniesieniu do wszystkich danych przetwarzanych przez administratora, czy tylko wobec przetwarzania realizowanego w celach marketingowych. Administrator może też poprosić o doprecyzowanie żądania, jeśli nie ma pewności, czy podmiot danych chce skorzystać z prawa do sprzeciwu, czy chce wycofać zgodę na przetwarzanie jego danych osobowych.

bezpośrednio od osoby, której dane dotyczą”[257]. Nadto szczególna sytuacja osoby, której dane dotyczą, „powinna wpływać na przetwarzanie jej danych osobowych w ten sposób, że dojdzie do zachwiania równowagi interesów tej osoby oraz administratora danych – w wyniku tego interes osoby, której dane dotyczą, powinien przeważyć nad interesem administratora danych. Innymi słowy, potrzeba ochrony prywatności podmiotu danych powinna przeważyć nad potrzebą przetwarzania tych danych przez administratora”[258].

Szczególna sytuacja podmiotu danych nie musi dotyczyć okoliczności o charakterze obiektywnym; mogą to być okoliczności subiektywne, oceniane z perspektywy podmiotu danych. Za przyczyny związane ze szczególną sytuacją podmiotu danych, uzasadniające zaprzestanie przetwarzania danych osobowych wnioskodawcy, można uznać przyczyny wywołujące negatywne konsekwencje w sferze praw i wolności podmiotu danych, takie jak utrata prywatności, dobrego imienia, ujawnienie okoliczności dotyczących życia rodzinnego itp. Uzasadnienie przez podmiot danych wnoszonego sprzeciwu jest niezbędne do oceny przez administratora:

– czy istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności podmiotu danych, lub czy istnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń – jeśli sprzeciw wobec przetwarzania wnoszony jest na podstawie art. 21 ust. 1 RODO; lub
– czy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym – jeśli sprzeciw wobec przetwarzania wnoszony jest na podstawie art. 21 ust. 6 RODO.

We wskazanych wyżej przypadkach administrator musi dokonać ważenia interesów podmiotu danych i jego własnych w celu porównania, które z nich przeważają, a w konsekwencji, czy sprzeciw powinien być uwzględniony, czy też możliwe jest dalsze przetwarzanie danych osobowych. Bez podania uzasadnienia wniosku sprzeciw nie zostanie rozpoznany. W tym kontekście warto zwrócić uwagę na regulację art. 21 ust. 5 RODO, stanowiącą, że w związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE[259] osoba, której dane dotyczą, może wykonać prawo do sprzeciwu

[257] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 21 RODO.

[258] P. Litwiński (red.), *Ogólne rozporządzenie…*, komentarz do art. 21 RODO.

[259] Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. Urz. UE L 201 z dn. 31.07.2002 r., s. 37–47.

za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. Oznacza to, że jeśli dane osobowe są przetwarzane np. w serwisie internetowym, podmiot danych powinien mieć zapewnioną możliwość skorzystania ze swojego uprawnienia za pomocą odpowiedniej funkcjonalności dostępnej w tym serwisie, np. za pośrednictwem formularza lub innego rodzaju elektronicznego zgłoszenia. Podkreśla się, że stosowanie elektronicznych formularzy jest dobrym rozwiązaniem z tego względu, iż administrator może w nich przewidzieć odpowiednie pola, których wypełnienie będzie konieczne przed wysłaniem formularza[260]. Takim polem może być uzasadnienie sprzeciwu szczególną sytuacją podmiotu danych. Praktyka pokazuje, że osoby wnoszące sprzeciw wobec przetwarzania często zapominają, że co do zasady powinny uzasadnić swoje żądanie, za wyjątkiem sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego. Przygotowanie przez administratora odpowiedniego formularza dostępnego online mogłoby przynajmniej częściowo rozwiązać ten problem, należy bowiem pamiętać, że podmiot danych nie musi korzystać ze sposobu realizacji prawa do sprzeciwu sugerowanego przez administratora, ale może swoje żądanie zgłosić w dowolnej formie.

10.3. Sposób realizacji prawa do sprzeciwu

Analogicznie do innych praw przewidzianych na gruncie RODO, rozpoznanie wniosku zawierającego sprzeciw wobec przetwarzania danych osobowych administrator powinien rozpocząć od identyfikacji osoby występującej z wnioskiem i ustalenia, czy przetwarza on jej dane osobowe oraz czy jest ich administratorem. Sprzeciw wobec przetwarzania zgłoszony wobec podmiotu, który nie jest administratorem danych objętych żądaniem, podlega oddaleniu. Jeśli sprzeciw został skierowany wobec podmiotu przetwarzającego dane osobowe w imieniu administratora w ramach stosunku powierzenia, procesor powinien niezwłocznie przekazać żądanie do administratora, chyba że co innego wynika z wzajemnych ustaleń.

Po potwierdzeniu, że administrator przetwarza dane osoby występującej z żądaniem oraz po weryfikacji jej tożsamości, administrator powinien ocenić spełnienie poszczególnych przesłanek dopuszczalności sprzeciwu. Proces ten będzie wyglądał inaczej, w zależności od tego, na jakiej przesłance podmiot danych oparł swój sprzeciw wobec przetwarzania.

[260] M. Susałko, *Prawo do sprzeciwu* [w:] D. Lubasz (red.), *Meritum…*, s. 211.

Samo wniesienie sprzeciwu nie pociąga też konieczności natychmiastowego zaprzestania przetwarzania danych objętych sprzeciwem. Wyjątek stanowią sytuacje, w których sprzeciw dotyczy przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania – wówczas, zgodnie z dyspozycją art. 21 ust. 3 RODO, administrator nie może dalej przetwarzać tych danych osobowych w celu prowadzenia działań marketingowych.

Wniesienie sprzeciwu wobec przetwarzania danych opartego na art. 6 ust. 1 lit. e) lub f) RODO wymaga uzasadnienia go istnieniem szczególnej sytuacji podmiotu danych. Sprzeciw taki nie musi być zawsze przez administratora uwzględniony, ponieważ administrator może uznać, że po jego stronie zachodzą ważne prawnie uzasadnione podstawy do przetwarzania, które są nadrzędne wobec interesów, praw i wolności wnioskodawcy. Administrator może też wykazać, że przysługują mu ważne prawnie uzasadnione podstawy do ustalenia, dochodzenia lub obrony roszczeń, uzasadniające dalsze przetwarzanie danych osobowych mimo wniesionego sprzeciwu. Wykazanie tych okoliczności przez administratora wymaga więc przeprowadzenia wszechstronnej oceny z jednej strony okoliczności podniesionych przez podmiot danych, związanych z jego szczególną sytuacją, a z drugiej – ewentualnego istnienia okoliczności, które mogłyby uzasadniać dalsze przetwarzanie danych osobowych, ponieważ są „nadrzędne" i w danym stanie faktycznym mogą przeważyć nad potrzebą ochrony interesów podmiotu danych. Przeprowadzenie tego rodzaju analizy przez administratora powinno być odpowiednio udokumentowane w celu spełnienia wymogu rozliczalności z art. 5 ust. 2 RODO. Jednocześnie warto podkreślić, że **omawiany tu proces ważenia praw i interesów powinien być przeprowadzony niezależnie od tego, które jest wymagane przed rozpoczęciem przetwarzania danych osobowych w celu realizacji prawnie uzasadnionych interesów administratora lub strony trzeciej**, tj. na podstawie art. 6 ust. 1 lit. f) RODO. Rozpoznając sprzeciw wobec przetwarzania administrator nie może powołać się na wcześniej przeprowadzony proces ważenia interesów, choćby z tej przyczyny, że na gruncie art. 21 ust. 1 RODO administrator mus wykazać istnienie „ważnych" prawnie uzasadnionych podstaw do przetwarzania.

Analogicznie wniesienie sprzeciwu wobec przetwarzania realizowanego do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO powinno być uzasadnione przyczynami związanymi ze szczególną sytuacją podmiotu danych. W tym przypadku administrator również może kontynuować przetwarzanie danych osobowych, ale pod warunkiem, że wykaże, iż przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Administrator tym razem musi ze sobą

zestawić z jednej strony okoliczności związane ze szczególną sytuacją, na które powołuje się wnioskodawca, a z drugiej – okoliczności związane z wykonywaniem zadania w interesie publicznym, w szczególności niezbędność przetwarzania danych do osiągnięcia celu przetwarzania.

W jednym tylko przypadku sprzeciw wobec przetwarzania nie musi zawierać uzasadnienia, a mianowicie, gdy dotyczy on przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania. Zgłoszenie tego rodzaju sprzeciwu pociąga za sobą konieczność zaprzestania przetwarzania danych, bez konieczności wyważania praw i interesów podmiotu danych i administratora. Sprzeciw ten wywołuje więc „silniejszy" skutek, ponieważ jego uwzględnienie nie zależy ani od wagi okoliczności związanych z sytuacją podmiotu danych, ani od subiektywnej oceny administratora, przesądzającej o zasadności lub bezzasadności realizowanego prawa.

Jeśli administrator nie znajduje podstaw do uwzględnienia sprzeciwu, powinien poinformować o tym podmiot danych, odmawiając realizacji prawa **w całości lub w części – w zależności od okoliczności przetwarzania**. Przykładowo, administrator może częściowo uwzględnić sprzeciw i zaprzestać przetwarzania danych osobowych w celu marketingu bezpośredniego, a jednocześnie odmówić uwzględnienia sprzeciwu wobec pozostałych danych przetwarzanych na podstawie art. 6 ust. 1 lit. f) RODO z uwagi na istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności podmiotu danych lub podstaw do ustalenia, dochodzenia lub obrony roszczeń (np. gdy podmiot danych nie uregulował płatności za usługę świadczoną przez administratora – uwzględnienie sprzeciwu i zaprzestanie przetwarzania narazi administratora na ryzyko utraty możliwości dochodzenia jego roszczeń). W odpowiedzi administrator powinien też pouczyć o możliwości wniesienia skargi do PUODO, jeśli podmiot danych nie zgadza się z jego decyzją. Ponadto na czas rozpoznawania sprzeciwu wniesionego na podstawie art. 21 ust. 1 RODO – jeśli podmiot danych złożył stosowny wniosek – administrator powinien ograniczyć przetwarzanie danych objętych sprzeciwem[261].

W kontekście rozpoznawania sprzeciwu wobec przetwarzania danych warto też zaakcentować, że sprzeciw nie jest równoznaczny z cofnięciem zgody na przetwarzanie danych i odwrotnie – cofnięcie zgody nie jest tożsame ze zgłoszeniem sprzeciwu wobec

[261] Artykuł 18 ust. 1 lit. d) RODO.

przetwarzania. W obydwu przypadkach skutki oświadczenia podmiotu danych są z prawnej perspektywy inne, mimo że w praktyce mogą prowadzić do takiego samego efektu w postaci zaprzestania przetwarzania i usunięcia danych osobowych. Kluczowa różnica polega na tym, że w razie cofnięcia zgody na przetwarzanie danych osobowych, administrator nie może już przetwarzać danych osobowych, jeśli nie dysponuje inną przesłanką legalizującą przetwarzanie. Natomiast w razie zgłoszenia sprzeciwu, administrator jest uprawniony do dalszego przetwarzania danych objętych sprzeciwem pod warunkiem, że jest w stanie wykazać istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń[262]. Poza tym, sprzeciw wobec przetwarzania nie przysługuje, jeżeli dane przetwarzane są w oparciu o zgodę podmiotu danych. Jeśli mimo to podmiot danych zgłosi sprzeciw wobec przetwarzania, administrator powinien poinformować o odmowie jego uwzględnienia, podając przyczyny, i jednocześnie pouczyć, że z uwagi na przetwarzanie danych osobowych w oparciu o zgodę podmiotu danych, podmiot ten uprawniony jest do cofnięcia zgody na przetwarzanie. Taka praktyka z pewnością może być zakwalifikowana jako działanie mające na celu ułatwienie podmiotowi danych wykonywania jego praw zgodnie z rekomendacjami zawartymi w motywie 59 RODO.

Na potrzeby zasady rozliczalności, wynikającej z art. 5 ust. 2 RODO, administrator powinien udokumentować sposób rozpoznania żądania sprzeciwu, w tym datę wpłynięcia żądania, sposób przeprowadzenia i wynik procesu ważenia interesów **– jeśli jego przeprowadzenie było konieczne, termin rozpoznania żądania,** przyczyny odmowy żądania, sposób udzielenia odpowiedzi itp. Informacje te najlepiej zamieścić w rejestrze realizacji praw podmiotów danych w celu przechowywania ich w jednym, oznaczonym miejscu. W razie uwzględnienia sprzeciwu administrator musi też podjąć odpowiednie czynności w stosunku do danych objętych sprzeciwem, w szczególności powinien je usunąć, jeśli nie dysponuje inną podstawą legalizującą ich przetwarzanie.

Proces komunikacji z podmiotem danych w ramach realizacji jego prawa do sprzeciwu powinien zawsze spełniać wymogi zasady przejrzystości, o których mowa w art. 12 RODO. To, jak istotne jest przekazanie informacji o przysługującym podmiotowi danych prawie do sprzeciwu, prawodawca unijny dodatkowo podkreślił w art. 21 ust. 4 RODO, nakładając

[262] *Nota bene* za wyjątkiem sytuacji, w której sprzeciw dotyczy przetwarzania w celach marketingu bezpośredniego.

na administratora obowiązek poinformowania o nim, w sposób wyraźny, najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą[263]. Informacja ta powinna być przedstawiona jasno i odrębnie od wszelkich innych informacji. W praktyce oznacza to, że informacja o przysługującym prawie do sprzeciwu będzie przekazywana przez administratora przy okazji spełniania obowiązku informacyjnego z art. 13 lub 14 RODO, przy czym informacja ta powinna być zamieszczona najlepiej w osobnym punkcie, niepołączonym z innymi kwestiami (np. z informacjami o innych prawach przysługujących podmiotowi danych).

Administrator powinien udzielić informacji na temat sposobu rozpoznania żądania bez zbędnej zwłoki, najpóźniej w ciągu miesiąca od otrzymania żądania, chyba że skomplikowany charakter żądania lub liczba zgłoszonych żądań uzasadniają wydłużenie tego terminu o kolejne dwa miesiące[264]. Realizacja prawa do sprzeciwu jest co do zasady wolna od opłat, za wyjątkiem sytuacji, w których żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne[265]. Wtedy administrator może pobrać opłatę, ustaloną z uwzględnieniem administracyjnych kosztów udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych przez podmiot danych działań.

[263] Na marginesie warto dodać, że obowiązek wyraźnego poinformowania o prawie do sprzeciwu dotyczy tylko sprzeciwu wyrażonego na podstawie art. 21 ust. 1 lub 2 RODO, a zatem nie dotyczy sprzeciwu zgłoszonego na podstawie art. 21 ust. 6 RODO, tj. gdy dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO. Niemniej jednak nie oznacza to, że administrator w tym przypadku w ogóle nie ma obowiązku poinformowania podmiotu danych o przysługującym mu prawie do sprzeciwu, obowiązek ten wynika bowiem z art. 13 ust. 2 lit. b) RODO oraz z art. 14 ust. 2 lit. c) RODO. Inaczej twierdzi M. Susałko wskazując, że „w przypadku przetwarzania danych osobowych na mocy art. 89 ust. 1 do celów badań naukowych lub historycznych lub do celów statystycznych nie ma potrzeby informowania podmiotu danych o prawie sprzeciwu" – zob. M. Susałko, *Prawo do sprzeciwu* [w:] D. Lubasz (red.), *Meritum…*, s. 211. Wydaje się, że taka interpretacja nie jest prawidłowa. Mimo to, warto jednocześnie zauważyć, że zgodnie z art. 89 ust. 2 i 3 RODO w prawie unijnym lub krajowym mogą być przewidziane wyjątki od realizacji prawa do sprzeciwu w przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych, do celów statystycznych lub do celów archiwalnych w interesie publicznym. W razie wprowadzenia takich wyjątków, administrator nie musi informować o prawo do sprzeciwu.

[264] Artykuł 12 ust. 3 RODO.

[265] Artykuł 12 ust. 5 RODO.

10.4. Wyłączenia

W art. 21 RODO nie wprowadzono wprost żadnych wyjątków od realizacji prawa do sprzeciwu poza sytuacjami, w których administrator może uznać sprzeciw na niezasadny, np. z uwagi na konieczność dalszego przetwarzania danych w celu obrony roszczeń. Niemniej jednak polski ustawodawca skorzystał z normy kompetencyjnej przewidzianej w art. 23 RODO, wprowadzając do polskiego porządku prawnego przepisy ograniczające możliwość skorzystania z prawa do sprzeciwu. Przepisy takie wprowadzono przykładowo do art. 16 ust. 2 ustawy Prawo o adwokaturze, art. 5a ust. 2 ustawy o radcach prawnych czy art. 78b § 2 ustawy Prawo o notariacie. We wszystkich wskazanych przypadkach ustawodawca wyłączył stosowanie art. 21 ust. 1 RODO, co oznacza, że osoba fizyczna korzystająca z usług adwokata, radcy prawnego lub notariusza nie może skutecznie zgłosić sprzeciwu wobec przetwarzania danych osobowych pozyskanych w związku z udzielaniem pomocy prawnej lub przy dokonywaniu czynności notarialnych.

11. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie – art. 22 RODO

11.1. Zakaz podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych – uwagi na tle art. 22 ust. 1 RODO

Każda osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa. Artykuł 22 ust. 1 RODO wprowadza ogólny zakaz podejmowania zautomatyzowanych decyzji wobec osób, których dane są przetwarzane, jeśli decyzje takie mogłyby wpłynąć na sytuację prawną podmiotu danych lub wywołać inne skutki o podobnym charakterze. Choć literalnie prawodawca unijny przyznał podmiotom danych „prawo do niepodlegania" decyzjom podejmowanym w sposób zautomatyzowany, konstrukcyjnie art. 22 RODO jest traktowany jako zakaz stosowania takiej praktyki, który doznaje jednak kilku wyjątków opisanych w art. 22 ust. 2 RODO. Funkcją zakazu jest przeciwdziałanie zagrożeniom dla praw i wolności podmiotów danych, jakie pojawiają się wraz z dynamicznym rozwojem nowoczesnych technologii oraz na skutek ich coraz powszechniejszego wykorzystywania, również w codziennym obrocie gospodarczym i prawnym (np. do oceny zdolności kredytowej lub w procesach rekrutacyjnych).

Analiza art. 22 ust. 1 RODO prowadzi do wyodrębnienia kilku przesłanek, których spełnienie przesądza o tym, czy administrator podlega reżimowi przepisu, a w konsekwencji także

o tym, czy podmiot danych może skorzystać z przysługujących mu w tym zakresie uprawnień. Podstawową przesłanką determinującą zastosowanie przepisu jest podejmowanie przez administratora decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Drugą przesłanką jest wpływ tego rodzaju decyzji na podmiot danych – jeśli decyzje oparte na zautomatyzowanym przetwarzaniu wywołują wobec podmiotu danych skutki prawne lub w podobny sposób istotnie na niego wpływają, wówczas administrator podlega reżimowi art. 22 RODO.

Podejmowanie decyzji wyłącznie w sposób zautomatyzowany to zdolność do podejmowania decyzji z wykorzystaniem rozwiązań technicznych bez interwencji ludzkiej[266]. Decyzje te mogą być podejmowane na podstawie danych przekazanych bezpośrednio przez podmiot danych (np. w trakcie wypełniania formularza, podawania danych do zawarcia umowy), danych zaobserwowanych przez administratora (np. dane o lokalizacji zbierane za pośrednictwem aplikacji lub urządzenia) czy też danych pochodnych lub wywnioskowanych przez administratora (np. stworzenie profilu konkretnej osoby fizycznej na podstawie zgromadzonych wcześniej danych). W ramach zautomatyzowanego podejmowania decyzji może dochodzić do profilowania[267]. W kontekście RODO i przetwarzania danych osobowych, do profilowania dochodzi wówczas, gdy:

– stanowi ono zautomatyzowaną formę przetwarzania,
– profilowaniu podlegają dane osobowe oraz
– jego celem jest ocena czynników osobowych osób fizycznych[268].

Profilowanie stosuje się do tworzenia prognoz na temat osób fizycznych – określonych grup społecznych lub konkretnych osób. Na podstawie danych pochodzących z różnych źródeł wyciąga się wnioski dotyczące określonej osoby lub grupy osób, posiłkując się przesłankami statystycznymi, tzn. oceniając tę osobę/grupę osób ze statystycznego punktu widzenia. Za Grupą Roboczą Art. 29 można więc przyjąć, że w praktyce profilowanie oznacza

[266] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, ostatnio zmienione i przyjęte w dn. 6.02.2018 r., WP251rev.01, s. 9.

[267] Na gruncie RODO profilowanie definiowane jest jako dowolna forma zautomatyzowanego przetwarzania danych osobowych, która 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 – zob. art. 4 pkt 4 RODO.

[268] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 7.

gromadzenie informacji o danej osobie lub grupie osób oraz ocenę ich cech lub wzorców zachowania w celu zakwalifikowania ich do określonej kategorii lub grupy, w szczególności w celach analizy lub prognozy takich aspektów jak zdolność do wykonania określonego zadania, wykazywane zainteresowania lub prawdopodobne zachowania. Jednak nie zawsze klasyfikacja osób fizycznych na podstawie ich cech prowadzi do profilowania. Przykładowo, klasyfikowanie klientów przez przedsiębiorcę – administratora ich danych osobowych – pod względem ich wieku lub płci, dokonywane w celu stworzenia statystyki osób odwiedzających sklep, nie zaś w celu poznania lub prognozowania ich preferencji zakupowych i wyciągania na tej podstawie wniosków dotyczących konkretnych osób lub grup osób, nie będzie kwalifikowane jako profilowanie na gruncie RODO. Warto równocześnie podkreślić, że nie każde profilowanie zawsze wiąże się ze zautomatyzowanym podejmowaniem decyzji. Jeśli profilowanie nie wywołuje skutków, o których mowa w art. 22 ust. 1 RODO, nie mieści się w reżimie tego przepisu, a w konsekwencji nie podlega przewidzianym w nim ograniczeniom.

Dla oceny, czy w konkretnym przypadku dochodzi do podejmowania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych, kluczowy jest czynnik ludzki. Jeśli proces decyzyjny odbywa się bez jakiegokolwiek zaangażowania człowieka (np. gdy decyzja podejmowana za pomocą algorytmu jest automatycznie przekazywana osobie fizycznej, której dotyczy, i nie podlega żadnej ocenie przez człowieka), to niewątpliwie proces ten jest w pełni zautomatyzowany i może mieścić się w dyspozycji art. 22 RODO.

Jeśli w proces decyzyjny jest zaangażowany człowiek, ale jego rola jest marginalna i pozostaje bez znaczenia dla treści wydanej decyzji, to również mamy do czynienia ze zautomatyzowanym podejmowaniem decyzji (np. gdy decyzja podejmowana jest przez algorytm, a udział człowieka sprowadza się wyłącznie do zakomunikowania treści decyzji osobie, której ona dotyczy).

Podobnie będzie w przypadku, gdy człowiek jest zaangażowany wyłącznie na etapie ustalania przebiegu procesu decyzyjnego (np. przy ustalaniu kryteriów lub czynników branych pod uwagę przy podejmowaniu decyzji) – jeśli sam proces decyzji przebiega bez jego udziału lub nawet z udziałem, lecz bez realnego wpływu na treść decyzji, również dochodzi do zautomatyzowanego podejmowania decyzji[269].

[269] Odnosi się to przykładowo do przypadków, w których człowiek tworzy algorytm, za pomocą którego następnie wydawana jest decyzja. Jeśli aktywność człowieka kończy się na etapie stworzenia algorytmu, nie można mówić o realnym wpływie na treść podejmowanych przez algorytm decyzji.

Jeśli natomiast w procesie podejmowania decyzji człowiek może kontrolować wynik działania zautomatyzowanego przetwarzania danych, np. przez weryfikację poprawności działania algorytmu czy ocenę innych czynników dotyczących osoby fizycznej, i ma faktyczny, a nie tylko teoretyczny wpływ na końcową decyzję, to nie dochodzi do wydania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, a tym samym nie ma zastosowania art. 22 RODO[270].

Druga przesłanka wymagająca uwzględnienia przy ocenie, czy przetwarzanie spełnia warunki art. 22 ust. 1 RODO, to skutki decyzji podjętej w sposób zautomatyzowany dla osoby fizycznej, przy czym nie chodzi tu o jakiekolwiek skutki, lecz skutki prawne lub takie, które w podobny sposób istotnie na nią wpływają. Spełnienie drugiej przesłanki zajdzie więc, gdy zautomatyzowane podejmowanie decyzji może wywołać poważne skutki dla podmiotu danych, o znacznym wpływie na jego sytuację[271]. W literaturze przedmiotu podaje się, że na gruncie art. 22 RODO decyzja wywołująca skutki prawne to taka, która powoduje powstanie stosunku zobowiązaniowego, zmianę jego treści lub jego ustanie[272]. Decyzja taka może mieć wpływ na prawa danej osoby przewidziane w przepisach, jak wolność do zrzeszania się, głosowania w wyborach, skorzystania z drogi sądowej, lub też wpływ na jej status prawny, na prawa przysługujące na mocy umowy itp.[273] Jako przykłady Grupa Robocza Art. 29 wymienia decyzje podjęte w sposób zautomatyzowany, które doprowadzają do rozwiązania umowy, udzielenia lub odmowy udzielenia określonego świadczenia społecznego przewidzianego w przepisach (świadczenia na dziecko, dodatku mieszkaniowego itp.), odmowy wjazdu na terytorium danego państwa lub odmowy nadania obywatelstwa.

Nawet jeśli decyzja nie wpływa na prawa lub obowiązki osoby fizycznej, to proces jej podejmowania i tak może wywrzeć na nią istotny wpływ, skutkujący potrzebą przyznania tej osobie ochrony na podstawie art. 22 ust. 1 RODO. Decyzja wywołująca inny istotny wpływ na osobę, której dane są przetwarzane, to decyzja, która stwarza ryzyko:

---

[270] Przykładowo, gdy proces oceny zdolności kredytowej obejmuje analizę danych osoby ubiegającej się o przyznanie finansowania, dokonywaną automatycznie przez algorytm, jednak jest to tylko jeden z etapów podejmowania decyzji. Jeśli następnie wynik działania algorytmu jest analizowany przez człowieka i poddawany weryfikacji, przy czym nie jest on wiążący dla człowieka, to należy uznać, że nie dochodzi do podejmowania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych.

[271] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 24.

[272] W. Chomiczewski, *Zautomatyzowane podejmowanie decyzji* [w:] D. Lubasz (red.), *Meritum…*, s. 215.

[273] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 24.

– wywarcia istotnego wpływu na sytuację danej osoby, jej zachowanie lub podejmowane przez nią wybory;
– wywarcia długotrwałego lub trwałego wpływu na osobę, której dane dotyczą; lub
– doprowadzenia do wykluczenia lub dyskryminacji podmiotu danych[274].

Jako przykłady decyzji wywołujących inne podobne skutki dla osoby fizycznej można podać decyzje skutkujące odmową zawarcia umowy (np. w następstwie automatycznego odrzucenia elektronicznego wniosku kredytowego, dyskwalifikacji kandydata z procesu rekrutacyjnego zorganizowanego w sposób w pełni zautomatyzowany[275]) lub różnicowaniem warunków przyszłej umowy (np. ze względu na różnicowanie cen w zależności od możliwości finansowych osoby fizycznej)[276].

11.2. Przesłanki dopuszczalności zautomatyzowanego podejmowania decyzji

W razie łącznego spełnienia omówionych wyżej przesłanek przetwarzanie danych osobowych podlega reżimowi określonemu w art. 22 RODO, co oznacza, że takie przetwarzanie jest zasadniczo zabronione. Od tej zasady są jednak wyjątki, w ramach których administrator ma prawo stosować zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie, wywołujące skutki prawne lub mające podobny istotny wpływ na osobę fizyczną. Wyjątki te odnoszą się do decyzji, która:
– jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem [art. 22 ust. 2 lit. a) RODO];
– jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą [art. 22 ust. 2 lit. b) RODO]; lub
– opiera się na wyraźnej zgodzie osoby, której dane dotyczą [art. 22 ust. 2 lit. c) RODO].

274 Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 24.
275 Na przykłady te wskazał też prawodawca unijny w motywie 71 RODO.
276 W. Chomiczewski, *Zautomatyzowane podejmowanie decyzji* [w:] D. Lubasz (red.), *Meritum…*, s. 215.

Pierwszy wyjątek dotyczy sytuacji, w których, w ocenie administratora, zautomatyzowane podejmowanie decyzji na potrzeby zawarcia lub wykonania umowy z podmiotem danych jest metodą najodpowiedniejszą do osiągniecia zamierzonego celu przetwarzania, i jednocześnie nie ma innej metody, której zastosowanie w mniejszym stopniu ingerowałoby w prywatność, a zarazem przyczyniłoby się w takim samym stopniu do osiągniecia celu przetwarzania[277]. „Niezbędność" oznacza w tym przypadku, że bez zautomatyzowanego podejmowania decyzji nie można zawrzeć lub wykonać umowy. Sam proces zawarcia umowy powinien być interpretowany szeroko, tzn. jako proces obejmujący również czynności podejmowane na wcześniejszym etapie, zmierzające do zawarcia umowy, np. przeprowadzenie rekrutacji na stanowisko, dokonanie ewaluacji zdolności kredytowej lub ryzyka ubezpieczeniowego. Podobnie wykonywanie umowy należy wykładać szeroko – jako wykonywanie praw i obowiązków przewidzianych w treści umowy, jak i praw i obowiązków wynikających z przepisów lub innych regulacji dotyczących określonego stosunku prawnego.

Drugi wyjątek odnosi się do przypadków, gdy zautomatyzowane podejmowanie decyzji jest wprost przewidziane i dozwolone w przepisach przyjętych na poziomie unijnym lub krajowym, przy czym dopuszczalność takiego przetwarzania powiązana jest z odpowiednimi gwarancjami dla podmiotu danych w postaci środków ochrony praw, wolności i prawnie uzasadnionych interesów podmiotu danych. Gwarancje te muszą wynikać z przepisów. Jak stanowi motyw 71 RODO, podejmowanie zautomatyzowanych decyzji powinno być dozwolone przykładowo do celów monitorowania i zapobiegania oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora.

Trzeci wyjątek pozwalający na zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub inne istotne skutki dla podmiotu danych, to wyraźna zgoda na tego rodzaju przetwarzanie danych osobowych. Spełnienie tej przesłanki wymaga zastosowania podwyższonego standardu względem oświadczenia woli składanego przez podmiot danych, przepis wskazuje bowiem na konieczność pozyskania „wyraźnej" zgody, takiej jak przy przetwarzaniu danych szczególnej kategorii, a nie „zwykłej" zgody – jak przy przetwarzaniu danych zwykłych. Osoba, której dane dotyczą, musi więc złożyć w sposób wyraźny oświadczenie o wyrażeniu zgody, czyli przykładowo pisemnie, potwierdzając je swoim podpisem. W kontekście składania oświadczeń drogą internetową podmiot danych może złożyć takie oświadczenie przez wypełnienie formularza elektronicznego, wysłanie

[277] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 26.

wiadomości e-mail, przesłanie zeskanowanego dokumentu opatrzonego jego podpisem lub złożenie na dokumencie podpisu elektronicznego[278].

Spełnienie jednej z powyższych przesłanek oznacza dopuszczalność zautomatyzowanego podejmowania decyzji, która wywołuje wobec osoby fizycznej skutki prawne lub w podobny sposób istotnie na nią wpływa. Dopuszczalność ta jest jednak dalej warunkowana kolejnymi ograniczeniami. Przede wszystkim w ramach zautomatyzowanego podejmowania decyzji nie można przetwarzać szczególnych kategorii danych osobowych, a zatem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby[279]. Dane szczególnych kategorii mogą stanowić podstawę decyzji podjętej w sposób zautomatyzowany jedynie wówczas, gdy zastosowanie znajduje art. 9 ust. 2 lit. a) lub g) RODO, a zatem gdy podmiot danych udzielił wyraźnej zgody lub gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, oraz pod warunkiem, że istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą[280]. Ponadto, zautomatyzowane podejmowanie decyzji nie może być stosowane wobec dzieci[281].

[278] Grupa Robocza Art. 29, *Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679*, ostatnio zmienione i przyjęte dn. 10.04.2018 r., WP259 rev.01, s. 21.

[279] Artykuł 9 ust. 1 RODO.

[280] Artykuł 22 ust. 4 RODO. *Nota bene*, art. 9 ust. 2 lit. a) i g) RODO dodatkowo precyzują, kiedy przetwarzanie szczególnych kategorii danych osobowych jest dozwolone. Zgodnie z art. 9 ust. 2 lit. a) RODO jest ono dopuszczalne, gdy wyraźna zgoda podmiotu danych dotyczy jednego lub kilku konkretnych celów przetwarzania, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania jej danych wrażliwych. Natomiast zgodnie z art. 9 ust. 2 lit. g) RODO przetwarzanie jest dopuszczalne, jeśli jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

[281] Motyw 71 RODO.

11.3. Obowiązki administratora związane ze zautomatyzowanym podejmowaniem decyzji

Administrator, który w ramach prowadzonej działalności i w ramach czynności przetwarzania danych osobowych stosuje profilowanie lub innego rodzaju techniki lub narzędzia służące do zautomatyzowanego przetwarzania danych, które jednocześnie wykorzystywane są w różnych procesach decyzyjnych wobec podmiotów danych, powinien zweryfikować, czy jego działania nie mieszczą się w zakresie stosowania art. 22 RODO. Jeśli tak, to oprócz sprawdzenia, czy spełnione są przesłanki dopuszczalności takiego przetwarzania, obowiązany jest wdrożyć odpowiednie zabezpieczenia gwarantujące poszanowanie praw i wolności osób, których dane są przetwarzane. Minimalny standard ochrony został ustanowiony przez prawodawcę w art. 22 ust. 3 RODO poprzez wskazanie, że „administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji". Obowiązek ten odnosi się tylko do zautomatyzowanego podejmowania decyzji w oparciu o przesłanki, o których mowa w art. 22 ust. 2 lit. a) i c) RODO, tj. w oparciu o przesłankę niezbędności podjęcia decyzji do zawarcia lub wykonania umowy lub w oparciu o wyraźną zgodę podmiotu danych. W przypadku, gdy zautomatyzowane podejmowanie decyzji jest dozwolone w prawie UE lub krajowym, właściwe zabezpieczenia muszą wynikać z przepisów.

Poza wymienionymi w art. 22 ust. 3 RODO zabezpieczeniami, takimi jak prawo do interwencji ludzkiej, wyrażenia własnego stanowiska i do zakwestionowania tej decyzji podjętej w sposób w pełni automatyczny, administrator zabezpiecza prawa i wolności osób, których dane przetwarza, poprzez rzetelne i przejrzyste informowanie o tym, że podlegają one tego rodzaju decyzjom oraz że przysługuje im prawo do uzyskania wyjaśnienia co do decyzji wynikłej z dokonanej w sposób zautomatyzowany oceny. Zabezpieczenia te są realizowane w formie obowiązków informacyjnych na podstawie art. 13 ust. 2 lit. f) RODO i art. 14 ust. 2 lit. g) RODO. Na mocy wspomnianych przepisów administrator jest bowiem zobligowany nie tylko do poinformowania o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, ale również do podania istotnych informacji o zasadach ich podejmowania oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla podmiotu danych.

Dodatkowo, motyw 71 RODO precyzuje, że administrator powinien:

– stosować odpowiednie matematyczne lub statystyczne procedury profilowania;
– wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę błędów powodujących nieprawidłowości w danych osobowych i zapewniających maksymalne zmniejszenia ryzyka takich błędów;
– zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną.

Z kolei Grupa Robocza Art. 29 zaleca, aby administratorzy przeprowadzali częste oceny zbiorów danych, które przetwarzają, pod kątem występowania elementów stronniczości, a także korzystali z systemów, w ramach których przeprowadza się audyty algorytmów, oraz regularne przeglądy prawidłowości i adekwatności zautomatyzowanego podejmowania decyzji, w tym profilowania. Powinni też wprowadzić odpowiednie procedury i środki zapobiegające błędom, nieprawidłowościom lub dyskryminacji na podstawie danych należących do szczególnych kategorii, przy czym środki te powinny być stosowane w sposób ciągły i przez cały cykl przetwarzania danych, a nie tylko na etapie projektowania systemu IT[282].

Przed rozpoczęciem procesu zautomatyzowanego podejmowania decyzji, o którym mowa w art. 22 RODO, administrator powinien przeprowadzić ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jak stanowi art. 35 ust. 3 lit. a) RODO, ocena ta jest wymagana zwłaszcza w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną. Co prawda przepis ten odnosi się do oceny czynników osobowych opartej na zautomatyzowanym przetwarzaniu, nie zaś do samych decyzji podejmowanych w oparciu wyłącznie o zautomatyzowane przetwarzanie. Jednak jak wskazuje Grupa Robocza Art. 29 – przepis ten ma szerokie zastosowanie, w związku z czym należy przyjąć, że ocena skutków dla ochrony danych powinna być dokonana także w tym przypadku[283].

[282] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 32.

[283] Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego…*, s. 34.

Administrator powinien też ustanowić w swojej organizacji odpowiednią procedurę realizacji przez podmiot danych prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych. Jeśli nawet zachodzi jedna z przesłanek z art. 22 ust. 2 RODO, administrator musi być przygotowany na to, że osoba fizyczna podlegająca tego rodzaju decyzji może chcieć skorzystać z przysługujących jej uprawnień, jak choćby prawa do interwencji ludzkiej lub prawa do zakwestionowania podjętej decyzji. Należy też pamiętać, że podmiot danych może w każdym czasie wycofać udzieloną na podstawie art. 22 ust. 2 lit. c) RODO zgodę na przetwarzanie jego danych osobowych.

Podobnie jak w przypadku realizacji innych praw przewidzianych w RODO, zastosowanie znajdą przepisy zobowiązujące administratora do prowadzenia komunikacji z podmiotem danych z uwzględnieniem zasady przejrzystości i wymogów z art. 12 RODO, tzn. w sposób zwięzły, przejrzysty, zrozumiały i w łatwo dostępnej formie, jasnym i prostym językiem. Administrator powinien ułatwiać podmiotowi danych korzystanie z przysługujących mu praw, a zatem może w tym celu wprowadzić dedykowane formularze elektroniczne lub specjalne opcje dostępne z poziomu serwisu internetowego lub panelu zarządzania kontem umożliwiające np. zakwestionowanie podjętej w sposób zautomatyzowany decyzji[284]. W razie skorzystania przez podmiot danych z prawa do niepodlegania zautomatyzowanemu podejmowaniu decyzji, administrator powinien poinformować wnioskodawcę o podjętych w tym zakresie działaniach bez zbędnej zwłoki, najpóźniej w ciągu miesiąca. Termin ten może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań[285]. Realizacja żądania jest zasadniczo bezpłatna, chyba że żądanie jest ewidentnie nieuzasadnione lub nadmierne[286].

Zgłoszenie żądania niepodlegania zautomatyzowanemu podejmowaniu decyzji administrator powinien odnotować w prowadzonym rejestrze realizacji praw podmiotów danych, wpisując w nim m.in. datę zgłoszenia i datę rozpoznania żądania, dokładną treść żądania (np. to czy podmiot danych domaga się interwencji ludzkiej, uzyskania dodatkowych informacji na temat sposobu podejmowania decyzji itp.) oraz to, jakie działania zostały przez administratora podjęte. Ujęcie wszystkich istotnych informacji związanych z realizacją prawa jest ważne z perspektywy oceny spełnienia zasady rozliczalności, o której mowa w art. 5 ust. 2 RODO.

[284] Artykuł 12 ust. 2 RODO.

[285] Artykuł 12 ust. 3 RODO.

[286] Artykuł 12 ust. 5 RODO.

Załącznik – lista wybranych decyzji krajowych organów nadzorczych dotyczących naruszeń na tle realizacji praw podmiotów danych[287]

1. decyzja szwedzkiego organu nadzorczego z dn. 28.03.2022 r. w sprawie Klarna Bank AB stwierdzająca naruszenie m.in. **art. 12 ust. 1, art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) RODO**. Zob. więcej: https://www.imy.se/en/news/administrative-fine-against-klarna-after-investigation/ oraz https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf.
2. decyzja rumuńskiego organu nadzorczego z dn. 10.03.2022 r. w sprawie Operatorul Briza Land S.R.L. stwierdzająca naruszenie **art. 15 RODO**. Zob. więcej: https://www.dataprotection.ro/?page=Comunicat_Presa_10_03_2022_3&lang=ro.
3. decyzja włoskiego organu nadzorczego z dn. 9.03.2022 r. w sprawie Clearview AI stwierdzająca naruszenie m.in. **art. 12, 13, 14 i 15 RODO**. Zob. więcej: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751323#english.
4. decyzja rumuńskiego organu nadzorczego z dn. 22.02.2022 r. w sprawie IAMSAT Muntenia SA stwierdzająca naruszenie **art. 12, 13 i 21 RODO**. Zob. więcej: https://www.dataprotection.ro/?page=Comunicat_Presa_22_02_2022_1&lang=ro.
5. decyzja greckiego organu nadzorczego z dn. 15.02.2022 r. w sprawie ΛΙΜΕΝΟΣ ΗΡΑΚΛΕΙΟΥ Α.Ε. stwierdzająca naruszenie **art. 12 ust. 1 i 2 oraz art. 15 ust. 1 RODO**. Zob. więcej: https://www.dpa.gr/sites/default/files/2022-02/61_2021anonym.pdf.
6. decyzja włoskiego organu nadzorczego z dn. 27.01.2022 r. w sprawie T.S.M. s.r.l. stwierdzająca naruszenie m.in. **art. 13, 15 i 21 RODO**. Zob. więcej: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9746068.
7. decyzja włoskiego organu nadzorczego z dn. 13.01.2022 r. w sprawie Medicina & Lavoro s.r.l. stwierdzająca naruszenie **art. 12 ust. 3 i art. 15 RODO**. Zob. więcej: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9744655.

[287] Dostęp do wszystkich wskazanych przy poszczególnych decyzjach stron internetowych datowany na 7.04.2022 r.

8. decyzja francuskiego organu nadzorczego z dn. 28.12.2021 r. w sprawie FREE MOBILE stwierdzająca naruszenie m.in. **art. 12, 15 i 21 RODO**. Zob. więcej: https://www.cnil.fr/fr/node/121974.
9. decyzja irlandzkiego organu nadzorczego z dn. 9.12.2021 r. w sprawie Limerick City and County Council stwierdzająca naruszenie **art. 12, 13 i 15 RODO**. Zob. więcej: https://www.dataprotection.ie/sites/default/files/uploads/2022-01/REDACTED_091221_Final%20DecisionLimerick_03-SIU-2018%20PDF%20FINAL.pdf.
10. decyzja hiszpańskiego organu nadzorczego z dn. 19.10.2021 r. w sprawie Vodafone España, S.A.U. stwierdzająca naruszenie **art. 21 RODO**. Zob. więcej: https://www.aepd.es/es/documento/ps-00142-2021.pdf.
11. decyzja francuskiego organu nadzorczego z dn. 15.09.2021 r. w sprawie Société nouvelle de l'annuaire français stwierdzająca naruszenie m.in. **art. 16 i 17 RODO**. Zob. więcej: https://www.cnil.fr/fr/sanction-de-3-000-euros-lencontre-de-la-societe-nouvelle-de-lannuaire-francais-snaf.
12. decyzja greckiego organu nadzorczego z dn. 3.09.2021 r. w sprawie Rhodes Municipal Transport Company stwierdzająca naruszenie **art. 5 ust. 1 lit. c), art. 12 ust. 3 i art. 15 RODO**. Zob. więcej: https://www.dpa.gr/sites/default/files/2021-09/39_2021anonym.pdf.
13. decyzja greckiego organu nadzorczego z dn. 26.08.2021 r. w sprawie National Bank of Greece stwierdzająca naruszenie **art. 12 ust. 1, 2 i 3 oraz art. 15 ust. 1 RODO**. Zob. więcej: https://www.dpa.gr/sites/default/files/2021-09/36_2021anonym.pdf.
14. decyzja irlandzkiego organu nadzorczego z dn. 20.08.2021 r. w sprawie WhatsApp Ireland Ltd stwierdzająca naruszenie **art. 12, 13 i 14 RODO** poprzez niewłaściwe realizowanie zasady przejrzystości w kontekście informowania podmiotów danych o przetwarzaniu ich danych osobowych. Zob. więcej: https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf.
15. decyzja węgierskiego organu nadzorczego z dn. 18.06.2021 r. w sprawie Magyar Telekom Nyrt. stwierdzająca naruszenie **art. 12 ust. 2, 3 i 4 oraz art. 17 ust. 1 RODO**. Zob. więcej: https://www.dataguidance.com/news/hungary-naih-fines-magyar-telekom-nyrt-huf-10m-failing.
16. decyzja greckiego organu nadzorczego z dn. 12.05.2021 r. w sprawie KARIERA A.E. stwierdzająca naruszenie m.in. **art. 17 i 21 RODO**. Zob. więcej: https://www.dpa.gr/sites/default/files/2021-05/20_2021anonym.pdf.
17. decyzja fińskiego organu nadzorczego z dn. 21.04.2021 r. w sprawie ParkkiPate Oy stwierdzająca naruszenie m.in. **art. 12 ust. 3,**

4 i 6, art. 14 ust. 2 lit. a), art. 14 ust. 3, art. 15 i 17 ust. 1 lit. a) RODO. Zob. więcej: https://tietosuoja.fi/documents/6927448/58640544/Seuraamuskollegion+päätös_henkilötietojen+käsittely+pysäköinninvalvontamaksujen+yhteydessä.pdf/9b105604-51e0-7beb-e21b-df1b504843e6/Seuraamuskollegion+päätös_henkilötietojen+käsittely+pysäköinninvalvontamaksujen+yhteydessä.pdf?t=1619763172841.

18. decyzja włoskiego organu nadzorczego z dn. 15.04.2021 r. w sprawie Istituto Nazionale Previdenza Sociale (INPS) stwierdzająca naruszenie **art. 5 ust. 1 lit. a), art. 12 i 15 RODO**. Zob. więcej: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9592133.
19. decyzja hiszpańskiego organu nadzorczego z dn. 8.04.2021 r. w sprawie Kutxabank S.A. stwierdzająca naruszenie **art. 17 RODO**. Zob. więcej: https://www.aepd.es/es/documento/ps-00473-2020.pdf.
20. decyzja hiszpańskiego organu nadzorczego z dn. 6.04.2021 r. w sprawie Promotech Digital S.L. stwierdzająca naruszenie **art. 21 RODO**. Zob. więcej: https://www.aepd.es/es/documento/ps-00087-2021.pdf.
21. decyzja włoskiego organu nadzorczego z dn. 25.03.2021 r. w sprawie TECNOMEDICAL S.r.l. stwierdzająca naruszenie **art. 12 ust. 3 i art. 15 RODO**. Zob. więcej: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9590711.
22. decyzja włoskiego organu nadzorczego z dn. 14.01.2021 r. w sprawie Poliambulatorio Talenti S.r.l. stwierdzająca naruszenie **art. 12 ust. 3 i art. 15 RODO**. Zob. więcej: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542096.
23. decyzja rumuńskiego organu nadzorczego z dn. 23.11.2020 r. w sprawie Vodafone România SA stwierdzająca naruszenie **art. 12, 15 i 17 RODO**. Zob. więcej: https://www.dataprotection.ro/?page=Comunicat_de_presa_23_/_11_/_2020&lang=ro
24. decyzja hiszpańskiego organu nadzorczego z dn. 31.07.2020 r. w sprawie Tour & People Max S.L. stwierdzająca naruszenie **art. 21 RODO**. Zob. więcej: https://www.aepd.es/es/documento/ps-00031-2020.pdf.
25. decyzja węgierskiego organu nadzorczego z dn. 16.07.2020 r. w sprawie Google Ireland Ltd. stwierdzająca naruszenie **art. 12 i 15 RODO**. Zob. więcej: https://www.naih.hu/files/NAIH-2020-5553-hatarozat.pdf.
26. decyzja belgijskiego organu nadzorczego z dn. 14.07.2020 r. w sprawie Google Belgium SA stwierdzająca naruszenie m.in. **art. 12 i 17 ust. 1 lit. a) RODO**. Zob. więcej: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf.

27. decyzja holenderskiego organu nadzorczego z dn. 6.07.2020 r. w sprawie Bureau Krediet Registration stwierdzająca naruszenie **art. 12 i 15 RODO**. Zob. więcej: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf.
28. decyzja włoskiego organu nadzorczego z dn. 2.07.2020 r. w sprawie GTL S.R.L. stwierdzająca naruszenie **art. 12 i 15 RODO**. Zob. więcej: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445710.
29. decyzja włoskiego organu nadzorczego z dn. 2.07.2020 r. w sprawie Mapei S.p.A. stwierdzająca naruszenie **art. 5, 12, 13 i 15 RODO**. Zob. więcej: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180.
30. decyzja hiszpańskiego organu nadzorczego z dn. 2.07.2020 r. w sprawie De Vere Spain S.L. stwierdzająca naruszenie **art. 21 RODO**. Zob. więcej: https://www.aepd.es/es/documento/ps-00475-2019.pdf.
31. decyzja fińskiego organu nadzorczego z dn. 22.05.2020 r. w sprawie Posti Group Oyj stwierdzająca naruszenie **art. 12, 13, 14 i 15 RODO**. Zob. więcej: https://tietosuoja.fi/documents/6927448/22406974/Henkilötietojen+käsittelyn+läpinäkyvyys+ja+rekisteröidylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-9c8a56998fc1/Henkilötietojen+käsittelyn+läpinäkyvyys+ja+rekisteröidylle+toimitettavat+tiedot.pdf.
32. decyzja duńskiego organu nadzorczego z dn. 15.05.2020 r. w sprawie JobTeam A/S DKK stwierdzająca naruszenie **art. 15 RODO**. Zob. więcej: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/jobteam-indstillet-til-boede/.
33. decyzja szwedzkiego organu nadzorczego z dn. 11.03.2020 r. w sprawie Google LLC stwierdzająca naruszenie m.in. **art. 17 RODO**. Zob. więcej: https://www.imy.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf.
34. decyzja francuskiego organu nadzorczego z dn. 21.11.2019 r. w sprawie Futura Internationale stwierdzająca naruszenie m.in. **art. 13, 14 i 21 RODO**. Zob. więcej: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039419459/.
35. decyzja niemieckiego organu nadzorczego z dn. 19.09.2019 r. w sprawie Delivery Hero stwierdzająca naruszenie **art. 15, 17 i 21 RODO**. Zob. więcej: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf.

O autorce

Adrianna Michałowicz – adwokat prowadzący indywidualną praktykę zawodową (Kancelaria Adwokacka Adwokat Adrianna Michałowicz, www.adwokat-michalowicz.pl), asystent naukowy na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego w Katedrze Europejskiego Prawa Gospodarczego. Kierownik projektu badawczego finansowanego przez Narodowe Centrum Nauki w ramach konkursu PRELUDIUM 20 pt. „Udostępnianie danych w interesie publicznym - filantropia danych z perspektywy prawnej" (nr umowy: UMO-2021/41/N/HS5/01490). Absolwentka Europejskiej Akademii Dyplomacji w Warszawie oraz Szkoły Prawa Francuskiego organizowanej przez Uniwersytet w Tours. Dwukrotna stypendystka Narodowej Agencji Wymiany Akademickiej (program PROM).

Autorka licznych publikacji naukowych i prelegentka na konferencjach, w tym o zasięgu międzynarodowym. Współautorka międzynarodowego bloga poświęconego tematyce prawa konsumenckiego „Recent Developments in European Consumer Law" (http://recent-ecl.blogspot.com).

Specjalizuje się w polskim i europejskim prawie gospodarczym, prawie ochrony danych osobowych, prawie własności intelektualnej i prawie nowych technologii. Pełni również funkcję mediatora przy Adwokackim Centrum Mediacji w Łodzi oraz stałego mediatora sądowego przy Sądzie Okręgowym w Łodzi.

Polska Agencja Rozwoju Przedsiębiorczości (PARP) jest agencją rządową, która została powołana w 2000 r. do wspierania rozwoju mikro, małych i średnich przedsiębiorstw. Przez ponad 20 lat działalności Agencja wypracowała wiele form wsparcia, które obejmują finansowanie przedsiębiorstw, usługi rozwojowe, działalność edukacyjną i informacyjną oraz działania na rzecz budowy kultury przedsiębiorczości i innowacyjności w Polsce.

Obszary działalności PARP rozwijają się wraz z rozwojem gospodarczym i wyłanianiem się nowych trendów w przedsiębiorczości i innowacyjności. Tym samym PARP na przestrzeni lat stała się prekursorką w tworzeniu wielu nowych obszarów wsparcia i opracowywaniu zróżnicowanych sposobów udzielania pomocy (finansowanie, edukacja, promocja). Stymulowaniu przedsiębiorczości, innowacyjności i konkurencyjności polskich przedsiębiorców służą nowe instrumenty perspektywy finansowej Unii Europejskiej 2021–2027.

Aktywność PARP koncentruje się na pięciu obszarach:

- rozwoju przedsiębiorstw i przedsiębiorczości, przez wspieranie rozwoju nowych pomysłów i modeli biznesowych;
- innowacyjności przedsiębiorstw, przez inicjowanie i kompleksowe wspieranie aktywności przedsiębiorstw w tym obszarze;
- ekspansji międzynarodowej przedsiębiorstw, przez wsparcie przedsiębiorców sektora MSP we wchodzeniu na zagraniczne rynki;
- współpracy wśród przedsiębiorstw i otoczenia biznesu, a więc wsparciu budowania powiązań między nimi;
- tworzenia przyjaznej i innowacyjnej administracji, przez pomoc w kreowaniu polityki innowacyjnej państwa oraz rozwijanie i promowanie takich rozwiązań w sektorze publicznym.

Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83
00-834 Warszawa
telefon: 22 432 80 80
e-mail: biuro@parp.gov.pl

Informatorium PARP
telefon: 0 801 332 202

PARP Grupa PFR / Centrum Rozwoju MŚP

ISBN: 978-83-7633-481-3