

Przewodnik administratora: Dostęp do danych



W TYM WYDANIU:

Dostęp do danych – jak zrealizować żądanie?

1

- Forma wniosku o dostęp do danych – czy można ograniczać formę otrzymania?

2

- Weryfikacja tożsamości wnioskodawcy

3

- Podejście organów nadzorczych

11

- Procedura realizacji prawa dostępu – zalecenia i dobre praktyki

14



Justyna Jurkowska
Data Protection Expert

Dostęp do danych – jak zrealizować żądanie?

Dostęp do danych osobowych na gruncie wytycznych GR 29, podejścia organów nadzorczych w Europie oraz na podstawie dotychczasowych postępowań organu polskiego – co powinien wiedzieć Administrator, aby prawidłowo zrealizować żądanie.

Cel i znaczenie prawa dostępu do danych

Prawo dostępu do danych osobowych gwarantowane w art. 15 RODO ma na celu zapewnienie osobom fizycznym **transparentności** w przetwarzaniu ich danych. Dzięki temu uprawnieniu każda osoba może uzyskać potwierdzenie czy administrator przetwarza jej dane, a jeśli tak to ma prawo uzyskać informacje o szczegółach tego przetwarzania oraz otrzymać kopię swoich danych osobowych. Praktyczne wskazówki dla administratorów oraz osób odpowiedzialnych za proces realizacji przysługującego prawa do dostępu do danych osobowych prezentuje na swojej stronie internetowej organ nadzorczy w Wielkiej Brytanii ([ICO](#)), we Francji ([CNIL](#)) oraz w Niemczech ([BfDI](#)), na których to wytycznych opierałam niniejszy artykuł.

RODO traktuje prawo dostępu do danych jako fundament umożliwiający osobie fizycznej kontrolę nad swoimi danymi. Pozwala zrozumieć osobie, której dane dotyczą, dlaczego i w jaki sposób dane osoby fizycznej są wykorzystywane przez administratora oraz sprawdzić legalność

przetwarzania danych osobowych.

Motyw 63 RODO wskazuje, że:

” każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. **Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane,**

odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania.

W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. 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. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

Należy podkreślić, że realizacja prawa dostępu do danych osobowych ma być ułatwiona i możliwa w dowolnym momencie, aby osoba fizyczna mogła bezpośrednio zweryfikować zakres danych osobowych i poprawność ich przetwarzania.

Co istotne, prawo dostępu do danych osobowych często stanowi początkowy etap do skorzystania z dalszych uprawnień i praw na gruncie RODO, w tym prawa do usunięcia, sprostowania danych osobowych dotyczących osoby fizycznej.

Forma wniosku o dostęp do danych – czy można ograniczyć formę otrzymania?



Wniosek o udostępnienie informacji, dostępu do danych osobowych zwany również żądaniem **może zostać złożony do administratora w dowolnej formie. Przepisy RODO nie wprowadzają wymogu specjalnej formy konstruowania czy też dostarczania treści wniosku. Najważniejsze jest, aby z treści otrzymanego wniosku wynikało, że osoba fizyczna domaga się dostępu do swoich danych osobowych lub informacji jej dotyczących** o czym wspomina organ nadzorczy Wielkiej Brytanii – ICO w opublikowanych [wskazówkach](#). Może to być zatem prośba wyrażona pisemnie lub ustnie, skierowana pocztą tradycyjną (np. listownie), za pomocą środków komunikacji elektronicznej (e-mail, formularz na stronie internetowej, a nawet wiadomość w mediach społecznościowych) czy osobiście w siedzibie administratora. Osoba nie ma obowiązku powoływać się na konkretny przepis ani używać formalnych sformułowań w brzmieniu przepisów prawa. Każda komunikacja, która wskazuje, że osoba fizyczna, chce uzyskać dostęp do swoich danych lub informacji jej dotyczących, powinna zostać zakwalifikowana jako wniosek w rozumieniu art. 15 RODO.

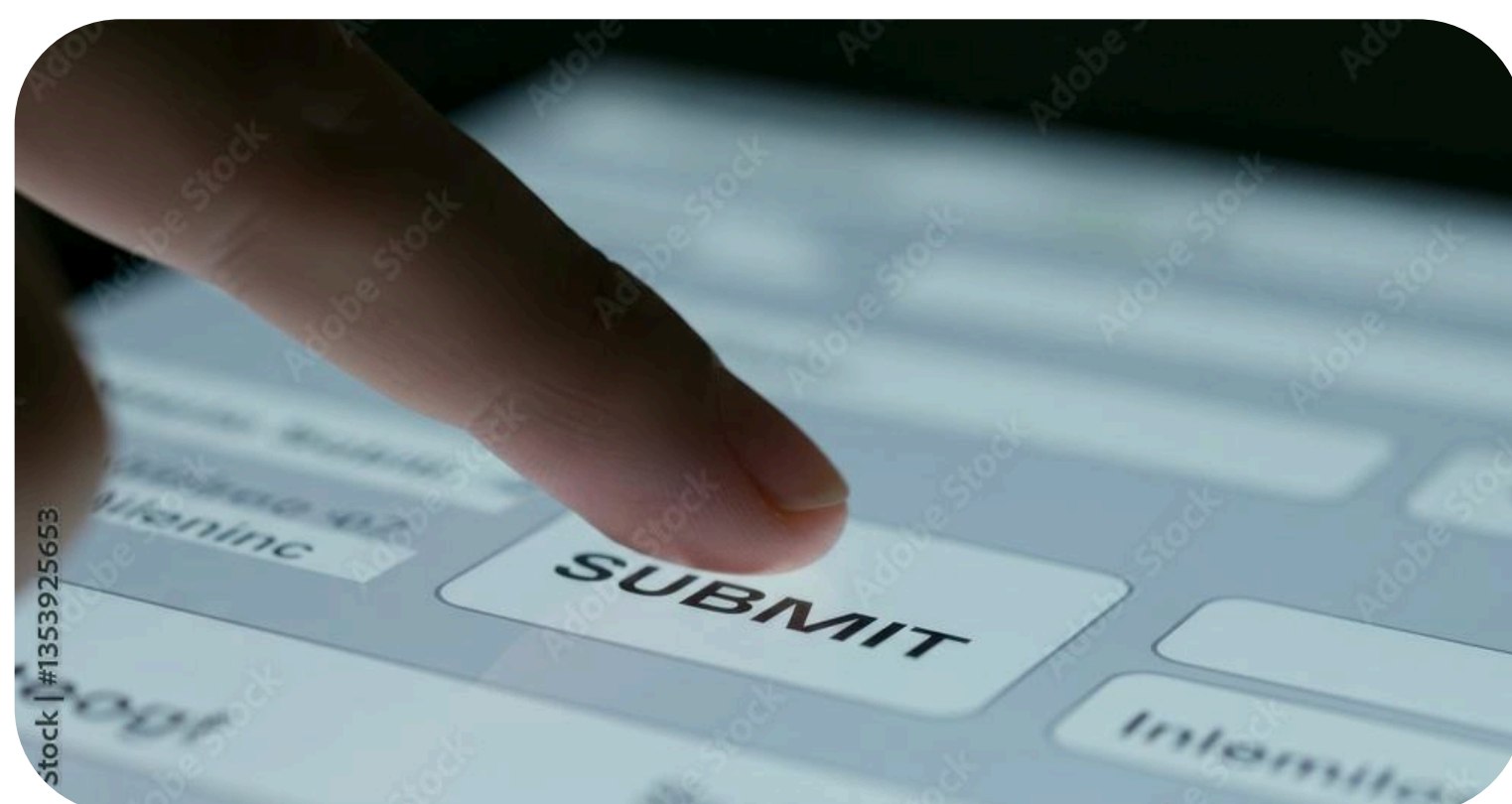


Administrator danych nie powinien ograniczać formy wniosków poprzez wymagania wypełnienia własnego formularza czy złożenia pisma w określony sposób i określonym kanałem komunikacji. Choć dopuszczalne jest stosowanie ułatwień poprzez udostępnienie formularzy, portali dla osób, których dane dotyczą, to **osoba fizyczna zachowuje prawo złożenia żądania w dowolnej formie w dogodny dla niej sposób**, a administrator ma obowiązek je przyjąć i rozpoznać na gruncie RODO. Odmowa realizacji dostępu do danych osobowych wyłącznie ze względu na to, że wniosek nie wpłynął określoną drogą przewidzianą przez administratora czy też kanałem komunikacji udostępnionego w klauzuli informacyjnej, byłaby niezgodna z zasadą rzetelności i przejrzystości przetwarzania danych. Urząd Ochrony Danych Osobowych w uzasadnieniu o sygn. akt [ZSPR.440.1055.2019](#) podkreśla powyższą tezę:

” Sytuacja, w której Skarżący nie może zrealizować swojego prawa, pomimo prawidłowo złożonego żądania, jest wynikiem uchybienia Spółki. Co więcej, skierowanie wynikającego z rozporządzenia 2016/679 żądania na każdy należący do Spółki adres e-mail jest dla niej wiążące. Adresatem do wykonywania praw osób, których dane dotyczą, jest administrator jako taki – jeśli administrator otrzyma żądanie, musi zostać przetworzone, nawet jeśli wewnętrznie ustalono zróżnicowany podział zadań w Spółce.

Z doświadczenia wynika, że w praktyce wielu administratorów przyjmuje wnioski realizacji przysługującego prawa wszystkimi kanałami komunikacji – np. mailem, pocztą tradycyjną, a nawet telefonicznie, dokumentując ustne żądania na potrzeby ewidencji. Prawidłowość realizacji żądań osób fizycznych i terminowości udzielania odpowiedzi uzależnione jest od wiedzy pracowników i szybkiej reakcji, w tym przekazania wniosku do odpowiedniej jednostki organizacyjnej, zarejestrowania wniosku w systemie informatycznym czy też przekazania jego treści do inspektora ochrony danych. Dlatego też administrator nie może zapominać o szkoleniach dla pracowników również w tym zakresie.

Warto wspomnieć, że wniosek o dostęp do danych osobowych może zostać złożony również przez [upoważnionego przedstawiciela](#) osoby, której dane dotyczą (np. prawnika, członka rodziny, opiekuna prawnego). W takim przypadku administrator powinien otrzymać dowód umocowania przedstawiciela do działania w postaci osoby w postaci pełnomocnictwa lub też postanowienia sądu o sprawowaniu opieki nad osobą fizyczną w przypadku np. ubezwłasnowolnienia. Administrator dopiero po weryfikacji otrzymanego umocowania przystępuje się do realizacji żądania dostępu do danych osobowych, aby zagwarantować, że dostęp do informacji otrzymuje osoba uprawniona.



Weryfikacja tożsamości wnioskodawcy

Przed udostępnieniem danych osobowych administrator musi upewnić się, że osobą wnioskującą o dostęp do danych osobowych jest osoba, której dane dotyczą. W tym celu zobowiązany

jest do potwierdzenia tożsamości osoby składającej wniosek. W ten sposób administrator zapobiegnie udostępnieniu danych osobowych nieuprawnionej osobie – w przeciwnym razie doszłoby do naruszenia poufności danych osobowych.



RODO zgodnie z art. 12 ust. 6 pozwala administratorowi zażądać dodatkowych informacji w celu potwierdzenia tożsamości, jeśli poweźmie uzasadnione wątpliwości co do tożsamości wnioskodawcy. Zgodnie z [Wytycznymi EROD 01/2022](#), żądanie takich dodatkowych danych powinno być proporcjonalne, więc administrator nie powinien gromadzić nadmiernych informacji, aby nie zbierać więcej danych osobowych niż to konieczne do ustalenia tożsamości osoby fizycznej.

W praktyce sposób weryfikacji tożsamości osoby, której dane dotyczą zależy od pewnych okoliczności:

- Jeżeli wniosek wpłynął kanałem komunikacji, który już zawiera swego rodzaju identyfikację np. z adresu e-mail przypisanego do konta naszego klienta, poprzez zalogowanie do profilu użytkownika, zazwyczaj dodatkowa weryfikacja nie jest potrzebna. Może okazać się, że z treści otrzymanego wniosku wynika uzasadniona obawa, że to nie jest osoba, której dane dotyczą lub zestaw żądanych informacji jest szeroki - aby zmniejszyć ryzyko ewentualnych skutków naruszenia poufności administrator może poprosić o dodatkowe informacje lub dokonać potwierdzenia tożsamości przez rozmowę telefoniczną.
- Jeśli jednak żądanie przyszło z nieznanego adresu lub formy np. e-mail, którego administrator nie ma w swojej bazie, lub ustnie przez infolinię, administrator może poprosić o podanie danych w celu weryfikacji tożsamości osoby, której dane dotyczą. Potwierdzenie tożsamości następuje poprzez pozyskanie zgodnych danych osobowych np. danych kontaktowych, numeru klienta, ostatniej transakcji itp. W przypadku otrzymania wniosku w siedzibie administratora potwierdzenie tożsamości może zostać potwierdzone poprzez okazanie dokumentu tożsamości lub innego dokumentu potwierdzającego tożsamość osoby. Ważne, by zakres żądanych informacji był uzasadniony.



Dobłą praktyką obserwowaną u niektórych administratorów jest wdrożenie procedury **uwierzytelniania**, np. klient dzwoniąc na infolinię przechodzi weryfikację poprzez podanie hasła generowanego w aplikacji dla dokonywanej czynności albo loguje się na konto w aplikacji potwierdzając swoje działanie u administratora. Należy pamiętać, aby nie tworzyć zbędnych barier – w tym nakazywać potwierdzenia tożsamości w określony sposób, który jest utrudnieniem dla osoby fizycznej np. kiedy osobę starszą, wymagającą opieki skłaniamy do potwierdzania tożsamości w aplikacji mobilnej. Celem potwierdzenie tożsamości jest zabezpieczenie danych, ale bez nadmiernego utrudniania realizacji przysługującego osobie prawa.

Oczywiście **do czasu potwierdzenia tożsamości termin udzielenia odpowiedzi nie rozpoczyna biegu** – miesiąc na realizację żądania liczy się od momentu potwierdzenia tożsamości oraz ewentualnego dostarczenia brakujących informacji. Administrator powinien więc niezwłocznie reagować na wnioski, a jeśli ma wątpliwości co do tożsamości osoby wnioskującej o dostęp do danych osobowych, **natychmiast** wystąpić o przekazanie danych niezbędnych do identyfikacji lub doprecyzowanie wniosku, aby nie tracić cennego czasu na realizację żądania. Powyższe działania administrator powinien przewidzieć we wdrażanych zasadach realizacji przysługujących praw w swojej organizacji, tak aby zapobiec przechowywaniu wniosków przez pracowników i wymóc podejmowania działań w określonym czasie.



Zakres prawa dostępu – jakie informacje i dane należy przekazać?

Prawo dostępu obejmuje dwa główne elementy określone w art. 15 [RODO](#):

1 Informacje o przetwarzaniu danych osobowych

Osoba fizyczna ma prawo uzyskać od administratora szereg informacji dotyczących jej danych osobowych i operacji dokonywanych na danych osobowych. Należą do nich m.in.: cel(e) przetwarzania, kategorie odnośnych danych osobowych, informacje o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, planowany okres przechowywania danych (lub kryteria jego ustalania), informacje o prawie do sprostowania, usunięcia, ograniczenia przetwarzania i sprzeciwu, prawo wniesienia skargi do organu nadzorczego, źródło danych (jeśli nie zostały zebrane od osoby) oraz informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu jeżeli miało miejsce. Administrator musi przedstawić pełny obraz tego **jakie dane, w jakim celu** i w jaki sposób przetwarza na temat danej osoby fizycznej, komu je przekazuje lub będzie przekazywać jak długo będzie przechowywał dane osobowe oraz jakie prawa przysługują osobie w związku z tym przetwarzaniem.

[Grupa robocza 29 w wytycznych 01/2022](#) dotyczących praw osób, których dane dotyczą – Prawo dostępu z dnia 28 marca 2023 r. wskazuje zakres danych osobowych podlegających przekazaniu. *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.

2 Kopia danych osobowych podlegających przetwarzaniu

Na żądanie osoba, której dane dotyczą powinna otrzymać **faktyczną kopię swoich danych** przetwarzanych przez administratora. Chodzi przy tym o dane osobowe dotyczące danej osoby, a nie tylko opisowe informacje o niej. Przykładowo, jeśli pracownik zwraca się o kopię swoich danych, które znajdują się w jego aktach pracowniczych, sam **spis dokumentów** znajdujących się w aktach osobowych pracownika nie spełni obowiązku dostępu do danych osobowych. W decyzji polskiego organu nadzorczego o sygn. akt [ZSZZS.440.842.2018](#) Urząd Ochrony Danych Osobowych podkreślił, że udostępnienie listy dokumentów zawierających dane osobowe pracownika jest niewystarczające podkreślają jednak, że udostępnienie kopii danych zawartych w dokumentacji pracowniczej, zgodnie z art. 15 ust. 3 RODO, nie jest równoznaczne z obowiązkiem udostępnienia danych w formie właściwej dla udostępnienia dokumentacji pracowniczej. Pracodawca będący administratorem, nie ma również obowiązku udostępniania osobie zainteresowanej nośnika, na którym przetwarzane są dane osobowe oraz danych, które nie stanowią danych osobowych w rozumieniu art. 4 pkt 1 RODO i nie dotyczą wnioskującego. Realizując obowiązek wynikający z art. 15 ust. 3 RODO, administrator może poprzestać na wskazaniu treści danych dotyczących osoby, z wyłączeniem pozostałych informacji zawartych na nośniku. Podobne stanowisko jest wskazane w decyzji o sygn. akt [ZSZZS.440.842.2018](#), w której Urząd Ochrony Danych podkreślił, że wykonanie obowiązku określonego w art. 15 ust. 3 RODO może być zatem realizowane zarówno poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe oraz inne dane, jak i poprzez podanie uprawnionemu treści jego danych osobowych, z pominięciem informacji znajdujących się w nośniku, które nie są danymi osobowymi w rozumieniu art. 4 pkt 1 RODO. W przypadku udostępniania kopii danych osobowych przetwarzanych w dokumentacji pracowniczej podstawowe znaczenie ma treść danych. RODO nie posługuje się pojęciem udostępniania kopii

dokumentów zawierających dane osobowe, jest w nim natomiast używane pojęcie kopii danych.

Podobnie, gdy klient żąda dostępu do treści rozmowy telefonicznej nagranej na infolinii, administrator powinien przekazać treść tej rozmowy np. w formie nagrania lub transkrypcji, ponieważ zawiera ona jego dane osobowe w postaci głosu lub wypowiedzi. W tych zakresie Urząd Ochrony Danych Osobowych wydał postanowienie o sygn. akt [DS.523.4826.2020](#) wskazując na obowiązek przekazania treści rozmowy z uwzględnieniem głosu osoby.



RODO precyzuje, że pierwsza kopia danych osobowych jest wolna od opłat, natomiast za kolejne kopie administrator może pobrać rozsądną opłatę odpowiadającą kosztom administracyjnym. Podkreśleniu zasługuje fakt, że pojęcie kopii danych osobowych nie jest tożsame z kopią dokumentu, w którym znajdują się dane osobowe osoby fizycznej. Celem tego prawa jest udostępnienie danych osobowych, dotyczących osoby fizycznej, ale **niekoniecznie całych dokumentów**. W praktyce dla administratora oznacza to, że może zrealizować obowiązek przekazania kopii na dwa sposoby, wybierając dogodniejszy dla siebie. Realizacja przysługującego prawa może nastąpić wówczas poprzez sporządzenie fizycznej kopii/wyciągu dokumentu zawierającego dane osobowe albo poprzez zestawienie i przekazanie samej treści, wykazu danych osobowych dotyczących osoby.

Co ważne, niedawne orzecznictwo doprecyzowało rozumienie kopii danych. Trybunał Sprawiedliwości UE w wyroku z 4 maja 2023 r. w sprawie o sygn. [C-487/21](#) uznał, że wierna i zrozumiała kopia wszystkich danych osobowych osoby może wymagać przekazania także **fragmentów dokumentów, całych dokumentów albo wyciągów z baz danych zawierających te dane** – jeśli jest to niezbędne, by osoba mogła skutecznie skorzystać ze swoich praw, przy czym wymaga podkreślenia, że należy w tym względzie uwzględnić prawa i wolności innych osób. Powyższe należy rozumieć w taki sposób, że jeżeli wyjęcie danych z kontekstu pozbawiłoby je sensu lub utrudniło zrozumienie sposobu przetwarzania, administrator może być zobowiązany udostępnić szerszy wycinek dokumentacji, włączając kontekst, ale w takim zakresie, który umożliwi realizację prawa dostępu bez nadmiernego ujawniania informacji niebędących danymi osoby. TSUE zastrzegł jednocześnie, że pojęcie „informacji” użyte w art. 15 ust.3 RODO odnosi się wyłącznie do danych osobowych osoby fizycznej, żądającej dostępu do swoich danych osobowych i nie oznacza obowiązku ujawniania wszelkich informacji ogólnie, które znajdują się w dokumentach zgromadzanych przez administratora.

Podsumowując, zakres prawa dostępu zależy od tego, o co wnioskuje osoba, której dane dotyczą. Może ona zażądać zarówno pełnego pakietu informacji o przetwarzaniu jej danych osobowych oraz przekazania jej kopii danych, jak i tylko wybranych

elementów (np. samej kopii danych, albo samych informacji bez załączania zakresu danych). Administrator w ramach wdrożonych zasad powinien więc zwrócić uwagę na prawidłowe odczytywanie treści wniosku. Jeśli jego treść nie jest precyzyjna, dobrą praktyką jest skontaktowanie się z osobą, której wniosek dotyczy, w celu doprecyzowania oczekiwań (np. czy chodzi o wszystkie dane, czy o konkretny typ danych, okres lub dokument), szczególnie gdy administrator przetwarza ogromne ilości danych o osobie. Przywoływany wcześniej motyw 63 RODO wprost przewiduje, że przy żądaniu zbyt ogólnym lub obejmującym dużą ilość danych administrator może poprosić o wskazanie, których danych lub których czynności przetwarzania dotyczy żądanie, zanim udzieli odpowiedzi, co służy usprawnieniu procesu. Organ nadzorczy Wielkiej Brytanii – ICO na swojej stronie internetowej wskazał [przykład](#) obliczania terminu udzielania odpowiedzi w przypadku konieczności doprecyzowania wniosku.

Pamiętajmy jednak, że takie dopytanie w sprawie otrzymanego żądania, nie wstrzymuje biegu terminu udzielenia odpowiedzi, jeżeli osoba nie udzieli administratorowi doprecyzowania. Wówczas administrator udziela odpowiedzi w zakresie w jakim w jego ocenie z kontekstu otrzymanego wniosku może wynikać żądanie oraz wskazuje, że administrator pozostaje do dyspozycji w zakresie uzupełnienia wniosku po otrzymaniu sprecyzowania lub udziela pełnej informacji.



Realizacja prawa dostępu – udzielenie odpowiedzi i przekazanie kopii danych

Administrator ma obowiązek udzielić odpowiedzi na wniosek bez zbędnej zwłoki, jednak nie później niż w ciągu miesiąca od otrzymania żądania (lub od potwierdzenia tożsamości, jeżeli było to konieczne). Termin jednego miesiąca liczymy od daty wpłynięcia wniosku – np. jeśli wniosek wpłynął 10 kwietnia, odpowiedź powinna zostać udzielona do 10 maja. RODO dopuszcza jednokrotne przedłużenie tego terminu o kolejne dwa miesiące (czyli łącznie maksymalnie do 3 miesięcy od otrzymania wniosku), wyłącznie w przypadku, gdy żądanie jest skomplikowane lub administrator otrzymał wiele żądań od danej osoby. Przedłużenie terminu musi zostać zasygnalizowane w ciągu pierwszego miesiąca. Wówczas administrator powinien poinformować osobę przed upływem pierwotnego terminu, że udzielenie odpowiedzi w wyznaczonym terminie 30 dni jest niemożliwe podając przyczynę opóźnienia. Brak udzielenia takiej informacji osobie, której dane dotyczą powoduje, że termin na udzielenie odpowiedzi nie zostaje przedłużony zgodnie z wymaganiami RODO. **Dlatego też, dla własnej ochrony, administrator powinien dokumentować daty wpływu wniosków i udzielenia odpowiedzi (np. ewidencja wniosków), aby móc wykazać dochowanie terminów i prowadzić kontrole realizacji przysługujących praw osobom fizycznym.**



Zasadniczo odpowiedź powinna zostać udzielona tą samą drogą, którą wpłynęło żądanie, o ile osoba nie zaznaczyła wyraźnie preferowanej formy odpowiedzi. Przykładowo, jeśli wniosek o kopię danych wpłynął e-mailem i wnioskodawca nie zażądał np. wydruku pocztą, to administrator powinien dostarczyć kopię danych elektronicznie, odpowiadając na tegoż e-maila. Ważne, aby format przekazywanych danych był powszechnie czytelny, niewymagający specjalistycznego oprogramowania. Dopuszczalne są np. pliki PDF, DOC, CSV, itp., które osoba może otworzyć na standardowym komputerze czy smartfonie. Jeśli osoba poprosi o inny format, należy w miarę możliwości uwzględnić taką prośbę i przekazać dane na papierze, jeżeli ktoś nie chce formy elektronicznej. Całość informacji najlepiej przekazać w sposób zorganizowany i zrozumiały. Często odpowiedź ma postać pisma przewodniego zawierającego wymagane informacje wymienione w art. 15 ust.1 RODO oraz załączników z kopiami danych osobowych np. dokumentów, zrzutów z baz danych, raportów z systemów.

Przy przygotowywaniu odpowiedzi administrator musi mieć na uwadze, że prawo dostępu nie może negatywnie wpłynąć na prawa i wolności innych osób zgodnie z art. 15 ust.4 RODO. W praktyce oznacza to konieczność wyłączenia lub zanonimizowania w przekazywanych materiałach takich danych, które dotyczą osób trzecich. Nie jest to jednak absolutna podstawa do odmowy, jeśli w dokumentach objętych żądaniem znajdują się dane innych osób, administrator powinien usunąć lub zablokować te fragmenty, zamiast odmawiać spełnienia wniosku w całości. Przykładowo, udostępniając e-mail z korespondencji z klientem, w którym widnieje nazwisko innego klienta, należy to nazwisko zaciemnić (zanonimizować). Jeśli zaś osoba żąda nagrania rozmowy telefonicznej, a na nagraniu słychać również głos pracownika lub innej osoby – administrator powinien poszukać technicznego rozwiązania, np. **wyciąć lub zmodyfikować fragmenty audio** tak, aby głos osoby trzeciej nie ujawniał jej tożsamości. UODO wskazuje, że obecność danych innych osób nie może być pretekstem do odmowy udzielenia dostępu do danych osobowych, należy więc podjąć rozsądne środki minimalizujące kolizję interesów. W skrajnych przypadkach, gdy udzielenie dostępu w jakiejkolwiek

formie naruszałoby prawa innych np. ujawniłoby tajemnicę przedsiębiorstwa lub czyjeś prywatne dane, administrator powinien móc wykazać, że dokonał **wyważenia interesów** i tylko w niezbędnym zakresie ograniczył odpowiedź. Takie stanowisko zaprezentował Trybunał Sprawiedliwości UE w [Wyroku z dnia 22 czerwca 2023 r.](#) w sprawie pojęcia „odbiorców”.

Odpowiedź powinna być sformułowana jasno i zrozumiale dla odbiorcy. **Należy unikać nadmiernie prawniczych czy technicznych określeń, gdyż celem jest, by osoba rzeczywiście dowiedziała się, co dzieje się z jej danymi osobowymi.** Dobrą praktyką jest przedstawienie informacji w uporządkowanej formie, np. w punktach odpowiadających poszczególnym kategoriom z art. 15 ust.1 (cele, kategorie danych, odbiorcy itd.), oraz załączenie kopii danych z odpowiednim opisem. Jeśli danych jest dużo, można pogrupować je tematycznie. Ważne, aby osoba otrzymała **kompletną realizację swojego prawa** – sama informacja „*tak, posiadamy Pani dane osobowe*” bez przedstawienia szczegółów i udostępnienia ich treści byłaby rażąco niewystarczająca. Również samo odesłanie osoby do już posiadanych przez nią informacji (np. „mamy tylko to, co nam Pani sama podała”) nie spełnia wymogów prawa dostępu. Administrator musi aktywnie dostarczyć wszystkie wymagane informacje i dane osobowe, które są przez niego przetwarzane w określonym celu.



Brak realizacji prawa dostępu w przewidzianym terminie lub zakresie stanowi naruszenie przepisów RODO, które może mieć poważne następstwa dla administratora.

Osoba, której odmówiono dostępu bądź która nie otrzymała odpowiedzi w terminie lub otrzymała odpowiedź nie w pełnym zakresie, ma prawo wnieść **skargę** do organu nadzorczego. W wyniku postępowania skargowego Urząd Ochrony Danych Osobowych może wydać decyzję administracyjną nakazującą udostępnienie danych lub podjęcie innych działań w celu realizacji prawa dostępu. Przykładowo, w opisywanej sprawie [pracowniczej Prezes UODO](#) nakazał pracodawcy dostarczenie byłemu pracownikowi kopii danych z akt osobowych a w innej – zobowiązał administratora do przekazania nagrania rozmowy klientce, [która się o to upomniała w zakresie jej głosu](#).



Nierespektowanie prawa dostępu może również skutkować sankcjami administracyjnymi. Organ nadzorczy, oprócz nakazania udostępnienia danych, może zastosować środki egzekucyjne przewidziane w RODO, np. upomnienie dla administratora lub **administracyjną karę pieniężną**. W praktyce Urząd Ochrony Danych Osobowych najpierw nakazuje wykonanie obowiązku, a gdy administrator uparcie go nie realizuje, może nałożyć karę. Przykładowo, w 2019 r. Urząd Ochrony Danych Osobowych w decyzji o syg. akt [ZSPR.440.1055.2019](#) udzielił upomnienia pewnej spółce za kompletny brak reakcji na żądanie osoby. Wniosek dotyczył wprowadzenia usunięcia danych, ale należy go postrzegać jako brak podjęcia działań. Upomnienie jest oficjalnym stwierdzeniem naruszenia i wezwaniem do zmiany postępowania. Gdyby jednak administrator nadal nie realizował obowiązku, organ może sięgnąć po karę finansową za nieprzestrzeganie przepisów.

Zgodnie z art. 83 ust.5 RODO naruszenie praw osób, w tym prawa dostępu, podlega pod najwyższy wymiar kar, który sięga nawet do 20 mln euro lub 4% rocznego światowego obrotu przedsiębiorstwa (w zależności od tego, która kwota jest wyższa). Wysokość kary jest ustalana z uwzględnieniem okoliczności – np. uporczywe ignorowanie wielu wniosków może skutkować dotkliwą sankcją.

Warto zauważyć, że poza sankcjami administracyjnymi, osoba może również dochodzić swoich praw na drodze cywilnej. Jeżeli odmowa dostępu spowodowała u niej szkodę (majątkową lub niemajątkową), ma prawo żądać od administratora **odszkodowania, zadośćuczynienia** na podstawie art. 82 RODO. Taka odpowiedzialność cywilna motywuje administratorów do rzetelnego wywiązywania się z obowiązków wobec podmiotów danych.

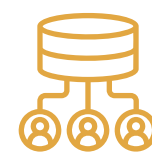


Polski organ nadzorczy – Prezes UODO – konsekwentnie stoi na straży realizacji prawa dostępu i w swoich decyzjach wyjaśnia obowiązki administratorów. Z dotychczasowych rozstrzygnięć można wyprowadzić następujące wnioski praktyczne:



Kopia danych to nie zawsze kopia dokumentu

UODO akcentuje, że liczy się przekazanie osobie jej **danych osobowych** w zrozumiałej formie, a niekoniecznie dokładna kopia oryginalnych dokumentów. Jeżeli więc w odpowiedzi administrator zdecyduje się nie udostępniać całych dokumentów, powinien zadbać, by w innej formie przedstawić całą treść danych dotyczących osoby. W decyzji [ZSZS.440.842.2018](#) Prezes UODO stwierdził wprost: *"RODO nie posługuje się pojęciem udostępniania kopii dokumentów zawierających dane osobowe, jest w nim natomiast używane pojęcie kopii danych"*. Oznacza to, że np. zamiast udostępniać oryginał teczek akt osobowych, administrator może wyciągnąć z niej wszystkie dane pracownika i przekazać je w odrębnym zestawieniu – to również będzie realizacja prawa dostępu, o ile dane te są kompletne i wiernie oddane. Obecnie po wyroku TSUE [C-487/21](#) wiadomo, że czasem trzeba jednak udostępnić dokument w całości lub w części, jeśli bez kontekstu dane osobowe byłyby nieczytelne.



Ochrona danych innych osób

Urząd Ochrony Danych Osobowych w decyzjach podkreśla, że art. 15 ust.4 RODO nakazuje uwzględniać prawa i wolności innych osób, lecz **nie zwalnia to z obowiązku** realizacji prawa dostępu. Administrator powinien znaleźć sposób, aby pogodzić interesy – np. poprzez anonimizację danych osób trzecich. W decyzji [DS.523.4826.2020](#) (dotyczącej nagrania z infolinii) Urząd Ochrony Danych Osobowych zaznaczył, że nie można odmówić klientowi wydania nagrania jego rozmowy tylko dlatego, że słyhać na nim także konsultanta. Zamiast tego wskazał rozwiązanie: użycie narzędzia do edycji audio i usunięcie lub zmiana głosu pracownika. To klarowny sygnał dla administratorów: należy **wykazać się inicjatywą**, by spełnić żądanie osoby, jednocześnie minimalizując ujawnianie cudzych danych.



Podejście do terminu i komunikacji

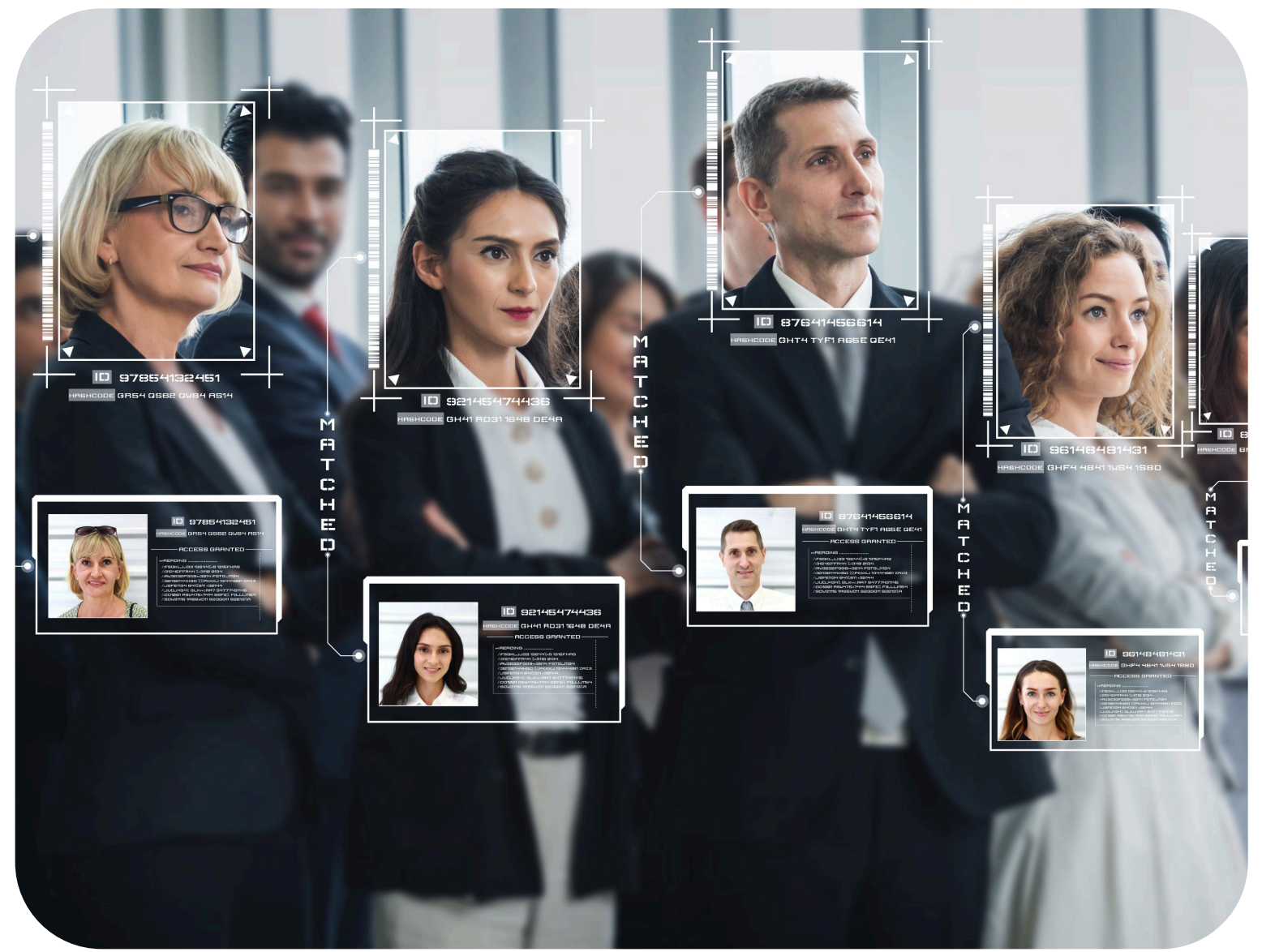
Polski organ nadzorczy oczekuje, że administratorzy będą dotrzymywać ustawowych terminów lub w razie potrzeby właściwie je przedłużać, informując osobę o powodach. Brak odpowiedzi w terminie jest traktowany jako naruszenie obowiązków informacyjnych i skutkuje interwencją organu. Przykładowo, w sprawie [ZSPR.440.1055.2019](#) spółka całkowicie zignorowała żądanie osoby. Urząd uznał to za naruszenie zasady rzetelności i udzielił upomnienia, wymuszając ustanowienie procedur obsługi takich wniosków.



Interpretacja prawa dostępu w kontekście pracowniczym

Kilka decyzji Urzędu Ochrony Danych Osobowych dotyczyło dostępu pracownika lub byłego pracownika do danych kadrowych. W postępowaniu o syg, akt [ZSZS.440.660.2018](#) w zakresie skargi pracownika na brak pełnej realizacji prawa dostępu została jednak przez organ oddalona. Pracodawca udzielił bowiem odpowiedzi, przekazując pracownikowi zestaw informacji i kopii danych. Urząd uznał, że choć pracownik oczekiwał więcej informacji w tym wskazania konkretnych osób przetwarzających jego dane osobowe, to administrator spełnił wymogi ustawowe. To pokazuje, że zakres prawa dostępu ma granice, jeśli administrator dostarczy wszystkie wymagane informacje i dane osobowe, osoba nie może domagać się np. danych dotyczących wewnętrznych procesów lub danych osobowych personelu szczególnie, gdy nie są to „odbiorcy” w rozumieniu RODO. Ten wątek rozwinął ostatnio TSUE w wyroku C-579/21 (o czym wspomnę poniżej).

Podsumowując, **UODO stoi na stanowisku, że prawo dostępu musi być skutecznie realizowane i nie akceptuje wymówek typu „to zbyt pracochłonne” czy „mamy własne procedury, których osoba nie dochowała”**. W razie sporu często staje po stronie osoby, nakazując administratorom skorygowanie podejścia i wydanie danych. Z drugiej strony uznaje pewne ograniczenia – np. ochronę tajemnicy przedsiębiorstwa czy danych pracowników – o ile administrator wykaże, że **zapewnił osobie wszystko, co konieczne**, a ograniczył jedynie elementy chronione innymi przepisami.



Podejście innych organów nadzorczych ([CNIL](#), [BfDI](#), [ICO](#))



Francuski organ CNIL

CNIL kładzie nacisk na praktyczne ułatwienia dla osób oraz kompletność odpowiedzi ze strony administratorów. W swoich wytycznych dla przedsiębiorców [CNIL](#) zaleca czteroetapowe podejście do realizacji prawa dostępu:

- 1 W razie potrzeby zweryfikuj tożsamość wnioskodawcy,
- 2 Jeśli żądanie jest bardzo szerokie, poproś o doprecyzowanie, jakich danych lub operacji dotyczy (zwłaszcza gdy organizacja przetwarza ogromne zbiory danych – ma to zapobiec nadmiernemu obciążeniu, zgodnie z motywem 63 RODO),
- 3 Upewnij się, że udostępnienie danych nie naruszy praw osób trzecich – w razie potrzeby przygotuj dane do wydania poprzez anonimizację informacji o innych osobach lub wyłączenie pewnych elementów (CNIL przypomina, że ktoś nie może np. żądać danych o swoim współmałżonku ani pracownik danych o koledze; również tajemnica zawodowa czy handlowa stanowi granicę – np. nie udostępnia się kodu źródłowego oprogramowania jako takiego, nawet jeśli zawiera dane).

4

Udziel odpowiedzi w terminie, przekazując wymagane informacje i dane. CNIL zwraca uwagę, że osoba może żądać zarówno informacji o przetwarzaniu, jak i kopii danych – administrator powinien zatem sprawdzić, czy ma dostarczyć jedno i drugie. Co ważne, CNIL stanowczo podkreśla, iż udzielając odpowiedzi nie można poprzestać na ogólnikach. Przykładowo nie jest prawidłową realizacją poinformowanie osoby jedynie, że posiada się jej dane, które sama podała, albo wymienienie samych kategorii danych – trzeba przekazać rzeczywiste dane osobowe. Dane zawarte w dokumentach należy udostępnić czy to poprzez kopię oryginału, czy poprzez wierną transkrypcję na inny nośnik. Jeżeli przekazanie kopii dokumentu (w całości lub części) jest niezbędne, by osoba zrozumiała kontekst, należy taką kopię zapewnić. CNIL wskazuje też, że przy wysyłaniu odpowiedzi warto zanonimizować to, co konieczne – np. imiona innych osób – zamiast nie wydawać dokumentu w ogóle. Podejście CNIL jest bardzo zbieżne z wytycznymi EROD i działaniami polskiego organu nadzorczego uwzględniając pełne poinformowanie osoby i poszanowanie jej prawa, przy jednoczesnym zabezpieczeniu danych osób trzecich oraz tajemnic prawnie chronionych.



Niemiecki organ BfDI

[Federalny Inspektor Ochrony Danych](#) (BfDI) również traktuje prawo dostępu jako szerokie uprawnienie gwarantujące osobom **kontrolę nad swoimi danymi**.

W oficjalnych informacjach wyjaśnia, że zakres obejmuje wszelkie dane osobowe osoby znajdujące się u administratora a nie tylko oczywiste dane typu imię, adres, ale także np. prowadzone z osobą komunikacje, notatki wewnętrzne na jej temat itp., o ile zawierają jej dane osobowe. Podkreśla, że często sens pewnych informacji ujawnia się dopiero w kontekście – np. z korespondencji z osobą – zatem **dla zrozumiałości należy udostępnić dokumenty w całości (w kopii)**, jeśli inaczej osoba nie odczyta właściwego znaczenia informacji. Niemiecki

regulator zaznacza przy tym, że prawo dostępu nie jest absolutne i trzeba chronić dane innych osób, a także chronić tajemnice przedsiębiorstwa. Jednak w razie występowania takich elementów nie należy automatycznie odmawiać, lecz zastosować środki ograniczające zakres (np. zanonimizować nazwiska osób trzecich, zaciemnić fragmenty będące tajemnicą handlową). BfDI wskazuje też na możliwość skorzystania z wyjątków przewidzianych w niemieckim prawie krajowym (BDSG) w szczególnych sytuacjach – np. gdy udostępnienie wymagałoby niewspółmiernego wysiłku przy danych archiwalnych, ale generalnie standardem powinna być pełna odpowiedź. Warto zauważyć, że stanowisko BfDI co do udostępniania całych dokumentów pokrywa się z późniejszym orzeczeniem TSUE. Już wcześniej niemiecki organ przyjmowali, że wewnętrzne notatki zawierające dane osoby podlegają dostępowi (np. notatka służbowa opisująca zdarzenie z udziałem tej osoby powinna zostać udostępniona, jeśli osoba o to wnosi, po ewentualnym usunięciu nazwisk innych osób).





Brytyjski organ ICO

Choć Wielka Brytania opuściła UE, jej podejście wypracowane na gruncie analogicznego prawa w UK GDPR i wcześniej Data Protection Act jest bardzo cenne w zakresie praktycznym. ICO publikuje rozbudowane wytyczne dla administratorów dot. tzw. [SAR \(Subject Access Request\)](#). Wskazuje na kluczowe elementy takie jak:

1

Procedury rozpoznawania i obsługi wniosków.

Pracownicy powinni wiedzieć, że nawet nieformalna prośba klienta „chciałbym zobaczyć, co o mnie wiecie” jest prawnie wiążącym wnioskiem o dostęp.

2

Rejestracja i monitorowanie wniosków:

ICO zaleca, by każdą prośbę odnotować (data otrzymania, treść żądania, kanał), a następnie odnotować również datę udzielenia odpowiedzi i zakres przekazanych informacji. Taka ewidencja pomaga śledzić terminy i dowodzić zgodności z obowiązkami.

3

Terminowość i ewentualne wyjaśnienia:

Organizacja powinna od razu liczyć 1-miesięczny termin i ewentualnie szybko decydować o przedłużeniu oraz poinformować o tym wnioskującego. Jeżeli przetwarza bardzo dużo danych o osobie, może uprzejmie poprosić o doprecyzowanie zakresu (np. „czy chodzi Pani o dane z konkretnej usługi lub okresu?”) – w tym czasie bieg terminu ulega zawieszeniu. Ważne, by prośba o doprecyzowanie nastąpiła szybko, tak aby po uzyskaniu wyjaśnień pozostało jeszcze wystarczająco czasu na zebranie danych.

4

Weryfikacja tożsamości:

Podobnie jak EROD, ICO dopuszcza poproszenie o dokument lub informacje weryfikujące, jeśli są wątpliwości. Zaleca jednak, by żądać tylko tyle, ile potrzeba, nie trzeba formalnie identyfikować osoby, jeśli jej tożsamość jest oczywista z okoliczności

np. prosi poprzez konto, do którego tylko ona ma dostęp.

5

Kompletny zakres odpowiedzi:

ICO przypomina, że osoba ma prawo zarówno do kopii danych, jak i do tzw. informacji uzupełniających, czyli właśnie informacji wymaganych przez art.15 ust.1, często pokrywających się z treścią klauzul informacyjnych z art.13/14. W związku z tym odpowiedź powinna zawierać jedno i drugie, chyba że żądanie dotyczyło tylko konkretnego aspektu.

6

Forma udzielenia informacji:

W miarę możliwości powinna być zgodna z preferencją osoby. ICO sugeruje, by w miarę możliwości odpowiadać tą samą drogą, którą przyszedł wniosek co jest zbieżne z zasadami RODO. W przypadku odpowiedzi elektronicznej, jeśli dane są wrażliwe, zaleca się stosowanie bezpiecznych kanałów (np. szyfrowane wiadomości, zabezpieczone pliki) lub oferowanie odbioru osobistego.



Ogólnie praktyka zagranicznych organów nie odbiega od wskazań UODO i EROD. CNIL, BfDI czy ICO kładą nacisk na: rzetelną weryfikację tożsamości, szybkie reagowanie na wnioski, pełne i zrozumiałe informowanie, wydawanie danych z poszanowaniem prywatności osób trzecich oraz na posiadanie przez administratorów procedur wewnętrznych ułatwiających realizację tych obowiązków. W wielu

krajach zaobserwowano też egzekwowanie prawa dostępu poprzez kary; np. francuska CNIL nakładała kary na duże podmioty za utrudnianie dostępu do danych (częścią głośnej kary dla Google w 2019 r. była kwestia nieprzejrzystego dostępu do danych), a hiszpańska AEPD ukarała kilka firm za ignorowanie wniosków osób. Trend w całej Europie jest jasny: prawo dostępu należy do najważniejszych praw osoby i organy nadzorcze wymagają, by administratorzy podchodzili do niego priorytetowo.

Procedura realizacji prawa dostępu – zalecenia i dobre praktyki

Aby skutecznie i prawidłowo obsługiwać wnioski o dostęp do danych, administratorzy powinni wdrożyć wewnętrzną **procedurę** regulującą ten proces. Taka procedura powinna obejmować co najmniej następujące elementy:

Kanały przyjmowania wniosków

Wskazanie, w jaki sposób osoba może złożyć żądanie (np. dedykowany adres e-mail, formularz, adres pocztowy, możliwość ustnego zgłoszenia). Uwaga: nawet jeśli preferujemy konkretny kanał, procedura powinna przewidywać, że wniosek otrzymany inną drogą (np. przez social media lub ustnie) też zostanie rozpoznany. Ważne jest przeszkolenie personelu, zwłaszcza pierwszej linii kontaktu z klientem, by rozpoznawał żądania dostępu niezależnie od formy i nie ignorował ich.



Ewidencja wniosków

Każdy wniosek powinien być niezwłocznie zarejestrowany w wewnętrznym rejestrze. Zaleca się odnotowanie daty wpływu, danych wnioskodawcy, sposobu otrzymania wniosku oraz zakresu żądania. Następnie w rejestrze odnotowujemy datę udzielenia odpowiedzi i ewentualnie datę przedłużenia terminu wraz z uzasadnieniem. Taka dokumentacja pozwoli wykazać terminowość i kompletność realizacji żądania w razie kontroli.



Weryfikacja tożsamości

Procedura powinna opisywać, jak weryfikujemy tożsamość osoby. Np. może przewidywać sprawdzenie danych w systemie CRM, zadanie osobie dodatkowych pytań weryfikujących albo poproszenie o okazanie dokumentu w zależności od kanału kontaktu. Należy uwzględnić różne scenariusze: wniosek od obecnego klienta, od osoby, której danych nie mamy w bazie, wniosek przez e-mail oraz wniosek telefoniczny itd. oraz określić, kto i jak podejmuje decyzję o uznaniu tożsamości za potwierdzoną. Wszystko w duchu minimalizacji dodatkowych danych – pytamy tylko o tyle, ile potrzeba do weryfikacji tożsamości.



Procedura zbierania danych

Po otrzymaniu ważnego (zweryfikowanego) żądania, należy ustalić, gdzie w organizacji mogą znajdować się dane osobowe wnioskodawcy. Dobra procedura powinna wskazywać jednostkę lub osobę odpowiedzialną za koordynację poszukiwania danych



(np. dedykowany zespół ds. prywatności). Następnie, zależnie od struktury firmy, uruchamia się proces przeszukania systemów, baz danych, archiwów papierowych itp. w zakresie objętym wnioskiem. W przypadku dużej organizacji pomocne jest przygotowanie wcześniej mapy lokalizacji danych, jakie działy przetwarzają dane klientów, pracowników itd. Administrator ma obowiązek podjąć uzasadnione starania, by znaleźć wszystkie dane osobowe osoby. Nie musi to oznaczać przeszukiwania każdej pojedynczej kopii zapasowej czy wszystkich e-maili służbowych, jeśli byłoby to nieproporcjonalne – np. ICO wskazuje, że nie trzeba spełniać żądania w sposób powodujący nieproporcjonalny wysiłek. Jednak należy udokumentować, jakie działania podjęto i dlaczego ewentualnie pewnych zasobów nie przeszukano. Z reguły jednak większość danych powinna być dostępna w systemach i tam należy ich poszukać.



Opracowanie odpowiedzi

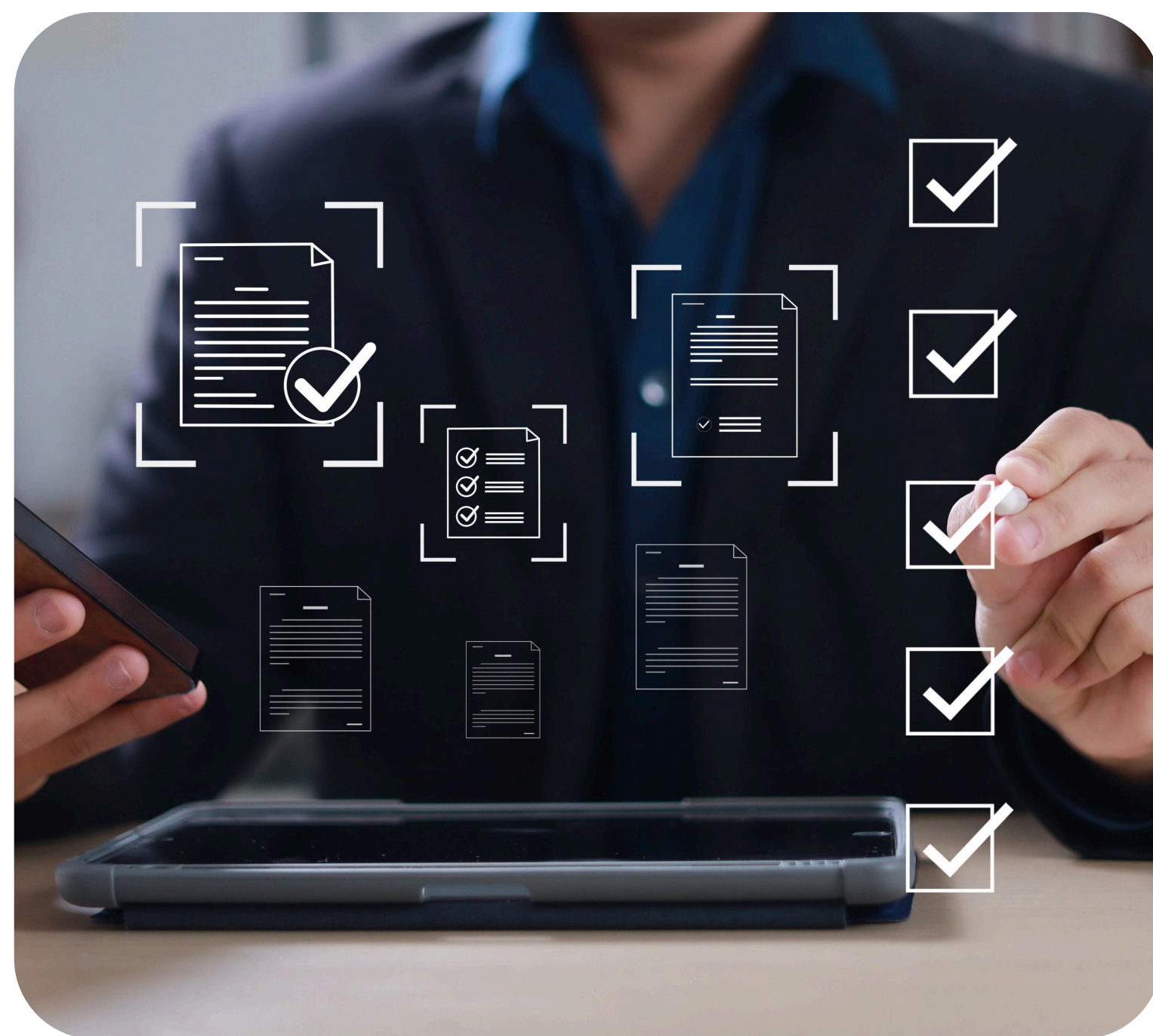
Po zebraniu danych przychodzi czas na przygotowanie odpowiedzi. Procedura powinna zawierać checklistę informacji do przekazania, wszystkie punkty z art. 15 ust.1 RODO oraz wskazówki co do formatu udostępnienia kopii danych np. czy tworzymy raport PDF, czy wyciągi z baz, czy robimy zrzuty ekranów. Dobrą praktyką jest korzystanie z wzorów pism – np. szablon odpowiedzi na żądanie dostępu, w którym uzupełnia się indywidualne dane. To zmniejsza ryzyko pominięcia któregoś obowiązkowego elementu. Warto też przewidzieć, że odpowiedź powinna zawierać informację o prawie do złożenia skargi do organu nadzorczego oraz o ewentualnym przedłużeniu terminu (jeśli miało miejsce) aby osoba była w pełni świadoma swoich praw. Jeśli jakieś dane zostały pominięte z uwagi na prawa innych osób lub tajemnicę, należy to krótko wyjaśnić w odpowiedzi (np. „pewne informacje zostały zanonimizowane z uwagi na prywatność osób trzecich, zgodnie z art. 15 ust.4 RODO”).



Redakcja danych osób trzecich

Procedura powinna opisywać, jak postępować, gdy dane osoby są powiązane z danymi innych osób. Należy określić, kto decyduje o tym, które fragmenty

trzeba zredagować. Zaleca się stosować zasadę minimalizacji redakcji co oznacza, że należy usuwać tylko te elementy, które identyfikują inne osoby lub ujawniają ich dane osobowe, zostawiając resztę treści czytelną. Technicznie, redakcja może polegać na zaczerwieniowaniu tekstu na kopii dokumentu, usunięciu pewnych pól z raportu, wyciszeniu fragmentu nagrania itp. Wszystkie takie modyfikacje również warto zarejestrować, np. zachować oryginał do ewentualnej kontroli, aby móc okazać, że faktycznie usunięto tylko konieczne elementy.



Weryfikacja kompletności odpowiedzi

Zanim odpowiedź zostanie wysłana, dobrze aby przeszła kontrolę jakości – np. przez IOD lub inną upoważnioną osobę. Chodzi o sprawdzenie, czy uwzględniono wszystkie elementy żądania, czy załączono właściwe pliki, czy nie pominięto żadnej kategorii informacji. Błędy na tym etapie mogą skutkować kolejnym wnioskiem od osoby lub skargą, więc warto dołożyć staranności.



Wysłanie odpowiedzi i archiwizacja

Procedura powinna też określać, jak przekazujemy odpowiedź, kto ją podpisuje np. upoważniony pracownik, jak ją wysyłamy (email, list polecony, przez konto online) i jak potwierdzamy nadanie/ odbiór. Po wysłaniu, kopię udzielonej odpowiedzi wraz z przekazanymi danymi należy zarchiwizować w wewnętrznej dokumentacji. Dzięki temu, jeśli osoba w przyszłości złoży np. skargę lub kolejne

żądanie, administrator ma dowód, co zostało wcześniej przekazane. Taka archiwizacja to element zasady rozliczalności – wykazujemy, że spełniliśmy obowiązek. Oczywiście archiwizowane pakiety danych należy zabezpieczyć i przechowywać nie dłużej niż to potrzebne. Można założyć, że przechowujemy kopie udzielonych odpowiedzi przez 5 lat na wypadek prawnej potrzeby wykazania faktów przed organem nadzorczym, po czym je usuwamy.



Obsługa kolejnych żądań

Procedura powinna przewidywać, co, jeśli ta sama osoba składa wnioski powtarzające się bardzo często. RODO pozwala przy nadmiernej częstotliwości uznać wniosek za nadmierny i ewentualnie pobrać opłatę albo odmówić (art. 12 ust.5). Jednak próg „ewidentnego nadmiaru” jest wysoki, o czym można przeczytać w [decyzji Urzędu Ochrony Danych Osobowych](#). Dobrze jest wyznaczyć wewnętrzne kryteria, kiedy wniosek traktujemy jako powtórny bez nowych okoliczności. Jeśli np. ktoś co miesiąc żąda pełnego dostępu, można po którymś razie poinformować, że dane od ostatniej odpowiedzi się nie zmieniły. Każdy przypadek należy oceniać indywidualnie i raczej ostrożnie korzystać z możliwości odmowy jako „nadmiernej”.



Szkolenia personelu i testy procedury

Na koniec, dobra praktyka to okresowe szkolenia pracowników z zakresu obsługi praw osób, w tym prawa dostępu. Warto przeprowadzać testy procedury – np. wewnętrzny audyt: wysłanie próbnego żądania i sprawdzenie, czy procedura zadziałała prawidłowo w praktyce. Pozwala to zidentyfikować słabe punkty i ulepszyć proces zanim dojdzie do realnego naruszenia.



Podsumowując, prawo dostępu do danych osobowych jest potężnym narzędziem w rękach jednostki, a dla administratorów obowiązkiem wymagającym dobrze zorganizowanego działania. Stosując się do powyższych wskazówek i czerpiąc z dobrych praktyk zarówno krajowych, jak i zagranicznych, administratorzy danych mogą skutecznie realizować te obowiązki. Zapewnia to nie tylko zgodność z prawem i unikanie sankcji, ale także buduje zaufanie. Transparentny administrator, który otwarcie dzieli się informacjami z osobami, których dane przetwarza, zyskuje reputację godnego zaufania partnera działającego zgodnie z duchem RODO. Dzięki temu prawo dostępu staje się faktycznie użyteczne zarówno dla osób fizycznych, które mogą lepiej chronić swoje dane, jak i dla administratorów, którzy doskonaląc procedury dostępu, podnoszą ogólną kulturę ochrony danych w swojej organizacji.





Newsletter RODO

Maj 2025 nr 4/2025

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

[SKONTAKTUJ SIĘ Z NAMI](#)