Wytyczne 01/2022 dotyczące praw osób, których dane dotyczą – Prawo dostępu

Wersja 2.0

Przyjęte 28 marca 2023 r.

Przyjęte

Historia wersji

Wersja 1.0	18 stycznia 2022 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	28 marca 2023 r.	Przyjęcie wytycznych po konsultacjach publicznych

STRESZCZENIE

Prawo dostępu osób, których dane dotyczą, jest zapisane w art. 8 Karty praw podstawowych Unii Europejskiej. Od samego początku stanowi ono część europejskich ram prawnych w zakresie ochrony danych, a obecnie jest w dalszym stopniu rozwijane za pomocą bardziej szczegółowych i precyzyjnych przepisów zawartych w art. 15 RODO.

Cel i ogólna struktura prawa dostępu

Ogólnym celem prawa dostępu jest zapewnienie osobom fizycznym wystarczających, przejrzystych i łatwo dostępnych informacji na temat przetwarzania ich danych osobowych, tak aby mogły one mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem oraz prawidłowość przetwarzanych danych. Ułatwi to wykonywanie przez osobę fizyczną innych praw, takich jak prawo do usunięcia lub sprostowania danych, ale nie jest tego warunkiem.

Prawo dostępu zgodnie z przepisami w dziedzinie ochrony danych należy odróżnić od podobnych praw o innych celach, na przykład prawa dostępu do dokumentów urzędowych, które ma na celu zagwarantowanie przejrzystości procesu decyzyjnego organów publicznych i dobrych praktyk administracyjnych.

Osoba, której dane dotyczą, nie musi jednak podawać uzasadnienia żądania dostępu, a administrator nie ma obowiązku analizowania, czy żądanie to rzeczywiście pomoże osobie, której dane dotyczą, w zweryfikowaniu zgodności z prawem danego przetwarzania lub w wykonaniu innych praw. Administrator będzie musiał rozpatrzyć żądanie, chyba że jest jasne, że żądanie wystosowano na podstawie przepisów innych niż przepisy w dziedzinie ochrony danych.

Prawo dostępu obejmuje trzy różne elementy:

- potwierdzenie, czy dane dotyczące danej osoby są przetwarzane,
- dostęp do tych danych osobowych oraz
- dostęp do informacji na temat przetwarzania, takich jak cel, kategorie danych i odbiorców, czas trwania przetwarzania, prawa osób, których dane dotyczą, oraz odpowiednie zabezpieczenia w przypadku przekazywania danych do państw trzecich.

Uwagi ogólne dotyczące oceny żądania osoby, której dane dotyczą

Analizując treść żądania, administrator musi ocenić, czy żądanie to dotyczy danych osobowych osoby fizycznej, która je wystosowała, czy wchodzi ono w zakres art. 15 i czy istnieją inne, bardziej szczegółowe przepisy regulujące dostęp w danym sektorze. Musi on również ocenić, czy żądanie odnosi się do całości czy jedynie do części przetwarzanych danych o osobie, której dane dotyczą.

Nie przewidziano żadnych szczegółowych wymogów dotyczących formatu żądania. Administrator powinien zapewnić odpowiednie i przyjazne dla użytkownika kanały komunikacyjne, z których osoba, której dane dotyczą, może z łatwością korzystać. Osoba, której dane dotyczą, nie jest jednak zobowiązana do korzystania z tych konkretnych kanałów i może przesłać żądanie do oficjalnego punktu kontaktowego administratora. Administrator nie jest zobowiązany do podejmowania działań w odpowiedzi na żądania wysyłane na adresy, które są całkowicie przypadkowe lub wyglądają na nieprawidłowe.

Jeżeli administrator nie jest w stanie zidentyfikować danych odnoszących się do osoby, której dane dotyczą, informuje o tym tę osobę i może odmówić udzielenia dostępu, chyba że osoba ta dostarczy

dodatkowych informacji umożliwiających identyfikację. Co więcej, jeżeli administrator ma wątpliwości co do tego, czy osoba, której dane dotyczą, jest tym, za kogo się podaje, może zażądać dodatkowych informacji w celu potwierdzenia jej tożsamości. Żądanie dodatkowych informacji musi być proporcjonalne do rodzaju przetwarzanych danych, ewentualnych szkód itp., aby uniknąć nadmiernego gromadzenia danych.

Zakres prawa dostępu

Zakres prawa dostępu jest uwarunkowany zakresem pojęcia danych osobowych w rozumieniu art. 4 pkt 1 RODO. Poza podstawowymi danymi osobowymi, takimi jak imię i nazwisko, adres, numer telefonu itp., definicja ta może obejmować szeroki zakres danych, takich jak informacje medyczne, historia zakupów, wskaźniki zdolności kredytowej, dzienniki aktywności, operacje wyszukiwania itp. Dane osobowe, które zostały poddane pseudonimizacji, są nadal danymi osobowymi w przeciwieństwie do danych zanonimizowanych. Prawo dostępu dotyczy danych osobowych osoby występującej z żądaniem. Nie należy go interpretować zbyt zawężająco – może ono obejmować dane, które mogą dotyczyć również innych osób, na przykład historię komunikacji obejmującą wiadomości przychodzące i wychodzące.

Oprócz zapewnienia dostępu do danych osobowych administrator musi przedstawić dodatkowe informacje na temat przetwarzania i praw osób, których dane dotyczą. Takie informacje mogą opierać się na tym, co zostało już zebrane w rejestrze czynności przetwarzania danych osobowych prowadzonym przez administratora (art. 30 RODO) i w oświadczeniu o ochronie prywatności (art. 13 i 14 RODO). Te ogólne informacje mogą jednak wymagać aktualizacji do momentu wystosowania żądania lub dostosowania ich w taki sposób, aby odzwierciedlały operacje przetwarzania przeprowadzane w odniesieniu do konkretnej osoby występującej z żądaniem.

Jak zapewnić dostęp?

Sposoby zapewnienia dostępu mogą się różnić w zależności od ilości danych i złożoności prowadzonego przetwarzania. O ile wyraźnie nie stwierdzono inaczej, żądanie należy rozumieć jako odnoszące się do *wszystkich* danych osobowych odnoszących się do osoby, której dane dotyczą, przy czym administrator może zwrócić się do tej osoby o sprecyzowanie żądania, jeśli przetwarza dużą ilość danych.

Administrator będzie musiał wyszukiwać dane osobowe we wszystkich informatycznych i innych niż informatyczne zbiorach danych na podstawie kryteriów wyszukiwania odzwierciedlających sposób, w jaki informacje są ustrukturyzowane, takich jak imię i nazwisko oraz numer klienta. Przekazywanie danych i innych informacji dotyczących przetwarzania musi odbywać się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Bardziej precyzyjne wymogi w tym zakresie zależą od okoliczności przetwarzania danych, a także od zdolności osoby, której dane dotyczą, do zrozumienia i przyswojenia komunikatu (np. biorąc pod uwagę fakt, że osoba, której dane dotyczą, jest dzieckiem lub osobą o specjalnych potrzebach). Jeżeli dane składają się z kodów lub innych „surowych danych", może zaistnieć konieczność ich wyjaśnienia, tak by miały one sens dla osoby, której dane dotyczą.

Głównym sposobem zapewnienia dostępu jest dostarczenie osobie, której dane dotyczą, kopii jej danych, ale na żądanie osoby, której dane dotyczą, można przewidzieć inne sposoby (takie jak informacje ustne i dostęp na miejscu). Dane można przesłać pocztą elektroniczną, pod warunkiem zastosowania wszystkich niezbędnych zabezpieczeń, biorąc pod uwagę na przykład charakter danych, lub przekazać je w inny sposób, na przykład za pomocą narzędzia samoobsługowego.

Czasami, gdy istnieje duża ilość danych, a osobie, której dane dotyczą, trudno byłoby zrozumieć informacje, gdyby podano je w formie zbiorczej – zwłaszcza w kontekście internetowym – najodpowiedniejszym środkiem mogłoby być podejście warstwowe. Dostarczanie informacji podzielonych na warstwy może ułatwić osobie, której dane dotyczą, zrozumienie danych. Administrator musi być w stanie wykazać, że podejście warstwowe ma wartość dodaną z punktu widzenia osoby, której dane dotyczą, przy czym wszystkie warstwy informacji powinny zostać dostarczone w tym samym czasie, jeżeli osoba, której dane dotyczą, się na to zdecyduje.

Kopię danych i dodatkowe informacje należy dostarczyć w trwałej formie, takiej jak tekst pisany, który może być w powszechnie stosowanej formie elektronicznej, tak aby osoba, której dane dotyczą, mogła go łatwo pobrać. Dane można podać w formie transkrypcji lub w formie skompilowanej, o ile wszystkie informacje są zawarte i nie powoduje to zmiany ani modyfikacji treści informacji.

Żądanie musi zostać spełnione tak szybko, jak to możliwe, a w każdym razie w ciągu jednego miesiąca od jego otrzymania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Osobę, której dane dotyczą, należy następnie poinformować o przyczynie opóźnienia. Administrator musi jak najszybciej wdrożyć środki niezbędne do rozpatrzenia żądań i dostosować te środki do okoliczności przetwarzania. W przypadku gdy dane są przechowywane jedynie przez bardzo krótki okres, muszą istnieć środki gwarantujące, że żądanie dostępu może zostać zrealizowane bez usuwania danych podczas rozpatrywania tego żądania. W przypadku przetwarzania dużej ilości danych administrator będzie musiał wprowadzić procedury i mechanizmy dostosowane do złożoności przetwarzania.

Ocena żądania powinna odzwierciedlać sytuację w momencie jego otrzymania przez administratora. Należy podać nawet dane, które mogą być nieprawidłowe lub przetwarzane niezgodnie z prawem. Dane, które zostały już usunięte, na przykład zgodnie z polityką zatrzymywania danych, a zatem nie są już dostępne dla administratora, nie mogą zostać przekazane.

Ograniczenia i restrykcje

W RODO dopuszcza się pewne ograniczenia prawa dostępu. Nie ma żadnych dalszych wyłączeń ani odstępstw. Prawo dostępu nie obejmuje żadnych ogólnych zastrzeżeń co do proporcjonalności w odniesieniu do starań, jakie administrator musi podjąć w celu spełnienia żądania osoby, której dane dotyczą.

Zgodnie z art. 15 ust. 4 prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych. EROD jest zdania, że prawa te należy brać pod uwagę nie tylko przy udzielaniu dostępu poprzez dostarczenie kopii, ale również w przypadku, gdy dostęp do danych jest zapewniany w inny sposób (np. dostęp na miejscu). Art. 15 ust. 4 nie ma jednak zastosowania do dodatkowych informacji na temat przetwarzania, o których mowa w art. 15 ust. 1 lit. a)–h). Administrator musi być w stanie wykazać, że w konkretnej sytuacji naruszone zostałyby prawa lub wolności innych osób. Zastosowanie art. 15 ust. 4 nie powinno skutkować całkowitym odrzuceniem żądania osoby, której dane dotyczą; skutkowałoby jedynie pominięciem lub uniemożliwieniem odczytu tych części, które mogą mieć negatywny wpływ na prawa i wolności innych osób.

Zgodnie z art. 12 ust. 5 RODO administratorzy mogą odrzucać żądania, które są ewidentnie nieuzasadnione lub nadmierne, lub pobierać rozsądną opłatę za takie żądania. Pojęcia te należy interpretować w sposób zawężający. Ponieważ żądania dostępu są obwarowane bardzo niewieloma warunkami wstępnymi, możliwość uznania żądania za ewidentnie nieuzasadnione jest raczej ograniczona. Nadmierne żądania zależą od specyfiki sektora, w którym działa administrator. Im częściej zachodzą zmiany w bazie danych administratora, tym częściej osoba, której dane dotyczą, może

występować z żądaniem dostępu, które nie zostanie uznane za nadmierne. Zamiast odmówić dostępu administrator może podjąć decyzję o pobraniu opłaty od osoby, której dane dotyczą. Miałoby to zastosowanie jedynie w przypadku nadmiernych żądań i miałoby na celu pokrycie kosztów administracyjnych, które mogą spowodować takie żądania. Administrator musi być w stanie wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.

Ograniczenia prawa dostępu mogą również być przewidziane w prawie krajowym państw członkowskich zgodnie z art. 23 RODO i z zawartymi w nim odstępstwami. Administratorzy, którzy zamierzają polegać na takich ograniczeniach, muszą dokładnie sprawdzić wymogi zawarte w przepisach krajowych i wziąć pod uwagę wszelkie szczególne warunki, które mogą mieć zastosowanie. Takie warunki mogą polegać na tym, że możliwość skorzystania z prawa dostępu jest jedynie tymczasowo opóźniona lub że ograniczenie ma zastosowanie wyłącznie do niektórych kategorii danych.

Spis treści

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

mając na uwadze, że prace przygotowawcze nad niniejszymi wytycznymi obejmowały gromadzenie informacji od zainteresowanych stron, zarówno w formie pisemnej, jak i podczas specjalnego wydarzenia z udziałem zainteresowanych stron poświęconego prawom osób, których dane dotyczą, w celu określenia wyzwań i problemów interpretacyjnych napotykanych przy stosowaniu odpowiednich przepisów RODO,

PRZYJMUJE NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE – UWAGI OGÓLNE

1. W dzisiejszym społeczeństwie dane osobowe są przetwarzane przez podmioty publiczne i prywatne podczas wielu działań, w wielu celach i na wiele różnych sposobów. Osoby fizyczne mogą często doświadczać problemów ze zrozumieniem sposobu przetwarzania ich danych osobowych, w tym technologii stosowanej w danym przypadku, niezależnie od tego, czy przetwarzaniem zajmuje się podmiot prywatny czy publiczny. Aby chronić dane osobowe osób fizycznych w takich sytuacjach, RODO stworzyło spójne i solidne ramy prawne, mające ogólne zastosowanie w odniesieniu do różnych rodzajów przetwarzania, w tym przepisy szczegółowe dotyczące praw osób, których dane dotyczą.

2. Prawo dostępu do danych osobowych jest jednym z praw osób, których dane dotyczą, przewidzianym w rozdziale III RODO, obok innych praw, takich jak prawo do sprostowania i usunięcia danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia, prawo do sprzeciwu lub prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach, w tym profilowaniu[2]. Prawo dostępu przysługujące osobie, której dane dotyczą, jest zapisane zarówno w Karcie praw podstawowych UE (karta)[3], jak i w art. 15 RODO, w którym precyzyjnie określono je jako prawo dostępu do danych osobowych i innych powiązanych informacji.

3. Zgodnie z RODO prawo dostępu obejmuje trzy elementy, tj. potwierdzenie, czy dane osobowe są przetwarzane, dostęp do nich oraz informacje na temat samego przetwarzania. Osoba, której dane dotyczą, może również otrzymać kopię przetwarzanych danych osobowych, przy czym możliwość ta

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Art. 15–22 RODO.
[3] Zgodnie z art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej każdy ma prawo do ochrony danych osobowych, które go dotyczą. Zgodnie z art. 8 ust. 2 zdanie drugie każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.

nie jest dodatkowym prawem osoby, której dane dotyczą, ale sposobem zapewnienia dostępu do danych. W związku z tym prawo dostępu można rozumieć zarówno jako możliwość zwrócenia się przez osobę, której dane dotyczą, do administratora z pytaniem, czy dotyczące jej dane osobowe są przetwarzane, jak i jako możliwość uzyskania dostępu do tych danych i ich weryfikacji. Administrator przekazuje osobie, której dane dotyczą, na jej żądanie informacje wchodzące w zakres art. 15 ust. 1 i 2 RODO.

4. Prawo dostępu jest wykonywane zarówno w ramach przepisów w dziedzinie ochrony danych, zgodnie z celami prawa o ochronie danych, jak i – mówiąc precyzyjniej – w ramach „podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych", zgodnie z art. 1 ust. 2 RODO. Prawo dostępu jest jednym z istotnych elementów całego systemu ochrony danych.

5. Praktycznym celem prawa dostępu jest umożliwienie osobom fizycznym kontroli nad własnymi danymi osobowymi[4]. Aby skutecznie osiągnąć ten cel w praktyce, RODO ma na celu ułatwienie tego zadania za pomocą szeregu gwarancji umożliwiających osobie, której dane dotyczą, łatwe korzystanie z tego prawa, bez zbędnych ograniczeń, w rozsądnych odstępach czasu i bez nadmiernej zwłoki lub nadmiernych kosztów. Wszystko to powinno prowadzić do skuteczniejszego egzekwowania prawa dostępu przez osoby, których dane dotyczą, w epoce cyfrowej, którego częścią w szerszym znaczeniu jest również prawo osoby, której dane dotyczą, do złożenia skargi do organu nadzorczego oraz prawo do skutecznej ochrony prawnej[5].

6. W odniesieniu do rozwoju prawa dostępu, jako części ram prawnych dotyczących ochrony danych, należy podkreślić, że od samego początku stanowi ono element europejskiego systemu ochrony danych. W porównaniu z dyrektywą 95/46/WE standard praw osób, których dane dotyczą, określony w RODO został zarówno dopracowany, jak i wzmocniony; dotyczy to również prawa dostępu. Ponieważ warunki korzystania z prawa dostępu są obecnie bardziej szczegółowo określone w RODO, prawo to ma również większą wartość z punktu widzenia zagwarantowania pewności prawa zarówno dla osoby, której dane dotyczą, jak i administratora. Ponadto szczegółowe brzmienie art. 15 oraz dokładny termin przekazania danych przewidziany w art. 12 ust. 3 RODO zobowiązują administratora do przygotowania się na zapytania osób, których dane dotyczą, dzięki opracowaniu procedur rozpatrywania żądań.

7. Prawa dostępu nie należy rozpatrywać w oderwaniu od innych przepisów RODO, ponieważ jest ono ściśle powiązane z tymi przepisami, w szczególności z zasadami ochrony danych, w tym z zasadami rzetelności przetwarzania i jego zgodności z prawem, obowiązkiem administratora w zakresie przejrzystości oraz z innymi prawami osób, których dane dotyczą, przewidzianymi w rozdziale III RODO.

8. W ramach praw osób, których dane dotyczą, ważne jest również zarówno podkreślenie znaczenia art. 12 RODO, w którym określono wymogi dotyczące odpowiednich środków przyjętych przez administratora przy przekazywaniu informacji, o których mowa w art. 13 i 14 RODO, jak i komunikacji, o której mowa w art. 15–22 i 34 RODO; w wymogach tych zasadniczo określono formę, sposób i termin udzielenia odpowiedzi osobie, której dane dotyczą, w szczególności gdy informacje są kierowane do dziecka.

9. EROD uważa, że konieczne jest przedstawienie bardziej precyzyjnych wytycznych dotyczących sposobu wdrażania prawa dostępu w różnych sytuacjach. Niniejsze wytyczne mają na celu analizę poszczególnych aspektów prawa dostępu. W szczególności celem poniższej sekcji jest przedstawienie

[4] Zob. motywy 7, 68, 75 i 85 RODO.
[5] Zob. rozdział VIII art. 77, 78 i 79 RODO.

ogólnego przeglądu i objaśnienia treści samego art. 15, natomiast kolejne sekcje zawierają głębszą analizę najczęstszych praktycznych kwestii i zagadnień dotyczących wdrażania prawa dostępu.

2 CEL PRAWA DOSTĘPU, STRUKTURA ART. 15 RODO I ZASADY OGÓLNE

2.1 Cel prawa dostępu

10. Prawo dostępu ma zatem na celu umożliwienie osobom fizycznym sprawowania kontroli nad dotyczącymi ich danymi osobowymi w tym sensie, że zapewnia im „[…] świadomość przetwarzania i [możliwość zweryfikowania zgodności] przetwarzania z prawem”[6]. Dokładniej rzecz ujmując, celem prawa dostępu jest umożliwienie osobom, których dane dotyczą, zrozumienia sposobu przetwarzania ich danych osobowych oraz konsekwencji takiego przetwarzania, a także sprawdzenie prawidłowości przetwarzanych danych bez konieczności uzasadniania swoich intencji. Innymi słowy, celem prawa dostępu jest zapewnienie osobom fizycznym wystarczających, przejrzystych i łatwo dostępnych informacji na temat przetwarzania danych, niezależnie od wykorzystywanych technologii, oraz umożliwienie im weryfikacji różnych aspektów konkretnej czynności przetwarzania zgodnie z RODO (np. zgodności z prawem, prawidłowości).

11. Wykładnia RODO przedstawiona w niniejszych wytycznych opiera się na dotychczasowym orzecznictwie TSUE. Biorąc pod uwagę znaczenie prawa dostępu, można oczekiwać, że powiązane orzecznictwo znacznie ewoluuje w przyszłości.

12. Zgodnie z orzeczeniami TSUE[7] prawo dostępu służy zagwarantowaniu ochrony prawa osób, których dane dotyczą, do prywatności i ochrony danych w odniesieniu do przetwarzania dotyczących ich danych[8] i może ułatwić wykonywanie ich praw wynikających na przykład z art. 16–19, 21–22 i 82 RODO. Wykonywanie prawa dostępu jest jednak prawem jednostki i nie jest uzależnione od wykonywania tych innych praw, a wykonywanie tych innych praw nie zależy od wykonywania prawa dostępu.

13. Biorąc pod uwagę szeroki cel prawa dostępu, cel tego prawa nie powinien być analizowany przez administratora jako jeden z warunków wstępnych wykonywania prawa dostępu w ramach oceny żądań dostępu. Administratorzy nie powinni zatem oceniać, „dlaczego” osoba, której dane dotyczą, żąda dostępu, lecz jedynie „czego” żąda (zob. sekcja 3 dotycząca analizy żądania) i czy dysponują danymi osobowymi dotyczącymi tej osoby (zob. sekcja 4). W związku z tym na przykład administrator nie powinien odmawiać dostępu na podstawie przesłanki lub podejrzenia, że żądane dane mogłyby zostać wykorzystane przez osobę, której dane dotyczą, do obrony przed sądem w przypadku zwolnienia lub wejścia w spór handlowy z administratorem[9]. Jeśli chodzi o ograniczenia i restrykcje dotyczące prawa dostępu, zob. sekcja 6.

Przykład 1: Pracodawca zwolnił osobę fizyczną. Tydzień później osoba ta postanawia zebrać dowody w celu wniesienia powództwa o niesprawiedliwe zwolnienie przeciwko temu byłemu pracodawcy. W związku z tym osoba ta – jako osoba, której dane dotyczą – zwraca się do byłego pracodawcy z żądaniem dostępu do wszystkich danych osobowych jej dotyczących, przetwarzanych przez byłego pracodawcę jako administratora.

[6] Motyw 63 RODO.
[7] TSUE, C-434/16, Nowak, i sprawy połączone C-141/12 i C-372/12, YS i in.
[8] TSUE, C-434/16, Nowak, pkt 56.
[9] Kwestie związane z tym zagadnieniem są przedmiotem sprawy zawisłej obecnie przed TSUE (C-307/22).

Administrator nie ocenia intencji osoby, której dane dotyczą, a osoba, której dane dotyczą, nie musi podawać administratorowi przyczyny żądania. W związku z tym, jeżeli żądanie spełnia wszystkie pozostałe wymogi (zob. sekcja 3), administrator musi spełnić to żądanie, chyba że okaże się ono ewidentnie nieuzasadnione lub nadmierne zgodnie z art. 12 ust. 5 RODO (zob. sekcja 6.3), co administrator jest zobowiązany wykazać.

Wariant: Osoba, której dane dotyczą, korzysta z prawa dostępu do dotyczących jej danych osobowych w toku postępowania sądowego. Prawo krajowe państwa członkowskiego, które reguluje stosunek pracy między administratorem a osobą, której dane dotyczą, zawiera jednak pewne przepisy ograniczające zakres informacji, które mają być przekazywane stronom lub wymieniane między stronami toczącego się lub przyszłego postępowania sądowego, które to przepisy mają zastosowanie do powództwa o niesprawiedliwe zwolnienie wytoczonego przez osobę, której dane dotyczą. W tym kontekście i pod warunkiem że te przepisy krajowe są zgodne z wymogami określonymi w art. 23 RODO[10], osoba, której dane dotyczą, nie jest uprawniona do otrzymywania od administratora większej ilości informacji, niż jest to przewidziane w przepisach prawa krajowego państwa członkowskiego regulujących wymianę informacji między stronami sporów prawnych.

14. Chociaż cel prawa dostępu jest szeroki, TSUE zilustrował również granice zakresu przepisów w dziedzinie ochrony danych i prawa dostępu. Na przykład TSUE stwierdził, że cel prawa dostępu gwarantowanego przez unijne przepisy w zakresie ochrony danych należy odróżnić od celu prawa dostępu do dokumentów urzędowych ustanowionego w przepisach unijnych i krajowych, które służy zapewnieniu „przejrzystości procesowi decyzyjnemu władz publicznych i promowaniu dobrych praktyk administracyjnych”[11], co nie jest celem określonym w prawie o ochronie danych. TSUE stwierdził, że prawo dostępu do danych osobowych ma zastosowanie niezależnie od tego, czy zastosowanie ma inny rodzaj prawa dostępu mający odrębny cel, na przykład w kontekście procedury sprawdzającej.

2.2 Struktura art. 15 RODO

15. Aby odpowiedzieć na żądanie udzielenia dostępu i zapewnić, aby żaden z jego aspektów nie został pominięty, należy najpierw zrozumieć strukturę art. 15 i elementy składowe prawa dostępu określone w tym artykule.

16. Art. 15 można podzielić na osiem różnych elementów wymienionych w poniższej tabeli:

1.	Potwierdzenie, czy administrator przetwarza dane osobowe dotyczące osoby występującej z żądaniem	Art. 15 ust. 1 pierwsza połowa zdania
2.	Dostęp do danych osobowych dotyczących osoby występującej z żądaniem	Art. 15 ust. 1 druga połowa zdania (część pierwsza)
3.	Dostęp do następujących informacji dotyczących przetwarzania: a) cele przetwarzania; b) kategorie danych osobowych; c) odbiorcy lub kategorie odbiorców danych; d) planowany czas trwania przetwarzania lub kryteria ustalania tego czasu;	Art. 15 ust. 1 druga część zdania (część druga)

[10] Wytyczne EROD 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO, wersja do konsultacji publicznych, 18 grudnia 2020 r.
[11] TSUE, sprawy połączone C-141/12 i C-372/12, YS i in., pkt 47.

	e) informacje o prawie do sprostowania, usunięcia, ograniczenia przetwarzania i sprzeciwu wobec przetwarzania; f) informacje o prawie wniesienia skargi do organu nadzorczego; g) wszelkie dostępne informacje na temat źródła danych, jeśli dane nie zostały zebrane od osoby, której dane dotyczą; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz inne informacje z tym związane.	
4.	Informacje o zabezpieczeniach zgodnie z art. 46, w przypadku gdy dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej	Art. 15 ust. 2
5.	Spoczywający na administratorze obowiązek dostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu.	Art. 15 ust. 3 zdanie pierwsze
6.	Pobieranie przez administratora opłaty w rozsądnej wysokości wynikającej z kosztów administracyjnych za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą	Art. 15 ust. 3 zdanie drugie
7.	Dostarczanie informacji w formie elektronicznej	Art. 15 ust. 3 zdanie trzecie
8.	Uwzględnianie praw i wolności innych	Art. 15 ust. 4

Podczas gdy wszystkie elementy art. 15 ust. 1 i 2 łącznie określają treść prawa dostępu, art. 15 ust. 3 dotyczy warunków dostępu, oprócz ogólnych wymogów określonych w art. 12 RODO. W art. 15 ust. 4 uzupełniono ograniczenia i restrykcje przewidziane w art. 12 ust. 5 RODO w odniesieniu do wszystkich praw osób, których dane dotyczą, ze szczególnym uwzględnieniem praw i wolności innych w kontekście dostępu.

2.2.1 Określenie treści prawa dostępu

17. Art. 15 ust. 1 i 2 obejmują następujące trzy aspekty: po pierwsze, potwierdzenie, czy dane osobowe osoby występującej z żądaniem są przetwarzane; jeżeli tak, po drugie, dostęp do tych danych; po trzecie, informacje o przetwarzaniu. Można je postrzegać jako trzy różne elementy, które wspólnie tworzą prawo dostępu.

2.2.1.1 Potwierdzenie, „czy" dane osobowe są przetwarzane

18. Występując z żądaniem dostępu do danych osobowych, osoby, których dane dotyczą, muszą przede wszystkim wiedzieć, czy administrator przetwarza dotyczące ich dane. W związku z tym informacje te stanowią pierwszy element prawa dostępu przewidzianego w art. 15 ust. 1. W przypadku gdy administrator nie przetwarza danych osobowych odnoszących się do osoby, której dane dotyczą, żądającej dostępu, informacje, które należy przekazać, ograniczałyby się do potwierdzenia, że żadne dane osobowe odnoszące się do osoby, której dane dotyczą, nie są przetwarzane. Jeżeli administrator przetwarza dane dotyczące osoby występującej z żądaniem, musi potwierdzić ten fakt tej osobie. Potwierdzenie to może zostać przekazane oddzielnie lub może zostać włączone do informacji o przetwarzanych danych osobowych (zob. poniżej).

2.2.1.2 Dostęp do przetwarzanych danych osobowych

19. Dostęp do danych osobowych jest drugim elementem prawa dostępu przewidzianego w art. 15 ust. 1, stanowiącym jego rdzeń. Odnosi się on do pojęcia danych osobowych w rozumieniu w art. 4 pkt 1 RODO. Oprócz podstawowych danych osobowych, takich jak imię i nazwisko i adres, definicja ta może obejmować nieograniczoną liczbę różnych danych, pod warunkiem że są one objęte materialnym zakresem stosowania RODO, w szczególności w odniesieniu do sposobu ich przetwarzania (art. 2 RODO). Dostęp do danych osobowych oznacza zatem dostęp do samych danych osobowych, a nie tylko ogólny opis danych czy zwykłe odniesienie do kategorii danych osobowych przetwarzanych przez administratora. Jeżeli nie mają zastosowania żadne ograniczenia ani restrykcje[12], osoby, których dane dotyczą, mają prawo dostępu do wszystkich przetwarzanych danych, które ich dotyczą, lub do części danych, w zależności od zakresu żądania (zob. sekcja 2.3.1). Obowiązek zapewnienia dostępu do danych nie zależy od rodzaju ani źródła tych danych. Ma on w pełni zastosowanie nawet w przypadkach, gdy osoba występująca z żądaniem początkowo przekazała dane administratorowi, ponieważ jego celem jest poinformowanie osoby, której dane dotyczą, o faktycznym przetwarzaniu tych danych przez administratora. Zakres danych osobowych zgodnie z art. 15 szczegółowo wyjaśniono w sekcjach 4.1 i 4.2.

2.2.1.3 Informacje o przetwarzaniu i prawach osób, których dane dotyczą

20. Trzecim elementem prawa dostępu są informacje o przetwarzaniu i prawach osób, których dane dotyczą, które to prawa administrator musi zapewnić zgodnie z art. 15 ust. 1 lit. a)–h) i art. 15 ust. 2. Takie informacje mogą opierać się na tekście zaczerpniętym na przykład z oświadczenia o ochronie prywatności administratora[13] lub z rejestru czynności przetwarzania prowadzonego przez administratora, o którym to rejestrze mowa w art. 30 RODO, ale mogą wymagać aktualizacji i dostosowania do żądania osoby, której dane dotyczą. Treść i stopień szczegółowości informacji omówiono szerzej w sekcji 4.3.

2.2.2 Przepisy dotyczące warunków

21. W art. 15 ust. 3 uzupełniono wymogi dotyczące warunków udzielania odpowiedzi na żądania dostępu określone w art. 12 RODO o pewne doprecyzowania w kontekście żądań dostępu.

2.2.2.1 Dostarczenie kopii

22. Zgodnie z art. 15 ust. 3 zdanie pierwsze RODO administrator dostarcza nieodpłatną kopię danych osobowych, których dotyczy przetwarzanie. Kopia odnosi się zatem jedynie do drugiego elementu prawa dostępu („dostęp do przetwarzanych danych osobowych", zob. powyżej). Administrator musi zapewnić, aby pierwsza kopia była bezpłatna, nawet jeżeli uważa, że koszt powielania jest wysoki (przykład: koszt dostarczenia kopii nagrania rozmowy telefonicznej).

23. Obowiązku dostarczenia kopii nie należy rozumieć jako dodatkowego prawa osoby, której dane dotyczą, lecz jako sposób zapewnienia dostępu do danych. Obowiązek ten wzmacnia prawo dostępu do danych[14] i pomaga w interpretacji tego prawa, ponieważ umożliwia zrozumienie, że prawo dostępu do danych zgodnie z art. 15 ust. 1 obejmuje udzielenie pełnych informacji na temat wszystkich danych i nie może być rozumiane jako udzielenie dostępu jedynie do streszczenia danych. Jednocześnie

[12] Zob. sekcja 6. niniejszych wytycznych.
[13] Aby uzyskać informacje na ten temat, zob. Grupa Robocza Art. 29, WP 260 rev.01, 11 kwietnia 2018 r., Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 – zatwierdzone przez EROD (zwane dalej „wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzonymi przez EROD").
[14] Obowiązku dostarczenia kopii nie wymieniono w dyrektywie o ochronie danych 95/46/WE.

obowiązek dostarczenia kopii nie ma na celu rozszerzenia zakresu prawa dostępu: odnosi się on (jedynie) do kopii danych osobowych podlegających przetwarzaniu, niekoniecznie do kopii oryginalnych dokumentów (zob. sekcja 5 pkt 152). W ogólniejszym ujęciu nie ma żadnych dodatkowych informacji, które należy przekazać osobie, której dane dotyczą, przy dostarczaniu kopii: zakres informacji, które mają być zawarte w kopii, odpowiada zakresowi dostępu do danych zgodnie z art. 15 ust. 1 (drugi element prawa dostępu, o którym mowa powyżej, zob. pkt 19), który obejmuje wszystkie informacje niezbędne do umożliwienia osobie, której dane dotyczą, zrozumienia i weryfikacji zgodności przetwarzania z prawem[15].

24. W świetle powyższego, jeżeli dostęp do danych w rozumieniu art. 15 ust. 1 jest zapewniony poprzez dostarczenie kopii, obowiązek dostarczenia kopii, o którym mowa w art. 15 ust. 3, jest spełniony. Obowiązek dostarczenia kopii służy osiągnięciu celów prawa dostępu, tj. by osoba, której dane dotyczą, miała świadomość przetwarzania i mogła zweryfikować zgodność przetwarzania z prawem (motyw 63). Aby możliwe było osiągnięcie tych celów, osoba, której dane dotyczą, będzie w większości przypadków potrzebowała wglądu do informacji nie tylko tymczasowo. W związku z tym osoba, której dane dotyczą, będzie potrzebowała uzyskać dostęp do informacji poprzez otrzymanie kopii danych osobowych.

25. W świetle powyższego pojęcie kopii należy interpretować rozszerzająco – obejmuje ono poszczególne rodzaje dostępu do danych osobowych, o ile są one kompletne (tj. obejmują wszystkie żądane dane osobowe) i mogą być przechowywane przez osobę, której dane dotyczą. Wymóg dostarczenia kopii oznacza zatem, że informacje o danych osobowych dotyczących osoby występującej z żądaniem są przekazywane osobie, której dane dotyczą, w sposób umożliwiający tej osobie zachowanie wszystkich informacji i powrót do nich.

26. Mimo że pojęcie kopii jest rozumiane tak szeroko i że dostarczenie kopii jest głównym sposobem, w jaki należy zapewnić dostęp, w pewnych okolicznościach właściwe mogą być inne sposoby. Dalsze wyjaśnienia dotyczące kopii i innych sposobów udzielania dostępu znajdują się w sekcji 5, w szczególności w pkt 5.2.2–5.2.5.

2.2.2.2 Dostarczanie kolejnych kopii

27. Art. 15 ust. 3 zdanie drugie dotyczy sytuacji, w których osoba, której dane dotyczą, zwraca się do administratora o więcej niż jedną kopię, na przykład w przypadku utraty lub uszkodzenia pierwszej kopii lub gdy osoba, której dane dotyczą, chce przekazać kopię innej osobie lub organowi nadzorczemu. Jeżeli administrator musi dostarczyć kolejne kopie na żądanie osoby, której dane dotyczą, zgodnie z art. 15 ust. 3 za każdą kolejną kopię, o którą zwróci się ta osoba, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych (art. 15 ust. 3 zdanie drugie).

28. Jeżeli osoba, której dane dotyczą, zwraca się o dodatkową kopię po wystosowaniu pierwszego żądania, może pojawić się pytanie, czy należy je traktować jako nowe żądanie, czy też osoba, której dane dotyczą, wnosi o dodatkową kopię danych w rozumieniu art. 15 ust. 3 zdanie drugie, w którym to przypadku można pobrać opłatę za dodatkową kopię. Odpowiedź na te pytania zależy wyłącznie od treści żądania: żądanie należy interpretować jako prośbę o dodatkową kopię, o ile pod względem czasu i zakresu dotyczy ono tego samego przetwarzania danych osobowych, co poprzednie żądanie. Jeśli jednak osoba, której dane dotyczą, chce uzyskać informacje na temat danych przetwarzanych w innym momencie lub odnoszących się do innego zestawu danych niż ten, którego pierwotnie żądała, prawo

[15] Kwestie związane z tematem niniejszego punktu są przedmiotem sprawy zawisłej obecnie przed TSUE (C-487/21).

do uzyskania bezpłatnej kopii zgodnie z art. 15 ust. 3 ma zastosowanie ponownie. Dotyczy to również przypadków, w których osoba, której dane dotyczą, wystąpiła z pierwszym żądaniem niewiele wcześniej. Osoba, której dane dotyczą, może wykonać przysługujące jej prawo dostępu poprzez wystąpienie z kolejnym żądaniem i uzyskać bezpłatną kopię, chyba że żądanie zostanie uznane za nadmierne zgodnie z art. 12 ust. 5, z możliwością pobrania rozsądnej opłaty zgodnie z art. 12 ust. 5 lit. a) (informacje na temat ustawicznego charakteru nadmiernych żądań znajdują się w sekcji 6).

Przykład 2: Klient występuje do spółki giełdowej z żądaniem dostępu. Rok po udzieleniu odpowiedzi przez spółkę ten sam klient występuje z żądaniem dostępu na podstawie art. 15 do tej samej spółki. Niezależnie od tego, czy od czasu wystąpienia z poprzednim żądaniem między stronami doszło do zawarcia nowych transakcji handlowych lub nawiązania innych kontaktów, drugie żądanie należy traktować jako nowe żądanie. Nawet jeśli nie nastąpiła żadna zmiana w zakresie przetwarzania danych przez spółkę – co niekoniecznie jest oczywiste dla osoby, której dane dotyczą – osoba ta ma prawo do uzyskania bezpłatnej kopii danych.

Wariant 1: Nawet jeśli w powyższych przypadkach klient wystąpi z nowym żądaniem, na przykład zaledwie tydzień po wystąpieniu z pierwszym żądaniem, można to uznać za nowe żądanie zgodnie z art. 15 ust. 1 i art. 15 ust. 3 zdanie pierwsze, o ile nie należy tego interpretować jako zwykłego przypomnienia pierwszego żądania. W odniesieniu do krótkiego odstępu czasu i w zależności od konkretnych okoliczności dotyczących nowego żądania jego nadmierny charakter, o którym mowa w art. 12 ust. 5, jest kwestią sporną (zob. sekcja 6).

Wariant 2: Żądanie wydania „nowej kopii" informacji, która została już przekazana w formie kopii w odpowiedzi na poprzednie żądanie, na przykład w przypadku, gdy klient utracił poprzednio otrzymaną kopię, należy oczywiście traktować jako żądanie wydania dodatkowej kopii, ponieważ odnosi się do poprzedniego żądania co do zakresu i czasu przetwarzania.

29. Jeżeli osoba, której dane dotyczą, ponownie występuje z pierwszym żądaniem dostępu ze względu na fakt, że otrzymana odpowiedź nie była kompletna lub że nie podano powodów odmowy, żądania tego nie należy traktować jako nowego żądania, ponieważ stanowi ono jedynie przypomnienie pierwszego niezrealizowanego żądania.

30. Jeśli chodzi o podział kosztów w przypadku zwrócenia się o dodatkową kopię, art. 15 ust. 3 stanowi, że administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych w związku z żądaniem. Oznacza to, że koszty administracyjne są istotnym kryterium ustalania wysokości opłaty. Jednocześnie wysokość opłaty powinna być odpowiednia, biorąc pod uwagę znaczenie prawa dostępu jako prawa podstawowego przysługującego osobie, której dane dotyczą. Administrator nie powinien przenosić kosztów ogólnych lub innych wydatków ogólnych na osobę, której dane dotyczą, lecz skupić się na konkretnych kosztach związanych z przekazaniem dodatkowej kopii. Podczas realizacji tego procesu administrator powinien efektywnie wykorzystywać swoje zasoby ludzkie i materialne, aby utrzymać koszty wydania kopii na niskim poziomie, w tym jeśli administrator korzysta ze wsparcia zewnętrznego.

31. W przypadku gdy administrator zdecyduje się na pobranie opłaty, powinien z wyprzedzeniem wskazać, że opłata ta zostanie pobrana oraz – podać możliwie najdokładniejszą – kwotę kosztów, którymi planuje obciążyć osobę, której dane dotyczą, aby umożliwić jej podjęcie decyzji o podtrzymaniu lub wycofaniu żądania.

2.2.2.3 Udostępnianie informacji w powszechnie stosowanej formie elektronicznej

32. W przypadku przekazania żądania elektronicznie w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy (zob. art. 12 ust. 3 RODO). Art. 15 ust. 3 zdanie trzecie uzupełnia ten wymóg w kontekście żądania dostępu, stanowiąc, że administrator jest dodatkowo zobowiązany do udzielenia odpowiedzi w powszechnie stosowanej formie elektronicznej, jeżeli osoba, której dane dotyczą, nie zaznaczy inaczej. W art. 15 ust. 3 zakłada się, że w przypadku administratorów, którzy są w stanie otrzymywać żądania elektroniczne, możliwe będzie udzielenie odpowiedzi na żądanie w powszechnie stosowanej formie elektronicznej (szczegółowe informacje znajdują się w sekcji 5.2.5). Przepis ten odnosi się do wszystkich informacji, które należy przekazać zgodnie z art. 15 ust. 1 i 2. W związku z tym, jeżeli osoba, której dane dotyczą, zwraca się o udzielenie dostępu drogą elektroniczną, wszystkie informacje muszą zostać przekazane w powszechnie stosowanej formie elektronicznej. Kwestie formatu omówiono bardziej szczegółowo w sekcji 5. Administrator zawsze powinien wdrożyć odpowiednie środki bezpieczeństwa, w szczególności gdy ma do czynienia ze szczególną kategorią danych osobowych (zob. sekcja 2.3.4 poniżej).

2.2.3 Możliwe ograniczenie prawa dostępu

33. Ponadto – w kontekście prawa dostępu – w art. 15 ust. 4 przewidziano konkretne ograniczenie. Stanowi on, że należy wziąć pod uwagę możliwy niekorzystny wpływ na prawa i wolności innych osób. Kwestie dotyczące zakresu i konsekwencji tego ograniczenia, jak również dodatkowych ograniczeń i ograniczeń określonych w art. 12 ust. 5 RODO lub w art. 23 RODO wyjaśniono w sekcji 6.

2.3 Ogólne zasady dotyczące prawa dostępu

34. W przypadku gdy osoby, których dane dotyczą, występują z żądaniem dostępu do swoich danych, co do zasady informacje, o których mowa w art. 15 RODO, muszą być zawsze przekazywane w całości. W związku z tym, jeżeli administrator przetwarza dane dotyczące osoby, której dane dotyczą, przekazuje on wszystkie informacje, o których mowa w art. 15 ust. 1, oraz – w stosownych przypadkach – informacje, o których mowa w art. 15 ust. 2. Administrator musi wprowadzić odpowiednie środki w celu zapewnienia, by informacje były kompletne, prawidłowe i aktualne oraz jak najlepiej odpowiadały stanowi przetwarzania danych w momencie otrzymania żądania[16]. Jeżeli co najmniej dwóch administratorów przetwarza dane wspólnie, ustalenia współadministratorów dotyczące ich odpowiednich obowiązków w zakresie wykonywania praw osób, których dane dotyczą, w szczególności w odniesieniu do udzielania odpowiedzi na żądania dostępu, nie mają wpływu na prawa osób, których dane dotyczą, wobec administratora, do którego kierują swoje żądanie[17].

2.3.1 Kompletność informacji

35. Osoby, których dane dotyczą, mają prawo do uzyskania – z wyjątkami wymienionymi poniżej – pełnego ujawnienia wszystkich dotyczących ich danych (szczegółowe informacje na temat zakresu takiego ujawnienia znajdują się w sekcji 4.2). O ile osoba, której dane dotyczą, wyraźnie nie zaznaczy inaczej, żądanie wykonania prawa dostępu należy rozumieć w sposób ogólny jako obejmujące wszystkie dane

[16] Wytyczne dotyczące odpowiednich środków znajdują się w sekcji 5 pkt 123–129.
[17] Wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, pkt 162 lit. f). Podmioty przetwarzające muszą pomagać administratorowi, ibid., pkt 129.

osobowe dotyczące osoby, której dane dotyczą[18]. W następujących przypadkach można rozważyć ograniczenie dostępu do części informacji:

a) Osoba, której dane dotyczą, wyraźnie ograniczyła swoje żądanie do podzbioru danych. Aby uniknąć podawania niekompletnych informacji, administrator może uwzględnić to ograniczenie żądania osoby, której dane dotyczą, tylko wtedy, gdy można mieć pewność, że taka interpretacja odpowiada życzeniu osoby, której dane dotyczą (więcej informacji szczegółowych można znaleźć w sekcji3.1.1 pkt 51). Co do zasady, osoba, której dane dotyczą, nie musi ponownie zwracać się o przekazanie wszystkich danych, do których uzyskania jest uprawniona.

b) W sytuacjach, w których administrator przetwarza dużą ilość danych dotyczących osoby, której dane dotyczą, może mieć wątpliwości, czy żądanie dostępu, które zostało wyrażone w sposób bardzo ogólny, faktycznie ma na celu uzyskanie szczegółowych informacji o wszystkich rodzajach przetwarzanych danych lub o wszystkich obszarach działalności administratora. Wątpliwości te mogą się pojawić w szczególności w sytuacjach, w których już na początku osobie, której dane dotyczą, nie można było zapewnić narzędzi umożliwiających sprecyzowanie żądania lub gdy osoba, której dane dotyczą, z nich nie skorzystała. Administrator mierzy się wówczas z problemem, jak udzielić pełnej odpowiedzi, a zarazem uniknąć przekazania osobie, której dane dotyczą, nadmiaru informacji, którymi osoba ta nie jest zainteresowana i z którymi nie jest w stanie się skutecznie zapoznać. W zależności od okoliczności i możliwości technicznych możliwe są różne rozwiązania tego problemu, na przykład przez zapewnienie narzędzi samoobsługowych w kontekście usług internetowych (zob. sekcja 5 poświęcona podejściu warstwowemu). Jeśli takie rozwiązania nie mają zastosowania, administrator, który przetwarza duże ilości informacji o osobie, której dane dotyczą, może zażądać, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie (zob. motyw 63 RODO). Przykładem może być spółka prowadząca działalność w kilku obszarach lub organ publiczny z różnymi jednostkami administracyjnymi, jeśli administrator stwierdził, że w tych oddziałach przetwarzane są duże ilości danych dotyczących osoby, której dane dotyczą. Ponadto duża ilość danych może być przetwarzana przez administratorów, którzy gromadzą dane dotyczące często wykonywanych działań przez osobę, której dane dotyczą, przez dłuższy czas.

Przykład 3: Organ publiczny przetwarza dane dotyczące osoby, której dane dotyczą, w wielu różnych działach w odniesieniu do różnych kontekstów. Informacje dotyczące zarządzania dokumentacją i przechowywania dokumentacji są częściowo przetwarzane w sposób niezautomatyzowany, a większość danych jest przechowywana tylko w dokumentacji papierowej. Jeśli chodzi o ogólne sformułowanie żądania, organ publiczny ma wątpliwości, czy osoba, której dane dotyczą, jest świadoma zakresu żądania, w szczególności różnorodności operacji przetwarzania, które będzie ono obejmowało, ilości informacji i liczby stron, które otrzyma osoba, której dane dotyczą.

Przykład 4: Duży zakład ubezpieczeń otrzymuje pisemne ogólne żądanie dostępu do danych od osoby, która jest jego długoletnim klientem. Nawet jeśli okresy usuwania danych są w pełni przestrzegane, zakład faktycznie przetwarza ogromną ilość danych dotyczących klienta, ponieważ przetwarzanie nadal jest niezbędne do wypełnienia zobowiązań umownych wynikających ze stosunku umownego z klientem (w tym na przykład stałych zobowiązań, komunikacji z klientem i stronami trzecimi w zakresie kontrowersyjnych kwestii itp.) lub do wypełnienia zobowiązań prawnych (dane zarchiwizowane, które muszą być przechowywane do celów podatkowych itp.). Zakład ubezpieczeń może mieć wątpliwości, czy żądanie, które zostało sformułowane w sposób bardzo ogólny,

[18] Informacje szczegółowe można znaleźć w sekcji 5.2.3 poniżej poświęconej podejściu warstwowemu.

rzeczywiście ma obejmować wszystkie rodzaje tych danych. Może to być szczególnie problematyczne, jeśli zakład ubezpieczeń posiada jedynie adres pocztowy osoby, której dane dotyczą, i w związku z tym musi wysyłać wszelkie informacje w formie papierowej. Te same wątpliwości mogą być jednak istotne również w przypadku przekazywania informacji w innej formie.

Jeżeli w takich przypadkach administrator zdecyduje się zwrócić do osoby, której dane dotyczą, o sprecyzowanie żądania w celu wywiązania się z obowiązku ułatwienia wykonania prawa dostępu (art. 12 ust. 2 RODO), przekazuje wówczas jednocześnie istotne informacje dotyczące operacji przetwarzania, które mogą dotyczyć osoby, której dane dotyczą, informując o odpowiednich obszarach swojej działalności, bazach danych itp.

Przykład 5: W ramach stosunku pracy, w przypadku ogólnie sformułowanego żądania dostępu, nie jest dorozumiane, że pracownik chce otrzymać wszystkie dane użytkownika dotyczące logowania, dane dotyczące dostępu do miejsca pracy, dane dotyczące rozliczeń z tytułu korzystania ze stołówki, dane dotyczące wypłat wynagrodzeń itp. Zwrócenie się przez pracodawcę o sprecyzowanie żądania może na przykład prowadzić do wyjaśnienia, że pracownik jest zainteresowany zrozumieniem lub sprawdzeniem, komu przekazano jego ocenę pracy. Bez takiego sprecyzowania pracownik otrzymałby dużą ilość informacji, nie będąc zainteresowanym większością z nich. Jednocześnie pracodawca będzie musiał przekazać informacje na temat różnych kontekstów przetwarzania, które mogą dotyczyć pracownika, aby umożliwić mu rozsądne sprecyzowanie żądania.

Należy podkreślić, że zwrócenie się o sprecyzowanie żądania nie ma na celu ograniczenia odpowiedzi na żądanie dostępu i nie jest wykorzystywane do ukrywania jakichkolwiek informacji na temat danych lub przetwarzania danych dotyczących osoby, której dane dotyczą. Jeśli osoba, której dane dotyczą, do której zwrócono się o sprecyzowanie zakresu żądania, potwierdzi, że chce uzyskać wszystkie dane osobowe jej dotyczące, administrator musi oczywiście dostarczyć te dane w całości.

Tak czy inaczej, administrator powinien zawsze być w stanie wykazać, że sposób rozpatrzenia żądania ma na celu nadanie jak największej mocy prawu dostępu i że jest zgodny z jego obowiązkiem ułatwiania wykonywania praw przysługujących osobom, których dane dotyczą (art. 12 ust. 2 RODO). Z zastrzeżeniem tych zasad administrator może oczekiwać na odpowiedź osoby, której dane dotyczą, przed przekazaniem danych dodatkowych zgodnie z życzeniem tej osoby, jeżeli administrator zapewnił osobie, której dane dotyczą, jasny przegląd wszystkich operacji przetwarzania, które mogą dotyczyć tej osoby, w tym w szczególności tych, których osoba, której dane dotyczą, mogła się nie spodziewać, jeżeli administrator zapewnił również dostęp do wszystkich danych, o które osoba, której dane dotyczą, wyraźnie zabiegała, oraz jeżeli informacjom tym towarzyszy również wyraźne wskazanie, w jaki sposób uzyskać dostęp do pozostałych części przetwarzanych danych.

c) Obowiązują wyjątki lub ograniczenia w zakresie prawa dostępu (zob. sekcja 6 poniżej). W takich przypadkach administrator powinien dokładnie sprawdzić, których części informacji dotyczy dany wyjątek i przekazać wszystkie nieobjęte nim informacje. Na przykład wyjątek nie może dotyczyć samego potwierdzenia przetwarzania danych osobowych (element 1). W związku z tym należy przekazać informacje o wszystkich danych osobowych i wszystkich informacjach, o których mowa w art. 15 ust. 1 i 2, które nie są objęte wyjątkiem lub ograniczeniem.

2.3.2 Prawidłowość informacji

36. Informacje zawarte w kopii danych osobowych przekazanej osobie, której dane dotyczą, muszą obejmować rzeczywiste informacje lub przechowywane dane osobowe dotyczące osoby, której dane dotyczą. Obejmuje to obowiązek przekazywania informacji o danych, które są niedokładne lub

o przetwarzaniu danych, które nie jest lub przestało być zgodne z prawem. Osoba, której dane dotyczą, może na przykład wykonać przysługujące jej prawo dostępu, aby poznać źródło niedokładnych danych przekazywanych przez różnych administratorów. Jeśli administrator sprostuje niedokładne dane przed poinformowaniem o tym osoby, której dane dotyczą, osoba ta zostanie pozbawiona tej możliwości. To samo dotyczy niezgodnego z prawem przetwarzania. Możliwość uzyskania informacji o niezgodnym z prawem przetwarzaniu danych dotyczących osoby, której dane dotyczą, jest jednym z głównych celów prawa dostępu. Obowiązek informowania o niezmienionym stanie przetwarzania pozostaje bez uszczerbku dla obowiązku administratora w zakresie zaprzestania niezgodnego z prawem przetwarzania lub sprostowania nieprawidłowych danych. Kwestie dotyczące kolejności, w jakiej obowiązki te powinny być wypełniane, omówiono poniżej.

2.3.3 Czasowy punkt odniesienia, w którym dokonano oceny

37. Ocena przetwarzanych danych powinna jak najlepiej odzwierciedlać sytuację, w której administrator otrzymał żądanie, a odpowiedź powinna obejmować wszystkie dane dostępne w danym momencie. Oznacza to, że administrator musi bez zbędnej zwłoki dowiedzieć się o wszystkich czynnościach przetwarzania dotyczących osoby, której dane dotyczą. Administratorzy nie są zatem zobowiązani do przekazywania danych osobowych, które przetwarzali w przeszłości, ale którymi już nie dysponują[19]. Na przykład administrator mógł usunąć dane osobowe zgodnie ze swoją polityką zatrzymywania danych lub przepisami ustawowymi, a zatem może nie być już w stanie przekazać żądanych danych osobowych. W tym kontekście należy przypomnieć, że czas przechowywania danych należy ustalić zgodnie z art. 5 ust. 1 lit. e) RODO, ponieważ każde zatrzymywanie danych musi być obiektywnie uzasadnione.

38. Jednocześnie administrator z wyprzedzeniem wprowadza niezbędne środki w celu ułatwienia wykonania prawa dostępu i rozpatrzenia takich żądań tak szybko, jak to możliwe (zob. art. 12 ust. 3) i zanim dane będą musiały zostać usunięte. W związku z tym, w przypadku krótkich okresów zatrzymywania, środki wprowadzone w celu udzielenia odpowiedzi na żądanie powinny być dostosowane do odpowiedniego okresu zatrzymywania w celu ułatwienia wykonania prawa dostępu i uniknięcia trwałej niemożności zapewnienia dostępu do danych przetwarzanych w momencie wystąpienia z żądaniem[20]. W niektórych przypadkach udzielenie odpowiedzi na żądanie przed wyznaczonym terminem zaplanowanego usunięcia danych może jednak nie być możliwe. Na przykład, jeśli w trakcie niezwłocznego udzielania odpowiedzi na żądanie, administrator pobierze dane osobowe, które miały zostać usunięte następnego dnia, może potrzebować dodatkowego czasu na rozważenie, czy należy utajnić pewne informacje w celu ochrony wolności innych osób przed wydaniem kopii danych osobowych osobie występującej z żądaniem. Jeśli dane pobrano w zaplanowanym okresie zatrzymywania, administrator nadal może przetwarzać te dane w celu wypełnienia obowiązku udzielenia odpowiedzi na żądanie. W takich przypadkach podstawą

[19] Zob. w tym celu dalsze wyjaśnienia w sekcji 4 niniejszych wytycznych, a także w wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 7 maja 2009 r., C-553/07, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer dotyczącym prawa dostępu do informacji dotyczących odbiorców lub kategorii odbiorców w odniesieniu do przeszłości.

[20] Aby ułatwić podjęcie natychmiastowych działań, można na przykład rozważyć wdrożenie narzędzia samoobsługowego zapewniającego osobie, której dane dotyczą, łatwy dostęp do żądanych danych osobowych oraz systemu powiadamiania administratora o żądaniu, które dotyczy danych osobowych o krótkich okresach zatrzymywania.

przetwarzania może być art. 6 ust. 1 lit. c) w związku z art. 15 RODO, a czas jego trwania musi być zgodny z wymogami określonymi w art. 12 ust. 3 RODO[21]. Zastosowanie tej podstawy prawnej jest ograniczone do przetwarzania danych określonych jako niezbędne do udzielenia odpowiedzi na konkretne żądanie i nie może stanowić uzasadnienia dla ogólnego przedłużenia okresów zatrzymywania.

39. Administrator nie może ponadto celowo uchylać się od obowiązku przekazania żądanych danych osobowych poprzez usuwanie lub modyfikowanie danych osobowych w odpowiedzi na żądanie dostępu (zob. sekcja 2.3.2). Jeśli w trakcie rozpatrywania żądania dostępu administrator wykryje nieprawidłowe dane lub przetwarzanie niezgodne z prawem, musi ocenić stan przetwarzania i poinformować o tym osobę, której dane dotyczą, przed wypełnieniem pozostałych obowiązków. Działając we własnym interesie, aby uniknąć konieczności dalszej komunikacji w tej sprawie, a także aby zachować zgodność z zasadą przejrzystości, administrator powinien dodać informacje o późniejszych sprostowaniach lub usunięciach.

Przykład 6: Odpowiadając na żądanie dostępu, administrator dowiaduje się, że wniosek osoby, której dane dotyczą, dotyczący wakatu w przedsiębiorstwie administratora był przechowywany po upływie okresu zatrzymywania. W takim przypadku administrator nie może najpierw usunąć danych, a następnie udzielić odpowiedzi osobie, której dane dotyczą, że żadne dane (dotyczące wniosku) nie są przetwarzane. Musi on najpierw udzielić dostępu, a następnie usunąć dane. Aby zapobiec kolejnym żądaniom usunięcia danych, zaleca się dodanie informacji o okolicznościach i czasie takiego usunięcia.

Aby zachować zgodność z zasadą przejrzystości, administratorzy powinni informować osobę, której dane dotyczą, o konkretnym momencie przetwarzania, do którego odnosi się odpowiedź administratora. W niektórych przypadkach, na przykład w kontekście częstych działań komunikacyjnych, może dojść do dodatkowego przetwarzania lub modyfikacji danych między czasowym punktem odniesienia, w którym dokonano oceny przetwarzania, a odpowiedzią administratora. Jeśli administrator wie o takich zmianach, zaleca się uwzględnienie informacji o tych zmianach, a także informacji o dodatkowym przetwarzaniu niezbędnym do udzielenia odpowiedzi na żądanie.

2.3.4 Zgodność z wymogami bezpieczeństwa danych

40. Z uwagi na fakt, że przekazywanie i udostępnianie danych osobowych osobie, której dane dotyczą, stanowi operację przetwarzania, administrator jest w każdym przypadku zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiadającego ryzyku związanemu z przetwarzaniem (zob. art. 5 ust. 1 lit. f) oraz art. 24 i 32 RODO). Ma to zastosowanie niezależnie od sposobu zapewnienia dostępu. W przypadku przekazania danych osobie, której dane dotyczą, za pomocą środków nieelektronicznych, w zależności od ryzyka związanego z przetwarzaniem, administrator może rozważyć wysłanie listu poleconego bądź zaoferować osobie, której dane dotyczą, odebranie dokumentacji za potwierdzeniem odbioru bezpośrednio z jednej z placówek administratora, lecz nie może jej do tego zobowiązać. Jeżeli zgodnie z art. 12 ust. 1 i 3 informacje są przekazywane elektronicznie, administrator wybiera środki elektroniczne, które spełniają wymogi bezpieczeństwa danych. Również w przypadku dostarczenia kopii danych w powszechnie stosowanej formie elektronicznej (zob. art. 15 ust. 3 RODO) administrator uwzględnia wymogi bezpieczeństwa danych przy wyborze sposobu przekazania pliku elektronicznego

[21] Pozostaje to bez uszczerbku dla późniejszego przetwarzania danych do celów dowodowych w związku z rozpatrywaniem żądania dostępu przez odpowiedni okres.

osobie, której dane dotyczą. Możliwe jest zastosowanie szyfrowania, ochrony hasłem itp. W celu ułatwienia dostępu do zaszyfrowanych danych administrator powinien również zapewnić przekazanie odpowiednich informacji, aby osoba, której dane dotyczą, mogła uzyskać dostęp do odszyfrowanych danych. W przypadkach, w których zgodnie z wymogami bezpieczeństwa danych konieczne byłoby szyfrowanie wiadomości e-mail od końca do końca, lecz administrator byłby w stanie wysłać tylko zwykłą wiadomość e-mail, będzie on musiał skorzystać z innych środków, takich jak wysłanie pamięci USB listem (poleconym) osobie, której dane dotyczą.

3 OGÓLNE UWAGI DOTYCZĄCE OCENY ŻĄDAŃ DOSTĘPU

3.1 Wprowadzenie

41. Przy otrzymywaniu żądań dostępu do danych osobowych administrator musi ocenić każde żądanie indywidualnie. Administrator bierze pod uwagę m.in. następujące kwestie, omówione bardziej szczegółowo w kolejnych punktach: czy żądanie dotyczy danych osobowych powiązanych z osobą występującą z żądaniem oraz kim jest taka osoba. Niniejsza sekcja ma na celu wyjaśnienie, jakie elementy żądania dostępu administrator powinien wziąć pod uwagę przy przeprowadzaniu oceny oraz omówienie możliwych scenariuszy takiej oceny, a także jej konsekwencji. Administrator, oceniając żądanie dostępu do danych osobowych, bierze również pod uwagę obowiązek ułatwienia wykonania praw przysługujących osobie, której dane dotyczą, o którym mowa w art. 12 ust. 2 RODO, przy jednoczesnym zachowaniu odpowiedniego bezpieczeństwa danych osobowych[22].

42. W związku z tym administratorzy powinni być gotowi do rozpatrywania żądań dostępu do danych osobowych. Oznacza to, że administrator powinien być przygotowany na otrzymanie żądania, przeprowadzenie jego prawidłowej oceny (ocena ta jest przedmiotem niniejszej sekcji wytycznych) oraz udzielenie stosownej odpowiedzi osobie występującej z żądaniem bez zbędnej zwłoki. Sposób, w jaki administratorzy przygotują się do rozpatrywania żądań dostępu, powinien być odpowiedni i proporcjonalny oraz zależeć od charakteru, zakresu, kontekstu i celów przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych zgodnie z art. 24 RODO. W zależności od konkretnych okoliczności administratorzy mogą być na przykład zobowiązani do wdrożenia odpowiedniej procedury, co powinno zagwarantować bezpieczeństwo danych, pozostając bez uszczerbku dla wykonywania przez osobę, której dane dotyczą, przysługujących jej praw.

3.1.1 Analiza treści żądania

43. Kwestię tę można ocenić dokładniej, zadając następujące pytania.

    a) <u>Czy żądanie dotyczy danych osobowych?</u>

[22] Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych zgodnie z zasadą integralności i poufności (art. 5 ust. 1 lit. f) RODO), wdrażając odpowiednie środki techniczne i organizacyjne, o których mowa w art. 32 RODO i które omówiono bardziej szczegółowo w art. 24 RODO. Administrator musi być w stanie wykazać, że zapewnia odpowiedni poziom ochrony danych zgodnie z zasadą rozliczalności (zob. również: Opinia 3/2010 Grupy Roboczej Art. 29 w sprawie zasady rozliczalności przyjęta w dniu 13 lipca 2010 r., 00062/10/EN WP 173 oraz Wytyczne EROD nr 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO).

44. Zgodnie z RODO zakres żądania obejmuje wyłącznie dane osobowe[23]. W związku z tym wszelkich żądań udzielenia informacji dotyczących innych kwestii, w tym ogólnych informacji dotyczących administratora, jego modeli biznesowych lub czynności przetwarzania niepowiązanych z danymi osobowymi, nie należy uznawać za żądania składane na podstawie art. 15 RODO. Ponadto żądanie udzielenia informacji na temat informacji anonimowych lub danych, które nie dotyczą osoby występującej z żądaniem lub osoby, w imieniu której osoba upoważniona wystąpiła z żądaniem, nie będzie objęte zakresem prawa dostępu. Kwestia ta zostanie przeanalizowana bardziej szczegółowo w sekcji 4.

45. W przeciwieństwie do informacji anonimowych (które nie są danymi osobowymi), dane spseudonimizowane, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, są danymi osobowymi[24]. W związku z tym dane spseudonimizowane, które można powiązać z osobą, której dane dotyczą – np. gdy osoba, której dane dotyczą, dostarczy odpowiedni identyfikator umożliwiający jej identyfikację lub gdy administrator jest w stanie powiązać dane z osobą występującą z żądaniem za pomocą własnych środków – należy uznać za objęte zakresem żądania[25].

b) Czy żądanie dotyczy osoby występującej z żądaniem (lub osoby, w imieniu której osoba upoważniona występuje z żądaniem)?

46. Co do zasady żądanie może dotyczyć wyłącznie danych osoby występującej z żądaniem. Dostępu do danych innych osób można żądać wyłącznie po uzyskaniu odpowiedniego pozwolenia[26].

Przykład 7: Osoba X, której dane dotyczą, pracuje jako kierownik działu w przedsiębiorstwie, które zapewnia swoim kierownikom miejsca parkingowe na parkingu służbowym. Chociaż osoba X, której dane dotyczą, ma stałe miejsce parkingowe, gdy osoba ta przyjeżdża do biura na drugą zmianę, miejsce to jest już często zajęte przez inny samochód. Z uwagi na to, że sytuacja ta się powtarza w celu zidentyfikowania kierowcy, który w sposób nieuprawniony zajmuje miejsce parkingowe, osoba, której dane dotyczą, zwraca się do administratora systemu monitoringu wizyjnego obejmującego swym zasięgiem obszar parkingowy biura o dostęp do danych osobowych tego kierowcy. W takim przypadku żądanie osoby X, której dane dotyczą, nie będzie żądaniem dostępu do jej danych osobowych, ponieważ nie dotyczy ono danych osoby występującej z żądaniem, lecz danych innej osoby – a zatem nie należy go uznawać za żądanie, o którym mowa w art. 15 RODO.

c) Czy zastosowanie mają przepisy inne niż RODO regulujące dostęp do określonej kategorii danych?

47. Osoby, których dane dotyczą, nie muszą określać podstawy prawnej w swoim żądaniu. Jeżeli jednak osoby, których dane dotyczą, wyjaśnią, że podstawę ich żądania stanowią przepisy sektorowe lub krajowe regulujące konkretną kwestię dostępu do określonych kategorii danych, a nie RODO, takie żądanie – w stosownych przypadkach – zostanie rozpatrzone przez administratora zgodnie z takimi

[23] Chyba że żądanie obejmuje również dane nieosobowe nierozerwalnie związane z danymi osobowymi osoby, której dane dotyczą. Dalsze wyjaśnienia znajdują się w pkt 100.

[24] Zob. motyw 26 RODO. Dalsze wyjaśnienia dotyczące pojęć informacji anonimowych i danych spseudonimizowanych można znaleźć w Opinii 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych, s. 18–21.

[25] Grupa Robocza Art. 29, WP242 rev.01, 5 kwietnia 2017 r., Wytyczne dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD (zwane dalej „Wytycznymi Grupy Roboczej Art. 29 dotyczącymi prawa do przenoszenia danych – zatwierdzonymi przez EROD"), s. 9.

[26] Zob. sekcja 3.4 („Żądania składane za pośrednictwem stron trzecich/pełnomocników").

przepisami sektorowymi lub krajowymi. Często, w zależności od odpowiednich przepisów krajowych, administratorzy mogą być zobowiązani do udzielenia oddzielnych odpowiedzi, z których każda dotyczy konkretnych wymogów określonych w poszczególnych aktach ustawodawczych. Nie należy tego mylić z przepisami krajowymi lub przepisami UE ustanawiającymi ograniczenia prawa dostępu, których należy przestrzegać, odpowiadając na żądania dostępu.

48. Jeśli administrator ma wątpliwości co do tego, które prawo chce wykonać osoba, której dane dotyczą, zaleca się zwrócenie się do osoby, której dane dotyczą, występującej z żądaniem o wyjaśnienie przedmiotu tego żądania. Taka korespondencja z osobą, której dane dotyczą, nie wpływa na obowiązek administratora do działania bez zbędnej zwłoki[27]. W przypadku wątpliwości, jeżeli administrator zwróci się do osoby, której dane dotyczą, o przedstawienie dalszych wyjaśnień i nie otrzyma odpowiedzi, mając na uwadze obowiązek ułatwienia wykonania prawa dostępu przysługującego tej osobie, administrator powinien jednak zinterpretować informacje zawarte w pierwszym żądaniu i działać na tej podstawie. Zgodnie z zasadą rozliczalności administrator może określić odpowiednie ramy czasowe, w których osoba, której dane dotyczą, może udzielić dalszych wyjaśnień. Ustalając takie ramy czasowe, administrator powinien pozostawić wystarczająco dużo czasu na spełnienie żądania po jego upływie, a zatem rozważyć, ile czasu jest obiektywnie niezbędne do przygotowania i przekazania żądanych danych po przekazaniu (lub nie) specyfikacji przez osobę, której dane dotyczą.

49. Jeśli żądanie jest objęte zakresem RODO, istnienie tego rodzaju przepisów szczególnych nie powoduje uchylenia ogólnego zastosowania prawa dostępu, jak przewidziano w RODO. Mogą istnieć ograniczenia przewidziane w prawie UE lub w prawie krajowym, o ile pozwala na to art. 23 RODO (zob. sekcja 6.4).

d) Czy żądanie wchodzi w zakres *art. 15?*

50. Należy zauważyć, że w RODO nie wprowadza się żadnych formalnych wymogów dla osób żądających dostępu do danych. Wyrażenie przez osoby występujące z żądaniem chęci uzyskania informacji na temat tego, które dane osobowe ich dotyczące są przetwarzane przez administratora, jest wystarczającym warunkiem wystąpienia z żądaniem dostępu. Administrator nie może zatem odmówić przekazania danych powołując się na brak wskazania podstawy prawnej żądania, w szczególności na brak konkretnego odniesienia do prawa dostępu lub RODO.

Na przykład wystarczającym warunkiem wystąpienia z żądaniem jest to, aby osoba występująca z żądaniem wskazała, że:

- chce uzyskać dostęp do dotyczących jej danych osobowych;
- wykonuje przysługujące jej prawo dostępu; lub
- chce uzyskać dotyczące jej informacje przetwarzane przez administratora.

Należy pamiętać, że wnioskodawcy mogą nie posiadać wiedzy na temat złożoności przepisów RODO i że zaleca się wyrozumiałość wobec osób wykonujących przysługujące im prawo dostępu, w szczególności gdy wykonują je małoletni. Jak wskazano powyżej, w przypadku jakichkolwiek wątpliwości zaleca się, aby administrator zwrócił się do osoby, której dane dotyczą, o sprecyzowanie przedmiotu żądania.

[27] Więcej informacji na temat terminów znajduje się w sekcji 5.3.

e) <u>Czy osoby, których dane dotyczą, chcą uzyskać dostęp do wszystkich czy do części przetwarzanych informacji na swój temat?</u>

51. Ponadto administrator musi ocenić, czy żądania składane przez osoby występujące z żądaniem odnoszą się do wszystkich czy do części przetwarzanych informacji na ich temat. Wszelkie ograniczenia zakresu żądania do przepisu szczegółowego zawartego w art. 15 RODO dokonane przez osoby, których dane dotyczą, muszą być jasne i jednoznaczne. Na przykład, jeżeli osoby, których dane dotyczą, żądają pełnych „informacji na temat przetwarzanych w odniesieniu do nich danych", administrator powinien założyć, że osoby, których dane dotyczą, zamierzają w pełni wykonać prawa przysługujące im na mocy art. 15 ust. 1–2 RODO. Takie żądanie nie powinno być interpretowane w ten sposób, że osoby, których dane dotyczą, chcą otrzymywać tylko te kategorie danych osobowych, które są przetwarzane i zrzekają się prawa do otrzymywania informacji wymienionych w art. 15 ust. 1 lit. a)–h) RODO. Byłoby inaczej na przykład w sytuacji, gdy osoby, których dane dotyczą, chciałyby, w odniesieniu do wskazywanych danych, mieć dostęp do informacji dotyczących źródła lub pochodzenia danych osobowych lub określonego okresu przechowywania. W takim przypadku administrator może ograniczyć swoją odpowiedź do konkretnych żądanych informacji.

3.1.2 Forma żądania

52. Jak wspomniano wcześniej, w RODO nie nakłada się na osoby, których dane dotyczą, żadnych wymogów dotyczących formy żądania dostępu do danych osobowych. W związku z tym, co do zasady, w RODO nie ustanowiono żadnych wymogów, które osoby, których dane dotyczą, muszą przestrzegać przy wyborze kanału komunikacyjnego, za pośrednictwem którego nawiązują kontakt z administratorem.

53. EROD zachęca administratorów do zapewnienia najbardziej odpowiednich i przyjaznych dla użytkownika kanałów komunikacyjnych zgodnie z art. 12 ust. 2 i art. 25 RODO, aby umożliwić osobie, której dane dotyczą, złożenie skutecznego żądania. Jeżeli jednak osoba, której dane dotyczą, wystąpi z żądaniem za pośrednictwem kanału komunikacyjnego udostępnionego przez administratora[28], który różni się od kanału wskazanego jako preferowany, takie żądanie będzie zasadniczo uznawane za skuteczne, a administrator powinien odpowiednio rozpatrzeć takie żądanie (zob. przykłady poniżej). Administratorzy powinni podjąć wszelkie uzasadnione starania w celu ułatwienia wykonania praw przysługujących osobie, której dane dotyczą (na przykład, gdy osoba, której dane dotyczą, wysyła żądanie dostępu pracownikowi, który jest na urlopie; automatyczna wiadomość informująca osobę, której dane dotyczą, o alternatywnym kanale komunikacyjnym dotyczącym tego żądania może stanowić uzasadnione staranie).

54. Należy zauważyć, że administrator nie jest zobowiązany do podjęcia działań w związku z żądaniem przesłanym na przypadkowy lub nieprawidłowy adres e-mail (lub adres pocztowy), który nie został bezpośrednio wskazany przez administratora, lub na jakikolwiek kanał komunikacyjny, który ewidentnie nie jest przeznaczony do otrzymywania żądań dotyczących praw osoby, której dane dotyczą, jeżeli administrator zapewnił odpowiedni kanał komunikacyjny, z którego może skorzystać osoba, której dane dotyczą.

[28] Może to obejmować na przykład dane komunikacyjne administratora zawarte w komunikatach skierowanych bezpośrednio do osób, których dane dotyczą, lub dane kontaktowe udostępnione publicznie przez administratora, np. w polityce ochrony prywatności administratora lub innych obowiązkowych zastrzeżeniach prawnych administratora (np. dane kontaktowe właściciela lub przedsiębiorstwa na stronie internetowej).

55. Administrator nie jest również zobowiązany do podjęcia działań w związku z żądaniem przesłanym na adres e-mail pracownika administratora, który nie może być zaangażowany w rozpatrywanie żądań dotyczących praw osób, których dane dotyczą (np. kierowców, personelu sprzątającego itp.). Takie żądania nie zostaną uznane za skuteczne, jeżeli administrator w sposób wyraźny zapewnił osobie, której dane dotyczą, odpowiedni kanał komunikacyjny. Jeżeli jednak osoba, której dane dotyczą, wyśle żądanie do pracownika administratora, który został jej przypisany jako osoba wyznaczona do regularnych kontaktów (np. osoba zarządzająca rachunkiem osobistym w banku lub stały konsultant u operatora telefonii komórkowej), takiego kontaktu nie należy traktować jako przypadkowego, a administrator powinien dołożyć wszelkich starań, aby rozpatrzeć takie żądanie, aby można je było przekierować do punktu kontaktowego i odpowiedzieć na nie w terminach przewidzianych w RODO.

56. EROD zaleca jednak, aby administratorzy w ramach dobrej praktyki wprowadzili odpowiednie mechanizmy ułatwiające wykonywanie praw przysługujących osobom, których dane dotyczą, w tym zapewnili systemy automatycznego powiadamiania o nieobecności pracowników i odpowiednią zastępczą osobę wyznaczoną do kontaktów oraz, w miarę możliwości, mechanizmy usprawniające wewnętrzną komunikację między pracownikami w sprawie żądań otrzymanych przez osoby, które mogą nie być właściwe do rozpatrywania takich żądań.

Przykład 8: Administrator X podaje zarówno na swojej stronie internetowej, jak i w oświadczeniu o ochronie prywatności, dwa adresy e-mail – ogólny adres e-mail administratora: CONTACT@X.COM oraz adres e-mail punktu kontaktowego ds. ochrony danych administratora: QUERIES@X.COM. Ponadto administrator X wskazuje na swojej stronie internetowej, że w celu złożenia jakichkolwiek zapytań lub żądań dotyczących przetwarzania danych osobowych osoby fizyczne powinny skontaktować się z punktem kontaktowym ds. ochrony danych za pośrednictwem podanego adresu e-mail. Osoba, której dane dotyczą, wysyła jednak żądanie na ogólny adres e-mail administratora: CONTACT@X.COM.

W takim przypadku administrator powinien dołożyć wszelkich starań, aby poinformować swoje służby o żądaniu, które zostało wysłane na ogólny adres e-mail, w celu jego przekierowania do punktu kontaktowego ds. ochrony danych i udzielenia na nie odpowiedzi w terminach przewidzianych w RODO. Ponadto administrator nie jest uprawniony do przedłużenia terminu udzielenia odpowiedzi na żądanie tylko dlatego, że osoba, której dane dotyczą, wysłała żądanie na ogólny adres e-mail administratora, a nie na adres e-mail punktu kontaktowego administratora ds. ochrony danych.

Przykład 9: Administrator Y prowadzi sieć klubów fitness. Administrator Y wskazuje na swojej stronie internetowej oraz w oświadczeniu o ochronie prywatności dla klientów klubu fitness, że w celu złożenia jakichkolwiek zapytań lub żądań dotyczących przetwarzania danych osobowych osoby fizyczne powinny skontaktować się z administratorem za pośrednictwem adresu e-mail: QUERIES@Y.COM. Osoba, której dane dotyczą, wysyła jednak żądanie na adres e-mail znajdujący się w szatni, gdzie znajduje się informacja o treści „Jeśli masz zastrzeżenia do czystości tego pomieszczenia, skontaktuj się z nami pod adresem: CLEANERS@Y.COM”, który jest adresem e-mail personelu sprzątającego zatrudnionego przez Y. Personel sprzątający nie odpowiada oczywiście za rozpatrywanie spraw dotyczących wykonywania praw przysługujących osobom, których dane dotyczą – klientów klubu fitness. Chociaż adres e-mail był dostępny na terenie klubu fitness, osoba, której dane dotyczą, nie mogła racjonalnie oczekiwać, że jest to odpowiedni adres kontaktowy do przesyłania takich żądań, ponieważ strona internetowa i oświadczenie o ochronie prywatności zawierały wyraźne informacje na temat kanału komunikacyjnego umożliwiającego wykonanie praw przysługujących osobom, których dane dotyczą.

57. Z dniem otrzymania żądania przez administratora, co do zasady, rozpoczyna się bieg miesięcznego terminu na przekazanie przez administratora informacji o działaniach podjętych w związku z żądaniem zgodnie z art. 12 ust. 3 RODO (dalsze wytyczne dotyczące terminów znajdują się w sekcji 5.3). EROD uważa za dobrą praktykę, aby administratorzy potwierdzali otrzymanie żądań na piśmie, na przykład wysyłając e-maile (lub, w stosownych przypadkach, informacje drogą pocztową) do osób występujących z żądaniem, potwierdzające, że ich żądania zostały otrzymane i że okres jednego miesiąca biegnie od dnia X do dnia Y.

3.2 Identyfikacja i uwierzytelnianie

58. Aby zapewnić bezpieczeństwo przetwarzania danych i zminimalizować ryzyko nieuprawnionego ujawnienia danych osobowych, administrator musi być w stanie ustalić, które dane odnoszą się do osoby, której dane dotyczą (identyfikacja), i potwierdzić tożsamość tej osoby (uwierzytelnienie).

59. Warto przypomnieć, że w sytuacjach, w których cel przetwarzania danych osobowych nie wymaga lub już nie wymaga zidentyfikowania osoby, której dane dotyczą, administrator nie ma obowiązku zachowania informacji w celu identyfikacji wyłącznie po to, by przestrzegać praw osób, których dane dotyczą, również w świetle zasady minimalizacji danych. Sytuacje te reguluje art. 11 ust. 1 RODO.

60. Art. 12 ust. 2 RODO stanowi, że administrator nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać przysługujące jej prawa, chyba że administrator przetwarza dane osobowe w celu, który nie wymaga zidentyfikowania przez niego osoby, której dane dotyczą, i wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą. W takich okolicznościach osoba, której dane dotyczą, może jednak podjąć decyzję o dostarczeniu dodatkowych informacji, które pozwolą ją zidentyfikować (art. 11 ust. 2 RODO)[29].

61. Administrator nie ma obowiązku uzyskania takich dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, aby spełnić żądanie osoby, której dane dotyczą, również w świetle zasady minimalizacji danych. Nie powinien on jednak odmawiać przyjęcia takich dodatkowych informacji od osoby, której dane dotyczą, by ułatwić jej wykonywanie jej praw (motyw 57 RODO).

Przykład 10: X jest administratorem danych przetwarzanych w związku z monitoringiem wizyjnym budynku. Zgodnie z art. 11 ust. 1 RODO administrator nie jest zobowiązany do zidentyfikowania wszystkich osób, które zostały zarejestrowane przez kamerę bezpieczeństwa w ramach monitoringu (cel niewymagający identyfikacji). Administrator otrzymuje żądanie dostępu do danych osobowych od osoby, która twierdzi, że została zarejestrowana w ramach monitoringu wizyjnego administratora. Działania administratora będą zależały od dostarczonych dodatkowych informacji. Jeżeli osoba występująca z żądaniem wskaże konkretny termin (dzień i godzinę), w którym kamery mogły zarejestrować odnośne zdarzenie, prawdopodobne jest, że administrator będzie w stanie dostarczyć takie dane (art. 11 ust. 2 RODO). Jeżeli jednak administrator nie jest w stanie zidentyfikować osoby, której dane dotyczą (np. jeżeli nie ma pewności, że osoba występująca z żądaniem jest w rzeczywistości osobą, której dane dotyczą, lub jeżeli żądanie dotyczy np. długiego okresu nagrań, przy czym administrator nie jest w stanie przetwarzać tak dużej ilości danych), administrator może odmówić podjęcia działań, jeżeli wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą (art. 12 ust. 2 RODO).

[29] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 13.

Przykład 11: Administrator C przetwarza dane osobowe w celu kierowania reklamy behawioralnej do użytkowników sieci. Dane osobowe gromadzone na potrzeby reklamy behawioralnej są zazwyczaj gromadzone za pomocą plików cookie i powiązane z pseudonimicznymi identyfikatorami losowymi. Osoba, której dane dotyczą, Pan X, wykonuje swoje prawo dostępu wobec C za pośrednictwem strony internetowej C. C jest w stanie dokładnie zidentyfikować Pana X, aby wyświetlać reklamę behawioralną skierowaną do osoby, której dane dotyczą, poprzez powiązanie urządzenia końcowego Pana X z jego profilem reklamowym za pomocą plików cookie zapisanych na urządzeniu końcowym. C powinien być również w stanie dokładnie zidentyfikować Pana X, aby udzielić mu dostępu do jego danych osobowych, ponieważ można znaleźć powiązanie między przetwarzanymi danymi a osobą, której dane dotyczą. W związku z tym, biorąc pod uwagę zasady określone w RODO, powyższy przykład nie wchodziłby w zakres art. 11 RODO. Dokładniej rzecz ujmując, w powyższym przykładzie cele C wymagają identyfikacji osób, których dane dotyczą, podczas gdy art. 11 RODO dotyczy przypadku przetwarzania, który nie wymaga identyfikacji, jeżeli administrator nie ma obowiązku przetwarzania danych dodatkowych w rozumieniu art. 11 ust. 1 RODO wyłącznie po to, by zastosować się do RODO. W związku z tym w niektórych przypadkach nie należy żądać żadnych danych dodatkowych w celu umożliwienia osobie, której dane dotyczą, wykonania jej praw.

Jeśli jednak Pan X spróbuje skorzystać ze swojego prawa dostępu za pośrednictwem poczty elektronicznej lub poczty tradycyjnej, wówczas w tym kontekście C nie będzie miał innego wyboru niż zażądanie od Pana X przekazania „dodatkowych informacji" (art. 12 ust. 6 RODO), aby móc zidentyfikować profil reklamowy powiązany z Panem X. W takim przypadku dodatkową informacją będzie identyfikator pliku cookie przechowywany w urządzeniu końcowym Pana X.

62. W przypadku wykazanej niemożności zidentyfikowania osoby, której dane dotyczą (art. 11 RODO), administrator musi w miarę możliwości poinformować o tym osobę, której dane dotyczą, ponieważ administrator udziela odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki, a jeżeli nie zamierza spełnić takich żądań – podaje tego przyczyny. Administrator przekazuje takie informacje tylko „w miarę możliwości", ponieważ może on nie być w stanie przekazać ich osobom, których dane dotyczą, jeżeli ich identyfikacja jest niemożliwa.

63. Zarówno gdy przetwarzanie nie wymaga identyfikacji, jak i gdy jej wymaga, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO).

64. W RODO nie nakłada się żadnych wymogów dotyczących sposobu uwierzytelnienia osoby, której dane dotyczą. W art. 11 i 12 RODO określono jednak warunki wykonywania wszystkich praw osób, których dane dotyczą, w tym prawa dostępu do danych osobowych.

65. Należy pamiętać, że co do zasady administrator nie może żądać większej ilości danych osobowych, niż jest to konieczne do umożliwienia tego uwierzytelnienia, oraz że wykorzystanie takich informacji powinno być ściśle ograniczone do spełnienia żądania osób, których dane dotyczą.

66. Procedury uwierzytelniania często istnieją już między osobami, których dane dotyczą, a administratorami. Administratorzy mogą korzystać z tych procedur uwierzytelniania w celu ustalenia tożsamości osób, których dane dotyczą, żądających swoich danych osobowych lub wykonujących

prawa przyznane na mocy RODO[30]. W przeciwnym razie administratorzy powinni wdrożyć w tym celu procedurę uwierzytelnienia[31].

67. W przypadku gdy administrator żąda dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą, lub otrzymuje takie informacje od osoby, której dane dotyczą, każdorazowo ocenia, jakie informacje umożliwią mu potwierdzenie tożsamości osoby, której dane dotyczą, i ewentualnie zadaje dodatkowe pytania osobie występującej z żądaniem, lub żąda od osoby, której dane dotyczą, przedstawienia dodatkowych elementów umożliwiających jej identyfikację, jeżeli jest to proporcjonalne (zob. sekcja 3.3).

68. Aby umożliwić osobie, której dane dotyczą, dostarczenie dodatkowych informacji wymaganych do zidentyfikowania jej danych, administrator powinien poinformować osobę, której dane dotyczą, o charakterze dodatkowych informacji wymaganych do identyfikacji. Takie dodatkowe informacje nie powinny wykraczać poza informacje początkowo potrzebne do uwierzytelnienia osoby, której dane dotyczą. Co do zasady możliwość żądania przez administratora danych dostarczenia dodatkowych informacji w celu oceny tożsamości osoby, której dane dotyczą, nie może prowadzić do nadmiernych żądań oraz do gromadzenia danych osobowych, które nie są istotne lub niezbędne do wzmocnienia powiązania między tą osobą fizyczną a danymi osobowymi objętymi żądaniem[32].

69. W związku z tym w przypadku gdy informacje gromadzone online są powiązane z pseudonimami lub innymi unikatowymi identyfikatorami, administrator może wdrożyć odpowiednie procedury umożliwiające osobie występującej z żądaniem wystosowanie żądania dostępu do danych i otrzymanie odnoszących się do niej danych[33].

Przykład 12: Osoba, której dane dotyczą, Pani X, żąda dostępu do swoich danych podczas rozmowy z konsultantem infolinii przedsiębiorstwa energetycznego, z którym zawarła umowę. Konsultant, mając wątpliwości co do tożsamości osoby występującej z żądaniem, generuje w systemie przedsiębiorstwa jednorazowy unikatowy kod wysłany na numer telefonu komórkowego użytkownika, podany przy zakładaniu konta, w ramach systemu podwójnej weryfikacji, które to działanie należy w tym przypadku uznać za proporcjonalne.

3.3 Ocena proporcjonalności w odniesieniu do uwierzytelnienia osoby występującej z żądaniem

70. Jak wskazano powyżej, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby występującej z żądaniem, może zażądać dodatkowych informacji w celu potwierdzenia tożsamości osoby, której dane dotyczą. Administrator musi jednak jednocześnie dbać o to, by nie gromadzić większej ilości danych osobowych, niż jest to konieczne do umożliwienia uwierzytelnienia osoby występującej z żądaniem. W związku z tym administrator przeprowadza ocenę proporcjonalności, która musi uwzględniać rodzaj przetwarzanych danych osobowych (np. szczególne kategorie danych lub ich brak), charakter żądania, kontekst, w jakim żądanie jest składane, a także wszelkie szkody, które

[30] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 14.
[31] Więcej informacji na temat uwierzytelniania znajduje się w sekcji 3.3.
[32] *Ibidem*, s. 14.
[33] *Ibidem*, s. 13–14.

mogłyby wyniknąć z niewłaściwego ujawnienia. Przy ocenie proporcjonalności należy pamiętać, aby unikać nadmiernego gromadzenia danych przy jednoczesnym zapewnieniu odpowiedniego poziomu bezpieczeństwa przetwarzania.

71. Administrator powinien wdrożyć procedurę uwierzytelniania w celu uzyskania pewności co do tożsamości osób żądających dostępu do swoich danych[34] oraz zapewnić bezpieczeństwo przetwarzania podczas całego procesu rozpatrywania żądań dostępu zgodnie z art. 32 RODO, w tym na przykład bezpieczny kanał przekazywania dodatkowych informacji przez osoby, których dane dotyczą. Metoda stosowana do uwierzytelniania powinna być odpowiednia, stosowna, proporcjonalna i zgodna z zasadą minimalizacji danych. Jeżeli administrator nakłada środki służące uwierzytelnieniu osoby, której dane dotyczą, które są uciążliwe, musi to odpowiednio uzasadnić i zapewnić zgodność ze wszystkimi podstawowymi zasadami, w tym minimalizacją danych i obowiązkiem ułatwienia osobom, których dane dotyczą, wykonywania ich praw (art. 12 ust. 2 RODO).

72. W kontekście internetowym mechanizm uwierzytelniania może obejmować te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora (motyw 57 RODO)[35].

73. W praktyce procedury uwierzytelniania często istnieją i administratorzy nie muszą wprowadzać dodatkowych zabezpieczeń, aby zapobiec nieuprawnionemu dostępowi do usług. Aby umożliwić osobom fizycznym dostęp do danych zawartych na ich kontach (takich jak konto e-mail, konta na portalach społecznościowych lub konta w sklepach internetowych), administratorzy najprawdopodobniej zażądają zalogowania się za pomocą loginu i hasła użytkownika, co w takich przypadkach powinno wystarczyć do uwierzytelnienia osoby, której dane dotyczą[36]. Co więcej, osoby, których dane dotyczą, często zostają już uwierzytelnione przez administratora przed zawarciem umowy lub uzyskaniem ich zgody na przetwarzanie, w związku z czym dane osobowe wykorzystywane do rejestracji osoby, której dotyczy przetwarzanie, można również wykorzystać jako dowód w celu uwierzytelnienia osoby, której dane dotyczą, do celów dostępu[37]. W związku z tym wymaganie kopii dokumentu tożsamości jest nieproporcjonalne, w przypadku gdy występująca z żądaniem osoba, której dane dotyczą, została już uwierzytelniona przez administratora.

74. Należy podkreślić, że wykorzystanie kopii dokumentu tożsamości jako części procesu uwierzytelniania stwarza ryzyko dla bezpieczeństwa danych osobowych i może prowadzić do nieuprawnionego lub niezgodnego z prawem przetwarzania i jako takie należy je uznać za niewłaściwe, chyba że jest to konieczne, odpowiednie i zgodne z prawem krajowym. W takich przypadkach administratorzy powinni dysponować systemami zapewniającymi odpowiedni poziom bezpieczeństwa, aby ograniczyć wyższe ryzyko dla praw i wolności osoby, której dane dotyczą, w celu otrzymywania takich danych. Należy również zauważyć, że uwierzytelnienie za pomocą dowodu tożsamości niekoniecznie jest pomocne

[34] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 14.

[35] Zob. dalsze wskazówki dotyczące metod uwierzytelniania w Wytycznych EROD 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych, przyjętych w dniu 14 stycznia 2021 r., s. 30-31, oraz w Wytycznych EROD 02/2021 w sprawie wirtualnych asystentów głosowych, wersja 2.0, przyjętych w dniu 7 lipca 2021 r., sekcja 3.7.

[36] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 14.

[37] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 14.

w kontekście internetowym (np. w przypadku użycia pseudonimów), jeżeli dana osoba nie może przedstawić żadnych innych dowodów, np. dalszych atrybutów odpowiadających kontu użytkownika.

75. Biorąc pod uwagę fakt, że wiele organizacji (np. hotele, banki, wypożyczalnie samochodów) żąda kopii dowodu tożsamości swoich klientów, metody tej zasadniczo nie należy uznawać za odpowiedni sposób uwierzytelnienia. Ewentualnie administrator może wdrożyć szybki i skuteczny środek bezpieczeństwa w celu zidentyfikowania osoby, której dane dotyczą, na podstawie uprzednio przeprowadzonego uwierzytelnienia, np. za pośrednictwem wiadomości e-mail lub wiadomości tekstowej zawierającej linki potwierdzające, pytania zabezpieczające lub kody potwierdzające[38].

76. Informacje na dowodzie tożsamości, które nie są niezbędne do potwierdzenia tożsamości osoby, której dane dotyczą, takie jak numer dostępu i numer seryjny, obywatelstwo, rozmiar, kolor oczu, zdjęcie i pole przeznaczone do odczytu maszynowego, w zależności od indywidualnej oceny każdego przypadku, mogą zostać utajnione lub ukryte przez osobę, której dane dotyczą, przed przekazaniem ich administratorowi, z wyjątkiem przypadków, w których przepisy krajowe wymagają kopii dowodu tożsamości bez informacji utajnionych (zob. pkt 78 poniżej). Zasadniczo data wydania lub data wygaśnięcia, organ wydający oraz pełne imię i nazwisko, które odpowiadają informacjom na koncie internetowym, są wystarczające, aby administrator mógł zweryfikować tożsamość, zawsze pod warunkiem zapewnienia autentyczności kopii i związku z osobą występującą z żądaniem. Dodatkowe informacje, takie jak data urodzenia osoby, której dane dotyczą, mogą być wymagane jedynie w przypadku utrzymującego się ryzyka pomylenia tożsamości, jeżeli administrator jest w stanie porównać je z informacjami, które już przetwarza.

77. Aby przestrzegać zasady minimalizacji danych, administrator powinien poinformować osobę, której dane dotyczą, o tym, które informacje nie są potrzebne, oraz o możliwości utajnienia lub ukrycia tych części dokumentu tożsamości. W takim przypadku jeśli osoba, której dane dotyczą, nie wie, w jaki sposób utajnić takie informacje, lub nie jest w stanie tego zrobić, dobrą praktyką jest, aby administrator utajnił je po otrzymaniu dokumentu, jeżeli ma taką możliwość, biorąc pod uwagę środki, którymi dysponuje w danych okolicznościach.

Przykład 13: Użytkowniczka, Pani Y, utworzyła konto chronione hasłem w sklepie internetowym, podając swój adres e-mail lub identyfikator użytkownika. Następnie właścicielka konta zwraca się do administratora o udzielenie informacji, czy przetwarza jej dane osobowe, a jeśli tak, żąda dostępu do nich w zakresie określonym w art. 15. Administrator zwraca się o dokument tożsamości do osoby występującej z żądaniem w celu potwierdzenia jej tożsamości. Działanie administratora w tym przypadku jest nieproporcjonalne i prowadzi do niepotrzebnego gromadzenia danych.

Aby jednak potwierdzić tożsamość osoby występującej z żądaniem, a jednocześnie zapobiec niepotrzebnemu gromadzeniu danych, administrator może wymagać od niej uwierzytelnienia poprzez zalogowanie się na konto lub zadać jej (nieinwazyjne) pytania zabezpieczające, na które odpowiedź powinna znać wyłącznie osoba, której dane dotyczą, lub użyć uwierzytelniania wieloskładnikowego, które zostało skonfigurowane, gdy osoba, której dane dotyczą, zarejestrowała swoje konto, lub skorzystać z innych istniejących środków komunikacji, o których wiadomo, że należą do osoby, której dane dotyczą, takich jak adres e-mail lub numer telefonu, w celu wysłania hasła dostępu.

[38]Zob. również rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, w którym wprowadzono różne usługi umożliwiające bezpieczną identyfikację na odległość.

Przykład 14: Klient banku, Pan Y, planuje uzyskać kredyt konsumencki. W tym celu Pan Y udaje się do oddziału banku w celu uzyskania informacji, w tym swoich danych osobowych, niezbędnych do oceny jego zdolności kredytowej. Aby zweryfikować tożsamość osoby, której dane dotyczą, konsultant zwraca się o notarialne poświadczenie jej tożsamości, aby móc udzielić jej żądanych informacji.

Administrator nie powinien wymagać notarialnego poświadczenia tożsamości, chyba że jest to konieczne, odpowiednie i zgodne z prawem krajowym (na przykład gdy dana osoba tymczasowo nie ma żadnego dokumentu tożsamości, a w prawie krajowym do dokonania czynności prawnej wymaga się dowodu tożsamości osoby, której dane dotyczą). Taka praktyka naraża osoby występujące z żądaniem na dodatkowe koszty i prowadzi do nadmiernego obciążenia osób, których dane dotyczą, utrudniając im korzystanie z przysługującego im prawa dostępu.

78. Bez uszczerbku dla powyższych zasad ogólnych, w określonych okolicznościach uwierzytelnienie na podstawie dowodu tożsamości może być uzasadnionym i proporcjonalnym środkiem, w szczególności dla podmiotów przetwarzających szczególne kategorie danych osobowych lub prowadzących przetwarzanie danych, które może stwarzać ryzyko dla osoby, której dane dotyczą (np. informacje medyczne lub zdrowotne). Jednocześnie należy jednak pamiętać, że niektóre przepisy krajowe przewidują ograniczenia przetwarzania danych zawartych w dokumentach urzędowych, w tym dokumentach potwierdzających tożsamość osoby (również na podstawie art. 87 RODO). Ograniczenia w przetwarzaniu danych pochodzących z tych dokumentów mogą dotyczyć w szczególności skanowania dowodów tożsamości lub sporządzania ich fotokopii lub przetwarzania oficjalnych osobistych numerów identyfikacyjnych[39].

79. Biorąc pod uwagę powyższe, w przypadku gdy administrator żąda dowodu tożsamości (i jest to zarówno zgodne z prawem krajowym, jak i uzasadnione i proporcjonalne zgodnie z RODO), musi on wdrożyć zabezpieczenia zapobiegające niezgodnemu z prawem przetwarzaniu tego dowodu. Niezależnie od obowiązujących przepisów krajowych dotyczących uwierzytelniania dowodu tożsamości, może to obejmować rezygnację ze sporządzenia kopii lub usunięcie kopii dowodu tożsamości natychmiast po pomyślnym uwierzytelnieniu tożsamości osoby, której dane dotyczą. Wynika to z faktu, że dalsze przechowywanie kopii dowodu tożsamości może stanowić naruszenie zasad ograniczenia celu i ograniczenia przechowywania (art. 5 ust. 1 lit. b) i e) RODO), a ponadto przepisów krajowych dotyczących przetwarzania krajowego numeru identyfikacyjnego (art. 87 RODO). EROD zaleca jako dobrą praktykę aby administrator, po sprawdzeniu dowodu tożsamości, sporządził notatkę, np. „sprawdzono dowód tożsamości", aby uniknąć niepotrzebnego kopiowania lub przechowywania kopii dowodów tożsamości.

3.4 Żądania składane za pośrednictwem stron trzecich/pełnomocników

80. Chociaż prawo dostępu jest zasadniczo wykonywane przez osoby, których dane dotyczą, ponieważ to prawo im przysługuje, możliwe jest, aby strona trzecia wystąpiła z żądaniem w imieniu osoby, której dane dotyczą. Może to dotyczyć m.in. działania za pośrednictwem pełnomocnika lub opiekunów prawnych w imieniu małoletnich, a także działania za pośrednictwem innych podmiotów

[39] Szereg państw członkowskich wprowadziło takie ograniczenie w swoich przepisach krajowych w tym zakresie, przewidując na przykład, że sporządzanie kopii dowodów tożsamości jest zgodne z prawem wyłącznie wówczas, gdy wynika to bezpośrednio z przepisów aktu prawnego.

z wykorzystaniem portali internetowych. W pewnych okolicznościach tożsamość osoby upoważnionej do wykonywania prawa dostępu, jak również upoważnienie do działania w imieniu osoby, której dane dotyczą, mogą wymagać weryfikacji, jeżeli jest to odpowiednie i proporcjonalne (zob. sekcja 3.3 powyżej)[40]. Należy przypomnieć, że udostępnienie danych osobowych osobie, która nie jest uprawniona do dostępu do nich, może stanowić naruszenie ochrony danych osobowych[41].

81. Należy przy tym uwzględnić przepisy krajowe regulujące zastępstwo prawne (np. pełnomocnictwo), które mogą nakładać szczególne wymogi dotyczące wykazania upoważnienia do wystąpienia z żądaniem w imieniu osoby, której dane dotyczą, ponieważ RODO nie reguluje tej kwestii. Zgodnie z zasadą rozliczalności, jak również z pozostałymi zasadami ochrony danych, administratorzy muszą być w stanie wykazać istnienie odpowiedniego upoważnienia do wystąpienia z żądaniem w imieniu osoby, której dane dotyczą, oraz do otrzymania żądanych informacji, chyba że prawo krajowe stanowi inaczej (np. prawo krajowe zawiera przepisy szczególne dotyczące statusu adwokata jako zawodu zaufania publicznego) i nakłada na administratora obowiązek zweryfikowania tożsamości pełnomocnika (np. w przypadku adwokatów – sprawdzenia wpisu na listę adwokatów). Zaleca się zatem gromadzenie odpowiedniej dokumentacji w tym zakresie w związku z wcześniej wskazanymi ogólnymi zasadami dotyczącymi potwierdzania tożsamości osoby fizycznej występującej z żądaniem, a jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby działającej w imieniu osoby, której dane dotyczą, zwraca się o dodatkowe informacje w celu potwierdzenia tożsamości tej osoby.

82. Korzystanie z prawa dostępu do danych osobowych osób zmarłych stanowi inny przykład dostępu strony trzeciej innej niż osoba, której dane dotyczą, jednak w motywie 27 określono, że RODO nie ma zastosowania do danych osobowych osób zmarłych. Kwestia ta jest zatem uregulowana w prawie krajowym – państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych. Należy jednak pamiętać, że dane te mogą ponadto odnosić się do żyjących osób trzecich, np. w kontekście żądanego dostępu do korespondencji osoby zmarłej. Poufność takich danych nadal wymaga ochrony.

3.4.1 Wykonywanie prawa dostępu w imieniu dzieci

83. Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych[42]. Wszelkie informacje i komunikaty kierowane do dziecka – w przypadku przetwarzania danych osobowych dziecka – powinny być sformułowane jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć[43].

84. Dzieci mają niezależny status osób, których dane dotyczą, w związku z czym to dziecku przysługuje prawo dostępu. W zależności od stopnia dojrzałości i zdolności dziecka może ono potrzebować strony trzeciej, aby działała w jego imieniu, np. osoby posiadającej odpowiedzialność rodzicielską.

[40] W odniesieniu do terminów wykonania prawa dostępu, w przypadku gdy administrator musi uzyskać dodatkowe informacje, zob. pkt 157.
[41] Art. 4 pkt 12 RODO.
[42] Motyw 38 RODO. Jak przewidziano w programie prac EROD, jej zamiarem jest zapewnienie wytycznych na temat danych dotyczących dzieci. Oczekuje się, że taki dokument zapewni więcej wskazówek na temat warunków, na jakich dziecko może wykonywać własne prawo dostępu, a osoba posiadająca odpowiedzialność rodzicielską może korzystać z prawa dostępu w imieniu dziecka.
[43] Motyw 58 RODO. Wytyczne 05/2020 EROD dotyczące zgody na mocy rozporządzenia 2016/679; sekcja 7.

85. Przy podejmowaniu wszelkich decyzji dotyczących wykonywania prawa dostępu w kontekście dzieci, w szczególności gdy prawo dostępu jest wykonywane w imieniu dziecka, na przykład przez osobę sprawującą władzę rodzicielską, należy kierować się przede wszystkim dobrem dziecka.

86. Ze względu na szczególną ochronę danych osobowych dzieci zawartą w RODO administrator wdraża odpowiednie środki w celu uniknięcia ujawnienia danych osobowych małoletniego osobie nieupoważnionej (zob. w tym zakresie również sekcja 3.4 powyżej).

87. Prawa osoby posiadającej odpowiedzialność rodzicielską do działania w imieniu dziecka nie należy ponadto mylić z przypadkami, które nie są objęte przepisami w dziedzinie ochrony danych, w których przepisy krajowe mogą przewidywać prawo osoby posiadającej odpowiedzialność rodzicielską do żądania i otrzymywania informacji na temat dziecka (np. na temat wyników dziecka w szkole).

3.4.2 Korzystanie z prawa dostępu za pośrednictwem portali internetowych/kanałów udostępnionych przez stronę trzecią

88. Istnieją przedsiębiorstwa świadczące usługi umożliwiające osobom, których dane dotyczą, występowanie z żądaniami dostępu za pośrednictwem portalu internetowego. Osoba, której dane dotyczą, rejestruje się i uzyskuje dostęp do portalu, za pośrednictwem którego może na przykład wystąpić do różnych administratorów z żądaniem dostępu, żądaniem sprostowania danych lub żądaniem usunięcia danych. W związku z korzystaniem z portali udostępnianych przez stronę trzecią pojawiają się różne wątpliwości.

89. Pierwszą kwestią, którą administratorzy muszą się zająć w takich okolicznościach, jest zapewnienie, by strona trzecia działała zgodnie z prawem w imieniu osoby, której dane dotyczą, ponieważ konieczne jest upewnienie się, że żadne dane nie zostaną ujawnione nieupoważnionym stronom.

90. Ponadto administrator, który otrzymuje żądanie złożone za pośrednictwem takiego portalu, musi zawsze rozpatrzyć to żądanie w odpowiednim czasie[44]. Administrator nie ma jednak obowiązku przekazywania danych na podstawie art. 15 RODO bezpośrednio do portalu internetowego, jeżeli na przykład administrator stwierdzi, że środki bezpieczeństwa są niewystarczające, lub jeżeli uznano by za właściwe skorzystanie z innego sposobu ujawnienia danych osobie, której dane dotyczą. W takich okolicznościach, jeżeli administrator dysponuje innymi procedurami umożliwiającymi skuteczne i bezpieczne rozpatrywanie żądań dostępu, może przekazać żądane informacje w ramach tych procedur.

4 ZAKRES PRAWA DOSTĘPU ORAZ DANE OSOBOWE I INFORMACJE, DO KTÓRYCH SIĘ ONO ODNOSI

91. Niniejsza sekcja ma na celu wyjaśnienie definicji danych osobowych (sekcja 4.1) oraz zakresu informacji objętych prawem dostępu w ujęciu ogólnym (sekcje 4.2 i 4.3). Należy zauważyć, że zakres pojęcia danych osobowych, a tym samym rozróżnienie danych osobowych i innych danych, stanowi integralną

[44] W odniesieniu do terminów wykonania prawa dostępu, w przypadku gdy administrator musi uzyskać dodatkowe informacje, zob. pkt 157.

część oceny przeprowadzanej przez administratora w celu określenia zakresu danych, do których osoba, której dane dotyczą, ma prawo uzyskać dostęp[45].

92. Na wstępie należy przypomnieć, że prawo dostępu może być wykonywane wyłącznie w odniesieniu do przetwarzania danych osobowych objętych materialnym i terytorialnym zakresem stosowania RODO. W związku z tym dane osobowe, które nie są przetwarzane w sposób zautomatyzowany lub które nie są częścią zbioru danych lub które nie mają stać się częścią zbioru danych zgodnie z art. 2 ust. 1 RODO, lub dane osobowe przetwarzane przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze zgodnie z art. 2 ust. 2 RODO, nie są objęte prawem dostępu.

4.1 Definicja danych osobowych

93. Art. 15 ust. 1 i 3 RODO odnoszą się odpowiednio do „danych osobowych" i „danych osobowych podlegających przetwarzaniu". W związku z tym zakres prawa dostępu jest uwarunkowany przede wszystkim zakresem pojęcia danych osobowych w rozumieniu art. 4 pkt 1 RODO[46]. Pojęcie danych osobowych było już przedmiotem szeregu dokumentów[47] Grupy Roboczej Art. 29[48] i zostało zinterpretowane przez TSUE, w tym w kontekście prawa dostępu przewidzianego w art. 12 dyrektywy 95/46/WE.

94. Grupa Robocza Art. 29 uznała, że definicja danych osobowych zawarta w dyrektywie 95/46/WE „jest ze strony prawodawcy europejskiego wyrazem woli przyjęcia szerokiej koncepcji »danych osobowych«"[49]. Zgodnie z RODO definicja ta nadal odnosi się do „wszelkich informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej". Poza podstawowymi danymi osobowymi, takimi jak imię i nazwisko oraz adres, numer telefonu itp., definicja ta może obejmować nieograniczoną liczbę różnych danych, w tym informacje medyczne, historię zakupów, wskaźniki zdolności kredytowej, treść komunikacji itp. W świetle szerokiego zakresu definicji danych osobowych zawężająca ocena tej definicji przez administratora doprowadziłaby do błędnej klasyfikacji danych osobowych[50], a ostatecznie do naruszenia prawa dostępu.

---

[45] Zgodnie z zasadą uwzględniania ochrony prywatności już w fazie projektowania taka analiza stanowi część oceny odpowiednich środków i zabezpieczeń mających na celu ochronę zasad ochrony danych i praw osób, których dane dotyczą, którą przeprowadza się „zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania", np. skrócenie czasu reakcji, gdy osoby, których dane dotyczą, korzystają ze swoich praw, może być jednym ze wskaźników. Dalsze wyjaśnienia znajdują się w Wytycznych nr 4/2019 dotyczących art. 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych".

[46] Zgodnie z art. 4 pkt 1 RODO „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;".

[47] Grupa Robocza Art. 29 to niezależna europejska grupa robocza, która zajmowała się kwestiami związanymi z ochroną prywatności i danych osobowych do 25 maja 2018 r. (rozpoczęcie stosowania RODO), poprzedniczka EROD.

[48] Np. Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, WP251 rev.01, s. 19; Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 9.

[49] Opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych, s. 4.

[50] jako informacje nieodnoszące się do określonej lub możliwej do zidentyfikowania osoby fizycznej.

95. We sprawach połączonych C-141/12 i C-372/12[51] TSUE orzekł, że prawo dostępu obejmuje dane osobowe zawarte w memorandum, a mianowicie „nazwisko, datę urodzenia, obywatelstwo, płeć, pochodzenie etniczne, religię i język wnioskodawcy" oraz „w stosownym przypadku dane figurujące w analizie prawnej zawartej w tym memorandum", ale nie samą analizę prawną[52]. W tym kontekście analiza prawna nie mogła sama w sobie być przedmiotem weryfikacji pod względem jej prawidłowości przez osobę, której dane dotyczą, ani sprostowania. Ponadto zapewnienie dostępu do analizy prawnej nie spełnia celu, jakim jest zagwarantowanie prywatności, lecz cel dotyczący zapewnienia dostępu do dokumentów administracyjnych.

96. W sprawie Nowak[53] TSUE dokonał szerszej analizy i stwierdził, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego oraz wszelkie naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe dotyczące osoby przystępującej do egzaminu. Dokładniej rzecz ujmując, takie subiektywne informacje są danymi osobowymi „w postaci opinii czy oceny, a jedynym warunkiem, które muszą one spełniać, jest to, aby »dotyczyły« danej osoby"[54], w przeciwieństwie do pytań egzaminacyjnych, które nie są uważane za dane osobowe[55]. W związku z tym ocena kontekstowa powinna wyjaśniać wpływ lub skutek, jaki dana informacja może mieć na osobę fizyczną, a tym samym na zakres prawa dostępu.

Przykład 15: Osoba fizyczna odbywa rozmowę kwalifikacyjną w przedsiębiorstwie. W tym kontekście kandydat ten przekazuje swoje CV i list motywacyjny. Podczas rozmowy pracownik działu kadr sporządza notatki na komputerze, aby udokumentować jej przebieg. Następnie kandydat, jako osoba, której dane dotyczą, żąda dostępu do dotyczących go danych osobowych, które przedsiębiorstwo, jako administrator, gromadzi w trakcie procedury rekrutacyjnej.

Administrator jest zobowiązany do przekazania osobie, której dane dotyczą, danych osobowych aktywnie przekazanych przez nią w CV i liście motywacyjnym. Administrator musi ponadto udostępnić osobie, której dane dotyczą, podsumowanie rozmowy, w tym subiektywne uwagi na temat zachowania tej osoby, które pracownik działu kadr ludzkich odnotował podczas rozmowy kwalifikacyjnej, z zastrzeżeniem wszelkich wyłączeń na mocy prawa krajowego i zgodnie z art. 23 RODO.

97. W związku z tym, z zastrzeżeniem konkretnych okoliczności danej sprawy, przy ocenie konkretnego żądania dostępu administratorzy przekazują między innymi następujące rodzaje danych, bez uszczerbku dla art. 15 ust. 4 RODO:

- szczególne kategorie danych osobowych zgodnie z art. 9 RODO;
- dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10 RODO;
- dane świadomie i aktywnie dostarczone przez osobę, której dane dotyczą (np. dane dotyczące konta przekazywane za pośrednictwem formularzy, odpowiedzi na pytania zawarte w kwestionariuszu)[56];

[51] TSUE, sprawy połączone C-141/12 i C-372/12, YS/Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel/M i S, 17 lipca 2014 r.
[52] TSUE, sprawy połączone C-141/12 i C-372/12, YS i in., pkt 38 i 48.
[53] TSUE, C-434/16, Peter Nowak/Data Protection Commissioner, 20 grudnia 2017 r.
[54] TSUE, C 434/16, Nowak, pkt 34–35.
[55] TSUE, C-434/16, Nowak, pkt 58.
[56] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 9.

- dane zaobserwowane lub surowe dane dostarczone przez osobę, której dane dotyczą, w związku z korzystaniem z usługi lub urządzenia (np. dane przetwarzane przez przedmioty podłączone do internetu, historia transakcji, dzienniki aktywności, takie jak dzienniki dostępu, historia korzystania ze strony internetowej, operacje wyszukiwania, dane dotyczące lokalizacji, aktywność związana z klikaniem, unikalne aspekty zachowania danej osoby, takie jak pismo odręczne, uderzenia w klawisze, szczególny sposób chodzenia lub mówienia)[57];
- dane wywiedzione z innych danych, a nie bezpośrednio przekazane przez osobę, której dane dotyczą (np. ocena kredytowa, klasyfikacja oparta na wspólnych atrybutach osób, których dane dotyczą, państwo zamieszkania wywnioskowane na podstawie kodu pocztowego)[58];
- dane wywnioskowane z innych danych, a nie bezpośrednio przekazane przez osobę, której dane dotyczą (np. w celu przypisania punktów w ramach punktowej oceny kredytowej lub przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy, wyniki algorytmiczne, wyniki oceny stanu zdrowia lub dane uzyskane w procesie personalizacji lub rekomendacji)[59];
- Dane spseudonimizowane w przeciwieństwie do danych zanonimizowanych (zob. również sekcja 3 niniejszych wytycznych).

Przykład 16: Elementy, które wykorzystano do podjęcia decyzji np. o awansie pracownika, podwyżce wynagrodzenia lub przydzieleniu nowego stanowiska (np. roczne przeglądy wyników, wnioski o szkolenia, rejestry dyscyplinarne, ranking, potencjał zawodowy), to dane osobowe dotyczące tego pracownika. Osoba, której dane dotyczą, może zatem uzyskać dostęp do takich elementów na żądanie i z poszanowaniem art. 15 ust. 4 RODO, na przykład w przypadku gdy dane osobowe odnoszą się również do innej osoby fizycznej (np. dane dotyczące tożsamości lub elementy ujawniające tożsamość innego pracownika, którego opinia dotycząca wyników zawodowych jest zawarta w rocznym przeglądzie wyników, mogą podlegać ograniczeniom zgodnie z art. 15 ust. 4 RODO, a zatem możliwe jest, że nie będzie można ich przekazać osobie, której dane dotyczą, w celu ochrony praw i wolności tego pracownika). Zastosowanie mogą mieć jednak krajowe przepisy prawa pracy, na przykład w odniesieniu do dostępu pracowników do akt osobowych, lub inne przepisy krajowe, takie jak przepisy dotyczące tajemnicy zawodowej. We wszystkich okolicznościach takie ograniczenia w korzystaniu przez osobę, której dane dotyczą, z prawa dostępu (lub innych praw), przewidziane w prawie krajowym, muszą być zgodne z warunkami określonymi w art. 23 RODO (zob. sekcja 6.4).

98. Z powyższego niewyczerpującego wykazu danych osobowych, które mogą zostać przekazane osobie, której dane dotyczą, w kontekście żądania dostępu, można wyciągnąć szereg wniosków. Z powyższego wynika, że administrator nie może dokonywać rozróżnienia przy udzielaniu dostępu do danych osobowych między danymi zawartymi w aktach papierowych a danymi przechowywanymi elektronicznie, o ile są one objęte zakresem stosowania RODO. Innymi słowy, dane osobowe, które są zawarte w aktach papierowych jako część zbioru danych lub które mają stanowić część zbioru danych,

[57] Opinia 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych, s. 8.
[58] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 10–11.
[59] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 10–11; Grupa Robocza Art. 29, WP 251 rev.01, 6 lutego 2018 r., Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679 – zatwierdzone przez EROD (zwane dalej „Wytycznymi Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania – zatwierdzonymi przez EROD"), s. 9–10.

są objęte prawem dostępu w taki sam sposób jak dane osobowe przechowywane w pamięci komputera, na przykład za pomocą kodu binarnego lub nagrania wideo.

99. Ponadto, podobnie jak większość praw osób, których dane dotyczą, prawo dostępu obejmuje zarówno dane wywnioskowane, jak i wywiedzione, w tym dane osobowe stworzone przez dostawcę usług, podczas gdy prawo do przenoszenia danych obejmuje wyłącznie dane dostarczone przez osobę, której dane dotyczą[60]. W związku z tym w przypadku żądania dostępu i w przeciwieństwie do żądania przeniesienia danych osoba, której dane dotyczą, powinna otrzymać nie tylko dane osobowe przekazane administratorowi w celu dokonania późniejszej analizy lub oceny tych danych, ale również wynik takiej późniejszej analizy lub oceny.

100. Należy również przypomnieć, że istnieją informacje, takie jak informacje anonimowe[61], które są danymi nieodnoszącymi się bezpośrednio ani pośrednio do osoby możliwej do zidentyfikowania, a zatem są wyłączone z zakresu stosowania RODO. Na przykład lokalizacja serwera, na którym przetwarzane są dane osobowe osoby, której dane dotyczą, nie stanowi danych osobowych. Rozróżnienie to może być trudne, dlatego administratorzy mogą zadawać sobie pytanie, w jaki sposób można wyraźnie rozgraniczyć dane osobowe i nieosobowe, w szczególności w przypadku mieszanych zbiorów danych. W takim przypadku użyteczne może być rozróżnienie między mieszanymi zbiorami danych, w których dane osobowe i nieosobowe są nierozerwalnie powiązane, a tymi, w których nie ma to miejsca. Dane osobowe i nieosobowe mogą być nierozerwalnie ze sobą powiązane w mieszanych zbiorach danych i w całości wchodzić w zakres prawa dostępu osoby, której dane dotyczą, do której odnoszą się dane osobowe[62]. W innych przypadkach dane osobowe i nieosobowe w mieszanych zbiorach danych mogą nie być nierozerwalnie ze sobą powiązane, co sprawia, że jedynie dane osobowe znajdujące się w zbiorze są dostępne dla osoby, której dane dotyczą. Na przykład spółka może być zobowiązana do przekazania osobie, której dane dotyczą, indywidualnych zgłoszeń incydentów informatycznych, które wywołała, ale nie bazy wiedzy tej spółki na temat problemów informatycznych. Środków bezpieczeństwa wprowadzonych przez administratora zasadniczo nie należy jednak rozumieć jako danych osobowych, pod warunkiem że nie są one nierozerwalnie powiązane z danymi osobowymi, w związku z czym nie są one objęte prawem dostępu.

101. Przed zakończeniem tej sekcji EROD przypomina w tym kontekście, że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych obejmuje wszystkie rodzaje danych osobowych wymienione powyżej oraz że zawężająca wykładnia ich definicji jest sprzeczna z przepisami RODO i ostatecznie narusza art. 8 Karty praw podstawowych. Stosowanie odmiennego systemu wykonywania prawa w odniesieniu do niektórych rodzajów danych osobowych, którego nie przewidziano w RODO, można wprowadzić wyłącznie na mocy prawa, zgodnie z art. 23 RODO (jak wyjaśniono bardziej szczegółowo w sekcji 6.4). Administratorzy nie mogą zatem ograniczać wykonywania prawa dostępu poprzez nieuzasadnione ograniczanie zakresu danych osobowych.

[60] Jak stwierdzono wcześniej w Wytycznych Grupy Roboczej Art. 29 dotyczących prawa do przenoszenia danych – zatwierdzonych przez EROD, s. 10, i powtórzono w Wytycznych Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania – zatwierdzonych przez EROD, s. 17.

[61] Dalsze wyjaśnienia dotyczące pojęcia anonimizacji można znaleźć w Opinii 05/2014 Grupy Roboczej Art. 29 w sprawie technik anonimizacji, WP216, 10 kwietnia 2014 r., s. 5–19.

[62] Komunikat Komisji do Parlamentu Europejskiego i Rady, „Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej", COM(2019) 250 final z dnia 29 maja 2019 r.

4.2 Dane osobowe, do których odnosi się prawo dostępu

102. Zgodnie z art. 15 ust. 1 RODO „[o]soba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji" (podkreślenie dodane).

103. Z art. 15 ust. 1 RODO wynika kilka elementów. Ustęp ten odnosi się *expressis verbis* do „danych osobowych jej dotyczących" (sekcja 4.2.1), które „przetwarzane są" (sekcja 4.2.2) przez administratora:

4.2.1 „Dane osobowe jej dotyczące"

104. Prawo dostępu może być wykonywane wyłącznie w odniesieniu do danych osobowych osoby, której dane dotyczą, żądającej dostępu lub, w stosownych przypadkach, przez osobę upoważnioną lub pełnomocnika (zob. sekcja 3.4). Istnieją również sytuacje, w których dane nie mają związku z osobą korzystającą z prawa dostępu, lecz z inną osobą fizyczną. Osoba, której dane dotyczą, jest jednak uprawniona do otrzymania dostępu jedynie danych osobowych odnoszących się do niej samej, z wyłączeniem danych, które dotyczą wyłącznie innej osoby[63].

105. Zakwalifikowanie danych jako danych osobowych osoby, której dane dotyczą, nie zależy jednak od tego, czy dane te dotyczą również innej osoby[64]. Możliwe jest zatem, że dane osobowe odnoszą się jednocześnie do więcej niż jednej osoby fizycznej. Nie oznacza to automatycznie, że należy udzielić dostępu do danych osobowych dotyczących również innej osoby, ponieważ administrator musi przestrzegać art. 15 ust. 4 RODO.

106. Administratorzy nie powinni dokonywać „zbyt zawężającej" wykładni określenia „dane osobowe jej dotyczące", jak już stwierdziła Grupa Robocza Art. 29 w odniesieniu do prawa do przenoszenia danych[65]. W odniesieniu do prawa dostępu EROD uważa na przykład, że nagrania rozmów telefonicznych (i ich transkrypcja) między osobą, której dane dotyczą i która żąda dostępu, a administratorem mogą wchodzić w zakres prawa dostępu, pod warunkiem że są to dane osobowe[66]. Pod warunkiem że RODO ma zastosowanie i że przetwarzanie nie jest objęte wyłączeniem dotyczącym czynności o czysto domowym charakterze, o którym mowa w art. 2 ust. 2 lit. c) RODO, jeżeli osoba, której dane dotyczą, wykorzystuje uzyskane nagranie, które zawiera dane osobowe rozmówcy, do innych celów, na przykład publikując to nagranie, osoba, której dane dotyczą, stanie się

[63] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 9: „Zakresem żądania przeniesienia danych objęte są wyłącznie dane osobowe. W związku z tym wszelkie dane anonimowe lub nieodnoszące się do osoby, której dane dotyczą, nie będą objęte tym zakresem. Dane pseudonimiczne, które można jednoznacznie powiązać z osobą, której dane dotyczą (np. poprzez podanie przez nią odpowiedniego identyfikatora, por. art. 11 ust. 2), są jednak tym zakresem objęte".

[64] TSUE, wyrok w sprawie C-434/16, Peter Nowak/Data Protection Commissioner, 2017, pkt 44.

[65] Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych – zatwierdzone przez EROD, s. 9: „W wielu sytuacjach administratorzy danych przetwarzają informacje zawierające dane osobowe kilku osób, których dane dotyczą takim przypadku administratorzy danych nie powinni dokonywać zbyt zawężającej wykładni określenia »dane osobowe dotyczące osoby, której dane dotyczą«. Przykładowo rejestry połączeń telefonicznych, wiadomości interpersonalnych lub VoIP (w historii konta abonenta) mogą zawierać dane osób trzecich uczestniczących w połączeniach przychodzących i wychodzących. Chociaż rejestry będą w związku z tym zawierały dane osobowe dotyczące wielu osób, abonenci powinni mieć możliwość otrzymania tych rejestrów w odpowiedzi na żądania przeniesienia danych, ponieważ rejestry dotyczą (również) osoby, której dane dotyczą. Jeżeli tego rodzaju rejestry zostają następnie przesłane nowemu administratorowi danych, nie powinien on ich jednak przetwarzać w żadnym celu, który wpłynąłby niekorzystnie na prawa i wolności osób trzecich (zob. poniżej: trzeci warunek)".

[66] Zob. przykład 34 w sekcji 6.2.

administratorem w odniesieniu do tego przetwarzania danych osobowych dotyczących drugiej osoby, której głos został nagrany. Chociaż nie zwalnia to administratora z obowiązków w zakresie ochrony danych podczas należytej analizy, czy można udzielić dostępu do pełnego nagrania, zachęca się go do poinformowania osoby, której dane dotyczą, o tym, że w takim przypadku może ona stać się administratorem. Pozostaje to bez uszczerbku dla jakiejkolwiek dalszej oceny na podstawie art. 15 ust. 4 RODO szczegółowo opisanej w sekcji 6. W tym samym duchu wiadomości, które osoby, których dane dotyczą, przesłały innym osobom w formie osobistych wiadomości i same usunęły ze swojego urządzenia, które to wiadomości nadal są dostępne dla usługodawcy, mogą wchodzić w zakres prawa dostępu.

107. Również w tym przypadku istnieją sytuacje, w których powiązanie między danymi a kilkoma osobami fizycznymi może wydawać się administratorowi nieostre, np. w przypadku kradzieży tożsamości. W przypadku kradzieży tożsamości osoba działa w sposób oszukańczy w imieniu innej osoby. W tym kontekście należy przypomnieć, że ofiara powinna otrzymać informacje na temat wszystkich danych osobowych, które administrator przechowuje w związku z jej tożsamością, w tym danych zebranych na podstawie działań oszusta. Innymi słowy, nawet po tym, jak administrator dowiedział się o kradzieży tożsamości, dane osobowe związane z tożsamością ofiary lub dotyczące jej tożsamości stanowią dane osobowe osoby, której dane dotyczą.

Przykład 17: Osoba fizyczna w sposób oszukańczy wykorzystuje tożsamość innej osoby, aby grać w pokera w internecie. Sprawca płaci kasynu internetowemu za pomocą karty kredytowej, którą ukradł ofierze. Gdy ofiara dowiaduje się o kradzieży jej tożsamości, żąda od podmiotu prowadzącego kasyno internetowe udzielenia jej dostępu do jej danych osobowych, a w szczególności do gier online, w które grał sprawca w jej imieniu, i informacji o karcie kredytowej wykorzystywanej przez sprawcę.

Istnieje związek między zgromadzonymi danymi a ofiarą, ponieważ wykorzystano jej tożsamość. Po wykryciu oszustwa wyżej wymienione dane osobowe nadal mają związek ze względu na ich treść (karta kredytowa niewątpliwie zawiera jej dane), cel i skutek (informacje o grach online, w które grał sprawca, mogą być na przykład służyć do wystawiania faktur ofierze). W związku z tym kasyno internetowe musi zapewnić ofierze dostęp do wyżej wymienionych danych osobowych.

108. W stosownych przypadkach można wykorzystywać wewnętrzne dzienniki połączeń do przechowywania wpisów dotyczących dostępu do pliku oraz do śledzenia działań podjętych w związku z dostępem do rekordu, takich jak drukowanie, kopiowanie lub usuwanie danych osobowych. Dzienniki te mogą zawierać czas połączenia, powód dostępu do pliku, a także informacje identyfikujące osobę, która uzyskała dostęp. Kwestie związane z tym zagadnieniem są przedmiotem sprawy zawisłej obecnie przed TSUE (C-579/21). Wprowadzanie i przegląd dzienników połączeń oraz nadzór nad nimi wchodzą w zakres odpowiedzialności administratora i podlegają kontroli organów nadzorczych. Administrator powinien zatem dopilnować, aby osoby działające pod jego zwierzchnictwem, które mają dostęp do danych osobowych, przetwarzały je wyłącznie na polecenie administratora, zgodnie z art. 29 RODO. Jeżeli jednak dana osoba przetwarza dane osobowe do celów innych niż wykonanie polecenia administratora, może stać się administratorem w odniesieniu do tego przetwarzania i podlegać postępowaniu dyscyplinarnemu lub karnemu bądź karom administracyjnym nałożonym przez organy nadzorcze. EROD zauważa, że do obowiązków pracodawcy zgodnie z art. 24 RODO należy stosowanie odpowiednich środków, począwszy od edukowania, a skończywszy na prowadzeniu postępowań dyscyplinarnych, w celu zapewnienia, aby przetwarzanie było zgodne z RODO i aby nie dochodziło do naruszenia.

4.2.2 Dane osobowe, które „są przetwarzane”

109. Art. 15 ust. 1 RODO odnosi się ponadto do danych osobowych, które „są przetwarzane”. Punkt odniesienia czasowego dla określenia zakresu danych osobowych objętych żądaniem dostępu omówiono już w sekcji 2.3.3. Sformułowanie to sugeruje jednak również, że na gruncie prawa dostępu nie dokonuje się rozróżnienia między celami operacji przetwarzania.

> **Przykład 18**: Przedsiębiorstwo przetwarzało dane osobowe osoby, której dane dotyczą, w celu przetworzenia jej zamówienia i zorganizowania wysyłki na jej adres zamieszkania. Po zrealizowaniu tych pierwotnych celów, dla których zebrano dane osobowe, administrator przechowuje niektóre dane osobowe wyłącznie w celu wypełnienia swoich zobowiązań prawnych dotyczących prowadzenia rejestrów.
>
> Osoba, której dane dotyczą, żąda dostępu do dotyczących jej danych osobowych. Aby spełnić obowiązek wynikający z art. 15 ust. 1 RODO, administrator musi przekazać osobie, której dane dotyczą, żądane dane osobowe, które są przechowywane w celu wywiązania się przez niego z zobowiązań prawnych.

110. Zarchiwizowane dane osobowe należy odróżnić od danych zapasowych, które są danymi osobowymi przechowywanymi wyłącznie w celu przywrócenia danych w przypadku ich utraty. Należy podkreślić, że w odniesieniu do zasady uwzględniania ochrony danych już w fazie projektowania oraz zasady minimalizacji danych dane zapasowe są co do zasady podobne do danych znajdujących się w systemie będącym w użyciu. Jeżeli istnieją niewielkie różnice między danymi osobowymi w systemie kopii zapasowych i w systemie produkcyjnym będącym w użyciu, są one na ogół powiązane z gromadzeniem danych dodatkowych od czasu utworzenia ostatniej kopii zapasowej. Zmniejszenie ilości danych w systemie będącym w użyciu (np. usunięcie niektórych danych po zakończeniu okresu zatrzymywania lub po wniesieniu żądania usunięcia) zostanie w niektórych przypadkach odzwierciedlone w danych zapasowych dopiero w chwili wykonania kolejnej kopii zapasowej. W przypadku gdy żądanie dostępu wystosowano w momencie, gdy kopia zapasowa zawiera więcej danych osobowych osoby, której dane dotyczą, niż system będący w użyciu lub zawiera ona różne dane osobowe (co można zauważyć na przykład dzięki dziennikowi usunięć w systemie produkcyjnym będącym w użyciu, wdrożonym w pełnej zgodności z zasadą minimalizacji danych), administrator musi zachować przejrzystość w tej sytuacji i, jeżeli jest to technicznie wykonalne, zapewnić dostęp na żądanie osoby, której dane dotyczą, w tym do danych osobowych przechowywanych w kopii zapasowej. Na przykład w celu zapewnienia przejrzystości wobec osób, których dane dotyczą i które korzystają z przysługującego im prawa, dziennik usunięć w systemie produkcyjnym będącym w użyciu może umożliwić administratorowi sprawdzenie, czy dane zapasowe obejmują dane, które nie znajdują się już w działającym systemie, ponieważ zostały niedawno usunięte i nie zostały jeszcze nadpisane w kopii zapasowej.

4.2.3 Zakres nowego żądania dostępu

111. Należy jeszcze dodać, że osoby, których dane dotyczą, mają prawo dostępu do wszystkich przetwarzanych danych, które się do nich odnoszą, lub ich części, w zależności od zakresu żądania (zob. również pkt 2.3.1 dotyczący kompletności informacji i pkt 3.1.1 w odniesieniu do analizy treści żądania). W związku z tym, jeżeli administrator spełnił już żądanie dostępu w przeszłości i pod warunkiem że żądanie nie jest nadmierne, administrator nie może zawęzić zakresu tego nowego żądania. Oznacza to, że w odniesieniu do wszelkich dalszych żądań dostępu wystosowanych przez tę samą osobę, której dane dotyczą, administrator nie powinien informować tej osoby jedynie o samych zmianach w przetwarzanych danych osobowych lub o samym przetwarzaniu od czasu wystąpienia z ostatnim żądaniem, chyba że osoba, której dane dotyczą, wyraźnie na to wyrazi zgodę.

W przeciwnym razie osoby, których dane dotyczą, musiałyby zestawić dostarczone dane osobowe w celu uzyskania pełnego zestawu danych osobowych dotyczących ich informacji o przetwarzaniu i prawach osób, których dane dotyczą.

4.3 Informacje o przetwarzaniu i prawach osób, których dane dotyczą

112. Oprócz dostępu do samych danych osobowych administrator musi udzielić informacji na temat przetwarzania i praw osób, których dane dotyczą, zgodnie z art. 15 ust. 1 lit. a)–h) i art. 15 ust. 2 RODO. Większość informacji na temat tych konkretnych kwestii jest już zebrana, przynajmniej w formie ogólnej, w prowadzonym przez administratora rejestrze czynności przetwarzania, o którym mowa w art. 30 RODO, lub w jego oświadczeniu o ochronie prywatności opracowanym zgodnie z art. 12–14 RODO. W związku z tym w pierwszej kolejności pomocne może być zapoznanie się z „Wytycznymi dotyczącymi przejrzystości na mocy rozporządzenia 2016/679”[67] grupy Roboczej Art. 29 w odniesieniu do treści informacji, które należy podać na podstawie art. 13 i 14 RODO.

113. W celu zapewnienia zgodności z art. 15 ust. 1 lit. a)–h) i art. 15 ust. 2 administratorzy mogą uważnie wykorzystywać moduły tekstowe swojego oświadczenia o ochronie prywatności, o ile upewnią się, że są one aktualne i precyzyjne w odniesieniu do żądania osoby, której dane dotyczą. Przed przetwarzaniem lub na początku przetwarzania danych często nie można jeszcze podać pewnych informacji, takich jak identyfikacja konkretnych odbiorców lub konkretny czas przetwarzania danych. Niektóre informacje, takie jak prawo do złożenia skargi do organu nadzorczego (zob. art. 15 ust. 1 lit. f)), nie zmieniają się w zależności od osoby występującej z żądaniem dostępu. W związku z tym można je przekazać w sposób ogólny, tak jak ma to miejsce również w oświadczeniu o ochronie prywatności. Inne rodzaje informacji, takie jak informacje na temat odbiorców, kategorii i źródła danych, mogą się różnić w zależności od tego, kto występuje z żądaniem i jaki jest jego zakres. W kontekście żądania dostępu zgodnie z art. 15 wszelkie informacje na temat przetwarzania, którymi dysponuje administrator, mogą zatem wymagać aktualizacji i dostosowania do faktycznie przeprowadzonych operacji przetwarzania w odniesieniu do osoby, której dane dotyczą i która występuje z żądaniem. W związku z tym odniesienie do treści jego polityki ochrony prywatności nie byłoby wystarczającym sposobem przekazania przez administratora informacji wymaganych na mocy art. 15 ust. 1 lit. a)–h) i art. 15 ust. 2, chyba że „dostosowane i zaktualizowane” informacje są takie same jak informacje podane na początku przetwarzania. Wyjaśniając, które informacje dotyczą osoby występującej z żądaniem, administrator może, w stosownych przypadkach, odnieść się do określonych czynności (takich jak „jeżeli korzystali Państwo z tej usługi …”, „jeżeli zapłacili Państwo fakturę”), o ile dla osób, których dane dotyczą, takie odniesienie jest oczywiste. Poniżej wyjaśniono wymagany stopień szczegółowości w odniesieniu do poszczególnych rodzajów informacji.

114. Informacje na temat celów zgodnie z art. 15 ust. 1 lit. a) muszą być konkretne w odniesieniu do określonego celu lub określonych celów w faktycznym przypadku osoby, której dane dotyczą i która występuje z żądaniem. Nie wystarczyłoby wymienić ogólnych celów administratora bez wyjaśnienia, jaki cel lub jakie cele realizuje administrator w bieżącym przypadku osoby, której dane dotyczą i która występuje z żądaniem. Jeżeli przetwarzanie odbywa się w kilku celach, administrator musi wyjaśnić, które dane lub które kategorie danych są przetwarzane w jakim celu lub w jakich celach. W przeciwieństwie do art. 13 ust. 1 lit. c) i art. 14 ust. 1 lit. c) RODO informacje na temat przetwarzania, o których mowa w art. 15 ust. 1 lit. a), nie zawierają informacji na temat podstawy

[67] Grupa Robocza Art. 29, WP 260 rev.01, 11 kwietnia 2018 r., Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 – zatwierdzone przez EROD (zwane dalej „wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzonymi przez EROD”).

prawnej przetwarzania. Ponieważ jednak niektóre prawa osób, których dane dotyczą, zależą od mającej zastosowanie podstawy prawnej, informacje te są dla tych osób istotne, ponieważ umożliwiają zweryfikowanie zgodności przetwarzania danych z prawem oraz ustalenie, które z praw osób, których dane dotyczą, mają zastosowanie w szczególnej sytuacji. By zatem ułatwić osobom, których dane dotyczą, korzystanie z praw zgodnie z art. 12 ust. 2 RODO, zaleca się, aby administrator poinformował również osobę, której dane dotyczą, o mającej zastosowanie podstawie prawnej każdej operacji przetwarzania lub wskazał, gdzie może znaleźć te informacje. W każdym przypadku zasada przejrzystego przetwarzania wymaga, aby informacje na temat podstaw prawnych przetwarzania były udostępniane osobie, której dane dotyczą, w przystępny sposób (np. w oświadczeniu o ochronie prywatności).

115. Informacje na temat kategorii danych (art. 15 ust. 1 lit. b)) mogą również być dostosowane do sytuacji osoby, której dane dotyczą – w ten mianowicie sposób, że kategorie, które okazały się nieistotne w przypadku osoby występującej z żądaniem, powinny zostać pominięte.

Przykład 19: W kontekście informacji, o których mowa w art. 13/14 RODO, hotel oświadcza, że przetwarza szereg kategorii danych klientów (dane identyfikacyjne, dane kontaktowe, dane bankowe, numer karty kredytowej itp.). Jeżeli z żądaniem dostępu wystąpiono na podstawie art. 15, osoba, której dane dotyczą, musi – oprócz udzielenia jej dostępu do faktycznie przetwarzanych danych (element 2) – zostać również poinformowana, zgodnie z art. 15 ust. 1 lit. b), o konkretnych kategoriach danych przetwarzanych w tym konkretnym przypadku (np. dane bankowe lub dane karty kredytowej w przypadku płatności gotówką).

116. Przy udzielaniu informacji na temat „odbiorców lub kategorii odbiorców" (art. 15 ust. 1 lit. c)) konieczne jest przede wszystkim uwzględnienie definicji odbiorców zawartej w art. 4 pkt 9 RODO. Podstawą uznania za odbiorcę zgodnie z tą definicją jest fakt ujawnienia danych osobowych osobie fizycznej lub prawnej, organowi publicznemu, jednostce lub innemu podmiotowi[68]. Z art. 4 pkt 9 RODO wynika, że organy publiczne działające w ramach konkretnego postępowania podlegającego szczególnym przepisom krajowym nie są uznawane za odbiorców.

117. W odniesieniu do pytania, czy administrator ma swobodę wyboru między informacjami na temat odbiorców lub na temat kategorii odbiorców, należy zauważyć, że „w przeciwieństwie do art. 13 i 14 RODO, które ustanawiają ciążący na administratorze danych obowiązek (...), art. 15 RODO przewiduje rzeczywiste prawo dostępu na rzecz osoby, której dane dotyczą, w taki sposób, aby miała ona możliwość wyboru i uzyskania albo informacji dotyczących konkretnych odbiorców, którym dane zostały lub zostaną ujawnione, jeżeli jest to możliwe, albo informacji dotyczących kategorii odbiorców"[69]. Należy również przypomnieć, że – jak stwierdzono w wyżej wymienionych wytycznych dotyczących przejrzystości[70] – już na podstawie art. 13 i 14 RODO informacje na temat odbiorców lub kategorii odbiorców powinny być możliwie najbardziej konkretne, aby uczynić zadość zasadom przejrzystości i rzetelności. Zgodnie z art. 15, jeżeli osoba, której dane dotyczą, nie postanowiła inaczej,

[68] Należy ponadto zauważyć, że w ramach tego samego przedsiębiorstwa mogą istnieć różni administratorzy w rozumieniu art. 4 pkt 7 RODO. W tym wariancie możliwe jest ujawnienie danych między odbiorcami w ramach jednego przedsiębiorstwa.

[69] TSUE, C-154/21 (Österreichische Post AG), pkt 36.

[70] Grupa Robocza Art. 29, WP 260 rev.01, 11 kwietnia 2018 r., Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 – zatwierdzone przez EROD (zwane dalej „wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzonymi przez EROD", s. 37 (załącznik).

administrator jest zobowiązany do wskazania rzeczywistych odbiorców, chyba że zidentyfikowanie tych odbiorców jest niemożliwe lub administrator wykaże, że żądania dostępu, z którymi wystąpiła osoba, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne w rozumieniu art. 12 ust. 5 RODO[71] [72]. EROD przypomina w tym względzie, że przechowywanie informacji dotyczących faktycznych odbiorców jest niezbędne m.in. do wypełnienia obowiązków administratora wynikających z art. 5 ust. 2 i art. 19 RODO.

Przykład 20: W swoim oświadczeniu o ochronie prywatności pracodawca podaje informacje na temat kategorii danych przekazywanych „biurom podróży" lub „hotelom" w przypadku podróży służbowych, zgodnie z art. 13 ust. 1 lit. e) i art. 14 ust. 1 lit. e) RODO. Jeżeli pracownik występuje z żądaniem dostępu do danych osobowych po odbyciu podróży służbowych, pracodawca powinien wówczas, w odniesieniu do odbiorców danych osobowych zgodnie z art. 15 ust. 1 lit. c), wskazać w swojej odpowiedzi biura podróży i hotele, które otrzymały te dane. Chociaż pracodawca w sposób zgodny z prawem odniósł się do kategorii odbiorców w swoim oświadczeniu o ochronie prywatności zgodnie z art. 13 i 14, ponieważ na tym etapie nie było jeszcze możliwe podanie nazwy odbiorców, powinien, o ile pracownik nie postanowił inaczej, udzielić mu informacji na temat konkretnych odbiorców (nazwy biur podróży, hoteli itp.), jeżeli pracownik z takim żądaniem dostępu występuje.

W przypadku gdy, przy spełnieniu powyższych warunków, administrator może podać jedynie kategorie odbiorców, informacja powinna być tak szczegółowa, jak jest to możliwe, wskazując rodzaj odbiorcy (tj. odnosząc się do wykonywanych przez niego działań), branżę, sektor i podsektor oraz lokalizację odbiorców[73].

118. Zgodnie z art. 15 ust. 1 lit. d) w miarę możliwości należy podać informacje na temat planowanego okresu przechowywania danych osobowych. W przeciwnym razie należy przedstawić kryteria ustalenia tego okresu. Informacje podane przez administratora muszą być wystarczająco precyzyjne, aby osoba, której dane dotyczą, wiedziała, jak długo będą przechowywane dotyczące jej dane. Jeżeli nie jest możliwe określenie czasu usunięcia danych, należy określić czas trwania okresu przechowywania oraz początek tego okresu lub zdarzenia, które uruchamia jego bieg (np. rozwiązanie umowy, wygaśnięcie okresu gwarancji itp.). Samo odniesienie, na przykład do „usunięcia po upływie ustawowych okresów przechowywania", nie jest wystarczające. Wskazania dotyczące okresów przechowywania muszą dotyczyć konkretnych danych dotyczących osoby, której dane dotyczą. Jeżeli dane osobowe osoby, której dane dotyczą, podlegają różnym okresom usuwania (np. ponieważ nie wszystkie objęte są prawnym obowiązkom przechowywania), okresy te należy określić w odniesieniu do odpowiednich operacji przetwarzania i kategorii danych.

119. Podczas gdy informacje o prawie wniesienia skargi do organu nadzorczego (art. 15 ust. 1 lit. f)) nie zależą od konkretnych okoliczności, prawa, o których mowa w art. 15 ust. 1 lit. e), przysługujące osobom, których dane dotyczą, różnią się w zależności od podstawy prawnej przetwarzania. W odniesieniu do obowiązku ułatwienia wykonania praw osobom, których dane dotyczą, zgodnie z art. 12 ust. 2 RODO, odpowiedź administratora na temat tych praw musi być indywidualnie dostosowana do sprawy osoby, której dane dotyczą, i odnosić się do odpowiednich operacji przetwarzania. Należy unikać informowania o prawach, które nie mają zastosowania do osoby, której dane dotyczą, w jej szczególnej sytuacji.

[71] TSUE, C-154/21 (Österreichische Post AG).

[72] Fakt, że dane zostały ujawnione dużej liczbie odbiorców, nie powoduje sam w sobie, że żądanie jest nadmierne, zob. sekcja 6, pkt 188.

[73] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, s. 37 (załącznik).

120. Zgodnie z art. 15 ust. 1 lit. g) należy podać „wszelkie dostępne informacje" o źródle danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą. Zakres dostępnych informacji może się zmieniać z biegiem czasu.

Przykład 21: Polityka ochrony prywatności dużego przedsiębiorstwa stanowi:

„Oceny wypłacalności pomagają nam zapobiegać problemom w transakcjach płatniczych. Gwarantują one naszemu przedsiębiorstwu ochronę przed ryzykiem finansowym, które może również wpłynąć na ceny sprzedaży w perspektywie średnio- i długoterminowej. Ocenę wypłacalności przeprowadza się, gdy przesyłamy towary bez jednoczesnego otrzymania odpowiedniej ceny zakupu, np. w przypadku płatności w ramach kredytu handlowego. Bez przeprowadzania oceny wypłacalności zakup jest możliwy jedynie po dokonani przedpłaty (natychmiastowy przelew bankowy, płatność za pośrednictwem dostawcy usług płatniczych online, karta kredytowa).

Do celów oceny wypłacalności prześlemy Państwa imię i nazwisko, adres i datę urodzenia do następujących usługodawców, np.: 1) agencja informacji finansowej X, 2) dostawca informacji gospodarczych Y, 3) biuro informacji kredytowej Z.

Dane są przekazywane wyżej wymienionym instytucjom kredytowym wyłącznie w zakresie, w jakim jest to dopuszczalne na mocy prawa, i wyłącznie do celów analizy Państwa wcześniejszych zachowań płatniczych, jak również do celów oceny ryzyka niewykonania zobowiązania na podstawie procedur matematyczno-statystycznych z wykorzystaniem danych adresowych, jak również do celów weryfikacji Państwa adresu (sprawdzenia miejsca dostawy). W zależności od wyniku oceny wypłacalności możemy nie być w stanie zaoferować Państwu indywidualnych metod płatności, takich jak zakup na fakturę".

Oświadczenie o ochronie prywatności zawiera zatem ogólne informacje na temat możliwości uzyskania informacji od wymienionych biur informacji gospodarczej zgodnie z art. 13 i 14 RODO. Jeżeli nie jest jasne *ex ante*, które przedsiębiorstwa będą brać udział w przetwarzaniu, wystarczy podać nazwy kwalifikujących się przedsiębiorstw w polityce ochrony prywatności. W kontekście żądania na podstawie art. 15, oprócz informacji, że uzyskano informacje na temat zdolności kredytowej, konieczne byłoby następnie (*ex post*) ujawnienie, które z wymienionych przedsiębiorstw konkretnie brały udział w przetwarzaniu. W art. 15 ust. 1 lit. g) wyraźnie stwierdzono, że informacje na temat przetwarzania danych obejmują „wszelkie dostępne informacje o ich źródle", w przypadku gdy dane osobowe nie zostały zebrane od osoby, której dane dotyczą.

121. Art. 15 ust. 1 lit. h) stanowi, że każda osoba, której dane dotyczą, powinna mieć prawo do uzyskania istotnych informacji m.in. o stosowaniu i podstawowej logice zautomatyzowanego podejmowania decyzji, w tym profilowania dotyczącego osoby, której dane dotyczą, oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania[74]. W miarę możliwości informacje, o których mowa w art. 15 ust. 1 lit. h), muszą charakteryzować się większą szczegółowością w odniesieniu do uzasadnienia konkretnych decyzji podjętych w stosunku do występującej z żądaniem dostępu osoby, której dane dotyczą.

122. Zgodnie z art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO należy przekazać informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej, w tym na temat istnienia decyzji Komisji stwierdzającej odpowiedni stopień ochrony lub odpowiednich zabezpieczeń.

[74] Zob. w tym względzie Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 (WP 260), pkt 41, w związku z Wytycznymi w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, (WP 251).

W kontekście żądania dostępu na podstawie art. 15 w art. 15 ust. 2 wymaga się poinformowania o odpowiednich zabezpieczeniach zgodnie z art. 46 RODO wyłącznie w przypadkach faktycznego przekazywania danych do państwa trzeciego lub organizacji międzynarodowej.

5 W JAKI SPOSÓB ADMINISTRATOR MOŻE ZAPEWNIĆ DOSTĘP DO DANYCH?

123. W RODO nie sprecyzowano zbyt szczegółowo sposobu zapewnienia dostępu do danych przez administratora. W niektórych sytuacjach zastosowanie prawa dostępu może być proste, na przykład gdy mała organizacja posiada ograniczone informacje o osobie, której dane dotyczą. W innych przypadkach wykonanie prawa dostępu będzie bardziej skomplikowane, ponieważ przetwarzanie danych jest bardziej złożone – ze względu na liczbę osób, których dane dotyczą, kategorie przetwarzanych danych, a także przepływ danych w ramach różnych organizacji i między nimi. Biorąc pod uwagę różnice w przetwarzaniu danych osobowych, odpowiedni sposób zapewnienia dostępu może się różnić w zależności od sytuacji.

124. Niniejsza sekcja ma na celu przedstawienie pewnych wskazówek i praktycznych przykładów dotyczących różnych sposobów zastosowania się przez administratorów do żądania dostępu, a także znaczenia art. 12 ust. 1 RODO w odniesieniu do prawa dostępu. Zawiera ona również pewne wskazówki dotyczące tego, co uznaje się za powszechnie stosowane formularze elektroniczne, a także terminów udzielenia dostępu na podstawie art. 12 ust. 3 RODO.

5.1 W jaki sposób administrator może pobrać dane, których dotyczy żądanie?

125. Osoby, których dane dotyczą, powinny mieć dostęp do wszystkich informacji na swój temat, które administrator przetwarza. Oznacza to na przykład, że administrator jest zobowiązany do wyszukania danych osobowych we wszystkich swoich systemach informatycznych i zbiorach danych innych niż informatyczne. Przeprowadzając takie wyszukiwanie, administrator powinien wykorzystać dostępne w organizacji informacje dotyczące osoby, której dane dotyczą, jako że prawdopodobnie doprowadzą one do dopasowań w systemach, w zależności od sposobu ustrukturyzywania informacji[75]. Jeżeli na przykład informacje są posortowane w plikach na podstawie nazwy lub numeru referencyjnego, wyszukiwanie może ograniczać się do tych czynników. Jeżeli jednak struktura danych zależy od innych czynników, takich jak związki rodzinne lub stanowiska zawodowe, lub bezpośrednie lub pośrednie identyfikatory jakiegokolwiek rodzaju (np. numer klienta, nazwa użytkownika lub adresy IP), wyszukiwanie musi zostać rozszerzone o te czynniki, pod warunkiem że administrator posiada również tego rodzaju informacje odnoszące się do osoby, której dane dotyczą, lub że osoba ta przekaże te informacje. To samo dotyczy sytuacji, w której wpisy dotyczące stron trzecich mogą zawierać dane osobowe odnoszące się do osoby, której dane dotyczą. Administrator nie może jednak wymagać od osoby, której dane dotyczą, udzielenia większej ilości informacji niż jest to konieczne do jej zidentyfikowania. Jeżeli administrator korzysta z usług podmiotu przetwarzającego do celów czynności przetwarzania danych, wyszukiwanie należy oczywiście rozszerzyć również na dane osobowe przetwarzane przez podmiot przetwarzający.

126. Zgodnie z art. 25 RODO dotyczącym uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrona danych administrator (i wszelkie podmioty przetwarzające, z których usług

[75] Wyszukiwanie takie powinno oczywiście obejmować również informacje, które znajdują się w posiadaniu podmiotu przetwarzającego, zob. art. 28 ust. 3 lit. e) RODO.

administrator korzysta) powinien już także realizować funkcje umożliwiające wykonywanie praw osób, których dane dotyczą. Oznacza to w tym kontekście, że w ramach rozpatrywania żądania powinny istnieć odpowiednie sposoby wyszukiwania i pobierania informacji dotyczących osoby, której dane dotyczą. Należy jednak zauważyć, że zbyt daleko idąca wykładnia w tym zakresie mogłaby prowadzić do funkcji wyszukiwania i pobierania informacji, które same w sobie stanowiłyby zagrożenie dla prywatności osób, których dane dotyczą. Należy zatem pamiętać, że proces pobierania danych powinien być również zaprojektowany w sposób uwzględniający ochronę danych, tak aby nie zagrażał prywatności innych osób, na przykład pracowników administratora.

5.2 Odpowiednie środki w celu zapewnienia dostępu

5.2.1 Podejmowanie „odpowiednich środków"

127. W art. 12 RODO określono wymogi dotyczące zapewnienia dostępu, tj. przekazania potwierdzenia, danych osobowych i informacji uzupełniających zgodnie z art. 15, a także określono formę, sposób i termin w odniesieniu do prawa dostępu. „Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679"[76] Grupy Roboczej Art. 29 zawierają dalsze wskazówki dotyczące art. 12, głównie w odniesieniu do art. 13 i 14 RODO, ale również w odniesieniu do art. 15 i przejrzystości w ogóle. Dlatego treść tych wytycznych może mieć często takie samo zastosowanie w odniesieniu do udzielania dostępu na podstawie art. 15.

128. W art. 12 ust. 1 RODO stwierdzono, że administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą wszelkich informacji dotyczących przetwarzania, o których mowa w art. 15. Art. 12 ust. 2 stanowi, że administrator ułatwia osobie, której dane dotyczą, wykonanie jej prawa dostępu. Bardziej precyzyjne wymogi w tym zakresie należy oceniać indywidualnie dla każdego przypadku. Przy podejmowaniu decyzji, jakie środki są odpowiednie, administratorzy muszą wziąć pod uwagę wszystkie istotne okoliczności, w tym m.in. ilość przetwarzanych danych, złożoność przetwarzania danych oraz wiedzę posiadaną na temat osób, których dane dotyczą, na przykład jeżeli większość osób, których dane dotyczą, to dzieci, osoby starsze lub osoby z niepełnosprawnościami. Ponadto w sytuacjach, w których administrator poweźmie wiedzę o jakichkolwiek szczególnych potrzeb występującej z żądaniem osoby, której dane dotyczą, na przykład ze względu na dodatkowe informacje zawarte we wniosku, administrator musi wziąć te okoliczności pod uwagę. W rezultacie odpowiednie środki będą się różnić.

129. Przy ocenie należy pamiętać, że termin „odpowiednie" nigdy nie powinien być rozumiany jako sposób na ograniczenie zakresu danych objętych prawem dostępu. Termin „odpowiednie" nie oznacza, że starania zmierzające do udzielenia informacji można zrównoważyć, na przykład, z jakimkolwiek interesem, jaki osoba, której dane dotyczą, może mieć w uzyskaniu danych osobowych. Ocena powinna mieć bowiem na celu wybór najwłaściwszej metody udzielenia wszystkich informacji objętych tym prawem, w zależności od konkretnych okoliczności w każdym przypadku. W związku z tym administrator, który przetwarza dużą ilość danych na dużą skalę, musi liczyć się z koniecznością podjęcia daleko idących działań w celu zapewnienia osobom, których dane dotyczą, prawa dostępu do tych danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

[76] Grupa Robocza Art. 29, WP 260 rev.01, 11 kwietnia 2018 r., Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 – zatwierdzone przez EROD (zwane dalej „wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzonymi przez EROD".

130. Należy unikać kierowania osoby, której dane dotyczą, do różnych źródeł w odpowiedzi na żądanie dostępu do danych. Jak już stwierdzono w wytycznych Grupy Roboczej Art. 29 dotyczących przejrzystości (w odniesieniu do pojęcia „podania" w art. 13 i 14 RODO), pojęcie „podania" oznacza, że „osoba, której dane dotyczą, nie powinna być zmuszona do czynnego szukania informacji, o których mowa we wspomnianych artykułach, wśród innych informacji, takich jak regulamin korzystania ze strony internetowej lub z aplikacji"[77]. W związku z tym oraz zgodnie z zasadą przejrzystości osoby, których dane dotyczą, muszą uzyskać od administratora informacje i dane osobowe wymagane zgodnie z art. 15 ust. 1, 2 i 3 w sposób umożliwiający pełny dostęp do żądanych informacji. W szczególnych okolicznościach udostępnianie informacji administratorowi danych byłoby niewłaściwe lub nawet niezgodne z prawem, na przykład ze względu na wrażliwy charakter informacji (takich jak informacje związane z sygnalizowaniem nieprawidłowości). W takich przypadkach należałoby w ramach odpowiedzi na żądanie dostępu wystosowane przez osoby, których dane dotyczą, podzielić informacje na kilka odpowiedzi. Metoda wybrana przez administratora musi faktycznie zapewniać dostarczenie osobie, której dane dotyczą, żądanych danych i informacji, w związku z czym nie byłoby właściwe wyłącznie zalecenie tej osobie sprawdzenia żądanych danych na jej własnym urządzeniu, w tym np. sprawdzenia historii ruchu w sieci i adresów IP na jej telefonie komórkowym.

131. Zgodnie z zasadą rozliczalności administrator musi udokumentować swoje podejście, aby móc wykazać, w jaki sposób środki wybrane do udzielenia niezbędnych informacji zgodnie z art. 15 są odpowiednie w danych okolicznościach.

5.2.2 Różne środki służące do udzielenia dostępu

132. Jak już wyjaśniono w sekcji 2.2.2 powyżej, występujące z żądaniem dostępu osoby, których dane dotyczą, są uprawnione do otrzymania kopii swoich danych podlegających przetwarzaniu zgodnie z art. 15 ust. 3 wraz z informacjami uzupełniającymi, co uznaje się za główny sposób udzielania dostępu do danych osobowych.

133. Jednak w niektórych okolicznościach może być właściwe, aby administrator danych zapewnił dostęp w inny sposób niż w drodze dostarczenia kopii. Takie doraźne warunki dostępu do danych mogłyby obejmować na przykład: informacje ustne, wgląd do akt, dostęp na miejscu lub dostęp zdalny bez możliwości pobrania. Warunki te mogą być odpowiednimi sposobami udzielania dostępu na przykład w przypadkach, gdy leży to w interesie osoby, której dane dotyczą, lub gdy osoba, której dane dotyczą, o to wystąpi. Dostęp na miejscu mógłby być również właściwy, jako środek wstępny, w przypadku gdy administrator przetwarza dużą ilość danych niezdigitalizowanych, aby umożliwić osobie, której dane dotyczą, uzyskanie informacji na temat tego, jakie dane osobowe są przetwarzane, oraz podjęcie świadomej decyzji co do tego, jakie dane osobowe chce otrzymać w postaci kopii. Doraźne sposoby dostępu mogą być wystarczające i odpowiednie w niektórych sytuacjach; na przykład mogą zaspokoić potrzebę sprawdzenia przez osoby, których dane dotyczą, czy dane przetwarzane przez administratora są prawidłowe, umożliwiając tym osobom zapoznanie się z pierwotnymi danymi. Choć administrator danych nie jest zobowiązany do dostarczenia informacji w inny sposób niż w drodze przekazania kopii, powinien jednak przyjąć rozsądne podejście przy rozpatrywaniu takiego żądania. Udzielenie dostępu w inny sposób niż przez dostarczenie kopii nie wyklucza prawa osób, których dane dotyczą, do otrzymania także kopii, chyba że podejmą decyzję, że nie jest to konieczne.

[77] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, pkt 33.

134. Administrator może zdecydować, w zależności od sytuacji, o dostarczeniu kopii danych podlegających przetwarzaniu, wraz z informacjami uzupełniającymi, na różne sposoby, np. pocztą elektroniczną, pocztą tradycyjną lub za pomocą narzędzia samoobsługowego. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej, jak określono w art. 15 ust. 3. W każdym przypadku przy przekazywaniu informacji za pośrednictwem poczty elektronicznej lub internetowych narzędzi samoobsługowych administrator musi rozważyć odpowiednie środki techniczne i organizacyjne, w tym odpowiednie szyfrowanie.

135. Jeżeli administrator przetwarza dane osobowe dotyczące osoby występującej z żądaniem jedynie na niewielką skali, kopię danych osobowych i informacje uzupełniające można i należy przekazywać w ramach prostej procedury.

Przykład 22: Lokalna księgarnia prowadzi rejestr imion i nazwisk oraz adresów klientów, którzy zamówili dostawę do domu. Klient odwiedza księgarnię i zwraca się o dostęp do danych. W takiej sytuacji wystarczające byłoby wydrukowanie danych osobowych dotyczących klienta bezpośrednio z systemu przedsiębiorstwa, przy jednoczesnym przekazaniu informacji uzupełniających, o których mowa w art. 15 ust. 1 i 2.

Przykład 23: Osoba dokonująca co miesiąc darowizny na rzecz organizacji charytatywnej zwraca się o dostęp do danych pocztą elektroniczną. Organizacja charytatywna posiada informacje na temat darowizn dokonanych w ciągu ostatnich dwunastu miesięcy, a także imiona i nazwiska oraz adresy e-mail darczyńców. Administrator danych może przekazać kopię danych osobowych i informacje uzupełniające, odpowiadając na wiadomość e-mail, pod warunkiem że zastosowane zostaną wszystkie niezbędne zabezpieczenia, uwzględniające na przykład charakter danych.

136. Nawet administratorzy, którzy przetwarzają duże ilości danych, mogą zdecydować się na ręczne procedury rozpatrywania żądań dostępu. Jeżeli administrator przetwarza dane w kilku różnych działach, musi zebrać dane osobowe z każdego działu, aby móc odpowiedzieć na żądanie osoby, której dane dotyczą.

Przykład 24: Administrator wyznacza osobę zarządzającą danymi, która zajmuje się praktycznymi kwestiami dotyczącymi żądań dostępu. Po otrzymaniu żądania osoba zarządzająca danymi wysyła pocztą elektroniczną zapytanie do różnych poszczególnych działów organizacji, zwracając się do nich o zebranie danych osobowych dotyczących osoby, której dane dotyczą. Przedstawiciele każdego działu przekazują przetwarzane przez ten dział dane osobowe. Osoba zarządzająca danymi przesyła następnie wszystkie dane osobowe osobie, której dane dotyczą, wraz z niezbędnymi informacjami uzupełniającymi, na przykład, jeżeli jest to właściwe, pocztą elektroniczną.

137. Chociaż ręczne procesy rozpatrywania żądań dostępu można uznać za właściwe, w przypadku niektórych administratorów korzystne mogą być zautomatyzowane procesy tego rodzaju. Może tak być na przykład w przypadku administratorów, którzy otrzymują dużą liczbę żądań. Jednym ze sposobów przekazywania informacji na podstawie art. 15 jest zapewnienie osobie, której dane dotyczą, narzędzi samoobsługowych. Mogłoby to ułatwić skuteczne i terminowe rozpatrywanie żądań dostępu osób, których dane dotyczą, a także umożliwiłoby administratorowi włączenie mechanizmu weryfikacji do narzędzia samoobsługowego.

Przykład 25: Serwis mediów społecznościowych posiada zautomatyzowany proces rozpatrywania żądań dostępu, który umożliwia osobie, której dane dotyczą, dostęp do jej danych osobowych z poziomu konta użytkownika. Aby pobrać dane osobowe, użytkownicy mediów społecznościowych

mogą wybrać opcję „Pobierz swoje dane osobowe” po zalogowaniu się na swoje konto użytkownika. Ta opcja samoobsługi umożliwia użytkownikom pobranie pliku zawierającego ich dane osobowe bezpośrednio z konta użytkownika na ich własny komputer.

138. Korzystanie z narzędzi samoobsługowych nie powinno nigdy ograniczać zakresu przekazywanych danych osobowych. Jeżeli przekazanie wszystkich informacji na podstawie art. 15 za pośrednictwem narzędzia samoobsługowego nie jest możliwe, pozostałe informacje muszą zostać przekazane w inny sposób. Administrator może zachęcać osobę, której dane dotyczą, do korzystania z narzędzia samoobsługowego, które udostępnił w ramach procesu rozpatrywania żądań dostępu. Należy jednak zauważyć, że administrator musi również rozpatrywać żądania dostępu, które nie są przesyłane za pośrednictwem stałego kanału komunikacji[78].

5.2.3 Udzielenie dostępu w „zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem”

139. Zgodnie z art. 12 ust. 1 RODO administrator podejmuje odpowiednie środki w celu udzielenia dostępu zgodnie z art. 15 w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

140. Wymóg udzielenia osobie, której dane dotyczą, dostępu do informacji w zwięzłej i przejrzystej formie oznacza, że administratorzy powinni przedstawiać informacje w sposób efektywny i krótki, aby mogły być łatwo zrozumiałe przez osobę, której dane dotyczą, zwłaszcza jeżeli jest ona dzieckiem. Przy wyborze sposobów udzielania dostępu zgodnie z art. 15 administrator musi wziąć pod uwagę ilość i złożoność danych.

Przykład 26: Dostawca mediów społecznościowych przetwarza duże ilości informacji o osobie, której dane dotyczą. Znaczną część tych danych osobowych stanowią informacje zawarte w liczących setki stron plikach dziennika, w których rejestruje się działania osoby, której dane dotyczą, na stronie internetowej. Jeżeli osoby, których dane dotyczą, występują z żądaniem dostępu do swoich danych osobowych, dane osobowe zawarte w tych plikach dziennika są objęte prawem dostępu. Prawu dostępu może zatem zostać formalnie uczynić zadość, jeżeli te setki stron plików dziennika zostaną udostępnione osobie, której dane dotyczą. Jeżeli jednak nie zostaną przedsięwzięte środki mające na celu ułatwienie zrozumienia informacji zawartych w plikach dziennika, prawo dostępu osoby, której dane dotyczą, może nie być spełnione w praktyce, ponieważ z plików dziennika nie można łatwo uzyskać żądanej wiedzy, a zatem takie udostępnienie nie spełnia wymogu określonego w art. 12 ust. 1 RODO. Administrator musi zatem ostrożnie i starannie wybrać sposób przedstawienia informacji i danych osobowych osobie, której dane dotyczą.

141. W okolicznościach przedstawionych w powyższym przykładzie odpowiednim środkiem umożliwiającym spełnienie wymogów określonych w art. 15 oraz w art. 12 ust. 1 RODO może być zastosowanie podejścia warstwowego, podobnego do podejścia warstwowego zalecanego w wytycznych w sprawie przejrzystości w odniesieniu do oświadczeń o ochronie prywatności[79]. Kwestia ta zostanie doprecyzowana w sekcji 5.2.4 poniżej. Wymóg, aby informacje były „czytelne”,

[78] Zob. sekcja 3.1.2.
[79] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, pkt 35.

oznacza, że powinny być one zrozumiałe dla docelowych odbiorców[80], przy czym należy pamiętać o wszelkich szczególnych potrzebach, jakie osoba, której dane dotyczą, zgodnie z wiedzą administratora może mieć[81]. Ponieważ prawo dostępu często umożliwia wykonywanie innych praw osób, których dane dotyczą, istotne jest, aby przekazywane informacje były zrozumiałe i jasne. Osoby, których dane dotyczą, będą bowiem mogły rozważyć, czy powołać się na przykład na prawo do sprostowania danych zgodnie z art. 16 RODO dopiero wtedy, gdy wiedzą, jakie dane osobowe są przetwarzane, w jakich celach itp. W związku z tym może zaistnieć potrzeba, aby administrator udzielił osobie, której dane dotyczą, dodatkowych informacji wyjaśniających przekazane dane. Należy podkreślić, że złożoność przetwarzania danych zobowiązuje administratora do zapewnienia środków umożliwiających zrozumienie danych i nie może być wykorzystywana jako argument za ograniczeniem dostępu do wszystkich danych. Podobnie spoczywający na administratorze obowiązek przekazywania danych w zwięzły sposób nie może być wykorzystywany jako argument za ograniczeniem dostępu do wszystkich danych.

Przykład 27: Strona internetowa wykorzystywana do celów handlu elektronicznego gromadzi dane dotyczące przeglądanych lub zakupionych artykułów do celów marketingowych. Część tych danych będzie składać się z danych w formacie surowym[82], które nie zostały przeanalizowane i mogą nie mieć bezpośredniego znaczenia dla użytkownika (kody, historia aktywności itp.). Takie dane związane z działaniami osób, których dane dotyczą, są również objęte prawem dostępu i w związku z tym powinny być przekazywane osobie, której dane dotyczą, w odpowiedzi na żądanie dostępu. Przy przekazywaniu danych w formacie nieprzetworzonym administrator musi przedsięwziąć niezbędne środki w celu zapewnienia, aby osoba, której dane dotyczą, zrozumiała dane, na przykład dostarczyć dokument wyjaśniający, w którym przetłumaczono surowy format na formę przyjazną dla użytkownika. Dokument taki mógłby również wyjaśniać, że skróty i inne akronimy, na przykład „A", oznaczają, że zakup został przerwany, a „B" oznacza, że zakup został dokonany.

142. Element „łatwo dostępnej formy" oznacza, że informacje, o których mowa w art. 15, powinny być przedstawione osobie, której dane dotyczą, w sposób łatwo dla niej dostępny. Dotyczy to na przykład układu graficznego, odpowiednich nagłówków i podziału na akapity. Informacji należy zawsze udzielać jasnym i prostym językiem. Administrator, który oferuje usługę w danym państwie, powinien ponadto udzielić odpowiedzi w języku zrozumiałym dla osób, których dane dotyczą, w tym państwie. Zachęca się również do stosowania standardowych znaków graficznych, jeżeli poprawiają one zrozumiałość i dostępność informacji. Jeżeli żądanie udzielenia informacji dotyczy osób słabowidzących lub innych osób, których dane dotyczą, mogących mieć trudności z dostępem do informacji lub ich zrozumieniem, oczekuje się, że administrator przedsięweźmie środki ułatwiające zrozumienie przekazanych informacji, w tym, w stosownych przypadkach, informacji ustnych[83]. Administrator powinien szczególnie zadbać o to, by osoby starsze, dzieci, osoby słabowidzące lub osoby z zaburzeniami funkcji poznawczych lub innymi niepełnosprawnościami mogły korzystać ze swoich praw, na przykład

[80]Zrozumiałość jest ściśle związana z wymogiem użycia jasnego i prostego języka (wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, pkt 9). To, co zostało powiedziane o jasnym i prostym języku w pkt 12–16 w odniesieniu do informacji, o których mowa w art. 13 i 14 RODO, ma również zastosowanie do udzielania informacji zgodnie z art. 15.

[81] Zob. pkt 128.

[82] Surowy format w tym przykładzie należy rozumieć jako niepoddane analizie dane będące przedmiotem przetwarzania, a nie najniższy poziom surowych danych, które można odczytać jedynie maszynowo (takich jak „bity").

[83] Zob. wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, pkt 21.

w drodze proaktywnego udostępniania łatwo dostępnych elementów ułatwiających korzystanie z tych praw.

5.2.4 Duża ilość informacji pociąga za sobą szczegółowe wymogi dotyczące sposobu udzielania informacji.

143. Niezależnie od środków wykorzystywanych do zapewnienia dostępu zapewnienie równowagi między ilością informacji, które administrator jest zobowiązany przekazać osobom, których dane dotyczą, a wymogiem, aby informacje te były zwięzłe, może okazać się trudne. Jednym ze sposobów osiągnięcia obu tych celów, a także przykładem odpowiedniego środka dla niektórych administratorów, gdy ma zostać przekazana duża ilość danych, jest zastosowanie podejścia warstwowego. Podejście to może ułatwić osobom, których dane dotyczą, zrozumienie danych. Należy jednak podkreślić, że podejście to może być stosowane tylko w pewnych okolicznościach i musi być realizowane w sposób, który nie ogranicza prawa dostępu, jak wyjaśniono poniżej. Ponadto stosowanie podejścia warstwowego nie może stanowić dodatkowego obciążenia dla osoby, której dane dotyczą. Dlatego najlepiej byłoby, gdyby dostęp był udzielany w kontekście internetowym. Podejście warstwowe jest jedynie sposobem przedstawienia informacji zgodnie z art. 15, który to sposób jest ponadto zgodny z wymogami określonymi w art. 12 ust. 1 RODO i nie należy go mylić z możliwością zwrócenia się przez administratorów do osoby, której dane dotyczą, o sprecyzowanie informacji lub czynności przetwarzania, których dotyczy żądanie, jak określono w motywie 63 RODO[84].

144. Podejście warstwowe w odniesieniu do prawa dostępu oznacza, że administrator, w określonych okolicznościach, może przekazać dane osobowe i informacje uzupełniające wymagane zgodnie z art. 15 w różnych warstwach. Pierwsza warstwa powinna obejmować informacje o przetwarzaniu i prawach osoby, której dane dotyczą, zgodnie z art. 15 ust. 1 lit. a)–h) i art. 15 ust. 2, a także pierwszą część przetwarzanych danych osobowych. W drugiej warstwie należy przekazać dalsze dane osobowe.

145. Decydując o tym, jakie informacje należy przekazać w poszczególnych warstwach, administrator powinien rozważyć, jakie informacje osoba, której dane dotyczą, uznałaby ogólnie za najistotniejsze. Zgodnie z zasadą rzetelności pierwsza warstwa powinna również zawierać informacje na temat przetwarzania, które ma największy wpływ na osobę, której dane dotyczą[85]. W odniesieniu do podziału informacji na poszczególne warstwy administratorzy muszą być w stanie wykazać, że zdecydowali się na taki, a nie inny podział, z uwzględnieniem zasady rozliczalności.

> **Przykład 28:** Administrator analizuje duże zbiory danych w celu przypisania klientów do różnych segmentów w zależności od zachowania klientów w internecie. W tej sytuacji można założyć, że informacją, która jest najważniejsza dla osób, których dane dotyczą, jest informacja, do jakiego segmentu je przypisano. Informacja ta powinna zatem być zawarta w pierwszej warstwie. Dane w surowym formacie[86], które nie zostały jeszcze przeanalizowane lub przetworzone, takie jak aktywność użytkowników na stronie internetowej, są również danymi osobowymi objętymi prawem dostępu, jednak w niektórych przypadkach wystarczające może być podanie tych informacji w innej warstwie.

146. Aby zastosowanie podejścia warstwowego można było uznać za odpowiedni środek, konieczne jest poinformowanie osoby, której dane dotyczą, na samym początku, że informacje przekazywane zgodnie z art. 15 są podzielone na różne warstwy, oraz przedstawienie tej osobie opisu danych osobowych

[84] Zob. również sekcja 2.3.1.
[85] Zob. wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości – zatwierdzone przez EROD, pkt 36.
[86] Zob. przypis 82.

i informacji, które będą zawarte w poszczególnych warstwach. Dzięki temu osobie, której dane dotyczą, łatwiej będzie zdecydować, do których warstw chce uzyskać dostęp. Opis powinien obiektywnie odzwierciedlać wszystkie kategorie danych osobowych, które są faktycznie przetwarzane przez administratora. Należy również jasno określić, w jaki sposób osoba, której dane dotyczą, może uzyskać dostęp do poszczególnych warstw. Dostęp do poszczególnych warstw nie może wiązać się z nieproporcjonalnym wysiłkiem dla osoby, której dane dotyczą, i nie może być uzależniony od sformułowania nowego żądania dostępu. Oznacza to, że osoby, których dane dotyczą, muszą mieć możliwość wyboru, czy chcą uzyskać dostęp do wszystkich warstw jednocześnie, czy też do jednej lub dwóch warstw, jeśli to im wystarczy.

Przykład 29: Osoba, której dane dotyczą, występuje z żądaniem dostępu do usługi transmisji strumieniowej wideo. Żądanie można wnieść za pomocą opcji, która jest dostępna po zalogowaniu się dla osób, których dane dotyczą. Osoba, której dane dotyczą, ma możliwość wyboru dwóch opcji umieszczonych w formie przycisków na stronie internetowej. Opcja pierwsza polega na pobraniu pierwszej części danych osobowych i informacji uzupełniających. Obejmuje to na przykład aktualną historię transmisji strumieniowej, informacje o koncie i informacje o płatnościach. Opcja drugi polega na pobraniu drugiej części danych osobowych, która zawiera pliki dziennika technicznego dotyczące działań osób, których dane dotyczą, oraz informacje historyczne dotyczące konta. W tym przypadku administrator umożliwił osobom, których dane dotyczą, skorzystanie z przysługującego im prawa w sposób, który nie powoduje dla nich dodatkowego obciążenia.

Wariant 1: Jeżeli osoba, której dane dotyczą, wybiera tylko przycisk pobierania pierwszej części danych osobowych, administrator jest zobowiązany do przekazania tylko pierwszej części tych danych.

Wariant 2: Jeżeli osoba, której dane dotyczą, wybiera przycisk pobierania zarówno pierwszej, jak i drugiej części danych osobowych, administrator nie może przekazać tylko pierwszej części danych i zwrócić się o nowe potwierdzenie przed przekazaniem drugiej ich części. Musi przekazać osobie, której dane dotyczą, obie części danych, zgodnie z jej żądaniem.

147. Podejścia warstwowego nie uważa się za odpowiednie dla wszystkich administratorów ani we wszystkich sytuacjach. Powinno być stosowane tylko wtedy, gdy osobie, której dane dotyczą, trudno byłoby zrozumieć informacje, gdyby zostały przekazane w całości. Innymi słowy, administrator musi być w stanie wykazać, że zastosowanie podejścia warstwowego stanowi wartość dodaną z punktu widzenia osoby, której dane dotyczą, gdyż pomaga jej zrozumieć przekazywane informacje. Podejście warstwowe będzie więc uznane za właściwe jedynie w przypadku, gdy administrator przetwarza duże ilości danych osobowych występującej z żądaniem osoby, której dane dotyczą, oraz gdy osoba ta miałaby oczywiste trudności w zrozumieniu informacji, gdyby przekazano je na raz. Fakt, że przekazanie informacji zgodnie z art. 15 wymagałoby od administratora znacznego wysiłku i dużych zasobów, nie jest sam w sobie argumentem za stosowaniem podejścia warstwowego.

5.2.5 Format

148. Zgodnie z art. 12 ust. 1 RODO informacji, o których mowa w art. 15, udziela się na piśmie lub w inny sposób, w tym, w stosownych przypadkach, drogą elektroniczną. Jeśli chodzi o dostęp do przetwarzanych danych osobowych, art. 15 ust. 3 stanowi, że jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej. W RODO nie określono, czym jest powszechnie stosowana forma elektroniczna, a zatem istnieje kilka możliwych formatów, których można użyć. To, co uznaje się za powszechnie stosowaną formę elektroniczną, będzie się również zmieniać z biegiem czasu.

149. Decyzja, co można uznać za powszechnie stosowaną formę elektroniczną, powinna opierać się na obiektywnej ocenie, a nie formacie wykorzystywanym przez administratora w swojej codziennej działalności. Aby określić, jaki format należy uznać za powszechnie stosowany w danej sytuacji, administrator będzie musiał ocenić, czy istnieją konkretne formaty powszechnie stosowane w obszarze działalności administratora lub w danym kontekście. Jeżeli takie formaty nie są powszechnie stosowane, za powszechnie stosowane formaty elektroniczne należy zasadniczo uznać formaty otwarte określone w normie międzynarodowej, takiej jak ISO. EROD nie wyklucza jednak możliwości, że za powszechnie stosowane w rozumieniu art. 15 ust. 3 można również uznać inne formaty. EROD zwraca uwagę, że podczas oceny, czy dany format jest powszechnie stosowanym formatem elektronicznym, ważne jest wzięcie pod uwagę, jak łatwo zainteresowana osoba będzie mogła uzyskać dostęp do informacji przekazywanych w obecnym formacie. W związku z tym należy wziąć pod uwagę, jakie informacje administrator przekazał osobie, której dane dotyczą, na temat sposobu uzyskania dostępu do pliku przekazanego w określonym formacie, np. jakie programy lub oprogramowanie można zastosować, aby uczynić format bardziej dostępnym dla osoby, której dane dotyczą. Osoba, której dane dotyczą, nie powinna być jednak zobowiązana do zakupu oprogramowania w celu uzyskania dostępu do informacji.

150. Podejmując decyzję dotyczącą formatu, w jakim należy przekazać kopię danych osobowych i informacje zgodnie z art. 15, administrator musi pamiętać, że format musi umożliwiać przedstawienie informacji w sposób zarówno zrozumiały, jak i łatwo dostępny. Ważne, aby osoba, której dane dotyczą, otrzymywała informacje w zmaterializowanym i trwałym formacie (tekst, wersja elektroniczna). Ponieważ informacje powinny cechować się długoterminową trwałością, przekazywanie ich w formie pisemnej, w tym drogą elektroniczną, jest co do zasady preferowane w stosunku do innych form. Kopia danych osobowych może, w stosownych przypadkach, być przechowywana na elektronicznym urządzeniu do przechowywania danych, takim jak płyta CD lub pamięć USB.

151. Należy zauważyć, że aby administrator mógł uznać, że osobom, których dane dotyczą, przekazano kopię danych osobowych, nie wystarczy zapewnić im dostępu do ich danych osobowych. Aby spełnić wymóg przekazania kopii danych osobowych, a w przypadku gdy dane są przekazywane drogą elektroniczną/cyfrową, osoby, których dane dotyczą, muszą mieć możliwość pobrania swoich danych w powszechnie stosowanej formie elektronicznej.

152. Podjęcie decyzji o odpowiedniej formie, w jakiej dane osobowe zostaną przekazane, należy do obowiązków administratora. Administrator może, choć nie musi, przekazać dokumenty zawierające dane osobowe osób, których dane dotyczą i które zwróciły się z żądaniem, w oryginalnej formie. Administrator danych może na przykład w poszczególnych przypadkach zapewnić dostęp do kopii nośnika jako takiej, biorąc pod uwagę potrzebę przejrzystości (na przykład w celu sprawdzenia prawidłowości danych przechowywanych przez administratora w przypadku żądania dostępu do dokumentacji medycznej lub nagrania dźwiękowego, którego transkrypcja jest przedmiotem sporu). Dokonując wykładni prawa dostępu przewidzianego w dyrektywie 95/46/WE, TSUE stwierdził jednak, że „aby uczynić zadość [prawu dostępu], wystarczy, by wspomniany wnioskodawca znalazł się w posiadaniu kompletnego przeglądu tych danych w zrozumiałej formie, czyli w formie umożliwiającej mu zapoznanie się ze wspomnianymi danymi i sprawdzenie, czy dane te są prawidłowe i czy są przetwarzane w sposób zgodny ze wspomnianą dyrektywą, aby w razie potrzeby móc wykonać prawa przyznane mu w tej dyrektywie”[87]. W przeciwieństwie do dyrektywy RODO wyraźnie przewiduje

[87] TSUE, sprawy połączone C-141/12 i C-372/12, YS i in., pkt 60.

obowiązek przekazania osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu. Nie oznacza to jednak, że osoba, której dane dotyczą, ma zawsze prawo do uzyskania kopii dokumentów zawierających dane osobowe, lecz niezmienionej kopii danych osobowych przetwarzanych w tych dokumentach[88]. Taka kopia danych osobowych może zostać dostarczona w formie zestawienia zawierającego wszystkie dane osobowe objęte prawem dostępu, o ile takie zestawienie zapewnia osobie, której dane dotyczą, świadomość przetwarzania i możliwość zweryfikowania zgodności przetwarzania z prawem. W związku z tym nie ma sprzeczności między brzmieniem RODO a orzeczeniem TSUE w tej sprawie. Zawartego w orzeczeniu sformułowania „przegląd" nie należy błędnie interpretować jako oznaczającego, że zestawienie nie obejmuje wszystkich danych objętych prawem dostępu – stanowi ono jedynie sposób przedstawienia wszystkich tych danych bez udostępniania podstawowych dokumentów zawierających dane osobowe. Ponieważ zestawienie musi zawierać kopię danych osobowych, należy podkreślić, że nie może być wykonane w sposób, który w jakikolwiek sposób zmienia lub modyfikuje treść informacji.

Przykład 30: Osoba, której dane dotyczą, jest ubezpieczona w zakładzie ubezpieczeń od wielu lat. Wystąpiło kilka zdarzeń objętych ubezpieczeniem. W każdym przypadku prowadzona była pisemna korespondencja za pośrednictwem poczty elektronicznej między osobą, której dane dotyczą, a zakładem ubezpieczeń. Ponieważ osoba, której dane dotyczą, musiała udzielić informacji na temat szczególnych okoliczności każdego zdarzenia, korespondencja zawiera wiele danych osobowych osoby, której dane dotyczą (hobby, współlokatorzy, codzienne nawyki itp.). W niektórych przypadkach strony nie mogły dość do porozumienia co do obowiązku zakładu ubezpieczeń w zakresie wypłaty odszkodowania osobie, której dane dotyczą, co skutkowało intensywną komunikacją prowadzoną w obie strony. Cała ta korespondencja jest przechowywana przez zakład ubezpieczeń. Osoba, której dane dotyczą, występuje z żądaniem dostępu. W takiej sytuacji administrator niekoniecznie musi dostarczać wiadomości e-mail w ich oryginalnej formie, przekazując je osobie, której dane dotyczą. Zamiast tego administrator może zdecydować się na zestawienie korespondencji e-mail zawierającej dane osobowe osoby, której dane dotyczą, w pliku przekazanym tej osobie.

153. Niezależnie od formy, w jakiej administrator przekazuje dane osobowe, np. dostarczając same dokumenty zawierające dane osobowe lub zestawienie danych osobowych, informacje muszą być zgodne z wymogami dotyczącymi przejrzystości określonymi w art. 12 RODO. Sporządzenie pewnego rodzaju zestawienia lub wyciągu danych w sposób ułatwiający zrozumienie informacji może w niektórych przypadkach stanowić sposób spełnienia tych wymogów. W innych przypadkach informacje są lepiej zrozumiałe, gdy dostarczy się kopię samego dokumentu zawierającego dane osobowe. W związku z tym decyzję o tym, która forma jest najodpowiedniejsza, należy podejmować indywidualnie dla każdego przypadku.

154. W tym kontekście należy pamiętać, że istnieje rozróżnienie między prawem do uzyskania dostępu przewidzianym w art. 15 RODO a prawem do otrzymania kopii dokumentów administracyjnych uregulowanym w prawie krajowym, które stanowi uprawnienie do otrzymania kopii samego dokumentu. Nie oznacza to, że prawo dostępu przewidziane w art. 15 RODO wyklucza możliwość otrzymania kopii dokumentu/nośnika, na którym znajdują się dane osobowe.

155. W niektórych przypadkach same dane osobowe określają wymogi dotyczące formatu, w jakim dane te powinny być przekazywane. Na przykład jeżeli dane osobowe stanowią informacje napisane odręcznie przez osobę, której dane dotyczą, może zaistnieć potrzeba dostarczenia jej kserokopii tych odręcznych

[88] Kwestie związane z tym zagadnieniem są przedmiotem spraw zawisłych obecnie przed TSUE (C-487/21 i C-307/21).

informacji, ponieważ samo odręczne pismo stanowi dane osobowe. Może to mieć miejsce zwłaszcza w przypadku, gdy odręczne pismo ma znaczenie dla przetwarzania danych, np. przy analizie rękopisów. To samo dotyczy ogólnie nagrań dźwiękowych, ponieważ głos osoby, której dane dotyczą, stanowi dane osobowe. W niektórych przypadkach można jednak zapewnić dostęp, dostarczając transkrypcję rozmowy, na przykład jeżeli osoba, której dane dotyczą, i administrator tak uzgodnią.

156. Należy zauważyć, że przepisy dotyczące wymogów w zakresie formatu różnią się w odniesieniu do prawa dostępu i prawa do przenoszenia danych. Podczas gdy prawo do przenoszenia danych przewidziane w art. 20 RODO wymaga, aby informacje były przekazywane w formacie nadającym się do odczytu maszynowego, prawo do informacji przewidziane w art. 15 tego nie wymaga. W związku z tym formaty, które uznaje się za nieodpowiednie przy spełnianiu żądania przeniesienia danych, na przykład pliki pdf, mogą być nadal odpowiednie przy spełnianiu żądania dostępu.

5.3 Termin zapewnienia dostępu

157. W art. 12 ust. 3 RODO wymaga się, aby administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udzielił osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15. Termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, pod warunkiem że osoba, której dane dotyczą, została poinformowana o przyczynach takiego opóźnienia w terminie jednego miesiąca od otrzymania żądania przez administratora. Tego obowiązku poinformowania osoby, której dane dotyczą, o przedłużeniu terminu i jego powodach nie należy mylić z informacjami, które należy przekazać niezwłocznie, a najpóźniej w terminie jednego miesiąca, w przypadku gdy administrator nie podejmie działań w związku z żądaniem, jak określono w art. 12 ust. 4 RODO.

158. Administrator reaguje i, co do zasady, udziela informacji zgodnie z art. 15 bez zbędnej zwłoki, co oznacza, że informacje te należy przekazać możliwie najszybciej. Oznacza to, że jeżeli możliwe jest dostarczenie żądanych informacji w terminie krótszym niż jeden miesiąc, administrator powinien to zrobić. EROD uważa również, że termin udzielenia odpowiedzi na żądanie w niektórych sytuacjach musi zostać dostosowany do okresu przechowywania, aby móc zapewnić dostęp[89].

159. Bieg terminu rozpoczyna się w momencie otrzymania przez administratora żądania, o którym mowa art. 15, co oznacza, że żądanie dociera do administratora za pośrednictwem jednego z jego oficjalnych kanałów[90]. Nie jest konieczne, aby administrator faktycznie wiedział o żądaniu. Jeżeli jednak administrator musi skontaktować się z osobą, której dane dotyczą, ze względu na niepewność co do tożsamości osoby występującej z żądaniem, może nastąpić zawieszenie biegu terminu do czasu uzyskania przez niego niezbędnych informacji od osoby, której dane dotyczą, pod warunkiem że administrator zwrócił się o dodatkowe informacje bez zbędnej zwłoki. To samo dotyczy sytuacji, gdy administrator zwrócił się do osoby, której dane dotyczą, o określenie operacji przetwarzania, których dotyczy żądanie, jeżeli spełnione są warunki określone w motywie 63[91].

Przykład 31: Po otrzymaniu żądania administrator niezwłocznie reaguje i zwraca się o informacje niezbędne do potwierdzenia tożsamości osoby występującej z tym żądaniem. Osoba, której dane

[89] Zob. sekcja 2.3.3.
[90] W niektórych państwach członkowskich istnieją przepisy krajowe określające, kiedy wiadomość należy uznać za odebraną, biorąc pod uwagę weekendy i święta państwowe.
[91] Więcej informacji na ten temat znajduje się w sekcji 2.3.1.

dotyczą, odpowiada dopiero kilka dni później, a informacje, które przesyła w celu weryfikacji tożsamości, nie wydają się wystarczające, w związku z czym administrator musi zwrócić się do niej o wyjaśnienia. W takiej sytuacji nastąpi zawieszenie biegu terminu do czasu uzyskania przez administratora informacji wystarczających do zweryfikowania tożsamości osoby, której dane dotyczą.

160. Termin na udzielenie odpowiedzi na żądanie dostępu należy obliczać zgodnie z rozporządzeniem nr 1182/71[92].

Przykład 32: Organizacja otrzymuje żądanie 5 marca. Bieg terminu rozpoczyna się w tym samym dniu. Daje to organizacji możliwość spełnienia żądania najpóźniej do 5 kwietnia włącznie.

Przykład 33: Jeżeli organizacja otrzyma żądanie 31 sierpnia, biorąc pod uwagę, że następny miesiąc jest krótszy, nie ma odpowiadającej daty, w związku z czym odpowiedzi należy udzielić najpóźniej ostatniego dnia następnego miesiąca, czyli 30 września.

161. Jeżeli ostatni dzień tego terminu przypada na weekend lub dzień ustawowo wolny od pracy, administrator ma czas na udzielenie odpowiedzi do następnego dnia roboczego.

162. W określonych okolicznościach administrator może w razie potrzeby przedłużyć czas na udzielenie odpowiedzi na żądanie dostępu o kolejne dwa miesiące, biorąc pod uwagę skomplikowany charakter żądania lub liczbę żądań. Należy podkreślić, że możliwość ta stanowi odstępstwo od zasady ogólnej i nie powinna być nadużywana. Jeżeli administratorzy często są zmuszeni do przedłużenia terminu, może to wskazywać na potrzebę dalszego rozbudowania ogólnych procedur rozpatrywania żądań.

163. To, co stanowi skomplikowane żądanie, różni się w zależności od konkretnych okoliczności w danym przypadku. Wśród czynników, które można uznać za istotne w tym względzie, znajdują się na przykład:

- ilość danych przetwarzanych przez administratora,
- sposób przechowywania informacji, zwłaszcza gdy trudno jest je pobrać, na przykład gdy dane są przetwarzane przez różne jednostki organizacji,
- potrzebę utajniania informacji w przypadku zastosowania wyłączenia, na przykład informacji na temat innych osób, których dane dotyczą, lub stanowiących tajemnice handlowe, oraz
- gdy informacje wymagają dalszych prac, aby były zrozumiałe.

164. Sam fakt, że spełnienie żądania wymagałoby dużego wysiłku, nie sprawia, że żądanie uznaje się za skomplikowane. Podobnie fakt, że duże przedsiębiorstwo otrzymuje dużą liczbę żądań, nie spowodowałby automatycznego przedłużenia terminu ich wykonania. Jeżeli jednak administrator otrzymuje tymczasowo dużą liczbę żądań, na przykład ze względu na nadzwyczajne rozpowszechnienie informacji o jego działalności, można to uznać za uzasadniony powód przedłużenia czasu reakcji. Niemniej administrator, szczególnie gdy zajmuje się dużą ilością danych, powinien dysponować procedurami i mechanizmami umożliwiającymi rozpatrywanie żądań w określonych terminach w normalnych okolicznościach.

[92] Rozporządzenie Rady (EWG, Euratom) nr 1182/71 z dnia 3 czerwca 1971 r. określające zasady mające zastosowanie do okresów, dat i terminów.

6 OGRANICZENIA I RESTRYKCJE DOTYCZĄCE PRAWA DOSTĘPU

6.1 Uwagi ogólne

165. Prawo dostępu podlega ograniczeniom wynikającym z art. 15 ust. 4 RODO (prawa i wolności innych) i art. 12 ust. 5 RODO (ewidentnie nieuzasadnione lub nadmierne żądania). Prawo Unii lub prawo państwa członkowskiego mogą ponadto ograniczać prawo dostępu zgodnie z art. 23 RODO. Odstępstwa dotyczące przetwarzania danych osobowych do celów badań naukowych lub historycznych, do celów statystycznych lub do celów archiwalnych w interesie publicznym mogą opierać się odpowiednio na art. 89 ust. 2 i 3 RODO, a odstępstwa dotyczące przetwarzania realizowanego dla potrzeb dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej mogą opierać się na art. 85 ust. 2 RODO.

166. Należy zauważyć, że oprócz wyżej wymienionych ograniczeń, odstępstw i możliwych restrykcji RODO nie zezwala na żadne dalsze wyłączenia ani odstępstwa od prawa dostępu. Oznacza to między innymi, że prawo dostępu nie obejmuje żadnych ogólnych zastrzeżeń co do proporcjonalności w odniesieniu do starań, jakie administrator musi podjąć w celu spełnienia żądania osób, których dane dotyczą, na podstawie art. 15 RODO[93]. Co więcej, niedozwolone jest ograniczanie prawa dostępu w umowie między administratorem a osobą, której dane dotyczą.

167. Zgodnie z motywem 63 prawo dostępu przysługuje osobom, których dane dotyczą, po to, aby miały one świadomość przetwarzania i mogły zweryfikować zgodność przetwarzania z prawem. Prawo dostępu umożliwia między innymi osobie, której dane dotyczą, uzyskanie w razie potrzeby sprostowania, usunięcia lub zablokowania danych osobowych[94]. Osoby, których dane dotyczą, nie są jednak zobowiązane do podawania powodów ani do uzasadniania swojego żądania. O ile spełnione są wymogi określone w art. 15 RODO, cele wystąpienia z żądaniem należy uznać za nieistotne[95].

6.2 Art. 15 ust. 4 RODO

168. Zgodnie z art. 15 ust. 4 RODO prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych. Wyjaśnienia dotyczące tego ograniczenia znajdują się w motywie 63 zdania piąte i szóste. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie.
Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Przy dokonywaniu wykładni art. 15 ust. 4 RODO należy zachować szczególną ostrożność, aby w sposób nieuzasadniony nie rozszerzyć ograniczeń określonych w art. 23 RODO, które są dopuszczalne jedynie pod ściśle określonymi warunkami.

169. Art. 15 ust. 4 RODO ma zastosowanie do prawa do uzyskania kopii danych, co jest głównym sposobem udzielania dostępu do przetwarzanych danych (drugi element prawa dostępu). Ma on również zastosowanie, a prawa i wolności innych osób należy brać pod uwagę, jeżeli dostęp do danych osobowych jest udzielony w drodze wyjątku w inny sposób niż przy użyciu kopii. Na przykład nie ma

[93] Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, jak wspomniano w motywie 63 RODO, może on zażądać, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie. Zob. również sekcja 2.3.1.
[94] TSUE, sprawy połączone C-141/12 i C-372/12, YS i in.
[95] Pozostaje to bez uszczerbku dla wszelkich obowiązujących przepisów prawa krajowego, które są zgodne z wymogami określonymi w art. 23 RODO, zob. rozdział 6.4.

zasadnej różnicy, czy udostępnienie kopii lub udzielenie dostępu na miejscu osobie, której dane dotyczą, ma wpływ na tajemnice handlowe. Art. 15 ust. 4 RODO nie ma zastosowania do dodatkowych informacji na temat przetwarzania, o których mowa w art. 15 ust. 1 lit. a)–h) RODO.

170. Jak stwierdzono w motywie 63, kolidujące prawa i wolności obejmują tajemnice handlowe lub własność intelektualną, w szczególności prawa autorskie chroniące oprogramowanie. Te wyraźnie wskazane prawa i wolności należy traktować jedynie jako przykłady, ponieważ co do zasady wszelkie prawa lub wolności oparte na prawie Unii lub prawie państwa członkowskiego można uznać za powołujące się na ograniczenie określone w art. 15 ust. 4 RODO[96]. W związku z tym można również uznać, że prawo do ochrony danych osobowych (art. 8 Karty praw podstawowych Unii Europejskiej) jest jednym z praw, na które w rozumieniu art. 15 ust. 4 RODO nie można niekorzystnie wpływać. Jeżeli chodzi o prawo do uzyskania kopii, prawo do ochrony danych innych osób jest typowym przypadkiem, w którym należy ocenić zastosowanie ograniczenia. Należy ponadto wziąć pod uwagę prawo do poufności korespondencji, na przykład w odniesieniu do prywatnej korespondencji elektronicznej w kontekście zatrudnienia[97]. Należy zauważyć, że nie każdy interes stanowi „prawa i wolności" w rozumieniu art. 15 ust. 4 RODO. Na przykład interesy gospodarcze przedsiębiorstwa polegające na nieujawnianiu danych osobowych nie osiągają progu umożliwiającego skorzystanie z wyłączenia przewidzianego w art. 15 ust. 4, o ile nie ma to wpływu na tajemnice handlowe, własność intelektualną lub inne chronione prawa.

171. „Inni" oznaczają każdą osobę lub każdy podmiot niebędące korzystającą z prawa dostępu osobą, której dane dotyczą. W związku z tym można mieć na względzie również prawa i wolności administratora lub podmiotu przetwarzającego (np. związane z zachowaniem tajemnicy handlowej i poufności własności intelektualnej). Gdyby prawodawca Unii chciał wyłączyć z tego zakresu prawa i wolności administratorów lub podmiotów przetwarzających, użyłby terminu „strona trzecia" w rozumieniu art. 4 pkt 10 RODO.

172. Ogólna obawa, że spełnienie żądania dostępu może mieć wpływ na prawa i wolności innych, nie wystarczy, aby móc powołać się na art. 15 ust. 4 RODO. Administrator musi być w stanie wykazać, że w konkretnej sytuacji prawa lub wolności innych osób faktycznie zostałyby naruszone.

> **Przykład 34:**Osoba, która jest już dorosła, w przeszłości przez wiele lat była pod opieką Urzędu ds. Dzieci i Młodzieży. Związana z tym dokumentacja może zawierać szczególnie chronione informacje o innych osobach (rodzicach, pracownikach socjalnych, innych małoletnich). Zasadniczo nie jest to jednak powód, aby powołując się na art. 15 ust. 4 RODO, odrzucić żądanie udzielenia informacji wystosowane przez osobę, której dane dotyczą. Przeciwnie, Urząd ds. Dzieci i Młodzieży jako administrator musi szczegółowo przeanalizować i wykazać prawa i wolności innych. W zależności od branych pod uwagę interesów i ich względnej wagi żądanie podania takich konkretnych informacji może zostać odrzucone (np. przez utajnienie imion i nazwisk).

173. W odniesieniu do motywu 4 RODO i uzasadnienia art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej prawo do ochrony danych osobowych nie jest prawem bezwzględnym[98]. W związku z tym wykonanie prawa dostępu należy też wyważyć względem innych praw podstawowych w myśl zasady

[96] Waga lub pierwszeństwo kolidujących praw i wolności nie jest kwestią definicji terminów „prawa i wolności". Wyważenie takich interesów stanowi jednak część drugiego etapu oceny, czy art. 15 ust. 4 ma zastosowanie. Zob. pkt 173 poniżej.

[97] ETPC, Bărbulescu/Rumunia, sprawa nr 61496/08, pkt 80, 5 września 2017 r.

[98] Zob. również na przykład TSUE, sprawy połączone C-92/09 i C-93/09, Volker und Markus Schecke GbR i Hartmut Eifert/Land Hessen [GC], 9 listopada 2010 r., pkt 48.

proporcjonalności. W przypadku gdy ocena na podstawie art. 15 ust. 4 RODO wykaże, że zastosowanie się do żądania ma niekorzystny (negatywny) wpływ na prawa i wolności innych zainteresowanych osób (etap 1), należy rozważyć interesy wszystkich zainteresowanych osób, biorąc pod uwagę konkretne okoliczności w danym przypadku, a w szczególności prawdopodobieństwo i wagę ryzyka związanego z przekazaniem danych. Administrator powinien starać się pogodzić kolidujące prawa (etap 2), na przykład przez wdrożenie odpowiednich środków ograniczających ryzyko dla praw i wolności innych**.** Jak podkreślono w motywie 63, ochrona praw i wolności innych osób wynikająca z art. 15 ust. 4 RODO nie powinna skutkować odmową udzielenia wszystkich informacji osobie, której dane dotyczą. Oznacza to na przykład, że w przypadku gdy ograniczenie ma zastosowanie, zamiast odmowy przekazania kopii danych osobowych należy zapewnić, by informacje dotyczące innych osób były w miarę możliwości nieczytelne. Jeżeli jednak nie ma możliwości pogodzenia odpowiednich praw, w kolejnym etapie administrator musi zdecydować, które z kolidujących praw i wolności mają pierwszeństwo (etap 3).

Przykład 35: Sprzedawca detaliczny oferuje klientom możliwość zamawiania produktów za pośrednictwem infolinii obsługiwanej przez dział obsługi klienta. Na potrzeby potwierdzenia zawarcia transakcji handlowych sprzedawca detaliczny przechowuje nagranie połączenia telefonicznego, zgodnie ze ścisłymi wymogami obowiązującego prawodawstwa. Klient chce otrzymać kopię rozmowy, którą odbył z pracownikiem obsługi klienta. W pierwszym etapie sprzedawca analizuje żądanie i zdaje sobie sprawę, że wpis zawiera dane osobowe, które dotyczą również innej osoby, mianowicie pracownika obsługi klienta. W drugim etapie, aby ocenić, czy dostarczenie kopii może mieć wpływ na prawa i wolności innych, sprzedawca musi wyważyć kolidujące interesy, biorąc pod uwagę przede wszystkim prawdopodobieństwo i wagę możliwego ryzyka dla praw i wolności pracownika obsługi klienta związanego z przekazaniem nagrania klientowi. Stwierdza, że dane osobowe dotyczące pracownika obsługi klienta na nagraniu są bardzo ograniczone – to tylko jego głos. Sprzedawca/administrator stwierdza, że pracownik nie jest łatwy do zidentyfikowania. Treść rozmowy ma ponadto charakter zawodowy, a rozmówcą jest osoba, której dane dotyczą. Na podstawie powyższych okoliczności administrator obiektywnie stwierdza, że prawo dostępu nie wpływa niekorzystnie na prawa i wolności pracownika obsługi klienta, w związku z czym administrator może przekazać osobie, której dane dotyczą, pełne nagranie, w tym te części nagrania rozmowy, które odnoszą się do pracownika obsługi klienta.

Przykład 36: Klientka sklepu z wyposażeniem medycznym chce na podstawie art. 15 RODO uzyskać dostęp do wyników pomiarów jej nóg. Sklep z wyposażeniem medycznym zmierzył nogi osoby, której dane dotyczą, w celu wyprodukowania na zamówienie medycznych pończoch uciskowych. Sklep ma bogate doświadczenie i opracował specjalną technikę umożliwiającą dokładny pomiar. Po dokonaniu pomiaru w sklepie medycznym klientka chce wykorzystać wyniki pomiarów do zakupu tańszych pończoch w innym miejscu (zamierza zamówić je w sklepie internetowym). Sklep z wyposażeniem medycznym częściowo odmawia dostępu do danych na podstawie art. 15 ust. 4 RODO, twierdząc, że ze względu na specjalną technikę dokładnego pomiaru wyniki tego pomiaru są chronione jako tajemnica handlowa. W przypadku gdy – i w zakresie, w jakim – administrator jest w stanie udowodnić, że:

- przekazanie osobie, której dane dotyczą, informacji o wynikach pomiarów nie jest możliwe bez ujawnienia sposobu przeprowadzenia pomiarów oraz
- informacje o sposobie dokonywania pomiarów, w tym, w stosownych przypadkach, dokładne określenie punktów pomiarowych, stanowią tajemnice handlowe,

sklep może zastosować art. 15 ust. 4 RODO.

Administrator nadal musiałby przekazać informacje o wynikach pomiarów w takim zakresie, w jakim nie spowodowałoby to ujawnienia jego tajemnicy handlowej, nawet jeśli wiązałoby się to z koniecznością zmiany i modyfikacji wyników.

Przykład 37: GRACZ X jest zarejestrowany jako użytkownik na platformie gier o nazwie PLATFORMA Y. Pewnego dnia GRACZ X otrzymuje powiadomienie, że jego konto internetowe zostało zablokowane. Ponieważ GRACZ X nie może już się zalogować, zwraca się do administratora o dostęp do wszystkich dotyczących go danych osobowych. Oprócz tego żąda przedstawienia powodów zablokowania jego konta. PLATFORMA Y, administrator platformy gier online, do której skierowano żądanie, informuje użytkowników w swoich warunkach ogólnych dostępnych na jej stronie internetowej, że każda forma oszukiwania (głównie przy użyciu zewnętrznego oprogramowania) będzie się wiązać z czasowym lub stałym zakazem korzystania z platformy. Zgodnie z wymogami określonymi w art. 13 RODO, PLATFORMA Y informuje również użytkowników w swojej polityce prywatności, że przetwarza dane osobowe do celów wykrywania przypadków wykorzystywania kodów w grach.

Po otrzymaniu żądania dostępu od GRACZA X PLATFORMA Y powinna dostarczyć GRACZOWI X kopię dotyczących go przetwarzanych danych osobowych. Jeśli chodzi o powód zablokowania konta, PLATFORMA Y powinna potwierdzić GRACZOWI X, że zdecydowała się ograniczyć dostęp GRACZA X do gier online ze względu na jednokrotne lub wielokrotne użycie kodów w grach, co stanowi naruszenie ogólnych warunków użytkowania. Oprócz informacji na temat przetwarzania do celów wykrywania przypadków wykorzystywania kodów w grach PLATFORMA Y powinna zapewnić GRACZOWI X dostęp do przechowywanych przez nią informacji na temat kodów wykorzystywanych przez GRACZA X, które doprowadziły do zablokowania konta. W szczególności PLATFORMA Y powinna przekazać GRACZOWI X informacje, które doprowadziły do zablokowania jego konta (np. historię logowania, datę i godzinę oszustwa, wykrycie zewnętrznego oprogramowania itp.), aby osoba, której dane dotyczą (tj. GRACZ X), mogła sprawdzić, czy przetwarzanie danych było prawidłowe.

Zgodnie z art. 15 ust. 4 i motywem 63 RODO PLATFORMA Y nie jest jednak zobowiązana do ujawnienia informacji o żadnym elemencie technicznego funkcjonowania oprogramowania służącego do zwalczania oszustw, nawet jeśli informacje te odnoszą się do GRACZA X, w zakresie, w jakim można je uznać za tajemnice handlowe. Wynik niezbędnego wyważenia interesów w myśl art. 15 ust. 4 RODO będzie taki, że względy tajemnicy handlowej PLATFORMY Y wykluczają ujawnienie tych danych osobowych, ponieważ wiedza na temat technicznego funkcjonowania oprogramowania służącego do zwalczania oszustw może również umożliwić użytkownikowi obejście go w przyszłości i uniemożliwienie wykrycia oszustwa[99].

174. Jeżeli administratorzy odmówią podjęcia działań w związku z żądaniem dostępu w całości lub w części na podstawie art. 15 ust. 4 RODO, muszą niezwłocznie, a najpóźniej w terminie miesiąca, poinformować osobę, której dane dotyczą, o powodach odmowy (art. 12 ust. 4 RODO).

[99] Zakres informacji przekazywanych osobom fizycznym będzie w dużej mierze zależał od kontekstu, z uwzględnieniem charakteru administratora i charakteru naruszenia warunków świadczenia usług. W niektórych przypadkach administrator może jedynie udzielić podstawowych informacji w odpowiedzi na żądanie dostępu, do którego ma zastosowanie art. 15 ust. 4.

W uzasadnieniu należy odnieść się do konkretnych okoliczności, aby umożliwić osobom, których dane dotyczą, ocenę, czy chcą podjąć działania w związku z odmową. Uzasadnienie musi zawierać informacje na temat możliwości wniesienia skargi do organu nadzorczego (art. 77 RODO) oraz skorzystania ze środków ochrony prawnej przed sądem (art. 79 RODO).

6.3 Art. 12 ust. 5 RODO

175. Zgodnie z art. 12 ust. 5 RODO administratorzy mogą odrzucać żądania dostępu, które są ewidentnie nieuzasadnione lub nadmierne. Pojęcia te należy interpretować w sposób zawężający, tak aby nie podważać zasady przejrzystości i zasady nieodpłatnego wykonywania praw osób, których dane dotyczą.

176. Administratorzy muszą być w stanie wykazać osobie fizycznej, dlaczego uważają, że żądanie jest ewidentnie nieuzasadnione lub nadmierne, oraz przedstawić stosowne uzasadnienie właściwemu organowi nadzorczemu na jego wniosek. W celu podjęcia decyzji, czy dane żądanie jest ewidentnie nieuzasadnione lub nadmierne, należy je zawsze rozpatrywać indywidualnie w kontekście, w jakim zostało wystosowane.

6.3.1 Co oznacza określenie „ewidentnie nieuzasadnione”?

177. Żądanie dostępu jest ewidentnie nieuzasadnione, jeżeli wymogi określone w art. 15 RODO, obiektywnie rzecz biorąc, nie są w sposób wyraźny i oczywisty spełnione. Jak wyjaśniono w szczególności w sekcji 3 powyżej, żądania dostępu są jednak obwarowane bardzo nielicznymi warunkami wstępnymi. W związku z tym EROD podkreśla, że w przypadku żądania dostępu możliwości zastosowania przesłanki dotyczącej „ewidentnie nieuzasadnionego” żądania określonej w art. 12 ust. 5 RODO są bardzo ograniczone.

178. Należy ponadto przypomnieć, że przed powołaniem się na to ograniczenie, administratorzy muszą dokładnie przeanalizować treść i zakres żądania. Na przykład żądania nie powinno się uznawać za ewidentnie nieuzasadnione, jeżeli jest ono związane z przetwarzaniem danych osobowych nieobjętych RODO (w takim przypadku żądanie w ogóle nie powinno być rozpatrywane jako żądanie na podstawie art. 15).

179. Inne przypadki, w których zastosowanie art. 12 ust. 5 RODO jest wątpliwe, to żądania dotyczące informacji lub czynności przetwarzania, które w sposób wyraźny i oczywisty nie podlegają czynnościom przetwarzania prowadzonym przez administratora.

> **Przykład 38**: Osoba, której dane dotyczą, kieruje do organu władz gminy żądanie dotyczące danych przetwarzanych przez organy państwowe. Zamiast uznania żądania za ewidentnie nieuzasadnione właściwszym i łatwiejszym rozwiązaniem byłoby, aby organ, do którego skierowano żądanie, potwierdził, że przedmiotowe dane nie są przetwarzane przez ten organ (pierwszy element art. 15 RODO: „czy” dane osobowe są przetwarzane)[100].

180. Administrator nie powinien zakładać, że żądanie jest ewidentnie nieuzasadnione, ponieważ osoba, której dane dotyczą, przedkładała uprzednio żądania, które były ewidentnie nieuzasadnione lub nadmierne, lub jeżeli zastosowano w nim nieobiektywne lub niewłaściwe sformułowania.

[100] To, czy organ, do którego skierowano żądanie dostępu, jest uprawniony do przekazania żądania właściwemu organowi państwowemu, jest już inną kwestią.

6.3.2 Co oznacza określenie „nadmierne”?

181. W RODO nie ma definicji określenia „nadmierne”. Z jednej strony sformułowanie „w szczególności ze względu na swój ustawiczny charakter” w art. 12 ust. 5 RODO pozwala stwierdzić, że główny scenariusz stosowania tego elementu w odniesieniu do art. 15 RODO jest związany z liczbą żądań, z jakimi występuje osoba, której dane dotyczą, w związku z prawem dostępu. Z drugiej strony powyższy zwrot wskazuje, że inne przyczyny, które mogą powodować nadmierny charakter, nie są wykluczone *a priori*.

182. Nie ulega wątpliwości, że zgodnie z art. 15 ust. 3 RODO dotyczącym prawa do uzyskania kopii osoba, której dane dotyczą, może kilkukrotnie zwrócić się do administratora z żądaniami[101]. W przypadku żądań, które mogą być uznane za nadmierne, ocena „nadmiernego charakteru” zależy od analizy przeprowadzonej przez administratora oraz od specyfiki sektora, w którym administrator działa.

183. W przypadku kolejnych żądań należy ocenić, czy przekroczono próg rozsądnych odstępów czasu (zob. motyw 63). Administratorzy danych muszą w każdym przypadku dokładnie uwzględnić szczególne okoliczności.

184. Na przykład w przypadku sieci społecznościowych zmiany zbioru danych oczekuje się w krótszych odstępach czasu niż w przypadku rejestrów gruntów lub centralnych rejestrów przedsiębiorców. W przypadku wspólników biznesowych należy wziąć pod uwagę częstotliwość kontaktów z klientem. W związku z tym „rozsądne odstępy czasu”, w których osoby, których dane dotyczą, mogą ponownie korzystać z prawa dostępu, również są różne. Im częściej zachodzą zmiany w bazie danych administratora, tym częściej osoby, których dane dotyczą, mogą występować z żądaniem dostępu do swoich danych osobowych, które nie zostanie uznane za nadmierne. W pewnych okolicznościach można by natomiast uznać, że już drugie żądanie tej samej osoby, której dane dotyczą, ma charakter ustawiczny.

185. Przy decydowaniu, czy upłynął rozsądny odstęp czasu, administratorzy powinni wziąć pod uwagę następujące kwestie w świetle uzasadnionych oczekiwań osoby, której dane dotyczą:

- Jak często zmienia się dane – czy jest mało prawdopodobne, aby informacje zmieniły się między żądaniami? Jeżeli pula danych w sposób oczywisty nie podlega przetwarzaniu innemu niż przechowywanie, a osoba, której dane dotyczą, o tym wie, np. ponieważ już wcześniej występowała z żądaniem dostępu, może to wskazywać, że żądanie jest nadmierne.
- Jaki jest charakter danych? Może to obejmować kwestię tego, czy dane są szczególnie wrażliwe.
- Jakie są cele przetwarzania? Może to obejmować kwestię tego, czy przetwarzanie może wyrządzić szkodę osobie występującej z żądaniem w przypadku ujawnienia.
- Czy kolejne żądania dotyczą tego samego rodzaju informacji lub czynności przetwarzania czy innych[102]?

Przykład 39 (stolarz): Osoba, której dane dotyczą, **co dwa miesiące** występuje z żądaniem dostępu do stolarza, który wykonał dla niej stół. Stolarz udzielił pełnej odpowiedzi na pierwsze żądanie. Przy ustalaniu, czy upłynął rozsądny odstęp czasu, należy wziąć pod uwagę, że stolarz przetwarza i gromadzi

[101] Zgodnie z drugim zdaniem art. 15 ust. 3 za wszelkie kolejne kopie, o które się zwrócono, administrator może pobrać opłatę w rozsądnej wysokości.

[102] Jeżeli kolejne żądanie dotyczy tego samego rodzaju informacji w zakresie ORAZ czasie, nie jest to kwestia nadmiernego charakteru, ale żądania dodatkowej kopii, zob. sekcja 2.2.2.2.

dane osobowe jedynie sporadycznie (podpunkt pierwszy powyżej), a nie w ramach swojej podstawowej działalności, a jeszcze rzadziej zdarza się, żeby ponownie świadczył usługi na rzecz tej samej osoby, której dane dotyczą. Również w tym przypadku stolarz nie świadczył kolejny raz usługi na rzecz osoby, której dane dotyczą, co sprawia, że jest mało prawdopodobne, aby w zbiorze danych dotyczących osoby, której dane dotyczą, zaszły zmiany. W szczególności biorąc pod uwagę charakter i ilość przetwarzanych danych osobowych, ryzyko związane z przetwarzaniem można uznać za niskie (podpunkt drugi powyżej), podobnie jak cel przetwarzania (rozliczenie i wypełnienie obowiązku prowadzenia rejestru) prawdopodobnie nie wyrządzi szkody osobie, której dane dotyczą (podpunkt trzeci powyżej). Żądanie dotyczy ponadto tych samych informacji co poprzednie żądanie (podpunkt czwarty powyżej). W konsekwencji takie żądania mogą zostać uznane za nadmierne ze względu na ich ustawiczny charakter.

Przykład 40 (platforma mediów społecznościowych): Platforma mediów społecznościowych, której podstawową działalnością jest gromadzenie lub przetwarzanie danych osobowych osoby, której dane dotyczą, prowadzi złożone i ciągłe czynności przetwarzania na dużą skalę. Korzystająca z usług platformy osoba, której dane dotyczą, występuje z żądaniem dostępu **co trzy miesiące**. W tym przypadku częste zmiany danych osobowych dotyczących osoby, której dane dotyczą, są wysoce prawdopodobne (podpunkt pierwszy powyżej), szeroki zakres gromadzonych danych obejmuje wywnioskowane wrażliwe dane osobowe (podpunkt drugi powyżej) przetwarzane w celu pokazania osobie, której dane dotyczą, odpowiednich treści i członków sieci (podpunkt trzeci). W tych okolicznościach żądanie dostępu co trzy miesiące zasadniczo nie może być uznane za nadmierne ze względu na ustawiczny charakter.

Przykład 41 (biuro informacji kredytowej): Podobnie jak w przypadku sieci społecznościowych nie można wykluczyć, że zmiany odpowiednich danych będących w posiadaniu biur informacji kredytowej będą miały miejsce w znacznie krótszych odstępach czasu niż w innych obszarach (podpunkt pierwszy powyżej). Wynika to z wielu czynników, o których osoba, której dane dotyczą, jako osoba z zewnątrz, zazwyczaj nie jest świadoma ze względu na złożoność modelu biznesowego. Odpowiedź na pytanie, jakie rodzaje danych zostały zebrane przez administratora w celu obliczenia wartości punktowej i które dane są obecnie uwzględniane w obliczeniu, może zatem zostać udzielona wyłącznie przez samo biuro informacji kredytowej. Ponadto przetwarzanie danych za pośrednictwem biur informacji kredytowej i wynikająca z tego wartość punktowa mogą mieć daleko idące konsekwencje dla osoby, której dane dotyczą, w odniesieniu do planowanych transakcji prawnych, takich jak zawieranie umów sprzedaży, najmu lub leasingu (podpunkt trzeci powyżej).

Nie jest możliwe ogólne określenie żadnego konkretnego odstępu czasu, w którym wystąpienie z kolejnym żądaniem dostępu można by uznać za nadmierne zgodnie z art. 12 ust. 5 zdanie drugie RODO. Konieczne jest raczej całościowe rozważenie okoliczności w danym przypadku. Biorąc jednak pod uwagę znaczenie przetwarzania danych dla realiów codziennego życia osób, których dane dotyczą, można założyć, że **roczny odstęp czasu** między nieodpłatnym udzieleniem informacji będzie w każdym przypadku zbyt długi, aby uznać żądanie za nadmierne. W przypadku wystąpienia z żądaniem w bardzo krótkim odstępie czasu decydującym czynnikiem powinno być to, czy osoba, której dane dotyczą, ma powody, by przypuszczać, że informacje lub przetwarzanie zmieniły się od czasu ostatniego wystąpienia z żądaniem. Na przykład jeżeli osoba, której dane dotyczą, przeprowadziła transakcję finansową, taką jak zaciągnięcie pożyczki, wówczas taka osoba powinna

być uprawniona do wystąpienia z żądaniem dostępu do informacji kredytowych, mimo że niedawno już wystosowano takie żądanie i udzielono na nie odpowiedzi.

186. W przypadku gdy możliwe jest łatwe dostarczenie informacji drogą elektroniczną lub przez dostęp zdalny do bezpiecznego systemu, co oznacza, że spełnienie takich żądań faktycznie nie obciąża administratora, jest mało prawdopodobne, aby kolejne żądania mogły zostać uznane za nadmierne.

187. Jeżeli żądanie pokrywa się z poprzednim żądaniem, pokrywające się żądanie można zasadniczo uznać za nadmierne, jeżeli – i w zakresie, w jakim – obejmuje ono dokładnie te same informacje lub czynności przetwarzania, a administrator nie spełnił jeszcze poprzedniego żądania, choć nie można jeszcze mówić o „zbędnej zwłoce" (zob. art. 12 ust. 3 RODO). W praktyce oba żądania można by połączyć.

188. Fakt, że przekazanie informacji lub kopii osobie, której dane dotyczą, wymagałby od administratora dużo czasu i wysiłku, nie może sam w sobie powodować uznania żądania za nadmierne[103]. Duża liczba czynności przetwarzania zazwyczaj wiąże się z większym nakładami pracy przy spełnianiu żądania dostępu. Jak jednak stwierdzono powyżej, w określonych okolicznościach żądania można uznać za nadmierne z powodów innych niż ich ustawiczny charakter. Zdaniem EROD obejmuje to w szczególności przypadki nadużywania art. 15 RODO, a więc przypadki, w których osoby, których dane dotyczą, nadmiernie korzystają z prawa dostępu wyłącznie z zamiarem wyrządzenia szkody administratorowi.

189. W tym kontekście żądania nie należy uznawać za nadmierne ze względu na to, że:

- osoba, której dane dotyczą, nie przedstawiła uzasadnienia żądania lub administrator uważa, że żądanie jest bezprzedmiotowe;
- osoba, której dane dotyczą, posługuje się niewłaściwym lub nieuprzejmym językiem;
- osoba, której dane dotyczą, zamierza wykorzystać dane do zgłaszania dalszych roszczeń wobec administratora[104].

190. Żądanie można z kolei uznać za nadmierne, na przykład jeżeli:

- osoba fizyczna występuje z żądaniem, ale jednocześnie proponuje jego wycofanie w zamian za jakąś formę korzyści ze strony administratora lub
- żądanie jest zamierzone w złej wierze i jest wykorzystywane do nękania administratora lub jego pracowników wyłącznie w celu spowodowania zakłóceń, na przykład ze względu na fakt, że:
    - osoba fizyczna wyraźnie oświadczyła w samym żądaniu lub w innych komunikatach, że zamierza spowodować zakłócenia i nic innego lub

[103] Brak analizy proporcjonalności, zob. pkt 166 powyżej.
[104] Pozostaje to bez uszczerbku dla wszelkich obowiązujących przepisów prawa krajowego, które są zgodne z wymogami określonymi w art. 23 RODO, zob. rozdział 6.4.

- osoba fizyczna systematycznie występuje z różnymi żądaniami do administratora w ramach prowadzonej akcji, np. raz w tygodniu, z zamiarem i skutkiem spowodowania zakłóceń[105].

6.3.3 Skutki

191. W przypadku ewidentnie nieuzasadnionego lub nadmiernego żądania dostępu administratorzy mogą zgodnie z art. 12 ust. 5 RODO pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo odmówić spełnienia żądania.

192. EROD zwraca uwagę, że administratorzy – z jednej strony – nie są co do zasady zobowiązani do pobierania rozsądnej opłaty przed odmową podjęcia działań w związku z żądaniem. Z drugiej strony nie mają też oni całkowitej swobody wyboru między tymi dwoma możliwościami. Administratorzy muszą bowiem podjąć odpowiednią decyzję w zależności od konkretnych okoliczności w danym przypadku. O ile trudno sobie wyobrazić, że pobieranie rozsądnej opłaty jest odpowiednim środkiem w przypadku ewidentnie nieuzasadnionych żądań, o tyle w przypadku nadmiernych żądań – zgodnie z zasadą przejrzystości – często właściwsze będzie pobieranie opłaty jako rekompensaty za koszty administracyjne wynikające z żądań o charakterze ustawicznym.

193. Administratorzy muszą być w stanie wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter (art. 12 ust. 5 zdanie trzecie RODO). W związku z tym zaleca się zapewnienie właściwej dokumentacji podstawowych faktów. Zgodnie z art. 12 ust. 4 RODO, jeżeli administratorzy odmówią podjęcia działań w związku z żądaniem dostępu w całości lub w części, muszą niezwłocznie, a najpóźniej w terminie miesiąca od otrzymania żądania, poinformować osobę, której dane dotyczą, o:

- powodach odmowy,
- prawie wniesienia skargi do organu nadzorczego,
- możliwości skorzystania ze środków ochrony prawnej przed sądem.

194. Przed pobraniem rozsądnej opłaty na podstawie art. 12 ust. 5 RODO administratorzy powinni wskazać osobom, których dane dotyczą, że mają taki zamiar. Osoby, których dane dotyczą, muszą mieć możliwość zdecydowania, czy wycofają żądanie, aby uniknąć obciążenia opłatą.

195. Nieuzasadnione odrzucenie żądania dostępu można uznać za naruszenie praw osób, których dane dotyczą, zgodnie z art. 12–22 RODO, w związku z czym właściwe organy nadzorcze mogą wykonywać swoje uprawnienia naprawcze, w tym nakładać administracyjne kary pieniężne na podstawie art. 83 ust. 5 lit. b) RODO. Jeżeli osoby, których dane dotyczą, uważają, że doszło do naruszenia ich praw, mają prawo wnieść skargę na podstawie art. 77 RODO.

6.4 Ewentualne ograniczenia w prawie Unii lub prawie państw członkowskich na podstawie art. 23 RODO i odstępstwa

[105] „Systematyczne w ramach prowadzonej akcji" oznacza, że żądania, które można łatwo połączyć w jedno, są sztucznie dzielone nie tylko na kilka, ale na wiele pojedynczych części przez osobę, której dane dotyczą, z wyraźnym zamiarem spowodowania zakłóceń.

196. Zakres obowiązków i praw przewidzianych w art. 15 RODO może zostać ograniczony za pomocą aktów prawnych w prawie Unii lub w prawie państw członkowskich[106].

197. Administratorzy, którzy planują powołać się na ograniczenie oparte na prawie krajowym, muszą dokładnie sprawdzić wymogi określone w odpowiednich przepisach krajowych. Należy ponadto zauważyć, że ograniczenia prawa dostępu w prawie państw członkowskich (lub prawie Unii), które opierają się na art. 23 RODO, muszą ściśle spełniać warunki określone w tym przepisie. EROD opublikowała Wytyczne 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO zawierające dalsze wyjaśnienia na ten temat. W odniesieniu do prawa dostępu EROD przypomina, że administratorzy powinni znieść ograniczenia, gdy tylko ustaną okoliczności, które uzasadniają ich wprowadzenie[107].

198. Akty prawne dotyczące ograniczeń na podstawie art. 23 RODO mogą również przewidywać, że wykonanie prawa jest opóźnione w czasie, że prawo jest wykonywane częściowo lub ograniczone do określonych kategorii danych lub że prawo może być wykonywane pośrednio przy udziale niezależnego organu nadzorczego[108].

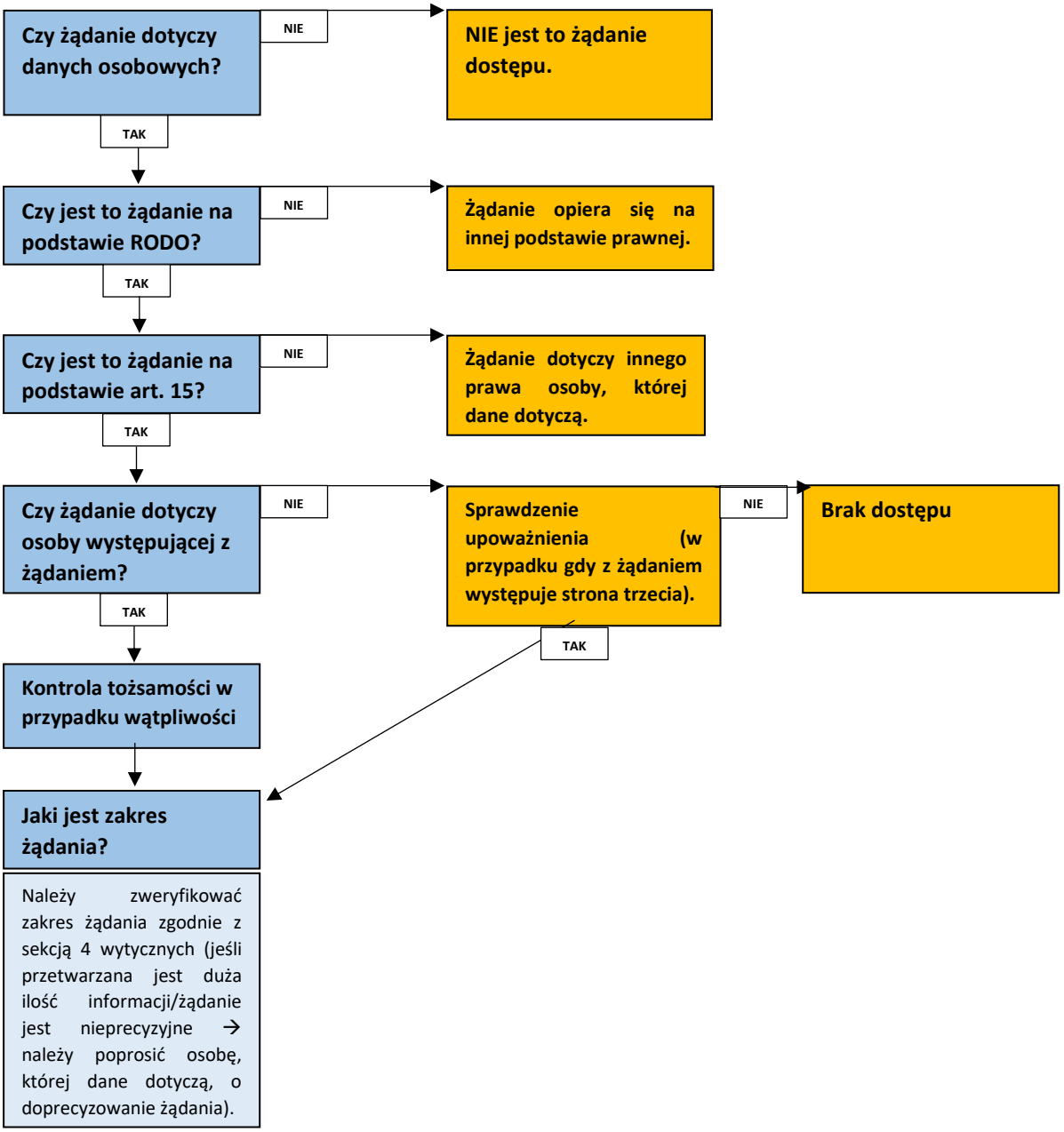
[106] Zob. na przykład sekcje 32–37 niemieckiej federalnej ustawy o ochronie danych (BDSG), sekcje 16 i 17 norweskiej ustawy o danych osobowych oraz rozdział 5 szwedzkiej ustawy o ochronie danych.

[107] Wytyczne 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO, wersja 2.0, przyjęte 13 października 2021 r., pkt 76.

[108] Wytyczne 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO, wersja 2.0, przyjęte 13 października 2021 r., pkt 12. Na przykład art. 34 ust. 3 niemieckiej ustawy federalnej o ochronie danych stanowi, że jeżeli organ publiczny nie udziela informacji osobie, której dane dotyczą, w odpowiedzi na żądanie dostępu ze względu na określone ograniczenia, informacje takie przekazuje się federalnemu organowi nadzorczemu na wniosek osoby, której dane dotyczą, chyba że właściwy najwyższy organ federalny (dla organu, do którego skierowano żądanie) stwierdzi w danym przypadku, że stanowiłoby to zagrożenie dla bezpieczeństwa federacji lub kraju związkowego. Włoski kodeks ochrony danych przewiduje pośredni dostęp (za pośrednictwem organu) w przypadku, gdy dostęp mógłby mieć negatywny wpływ na szereg interesów (np. interesy związane z przeciwdziałaniem praniu pieniędzy), zob. art. 2-L włoskiego kodeksu ochrony danych.

ZAŁĄCZNIK – SCHEMAT

Etap 1: Jak interpretować i ocenić żądanie?



Etap 2: Jak odpowiedzieć na żądanie (1)?

3 główne elementy prawa dostępu (struktura art. 15)		
Potwierdzenie, czy dane osobowe są przetwarzane	Dostęp do danych osobowych	Dodatkowe informacje na temat celów, odbiorców itp. (art. 15 ust. 1 lit. a)–h))

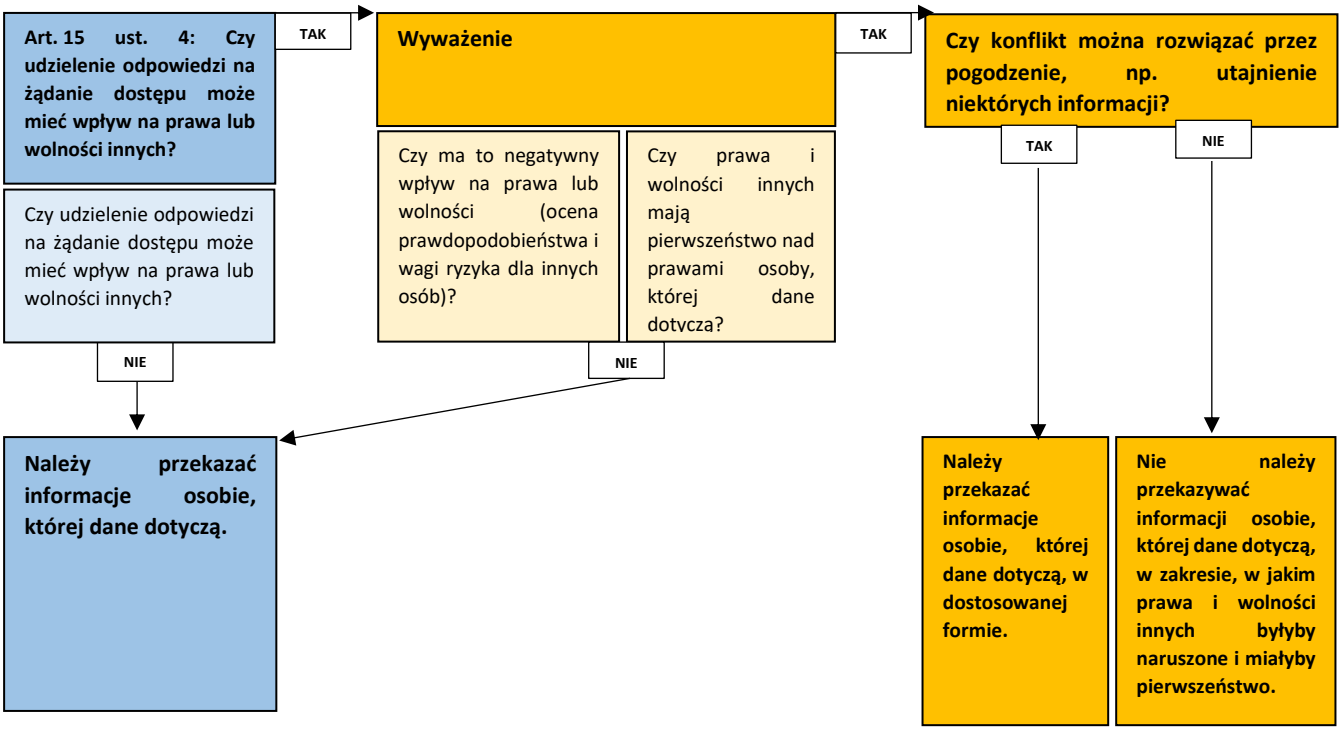
Etap 2: Jak odpowiedzieć na żądanie (2)?

Wprowadzenie odpowiednich środków			
Art. 12 ust. 1: zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma	Art. 12 ust. 2: ułatwienie wykonania prawa dostępu		
Należy wybrać spośród różnych środków.	Należy dostarczyć kopię, jeżeli nie uzgodniono inaczej (art. 15 ust. 3).	W stosownych przypadkach należy zastosować podejście warstwowe (najbardziej istotne w kontekście online).	Termin – bez zbędnej zwłoki, a w każdym razie w terminie miesiąca (wydłużenie o kolejne dwa miesiące w wyjątkowych przypadkach) (art. 12 ust. 3).

Etap 2: Jak odpowiedzieć na żądanie (3)?

W jaki sposób administrator może pobrać wszystkie dane o osobie, której dane dotyczą?			
Określenie kryteriów wyszukiwania – na podstawie informacji przekazanych przez osobę, której dane dotyczą, innych informacji posiadanych przez administratora na temat osoby, której dane dotyczą, oraz czynników, na podstawie których dane są uporządkowane (np. numer klienta, adresy IP, tytuł zawodowy, stosunki rodzinne itp.).	Wskazanie wszelkich dostępnych funkcji technicznych, za pomocą których można pobrać dane.	Wyszukiwanie za pomocą wszystkich odpowiednich zbiorów danych informatycznych lub innych.	Zestawienie, pobieranie lub gromadzenie w inny sposób danych o osobie, której dane dotyczą, w sposób w pełni odzwierciedlający przetwarzanie, tj. obejmujący wszystkie dane osobowe o osobie, której dane dotyczą, oraz umożliwiający osobie, której dane dotyczą, zapoznanie się z przetwarzaniem i weryfikację jego zgodności z prawem. Pobieranie informacji może odbywać się indywidualnie w każdym przypadku lub, w stosownych przypadkach, za pomocą wdrożonego przez administratora narzędzia uwzględniania ochrony prywatności już w fazie projektowania.

Etap 3: Sprawdzenie ograniczeń i restrykcji (1)



Etap 3: Sprawdzenie ograniczeń i restrykcji (2)