16/EN
WP 242 rev.01

Wytyczne dotyczące prawa do przenoszenia danych

Przyjęte w dniu 13 grudnia 2016 r.
Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

SPIS TREŚCI

Streszczenie

W art. 20 ogólnego rozporządzenia o ochronie danych (RODO) ustanowiono nowe prawo do przenoszenia danych, które jest ściśle związane z prawem dostępu, ale pod wieloma względami się od niego różni. Prawo to umożliwia osobom, których dane dotyczą, otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyły one administratorowi, oraz przesłanie tych danych osobowych innemu administratorowi. Celem tego nowego prawa jest wzmocnienie pozycji osoby, której dane dotyczą, i przyznanie jej większej kontroli nad danymi osobowymi jej dotyczącymi.

Prawo do przenoszenia danych umożliwia przesłanie danych osobowych przez jednego administratora bezpośrednio innemu administratorowi, w związku z czym jest ono również istotnym narzędziem, które wesprze swobodny przepływ danych osobowych w UE i będzie sprzyjać konkurencji między administratorami. Ułatwi ono zmianę dostawców usług i tym samym będzie sprzyjać rozwojowi nowych usług w kontekście strategii jednolitego rynku cyfrowego.

W opinii tej przedstawiono wytyczne dotyczące sposobu interpretacji i wdrożenia prawa do przenoszenia danych określonego w RODO. Ma ona na celu omówienie prawa do przenoszenia danych i zakresu jego stosowania. W opinii wyjaśniono warunki, pod jakimi to nowe prawo ma zastosowanie, z uwzględnieniem podstawy prawnej przetwarzania danych (zgody osoby, której dane dotyczą, albo konieczności wykonania umowy) oraz faktu, że prawo to ogranicza się do danych osobowych dostarczonych przez osobę, której dane dotyczą. Przedstawiono w niej również konkretne przykłady i kryteria, aby wyjaśnić okoliczności, w których prawo to ma zastosowanie. W tym względzie Grupa Robocza Art. 29 uważa, że prawo do przenoszenia danych obejmuje dane świadomie i czynnie dostarczone przez osobę, której dane dotyczą, oraz dane osobowe wygenerowane w wyniku działania tej osoby. Tego nowego prawa nie można naruszać i nie można go ograniczyć do danych osobowych przekazanych bezpośrednio przez osobę, której dane dotyczą, np. w formularzu online.

W ramach dobrej praktyki administratorzy danych powinni rozpocząć prace nad środkami, które będą pomocne przy udzielaniu odpowiedzi na żądania o przeniesienie danych, takimi jak narzędzia do pobierania i interfejsy programowania aplikacyjnego. Powinni oni zagwarantować, że dane osobowe przekazuje się w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, przy czym należy ich zachęcać, aby zapewnili interoperacyjność formatu, w którym dane przekazano w odpowiedzi na żądanie o przeniesienie danych.

Opinia pomaga również administratorom danych dokładnie zrozumieć ich poszczególne obowiązki, a także zawiera zalecenia odnośnie do najlepszych praktyk i narzędzi wspierających zgodność z prawem do przenoszenia danych. Ponadto w opinii zaleca się zainteresowanym stronom w branży i stowarzyszeniom branżowym współpracę nad opracowaniem wspólnego zbioru standardów i formatów interoperacyjnych celem spełnienia wymogów dotyczących prawa do przenoszenia danych.

I. Wprowadzenie

W art. 20 ogólnego rozporządzenia o ochronie danych (RODO) wprowadzono nowe prawo do przenoszenia danych. Prawo to umożliwia osobom, których dane dotyczą, otrzymanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych dostarczonych przez te osoby administratorowi danych oraz przesłanie, bez przeszkód, tych danych osobowych innemu administratorowi danych. To prawo, które stosuje się przy spełnieniu określonych warunków, wspiera wybór użytkownika, kontrolę użytkownika i wzmacnia pozycję użytkownika.

Osoby fizyczne korzystające z przysługującego im prawa dostępu przyznanego na mocy dyrektywy o ochronie danych 95/46/WE nie miały wpływu na format, w którym administrator danych postanowił przekazać żądane informacje. **Nowe prawo do przenoszenia danych ma na celu wzmocnienie pozycji osób, których dane dotyczą, w stosunku do ich własnych danych osobowych, ponieważ ułatwia ono tym osobom przenoszenie, kopiowanie lub przekazywanie danych osobowych między środowiskami IT** (bez względu na to, czy chodzi o ich własne systemy, systemy zaufanej osoby trzeciej lub systemy nowych administratorów danych).

Poprzez potwierdzenie praw osobistych osób fizycznych i sprawowanie kontroli nad danymi osobowymi ich dotyczącymi, przenoszenie danych stanowi również szansę na „przywrócenie równowagi" w stosunkach między osobami, których dane dotyczą, i administratorami danych[1].

Prawo do przenoszenia danych osobowych może też wzmocnić konkurencję między usługami (poprzez ułatwienie zmiany usługodawcy), jednak RODO reguluje dane osobowe, nie konkurencję. W szczególności w art. 20 nie ogranicza się danych podlegających przeniesieniu do tych danych, które są niezbędne lub użyteczne przy zmianie usługodawcy[2].

Chociaż przenoszenie danych jest nowym prawem, inne sposoby przenoszenia już istnieją lub są omawiane w innych dziedzinach prawodawstwa (np. w kontekstach rozwiązania umowy, roamingu w usługach komunikacyjnych i transgranicznego dostępu do usług[3]). Między poszczególnymi rodzajami przenoszenia mogą powstać synergie, a nawet korzyści dla osób fizycznych, jeżeli świadczy się je, przyjmując podejście łączone. Do analogii należy jednak podchodzić z ostrożnością.

W opinii tej przedstawiono wytyczne dla administratorów danych, aby mogli oni zaktualizować swoje praktyki, procedury i politykę, a także wyjaśniono w niej znaczenie przenoszenia danych, aby dać osobom, których dane dotyczą, możliwość efektywnego wykorzystania ich nowego prawa.

---

[1] Głównym celem przenoszenia danych jest wzmocnienie kontroli osoby fizycznej nad jej danymi osobowymi i zapewnienie tej osobie czynnej roli w ekosystemie danych.

[2] Np. prawo to może umożliwić bankom świadczenie dodatkowych usług – kontrolowanych przez użytkownika – przy wykorzystaniu danych osobowych zebranych początkowo w ramach świadczenia usługi dostaw energii.

[3] Zob. agenda jednolitego rynku cyfrowego Komisji Europejskiej: https://ec.europa.eu/digital-agenda/en/digital-single-market, w szczególności pierwszy filar polityki: „Lepszy dostęp do towarów i usług internetowych".

II. Jakie są główne elementy przenoszenia danych?

W art. 20 ust. 1 RODO prawo do przenoszenia danych zdefiniowano w następujący sposób:

> *Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe [...]*

- **Prawo do otrzymania danych osobowych**

Po pierwsze, przenoszenie danych jest **prawem osoby, której dane dotyczą, do otrzymania podzbioru danych osobowych** jej dotyczących przetworzonych przez administratora danych oraz do przechowywania tych danych do dalszego użytku osobistego. Dane można przechowywać na prywatnym urządzeniu lub w prywatnej chmurze, bez konieczności przekazywania ich innemu administratorowi danych.

Pod tym względem przenoszenie danych uzupełnia prawo dostępu. Swoistością przenoszenia danych jest fakt, że daje ono osobom, których dane dotyczą, możliwość łatwego osobistego zarządzania i ponownego wykorzystania danych osobowych. Te dane należy przekazać w „ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego". Na przykład osoba, której dane dotyczą, może być zainteresowana uzyskaniem swojej obecnej listy odtwarzania (lub historii słuchanych utworów) z serwisu strumieniowej transmisji muzyki, aby sprawdzić, ile razy odsłuchała konkretnych utworów lub sprawdzić, które utwory chce zakupić lub których utworów chce posłuchać na innej platformie. W podobny sposób osoba ta może również chcieć uzyskać swoją listę kontaktów z aplikacji webmail, np. aby stworzyć listę gości weselnych, uzyskać informacje na temat zakupów dokonanych przy użyciu różnych kart lojalnościowych lub ocenić swój ślad węglowy[4].

- **Prawo do przesyłania danych osobowych przez jednego administratora danych innemu administratorowi**

Po drugie, art. 20 ust. 1 nadaje osobom, których dane dotyczą, **prawo do przesyłania danych osobowych przez jednego administratora danych innemu administratorowi** „bez przeszkód". Na żądanie osoby, której dane dotyczą, administrator danych może również przesłać dane bezpośrednio innemu administratorowi danych, o ile jest to technicznie możliwe (art. 20 ust. 2). W tym zakresie w motywie 68 zachęca się administratorów danych do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych[5], nie nakładając jednak na administratorów obowiązku prowadzenia lub wprowadzenia

[4] W tych przypadkach przetworzenie danych przez osobę, której dane dotyczą, może mieć miejsce w ramach działalności domowej – jeżeli przetwarzanie jest w całości kontrolowane przez osobę, której dane dotyczą – albo przetworzenia w imieniu osoby, której dane dotyczą, może podjąć się osoba trzecia. W tej drugiej sytuacji wspomnianą osobę trzecią należy uznać za administratora danych nawet w przypadku wyłącznego celu przechowywania danych osobowych, w związku z czym ta osoba trzecia musi przestrzegać zasad i obowiązków określonych w RODO.

[5] Zob. również sekcja V.

kompatybilnych technicznie systemów przetwarzania[6]. W RODO nie zakazano jednak administratorom tworzenia barier utrudniających przesyłanie.

Zasadniczo ten element przenoszenia danych zapewnia osobom, których dane dotyczą, możliwość nie tylko uzyskania i ponownego wykorzystania, ale również przesyłania danych, które dostarczyły one innemu usługodawcy (w ramach tego samego sektora przedsiębiorstw albo w innym sektorze). Oczekuje się, że oprócz wzmocnienia pozycji konsumenta poprzez zapobieżenie uzależnieniu od jednego dostawcy prawo do przenoszenia danych będzie sprzyjać innowacji i wymianie danych osobowych między administratorami danych w sposób bezpieczny i pewny, pod kontrolą osoby, której dane dotyczą[7]. Przenoszenie danych może wspierać kontrolowaną i ograniczoną wymianę danych osobowych przez użytkowników między organizacjami i w ten sposób wzbogacić usługi i doświadczenia konsumentów[8]. Przenoszenie danych może ułatwić przesyłanie oraz ponowne wykorzystywanie danych osobowych dotyczących użytkowników w ramach różnych usług, którymi są oni zainteresowani.

[6] W związku z tym należy zwracać szczególną uwagę na format przesyłanych danych w celu zapewnienia, by dane mogły zostać z łatwością ponownie wykorzystane przez osobę, której dane dotyczą, lub przez innego administratora danych. Zob. również sekcja V.

[7] Zob. szereg eksperymentalnych aplikacji w Europie, na przykład aplikacja MiData w Wielkiej Brytanii, aplikacje MesInfos/SelfData stworzone przez FING we Francji.

[8] Sektory tzw. „mierzenia siebie" (ang. *quantified self*) i internetu rzeczy wykazały korzyści (i zagrożenia) związane z łączeniem danych osobowych z różnych aspektów życia danej osoby fizycznej, takich jak sprawność fizyczna, aktywność i liczba spożywanych kalorii, celem tworzenia pełniejszego obrazu życia tej osoby w jednym pliku.

- **Administrowanie**

Przenoszenie danych zapewnia prawo do otrzymywania danych osobowych oraz ich przetwarzania zgodnie z wolą osoby, której dane dotyczą[9].

Administratorzy danych odpowiadający na żądania przeniesienia danych – na warunkach określonych w art. 20 – nie są odpowiedzialni za przetwarzanie dokonywane przez osobę, której dane dotyczą, lub przez inne przedsiębiorstwo otrzymujące dane osobowe. Działają oni w imieniu osoby, której dane dotyczą, w tym wówczas, gdy dane osobowe są przesyłane bezpośrednio innemu administratorowi danych. W tym względzie administrator danych nie ponosi odpowiedzialności za przestrzeganie prawa ochrony danych przez otrzymującego administratora danych, biorąc pod uwagę fakt, że to nie wysyłający administrator danych wybiera odbiorcę. Jednocześnie administrator powinien ustanowić gwarancje w celu zapewnienia, by rzeczywiście działał on w imieniu osoby, której dane dotyczą. Przykładowo może on ustanowić procedury w celu zapewnienia, by rodzaj przesyłanych danych osobowych pokrywał się faktycznie z rodzajem danych, jaki osoba, której dane dotyczą, pragnie przesłać. Można osiągnąć ten cel poprzez uzyskanie potwierdzenia od osoby, której dane dotyczą, przed przesłaniem albo na wcześniejszym etapie – w chwili udzielania pierwotnej zgody na przetwarzanie lub finalizacji umowy.

Na administratorach danych odpowiadających na żądanie przeniesienia danych nie ciąży szczególny obowiązek sprawdzania i weryfikacji jakości danych przed ich przesłaniem. Nie ulega wątpliwości, że dane te powinny być już prawidłowe i aktualne zgodnie z zasadami określonymi w art. 5 ust. 1 RODO. Ponadto przenoszenie danych nie nakłada na administratora danych obowiązku zatrzymywania danych osobowych dłużej niż jest to konieczne ani po upływie wyznaczonego okresu zatrzymania[10]. Co istotne, nie istnieje dodatkowy wymóg zatrzymania danych po upływie okresów mających zazwyczaj zastosowanie, aby można je było wykorzystać do celów wszelkich potencjalnych przyszłych żądań przeniesienia danych.

Gdy dane osobowe objęte żądaniem są przetwarzane przez przetwarzającego, umowa zawarta zgodnie z art. 28 RODO musi zawierać obowiązek pomocy „administratorowi poprzez odpowiednie środki techniczne i organizacyjne, […] [aby] wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw". Administrator danych powinien zatem wdrożyć określone procedury we współpracy ze swoimi przetwarzającymi, aby odpowiedzieć na żądania przeniesienia danych. W przypadku wspólnego administrowania w umowie należy jednoznacznie rozdzielić między wszystkich administratorów danych obowiązki dotyczące przetwarzania żądań przeniesienia danych.

Ponadto otrzymujący administrator danych[11] jest odpowiedzialny za zapewnienie, by dostarczone dane podlegające przenoszeniu były stosowne i nie były nadmierne w odniesieniu do nowego przetwarzania danych. Przykładowo w przypadku żądania przeniesienia danych wniesionego do dostawcy aplikacji *webmail*, w ramach którego osoba, której dane dotyczą, wykorzystuje wniesione żądanie w celu uzyskania wiadomości e-mail i przesłania ich na

[9] Prawo do przenoszenia danych nie jest ograniczone do danych osobowych, które są przydatne i stosowne w odniesieniu do podobnych usług świadczonych przez konkurentów administratora danych.

[10] W powyższym przykładzie, jeżeli administrator danych nie zatrzymuje listy utworów muzycznych odtwarzanych przez użytkownika, nie można zawrzeć tych danych osobowych w żądaniu przeniesienia danych.

[11] Tj. administrator danych, który otrzymuje dane osobowe po wniesieniu przez osobę, której dane dotyczą, żądania przeniesienia danych do innego administratora danych.

zabezpieczoną platformę służącą archiwizacji, nowy administrator danych nie musi przetwarzać danych kontaktowych korespondentów osoby, której dane dotyczą. Jeżeli informacje te nie są stosowne w odniesieniu do celu nowego przetwarzania, nie należy ich przechowywać ani przetwarzać. W każdym przypadku otrzymujący administratorzy danych nie są zobowiązani do przyjmowania i przetwarzania danych osobowych przesłanych w następstwie żądania przeniesienia danych. Podobnie w przypadku, gdy osoba, której dane dotyczą, żąda przesłania informacji dotyczących jej transakcji bankowych do usługi, która pomaga jej w zarządzaniu budżetem, otrzymujący administrator danych nie musi przyjmować wszystkich danych ani zachowywać wszystkich informacji szczegółowych dotyczących transakcji po ich oznaczeniu do celów nowej usługi. Innymi słowy, przyjęte i zatrzymane dane powinny obejmować wyłącznie dane niezbędne i stosowne w odniesieniu do usługi świadczonej przez otrzymującego administratora danych.

Organizacja „otrzymująca" staje się nowym administratorem danych w odniesieniu do tych danych osobowych i musi przestrzegać zasad określonych w art. 5 RODO. W związku z tym „nowy" otrzymujący administrator danych musi jednoznacznie i bezpośrednio określić cel nowego przetwarzania przed wniesieniem jakiegokolwiek żądania przeniesienia danych podlegających przenoszeniu zgodnie z wymogami przejrzystości określonymi w art. 14[12]. Podobnie jak w przypadku wszystkich innych czynności przetwarzania danych, za które odpowiada administrator danych, powinien on stosować zasady ustanowione w art. 5, takie jak zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, integralność i poufność, ograniczenie przechowywania oraz rozliczalność[13].

Administratorzy danych przechowujący dane osobowe powinni być przygotowani do ułatwienia osobie, której dane dotyczą, wykonania przysługującego jej prawa do przenoszenia danych. Administratorzy danych mogą również zdecydować o przyjęciu danych od osoby, której dane dotyczą, ale nie są do tego zobowiązani.

- **Przenoszenie danych a inne prawa osób, których dane dotyczą**

Wykonanie przez osobę fizyczną przysługującego jej prawa do przenoszenia danych (lub wszelkich innych praw określonych w RODO) pozostaje bez uszczerbku dla wszelkich innych praw. Osoba, której dane dotyczą, może nadal korzystać z usług administratora danych nawet po zakończeniu operacji przenoszenia danych. Przenoszenie danych nie powoduje automatycznego usunięcia danych[14] z systemów administratora danych i pozostaje bez uszczerbku dla pierwotnego okresu zatrzymania mającego zastosowanie do danych, które przesłano. Osoba, której dane dotyczą, może korzystać ze swoich praw, o ile administrator danych nadal przetwarza dane.

Podobnie, jeżeli osoba, której dane dotyczą, pragnie wykonać przysługujące jej prawo do usunięcia danych („prawo do bycia zapomnianym" określone w art. 17), administrator danych

[12] Ponadto nowy administrator danych nie powinien przetwarzać danych osobowych, które nie są istotne, przy czym przetwarzanie musi być ograniczone do tego, co jest niezbędne do nowych celów, nawet jeżeli dane osobowe stanowią część bardziej globalnej bazy danych przesyłanych w ramach procedury przenoszenia. Dane osobowe, które nie są niezbędne do osiągnięcia celu nowego przetwarzania, należy jak najszybciej usunąć.

[13] Po otrzymaniu danych osobowych przez administratora danych dane osobowe przesłane w ramach wykonania prawa do przenoszenia danych można uznać za „dostarczone przez" osobę, której dane dotyczą, i ponownie je przesłać zgodnie z prawem do przenoszenia danych w zakresie, w jakim spełnione są pozostałe warunki umożliwiające wykonanie tego prawa (tj. podstawa prawna przetwarzania itd.).

[14] Jak wskazano w art. 17 RODO.

nie może wykorzystać przenoszenia danych jako sposobu opóźnienia lub odmowy takiego usunięcia.

Jeżeli osoba, której dane dotyczą, odkryje, że dane osobowe żądane w wykonaniu prawa do przenoszenia danych nie odpowiadają w pełni jej żądaniu, każde kolejne żądanie dostępu do danych osobowych w wykonaniu prawa dostępu należy spełnić w całości, zgodnie z art. 15 RODO.

Ponadto w przypadku, gdy w przepisach szczególnych innej gałęzi prawa europejskiego lub prawa państwa członkowskiego również przewiduje się pewną formę przenoszenia przedmiotowych danych, podczas spełniania żądania przeniesienia danych zgodnie z RODO należy uwzględnić również warunki określone w tego rodzaju przepisach szczególnych. Po pierwsze, jeżeli z żądania wniesionego przez osobę, której dane dotyczą, bezsprzecznie wynika, że jej zamiarem nie jest wykonanie uprawnień przewidzianych w RODO, lecz wyłącznie wykonanie uprawnień przewidzianych w przepisach sektorowych, przepisy RODO dotyczące przenoszenia danych nie będą miały zastosowania do tego żądania[15]. Jeżeli natomiast celem żądania jest przeniesienie na mocy RODO, istnienie tego rodzaju przepisów szczególnych nie powoduje uchylenia ogólnej zasady przenoszenia danych stosowanej wobec wszystkich administratorów danych, jak przewidziano w RODO. Zamiast tego należy ocenić w poszczególnych przypadkach, w jaki sposób, o ile w ogóle, tego rodzaju przepisy szczególne mogą wpłynąć na prawo do przenoszenia danych.

III. W jakich sytuacjach ma zastosowanie przenoszenie danych?

- **Które operacje przetwarzania są objęte prawem do przenoszenia danych?**

Aby zachować zgodność z RODO, administratorzy danych muszą mieć wyraźną podstawę prawną do przetwarzania danych osobowych.

Zgodnie z art. 20 ust. 1 lit. a) RODO, **aby wchodzić w zakres przenoszenia danych**, operacje przetwarzania muszą się odbywać:

- na podstawie zgody osoby, której dane dotyczą (w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), jeżeli chodzi o szczególne kategorie danych osobowych);

- albo na podstawie umowy, której stroną jest osoba, której dane dotyczą, w myśl art. 6 ust. 1 lit. b).

W ramach przykładu: tytuły książek nabytych przez osobę fizyczną w księgarni internetowej lub utwory muzyczne słuchane za pośrednictwem serwisu transmisji strumieniowej muzyki stanowią przykład danych osobowych, które co do zasady są objęte zakresem przenoszenia danych, ponieważ są przetwarzane na podstawie wykonywania umowy, której stroną jest osoba, której dane dotyczą.

[15] Przykładowo, jeżeli żądanie osoby, której dane dotyczą, ma w szczególności na celu zapewnienie dostępu do historii jej rachunku bankowego dostawcy świadczącemu usługę dostępu do informacji o rachunku do celów wskazanych w drugiej dyrektywie w sprawie usług płatniczych, tego rodzaju dostęp należy zapewnić zgodnie z przepisami tej dyrektywy.

W RODO nie ustanowiono ogólnego prawa do przenoszenia danych w przypadkach, w których przetwarzanie danych osobowych nie odbywa się na podstawie zgody lub umowy[16]. Przykładowo instytucje finansowe nie są zobowiązane do udzielenia odpowiedzi na żądania przeniesienia danych dotyczące danych osobowych przetwarzanych w wykonaniu ciążących na nich obowiązków w zakresie zapobiegania praniu pieniędzy i jego wykrywania, a także zapobiegania innym przestępstwom finansowych oraz ich wykrywania; podobnie przenoszenie danych nie obejmuje zawodowych danych kontaktowych przetwarzanych w relacji między przedsiębiorcami w przypadkach, gdy przetwarzanie nie opiera się ani na zgodzie osoby, której dane dotyczą, ani na umowie, której jest ona stroną.

Jeżeli chodzi o dane pracowników, prawo do przenoszenia danych ma co do zasady zastosowanie wyłącznie wówczas, gdy przetwarzanie opiera się na umowie, której stroną jest osoba, której dane dotyczą. W wielu przypadkach zgoda nie będzie w tym kontekście uznana za wyrażoną dobrowolnie ze względu na brak równowagi sił między pracodawcą a pracownikiem[17]. Niektóre operacje przetwarzania w kontekście zasobów ludzkich oparte są natomiast na podstawie prawnej w postaci prawnie uzasadnionego interesu lub są konieczne do zapewnienia wykonania określonych zobowiązań prawnych w obszarze zatrudnienia. W praktyce nie ulega wątpliwości, że prawo do przenoszenia danych w kontekście zasobów ludzkich dotyczyć będzie określonych operacji przetwarzania (takich jak usługi w zakresie płac i wynagrodzeń, wewnętrzna rekrutacja), ale w wielu innych sytuacjach potrzebne będzie przyjęcie indywidualnego podejścia, aby sprawdzić, czy spełnione są wszystkie warunki mające zastosowanie do prawa do przenoszenia danych.

Ponadto prawo do przenoszenia danych ma zastosowanie wyłącznie wówczas, gdy przetwarzanie danych „odbywa się w sposób zautomatyzowany", i w związku z tym nie obejmuje większości dokumentów w formie papierowej.

- **Które dane osobowe należy uwzględnić?**

Zgodnie z art. 20 ust. 1, aby dane były objęte zakresem prawa do przenoszenia danych:
- muszą to być dane osobowe dotyczące danej osoby; oraz
- muszą to być dane, które *dostarczyła* ona administratorowi danych.

Art. 20 ust. 4 stanowi również, że wykonanie tego prawa nie może niekorzystnie wpływać na prawa i wolności innych.

Pierwszy warunek: dane osobowe dotyczące osoby, której dane dotyczą

[16] Zob. motyw 68 i art. 20 ust. 3 RODO. W art. 20 ust. 3 i w motywie 68 przewidziano, że przenoszenie danych nie ma zastosowania do przetwarzania danych, jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub jeżeli administrator danych wykonuje obowiązki publiczne lub wywiązuje się z obowiązku prawnego.
W przytoczonych przypadkach administratorzy danych nie mają zatem obowiązku zapewniania przenoszenia danych. Dobrą praktyką jest jednak opracowanie procedur automatycznego odpowiadania na żądania przeniesienia, z poszanowaniem zasad regulujących prawo do przenoszenia danych. Przykładem tego rodzaju praktyki byłby serwis rządowy zapewniający łatwe pobieranie poprzednio złożonych deklaracji podatkowych dotyczących podatku dochodowego od osób fizycznych. W odniesieniu do przenoszenia danych jako dobrej praktyki w przypadku przetwarzania opartego na podstawie prawnej w postaci konieczności prawnie uzasadnionego interesu oraz istniejących programów dobrowolnych – zob. s. 47 i 48 opinii Grupy Roboczej Art. 29 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów (WP 217).

[17] Jak wskazała Grupa Robocza Art. 29 w opinii 8/2001 z dnia 13 września 2001 r. (WP 48).

Zakresem żądania przeniesienia danych objęte są wyłącznie dane osobowe. W związku z tym wszelkie dane anonimowe[18] 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.

W wielu sytuacjach administratorzy danych przetwarzają informacje zawierające dane osobowe kilku osób, których dane dotyczą. W 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).

Drugi warunek: dane dostarczone przez osobę, której dane dotyczą

Drugi warunek zawęża omawiany zakres do danych „dostarczonych przez" osobę, której dane dotyczą.

Istnieje wiele przykładów danych osobowych świadomie i aktywnie „dostarczanych przez" osobę, której dane dotyczą, takie jak dane dotyczące konta (np. adres e-mail, nazwa użytkownika, wiek) podawane w formularzach *online*. Dane „dostarczone przez" osobę, której dane dotyczą, wynikają jednak również z obserwacji jej działań. W związku z tym Grupa Robocza Art. 29 uważa, że aby nadać pełną wartość temu nowemu prawu, określenie „dostarczone przez" powinno obejmować również dane osobowe wynikające z obserwacji działań użytkowników, takie jak dane pierwotne przetwarzane przez inteligentny licznik lub inne rodzaje połączonych obiektów[19], dzienniki aktywności, historia korzystania ze strony internetowej lub czynności wyszukiwania.

Ta ostatnia kategoria danych nie obejmuje danych wytwarzanych przez administratora danych (z wykorzystaniem zaobserwowanych danych lub danych bezpośrednio dostarczonych jako dane wejściowe), takich jak profil użytkownika utworzony poprzez analizę danych pierwotnych zgromadzonych za pośrednictwem inteligentnego pomiaru.

Można wyróżnić różne kategorie danych w zależności od ich pochodzenia, aby określić, czy są one objęte prawem do przenoszenia danych. Następujące kategorie danych można zaklasyfikować jako „dostarczone przez osobę, której dane dotyczą":

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf

[19] Dzięki możliwości uzyskania danych wynikających z obserwacji jej działań, osoba, której dane dotyczą, będzie również mogła uzyskać lepszy obraz wyborów dotyczących wdrażania dokonywanych przez administratora danych w odniesieniu do zakresu obserwowanych danych i znajdzie się w korzystniejszej sytuacji, jeżeli chodzi o wybór danych, jakie jest gotowa dostarczyć, aby uzyskać podobną usługę, a także będzie świadoma stopnia, w jakim przestrzegane jest jej prawo do prywatności.

- **dane aktywnie i świadomie dostarczone przez osobę, której dane dotyczą** (na przykład adres e-mail, nazwa użytkownika, wiek itd.);
- **zaobserwowane dane dostarczone przez osobę, której dane dotyczą, poprzez korzystanie z danej usługi lub danego urządzenia.** Mogą one na przykład obejmować historię wyszukiwania danej osoby, dane o ruchu i dane dotyczące lokalizacji. Mogą również obejmować inne dane pierwotne, takie jak tętno monitorowane za pośrednictwem urządzenia do noszenia na ciele.

Dane wywnioskowane i dane wywiedzione są natomiast wytwarzane przez administratora danych na podstawie danych „dostarczonych przez osobę, której dane dotyczą". Przykładowo wyniku oceny zdrowia użytkownika lub profilu utworzonego w kontekście zarządzania ryzykiem i regulacji finansowych (np. w celu przypisania punktów w ramach punktowej oceny kredytowej lub przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy) nie można jako takich uznać za „dostarczone przez" osobę, której dane dotyczą. Chociaż tego rodzaju dane mogą stanowić część profilu zarządzanego przez administratora danych i zostały one wywnioskowane lub wywiedzione z analizy danych dostarczonych przez osobę, której dane dotyczą (na przykład poprzez jej działania), co do zasady nie zostaną one uznane za „dostarczone przez osobę, której dane dotyczą", i tym samym nie będą objęte zakresem tego nowego prawa[20].

Co do zasady, biorąc pod uwagę cele polityczne prawa do przenoszenia danych, należy dokonywać wykładni rozszerzającej określenia „dostarczone przez osobę, której dane dotyczą" i należy wyłączyć z jego zakresu „dane wywnioskowane" i „dane wywiedzione" obejmujące dane osobowe utworzone przez usługodawcę (na przykład wyniki algorytmiczne). Administrator danych może wyłączyć te wywnioskowane dane, jednak powinien uwzględnić wszystkie inne dane osobowe dostarczone przez osobę, której dane dotyczą, za pośrednictwem środków technicznych zapewnionych przez administratora[21].

Określenie „dostarczone przez" obejmuje zatem dane osobowe odnoszące się do działania osoby, której dane dotyczą, lub wyniku obserwacji zachowania określonej osoby fizycznej, lecz nie obejmuje danych wynikających z późniejszej analizy tego zachowania. Wszelkie dane osobowe wytworzone przez administratora danych w ramach przetwarzania danych, np. w procesie personalizacji lub rekomendacji, kategoryzację użytkownika lub jego profilowanie, stanowią dane wywiedzione lub wywnioskowane z danych osobowych dostarczonych przez osobę, której dane dotyczą, przy czym nie są one objęte prawem do przenoszenia danych.

Trzeci warunek: prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych

[20] Osoba, której dane dotyczą, jest jednak nadal „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" oraz informacji „o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą", zgodnie z art. 15 RODO (który dotyczy prawa dostępu).

[21] Obejmują one wszystkie dane na temat osoby, której dane dotyczą, zaobserwowane podczas działań, do celów których dane te są gromadzone, takie jak historia transakcji lub dziennik dostępu. Dane zgromadzone poprzez śledzenie i rejestrowanie osoby, której dane dotyczą (np. za pośrednictwem aplikacji rejestrującej tętno lub technologii wykorzystywanej w celu śledzenia zachowania dotyczącego przeglądania), również należy uznać za „dostarczone przez" tę osobę, nawet jeżeli dane te nie zostały przesłane aktywnie lub świadomie.

W odniesieniu do danych osobowych dotyczących innych osób, których dane dotyczą:

Trzeci warunek ma na celu uniknięcie uzyskiwania danych obejmujących dane osobowe innych osób, których dane dotyczą (które nie wyraziły odpowiedniej zgody), oraz przesyłania takich danych nowemu administratorowi danych w przypadkach, gdy istnieje prawdopodobieństwo, że dane te będą przetwarzane w sposób, który wpływałby niekorzystnie na prawa i wolności pozostałych osób, których dane dotyczą (art. 20 ust. 4 RODO)[22].

Tego rodzaju niekorzystny wpływ miałby miejsce na przykład wówczas, gdy przesyłanie danych przez jednego administratora danych innemu administratorowi uniemożliwia osobom trzecim wykonywanie uprawnień przysługujących im jako osobom, których dane dotyczą, na mocy RODO (np. prawa do informacji, prawa dostępu itd.).

Osoba, której dane dotyczą, inicjująca przesyłanie swoich danych innemu administratorowi danych, udziela zgody na przetwarzanie danych nowemu administratorowi danych albo zawiera umowę z tym administratorem. Jeżeli dane osobowe osób trzecich są zawarte w zbiorze danych, należy określić inną podstawę prawną przetwarzania. Przykładowo prawnie uzasadniony interes może być realizowany przez administratora danych na mocy art. 6 ust. 1 lit. f), w szczególności gdy celem administratora danych jest świadczenie usługi na rzecz osoby, której dane dotyczą, a usługa ta umożliwia wspomnianej osobie przetwarzanie danych osobowych w ramach czynności o czysto osobistym lub domowym charakterze. Operacje przetwarzania zainicjowane przez osobę, której dane dotyczą, w kontekście czynności o charakterze osobistym, które dotyczą osób trzecich i potencjalnie wywierają na nie wpływ, należą do zakresu odpowiedzialności tej osoby w stopniu, w jakim o takim przetwarzaniu nie decyduje w jakikolwiek sposób administrator danych.

Przykładowo usługa *webmail* może umożliwić utworzenie spisu kontaktów, znajomych, krewnych, członków rodziny i szerszego otoczenia osoby, której dane dotyczą. Ponieważ dane te dotyczą możliwej do zidentyfikowania osoby fizycznej, która pragnie wykonać przysługujące jej prawo do przenoszenia danych (i są wytwarzane przez tę osobę), administratorzy danych powinni przesłać cały spis przychodzących i wychodzących wiadomości e-mail tej osobie, której dane dotyczą.

Podobnie rachunek bankowy osoby, której dane dotyczą, może zawierać dane osobowe dotyczące transakcji dokonywanych nie tylko przez posiadacza rachunku, ale również przez inne osoby fizyczne (np. jeżeli przekazały one środki pieniężne posiadaczowi rachunku). Jest mało prawdopodobne, by przesłanie informacji dotyczących rachunku bankowego posiadaczowi rachunku niekorzystnie wpłynęło na prawa i wolności tych osób trzecich po wniesieniu żądania przeniesienia – pod warunkiem, że w obu przykładach dane są wykorzystywane w tym samym celu (tj. adres kontaktowy wykorzystywany wyłącznie przez osobę, której dane dotyczą, lub historia rachunku bankowego osoby, której dane dotyczą).

Prawa i wolności osób trzecich zostaną natomiast naruszone, jeżeli nowy administrator danych wykorzysta dane osobowe do innych celów, np. jeżeli otrzymujący administrator danych wykorzysta dane osobowe innych osób fizycznych figurujących w spisie kontaktów osoby, której dane dotyczą, do celów marketingowych.

[22] Motyw 68 stanowi, że „jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia".

W związku z tym, aby zapobiec wywarciu niekorzystnego wpływu na zaangażowane osoby trzecie, przetwarzanie takich danych osobowych przez innego administratora jest dopuszczalne wyłącznie w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą użytkownika wnoszącego żądanie i są zarządzane wyłącznie w celu zaspokojenia potrzeb o czysto osobistym lub domowym charakterze. Otrzymujący „nowy" administrator danych (któremu dane mogą zostać przesłane na żądanie użytkownika) nie może wykorzystywać przesłanych danych osób trzecich do własnych celów, np. w celu oferowania produktów i usług marketingowych tym innym osobom, których dane dotyczą, będącym osobami trzecimi. Przykładowo informacji tych nie należy wykorzystywać do wzbogacenia profilu osoby trzeciej, której dane dotyczą, oraz do odbudowy jej środowiska społecznego, bez jej wiedzy i zgody[23]. Nie można ich również wykorzystywać w celu uzyskania informacji na temat takich osób trzecich oraz tworzenia określonych profili, nawet jeżeli ich dane osobowe znajdują się już w posiadaniu administratora danych. W przeciwnym razie istnieje prawdopodobieństwo, że takie przetwarzanie będzie niezgodne z prawem i nieuczciwe, w szczególności jeżeli osoby trzecie, których sprawa dotyczy, nie są o tym poinformowane i nie mogą wykonywać uprawnień przysługujących im jako osobom, których dane dotyczą.

Ponadto dominującą praktyką w przypadku wszystkich administratorów danych (zarówno stron „przesyłających", jak i „otrzymujących") jest wdrażanie narzędzi umożliwiających osobom, których dane dotyczą, wybór istotnych danych, które pragną otrzymać i przesłać, oraz wyłączenie – w stosownych przypadkach – danych innych osób fizycznych. Praktyka ta w dalszym stopniu przyczyni się do ograniczenia zagrożeń dla osób trzecich, których dane osobowe mogą zostać przeniesione.

Ponadto administratorzy danych powinni wdrożyć mechanizmy zgody w odniesieniu do innych zaangażowanych osób, których dane dotyczą, aby ułatwić przesyłanie danych w przypadkach, gdy takie osoby są gotowe wyrazić zgodę, np. jeżeli również pragną przenieść swoje dane do innego administratora danych. Taka sytuacja może mieć miejsce na przykład w przypadku portali społecznościowych, jednak decyzja dotycząca wyboru dominującej praktyki pozostaje w gestii administratorów danych.

W odniesieniu do danych objętych prawem własności intelektualnej i tajemnicami handlowymi:
O prawach i wolnościach innych wspomniano w art. 20 ust. 4. Chociaż nie są one bezpośrednio związane z przenoszeniem, można je rozumieć jako „[obejmujące] tajemnice handlowe lub własność intelektualną, w szczególności [...] prawa autorskie chroniące oprogramowanie". Chociaż prawa te należy uwzględnić przed udzieleniem odpowiedzi na żądanie przeniesienia danych, „względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji". Ponadto administrator danych nie powinien odrzucać żądania przeniesienia danych ze względu na naruszenie innego prawa wynikającego z umowy (na przykład ze względu na niespłacony dług lub konflikt handlowy z osobą, której dane dotyczą).

[23] Serwis społecznościowy nie powinien wzbogacać profili swoich członków, wykorzystując dane osobowe przesłane przez osobę, której dane dotyczą, w wykonaniu przysługującego jej prawa do przenoszenia danych, nie przestrzegając zasady przejrzystości oraz nie upewniwszy się, że opiera się on na odpowiedniej podstawie prawnej w zakresie tego konkretnego przetwarzania.

Ponadto prawo do przenoszenia danych nie jest prawem danej osoby fizycznej do nadużywania informacji w sposób, który można by zaklasyfikować jako nieuczciwą praktykę lub który stanowiłby naruszenie praw własności intelektualnej.

Potencjalne ryzyko biznesowe nie może jednak samo w sobie stanowić podstawy do odmowy udzielenia odpowiedzi na żądanie przeniesienia, przy czym administratorzy danych mogą przesłać dane osobowe dostarczone przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicami handlowymi lub prawami własności intelektualnej.

IV. W jaki sposób do przenoszenia danych stosuje się przepisy ogólne regulujące wykonywanie praw przysługujących osobie, której dane dotyczą,?

- **Jakie informacje należy uprzednio przekazać osobie, której dane dotyczą?**

W celu zapewnienia zgodności z nowym prawem do przenoszenia danych administratorzy danych muszą informować osoby, których dane dotyczą, o istnieniu nowego prawa do przenoszenia danych. Jeżeli dane osobowe, których sprawa dotyczy, są bezpośrednio zbierane od osoby, której dane dotyczą, informacje te należy podać „podczas pozyskiwania danych osobowych". Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator danych musi przekazać osobie, której dane dotyczą, informacje określone w art. 13 ust. 2 lit. b) i art. 14 ust. 2 lit. c).

„Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą", zgodnie z art. 14 ust. 3 informacje należy podać w rozsądnym terminie nieprzekraczającym jednego miesiąca od dnia pozyskania danych osobowych, przy pierwszej komunikacji z osobą, której dane dotyczą, lub w przypadku ujawnienia danych osobom trzecim[24].

Przekazując wymagane informacje, administratorzy danych muszą zapewnić, że odróżniają prawo do przenoszenia danych od innych praw. W związku z tym Grupa Robocza Art. 29 zaleca w szczególności, aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, których dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych.

Ponadto Grupa Robocza zaleca, aby administratorzy danych zawsze przekazywali informacje dotyczące prawa do przenoszenia danych, zanim osoby, których dane dotyczą, zamkną jakiekolwiek konto, które posiadają. Umożliwia to użytkownikom przeanalizowanie swoich danych osobowych oraz ich łatwe przesłanie na własne urządzenie lub przesłanie innemu dostawcy przed rozwiązaniem umowy

Ponadto jako wiodącą praktykę do stosowania przez „otrzymujących" administratorów danych Grupa Robocza Art. 29 zaleca, aby zapewniali oni osobom, których dane dotyczą, kompletne informacje na temat charakteru danych osobowych, które są istotne dla świadczenia zapewnianych przez nich usług. Oprócz wspierania rzetelnego przetwarzania danych pozwala to użytkownikom ograniczyć zagrożenia dla osób trzecich, jak również ograniczyć wszelkie innego rodzaju niepotrzebne powielanie danych osobowych, nawet w przypadku braku zaangażowania jakichkolwiek innych osób, których dane dotyczą.

[24] Zgodnie z art. 12 administratorzy danych są zobowiązani do przekazywania „wszelkich informacji […] w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka".

- **W jaki sposób administrator danych może zidentyfikować osobę, której dane dotyczą, przed udzieleniem odpowiedzi na jej żądanie?**

W RODO nie ustanowiono żadnych bezwzględnie obowiązujących wymogów w zakresie sposobu uwierzytelniania osoby, której dane dotyczą. Art. 12 ust. 2 RODO stanowi jednak, że administrator danych nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać przysługujące jej prawa (w tym prawo do przenoszenia danych), chyba że przetwarza dane osobowe w celu, który nie wymaga identyfikacji osoby, której dane dotyczą, oraz może on wykazać, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. Zgodnie z art. 11 ust. 2 w takich okolicznościach osoba, której dane dotyczą, może jednak dostarczyć dodatkowe informacje pozwalające ją zidentyfikować. Ponadto art. 12 ust. 6 stanowi, że jeżeli administrator danych ma uzasadnione wątpliwości odnośnie do tożsamości osoby, której dane dotyczą, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Jeżeli osoba, której dane dotyczą, dostarczy dodatkowe informacje pozwalające ją zidentyfikować, administrator danych nie odmawia podjęcia działań na żądanie tej osoby. Jeżeli informacje i dane gromadzone *online* są powiązane z pseudonimami lub unikatowymi identyfikatorami, administratorzy danych mogą wdrożyć odpowiednie procedury umożliwiające osobie fizycznej wniesienie żądania przeniesienia danych i otrzymanie odnoszących się do niej danych. W każdym razie administratorzy danych muszą wdrożyć procedurę uwierzytelniania, aby uzyskać całkowitą pewność odnośnie do tożsamości osoby, której dane dotyczą i która żąda swoich danych osobowych lub w ogólniejszym ujęciu wykonuje przysługujące jej prawa przyznane na mocy RODO.

Procedury te w wielu przypadkach już istnieją. Osoby, których dane dotyczą, często zostają już uwierzytelnione przez administratora danych przed zawarciem umowy lub uzyskaniem ich zgody na przetwarzanie. W rezultacie dane osobowe wykorzystywane do rejestracji osoby fizycznej, której dotyczy przetwarzanie, można również wykorzystać jako dowód uwierzytelnienia osoby, której dane dotyczą, do celów przeniesienia[25].

Chociaż w tych przypadkach uprzednia identyfikacja osób, których dane dotyczą, może wymagać żądania przedstawienia dowodu potwierdzającego ich tożsamość prawną, tego rodzaju weryfikacja może nie być właściwa do oceny powiązania między danymi a osobą fizyczną, której sprawa dotyczy, ponieważ takie powiązanie nie jest związane z tożsamością urzędową lub prawną. Co do zasady możliwość żądania przez administratora danych dostarczenia dodatkowych informacji w celu oceny tożsamości danej osoby 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.

Takie procedury uwierzytelniania istnieją już w wielu przypadkach. Przykładowo nazwy użytkownika i hasła są często wykorzystywane, aby umożliwić osobom fizycznym uzyskanie dostępu do danych zawartych na posiadanych przez nie kontach e-mail, kontach na portalach społecznościowych oraz kontach wykorzystywanych w ramach różnych innych usług, a w niektórych przypadkach osoby fizyczne zdecydowały się na korzystanie z niektórych spośród nich bez ujawniania swojego imienia i nazwiska oraz swojej tożsamości.

[25] Przykładowo, jeżeli przetwarzanie danych jest związane z kontem użytkownika, dostarczenie odpowiedniego loginu i hasła może być wystarczające do identyfikacji osoby, której dane dotyczą.

Jeżeli rozmiar danych żądanych przez osobę, której dane dotyczą, powoduje, że ich przesłanie za pośrednictwem internetu może być problematyczne, zamiast potencjalnego skorzystania z możliwości przedłużenia terminu na spełnienie żądania o maksymalnie trzy miesiące[26] administrator danych może również rozważyć alternatywne środki dostarczenia danych, takie jak transmisja strumieniowa lub zapisanie na płycie CD, DVD lub innym nośniku fizycznym, bądź zezwolenie na przesłanie danych osobowych bezpośrednio innemu administratorowi danych (zgodnie z art. 20 ust. 2 RODO, o ile jest to technicznie możliwe).

- **Jaki termin wyznaczono na udzielenie odpowiedzi na żądanie przeniesienia?**

Zgodnie z art. 12 ust. 3 administrator danych udziela „informacji o działaniach podjętych w związku z żądaniem" osobie, której dane dotyczą, „bez zbędnej zwłoki", a w każdym razie „w terminie miesiąca od otrzymania żądania". Wspomniany miesięczny termin można przedłużyć o kolejne trzy miesiące z uwagi na skomplikowany charakter sprawy, pod warunkiem że osobę, której dane dotyczą, poinformowano o przyczynach takiego opóźnienia w terminie miesiąca od dnia wniesienia pierwotnego żądania.

Istnieje prawdopodobieństwo, że administratorzy danych świadczący usługi społeczeństwa informacyjnego będą lepiej przygotowani do spełniania żądań w bardzo krótkim terminie. Aby sprostać oczekiwaniom użytkownika, dobrą praktyką jest określenie terminu, w jakim co do zasady można uzyskać odpowiedź na żądanie przeniesienia danych, oraz powiadomienie o nim osób, których dane dotyczą.

Administratorzy danych, którzy odmawiają udzielenia odpowiedzi na żądanie przeniesienia zgodnie z art. 12 ust. 4, informują osobę, której dane dotyczą, „o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem" najpóźniej w terminie miesiąca od otrzymania żądania.

Administratorzy danych muszą przestrzegać obowiązku udzielenia odpowiedzi w wyznaczonych terminach, nawet jeżeli jest to odpowiedź odmowna. Innymi słowy, administrator danych nie może zachować milczenia w przypadku zwrócenia się do niego o udzielenie odpowiedzi na żądanie przeniesienia danych.

- **W jakich przypadkach można odrzucić żądanie przeniesienia danych lub pobrać opłatę?**

W art. 12 administratorom danych zakazuje się pobierania opłaty za przekazanie danych osobowych, chyba że administrator danych może wykazać, że żądania są ewidentnie nieuzasadnione lub nadmierne, „w szczególności ze względu na swój ustawiczny charakter". W przypadku usług społeczeństwa informacyjnego, które specjalizują się w zautomatyzowanym przetwarzaniu danych osobowych, wdrożenie zautomatyzowanych systemów, takich jak interfejs programowania aplikacyjnego[27], może ułatwić wymianę z osobą, której dane dotyczą, a zatem zmniejszyć potencjalne obciążenie wynikające z ustawicznych żądań. Powinno być zatem bardzo niewiele przypadków, w których

[26] Art. 12 ust. 3: „Administrator [...] udziela [...] informacji o działaniach podjętych w związku z żądaniem".
[27] Interfejs programowania aplikacyjnego oznacza interfejsy aplikacji lub usług sieciowych udostępniane przez administratorów danych w taki sposób, aby inne systemy lub aplikacje mogły łączyć się i pracować z ich systemami.

administrator danych byłby w stanie uzasadnić odmowę dostarczenia informacji objętych żądaniem, nawet w odniesieniu do wielokrotnych żądań przeniesienia danych.

Ponadto przy określaniu nadmiernego charakteru żądania nie należy brać pod uwagę całkowitego kosztu procedur ustanowionych w celu udzielania odpowiedzi na żądania przeniesienia danych. W istocie w art. 12 RODO skoncentrowano się na żądaniach wnoszonych przez jedną osobę, której dane dotyczą, a nie na łącznej liczbie żądań otrzymanych przez administratora danych. W związku z tym całkowitymi kosztami wdrożenia systemu nie można obciążać osób, których dane dotyczą, ani nie można wykorzystywać tego rodzaju kosztów jako uzasadnienia odmowy udzielenia odpowiedzi na żądania przeniesienia.

V. W jaki sposób należy przekazywać dane podlegające przenoszeniu?

- Jakie są oczekiwane środki, które powinien wdrożyć administrator danych w celu przekazania danych?

Art. 20 ust. 1 RODO stanowi, że osoby, których dane dotyczą, mają prawo przesłać dane innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Tego rodzaju przeszkody można określić jako bariery prawne, techniczne lub finansowe ustanowione przez administratora danych w celu powstrzymania lub spowolnienia dostępu, przesyłania lub ponownego wykorzystania przez osobę, której dane dotyczą, lub przez innego administratora danych. Przykładowo taką przeszkodę mogą stanowić: żądanie wniesienia opłaty z tytułu przekazania danych, brak interoperacyjności lub dostępu do formatu danych, interfejsu programowania aplikacyjnego lub dostarczonego formatu, nadmierna zwłoka lub złożoność w odniesieniu do uzyskania pełnego zbioru danych, celowe zamaskowanie zbioru danych lub szczególne i nieuzasadnione lub nadmierne żądania sektorowej normalizacji lub akredytacji[28].

Ponadto w art. 20 ust. 2 nałożono na administratorów danych obowiązki przesłania danych podlegających przenoszeniu bezpośrednio innym administratorom danych, „o ile jest to technicznie możliwe".

Techniczną możliwość przesłania danych przez administratora danych innemu administratorowi danych pod kontrolą osoby, której dane dotyczą, należy oceniać w poszczególnych przypadkach. W motywie 68 dokładniej wyjaśniono granice określenia „technicznie możliwe", wskazując, że omawiane prawo „nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania".

Od administratorów danych oczekuje się przesyłania danych osobowych w interoperacyjnym formacie, chociaż nie nakłada to obowiązku obsługi tych formatów na innych administratorów danych. Bezpośrednie przesłanie danych przez jednego administratora danych innemu administratorowi mogłoby mieć zatem miejsce wówczas, gdy możliwa jest

[28] Mogą wystąpić określone przeszkody prawne, takie jak przeszkody związane z prawami i wolnościami innych wskazane w art. 20 ust. 4 lub przeszkody związane z bezpieczeństwem własnych systemów administratorów. Uzasadnienie, dlaczego takie przeszkody byłyby zgodne z prawem oraz dlaczego nie stanowią one przeszkody w rozumieniu art. 20 ust. 1, należy do obowiązków administratora danych.

komunikacja między dwoma systemami w zabezpieczony sposób[29] oraz gdy system otrzymujący ma techniczną możliwość odebrania przychodzących danych. Jeżeli przeszkody techniczne uniemożliwiają bezpośrednie przesłanie, administrator danych wyjaśnia istotę tych przeszkód osobom, których dane dotyczą, ponieważ w przeciwnym razie jego decyzja wywoła skutek podobny do odmowy podjęcia działań w związku z żądaniem osoby, której dane dotyczą (art. 12 ust. 4).

Na poziomie technicznym administratorzy danych powinni zbadać i ocenić dwa różne i uzupełniające się sposoby udostępniania danych podlegających przenoszeniu osobom, których dane dotyczą, lub innym administratorom danych:

- bezpośrednie przesłanie całego zbioru danych zawierającego dane podlegające przenoszeniu (lub kilku fragmentów części globalnego zbioru danych);
- zautomatyzowane narzędzie umożliwiające wyodrębnianie istotnych danych.

Drugi sposób może być preferowany przez administratorów danych w przypadkach obejmujących złożone, obszerne zbiory danych, ponieważ umożliwia on wyodrębnienie jakiejkolwiek części zbioru danych, która jest istotna dla osoby, której dane dotyczą, w kontekście jej żądania, może pomóc zminimalizować ryzyko oraz potencjalnie umożliwia wykorzystanie mechanizmów synchronizacji danych[30] (np. w kontekście regularnej komunikacji między administratorami danych). Może być to lepszy sposób zapewnienia zgodności w przypadku „nowego" administratora oraz stanowiłby on dobrą praktykę w zakresie ograniczania zagrożeń dla prywatności ze strony pierwotnego administratora danych.

Powyższe dwa różne i potencjalnie uzupełniające się sposoby przekazywania istotnych danych podlegających przenoszeniu można wdrożyć, udostępniając dane za pośrednictwem różnych środków, takich jak np. zabezpieczona wymiana komunikatów, serwer SFTP, interfejs programowania aplikacyjnego sieci Web lub portal sieci Web. Osoby, których dane dotyczą, powinny mieć możliwość korzystania z usług przechowywania danych osobowych, z systemu zarządzania danymi osobowymi[31] lub z innych rodzajów usług świadczonych przez zaufane osoby trzecie w celu przechowywania danych osobowych i udzielania administratorom danych pozwolenia na dostęp do danych i na ich przetwarzanie według potrzeb.

- **Jaki jest oczekiwany format danych?**

W RODO nałożono na administratorów danych wymogi przekazywania danych osobowych żądanych przez osobę fizyczną w formacie umożliwiającym ich ponowne wykorzystanie. W szczególności art. 20 ust. 1 RODO stanowi, że dane osobowe należy przekazać „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu

[29] Za pośrednictwem uwierzytelnionej komunikacji o niezbędnym poziomie szyfrowania danych.
[30] Mechanizm synchronizacji może pomóc w wykonaniu ogólnych obowiązków przewidzianych w art. 5 RODO, który stanowi, że „dane osobowe muszą być [...] prawidłowe i w razie potrzeby uaktualniane".
[31] W odniesieniu do systemów zarządzania danymi osobowymi (PIMS) zob. na przykład opinia EIOD 9/2016 dostępna pod adresem https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

maszynowego". W motywie 68 przedstawiono dodatkowe wyjaśnienie, zgodnie z którym format ten powinien być interoperacyjny, przy czym termin ten definiuje się[32] w UE jako:

> „możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów TIK".

Terminy „ustrukturyzowany", „powszechnie używany" i „nadający się do odczytu maszynowego" stanowią zestaw minimalnych wymogów, które powinny umożliwiać interoperacyjność formatu danych przekazanych przez administratora danych. W ten sposób terminy „ustrukturyzowany, powszechnie używany i nadający się do odczytu maszynowego" stanowią określenia środków, natomiast interoperacyjność stanowi pożądany wynik.

W motywie 21 dyrektywy 2013/37/UE[3334] zdefiniowano termin „przeznaczony do odczytu komputerowego" jako:

> „format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, w tym poszczególne stwierdzenia faktów, i ich wewnętrzną strukturę. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne z powodu niemożności pozyskania danych lub utrudnień w ich pozyskaniu z tych dokumentów nie należy uznawać za sporządzone w formacie przeznaczonym do odczytu komputerowego. Państwa członkowskie powinny w stosownych przypadkach zachęcać do korzystania z formatów otwartych przeznaczonych do odczytu komputerowego".

Biorąc pod uwagę szeroki zakres potencjalnych rodzajów danych, które administrator danych może przetworzyć, w RODO nie przedstawiono szczegółowych zaleceń odnośnie do formatu przekazywanych danych osobowych. Najodpowiedniejszy format będzie zależał od sektora – odpowiednie formaty mogą już istnieć i zawsze należy je wybierać, dążąc do celu, jakim jest możliwość ich interpretacji i zapewnienie osobie, której dane dotyczą, znacznych możliwości przenoszenia danych. Formaty podlegające kosztownym ograniczeniom w zakresie udzielania licencji nie zostałyby jako takie uznane za właściwe podejście.

W motywie 68 wyjaśniono, że „przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie

[32] Art. 2 decyzji Parlamentu Europejskiego i Rady nr 922/2009/WE z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA), Dz.U. L 260 z 3.10.2009, s. 20.
[33] Zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego.
[34] Glosariusz UE (http://eur-lex.europa.eu/eli-register/glossary.html) zawiera dalsze wyjaśnienie dotyczące oczekiwań związanych z pojęciami stosowanymi w niniejszych wytycznych, takich jak „nadający się do odczytu maszynowego", „interoperacyjność", „format otwarty", „standard", „metadane".

systemów przetwarzania". **Celem przenoszenia jest zatem interoperacyjność systemów, a nie ich kompatybilność**[35].

Oczekuje się, że dane osobowe będą przekazywane w formatach o wysokim poziomie abstrakcji względem wszelkich formatów wewnętrznych lub zastrzeżonych. Przenoszenie danych oznacza zatem dodatkową warstwę przetwarzania danych przez administratorów danych w celu uzyskania danych z platformy i wyodrębnienia danych osobowych nieobjętych zakresem przenoszenia danych, takich jak dane wywnioskowane lub dane związane z bezpieczeństwem systemów. W ten sposób administratorów danych zachęca się do wcześniejszego zidentyfikowania danych objętych zakresem przenoszenia we własnych systemach. Tego rodzaju dodatkowe przetwarzanie danych będzie uznawane za pomocnicze w stosunku do głównego przetwarzania danych, ponieważ nie dokonuje się go, aby osiągnąć nowy cel określony przez administratora danych.

Jeżeli żadne formaty nie są powszechnie używane w danej branży lub w określonym kontekście, **administratorzy danych powinni przekazać dane osobowe w powszechnie używanych formatach otwartych (np. XML, JSON, CSV itd.) wraz z** przydatnymi **metadanymi o najwyższym możliwym poziomie szczegółowości** przy jednoczesnym zachowaniu wysokiego poziomu abstrakcji. Odpowiednie metadane należy jako takie wykorzystywać w celu prawidłowego opisania znaczenia informacji będących przedmiotem wymiany. Takie metadane powinny być wystarczające dla umożliwienia funkcjonowania i ponownego wykorzystywania danych, jednak oczywiście bez ujawniania tajemnic handlowych. Jest zatem mało prawdopodobne, by przekazanie osobie fizycznej wersji skrzynki odbiorczej e-mail w formacie PDF miało wystarczająco ustrukturyzowany lub opisowy charakter dla umożliwienia łatwego ponownego wykorzystania danych dotyczących skrzynki odbiorczej. Dane dotyczące wiadomości e-mail należy przekazywać w formacie zachowującym wszystkie metadane, aby umożliwić skuteczne ponowne wykorzystanie danych. W takiej sytuacji podczas wyboru formatu danych, w jakim dane osobowe mają zostać przekazane, administrator danych powinien uwzględnić sposób, w jaki format ten może wpłynąć na prawo danej osoby fizycznej do ponownego wykorzystania danych lub w jaki może on to prawo ograniczyć. W przypadkach, w których administrator danych może zapewnić osobie, której dane dotyczą, możliwość wyboru preferowanego formatu danych osobowych, należy udzielić tej osobie zrozumiałego wyjaśnienia skutków, jakie wywoła określony wybór. Przetwarzanie dodatkowych metadanych wyłącznie dlatego, że mogłyby one być potrzebne lub pożądane w celu udzielenia odpowiedzi na żądanie przeniesienia danych, nie zapewnia jednak podstawy prawnej takiego przetwarzania.

Grupa Robocza Art. 29 usilnie zachęca zainteresowane strony w branży i stowarzyszenia branżowe do współpracy i opracowania wspólnego zbioru standardów i formatów interoperacyjnych, aby spełnić wymogi dotyczące prawa do przenoszenia danych. Jednym z instrumentów stworzonych w celu stawienia czoła temu wyzwaniu są europejskie ramy interoperacyjności, które przyczyniły się do wypracowania uzgodnionego podejścia do interoperacyjności w odniesieniu do organizacji, które pragną wspólnie świadczyć usługi publiczne. W ramach tych – w zakresie ich stosowania – określono zestaw

[35] W ISO/IEC 2382-01 zdefiniowano interoperacyjność w następujący sposób: „zdolność różnych elementów funkcjonalnych systemów informatycznych do komunikacji, uruchamiania programów lub przesyłania danych pomiędzy nimi w sposób niewymagający od ich od użytkownika żadnej wiedzy lub wymagający od niego wiedzy minimalnej na temat unikalnych właściwości tych elementów".

wspólnych elementów, takich jak słownictwo, pojęcia, zasady, polityki, wytyczne, zalecenia, normy, specyfikacje i praktyki[36].

- **W jaki sposób należy postępować w przypadku zbierania danych osobowych na szeroką skalę lub złożonego gromadzenia danych?**

W RODO nie wyjaśniono, w jaki sposób można zmierzyć się z wyzwaniem udzielenia odpowiedzi w przypadku zbierania danych na szeroką skalę, złożonej struktury danych lub wystąpienia innych problemów technicznych, które mogą przysparzać trudności administratorom danych lub osobom, których dane dotyczą.

We wszystkich jednak przypadkach kluczowe jest, aby dana osoba fizyczna była w stanie w pełni zrozumieć definicję, schemat i strukturę danych osobowych, które mogą zostać przekazane przez administratora danych. Przykładowo dane można w pierwszej kolejności przekazać w skróconej formie z wykorzystaniem pulpitów nawigacyjnych, umożliwiając osobie, której dane dotyczą, przenoszenie podzbiorów danych osobowych, a nie wszystkich danych. Administrator danych powinien przedstawić sens „w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem" (zob. art. 12 ust. 1 RODO) w taki sposób, aby osoba, której dane dotyczą, zawsze dysponowała jednoznacznymi informacjami na temat danych, jakie należy pobrać lub przesłać innemu administratorowi danych w związku z określonym celem. Przykładowo osoby, których dane dotyczą, powinny być w stanie korzystać z aplikacji oprogramowania w celu łatwego zidentyfikowania, rozpoznania lub przetwarzania określonych danych, które są tam zawarte.

Jak wskazano powyżej, praktycznym sposobem, w jaki administrator danych może udzielić odpowiedzi na żądania przeniesienia danych, jest zapewnienie odpowiednio zabezpieczonego i udokumentowanego interfejsu programowania aplikacyjnego. Może to umożliwić osobom fizycznym wnoszenie żądań dotyczących ich danych osobowych do administratora danych za pośrednictwem własnego oprogramowania lub oprogramowania osoby trzeciej bądź udzielenie pozwolenia innym podmiotom na wniesienie żądania w ich imieniu (w tym innemu administratorowi danych), jak określono w art. 20 ust. 2 RODO. Udzielając dostępu do danych za pośrednictwem zewnętrznie dostępnego interfejsu programowania aplikacyjnego, można również zapewnić bardziej skomplikowany system dostępu, który umożliwia osobom fizycznym wnoszenie kolejnych żądań dotyczących danych w formie pełnego pobrania albo w formie funkcji delta obejmującej wyłącznie zmiany, które zaszły od czasu ostatniego pobrania, przy czym tego rodzaju dodatkowe żądania nie mogą być uciążliwe dla administratora danych.

- **W jaki sposób można zabezpieczyć dane podlegające przenoszeniu?**

Co do zasady zgodnie z art. 5 ust. 1 lit. f) RODO administratorzy danych powinni zapewnić „odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych".

Przekazywanie danych osobowych osobie, której dane dotyczą, może jednak wiązać się również z pewnymi problemami pod względem bezpieczeństwa:

[36] Źródło: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

W jaki sposób administratorzy danych mogą zapewnić bezpieczne przekazanie danych osobowych właściwej osobie?

Ponieważ przenoszenie danych ma na celu pozyskanie danych osobowych z systemu informacyjnego administratora danych, przesłanie może stać się potencjalnym źródłem zagrożenia dotyczącego tych danych (w szczególności naruszeń ochrony danych podczas przesyłania). Administrator danych odpowiada za podjęcie wszelkich środków bezpieczeństwa potrzebnych w celu zapewnienia nie tylko bezpiecznego przesłania danych osobowych (przy wykorzystaniu pełnego szyfrowania transmisji lub szyfrowania danych) do właściwego miejsca przeznaczenia (przy wykorzystaniu silnych środków uwierzytelniających), ale także dalszej ochrony danych osobowych, które pozostają w jego systemie, jak również przejrzystych procedur postępowania w przypadku możliwych naruszeń ochrony danych[37]. Administratorzy danych powinni zatem ocenić szczególne zagrożenia związane z przenoszeniem danych i podjąć właściwe środki zmniejszające ryzyko.

Tego rodzaju środki zmniejszające ryzyko mogłyby obejmować: jeżeli uwierzytelnienie osoby, której dane dotyczą, jest konieczne już w danym momencie – wykorzystanie dodatkowych informacji uwierzytelniających takich jak wspólna tajemnica lub innego składnika uwierzytelnienia takiego jak hasło jednorazowe; zawieszenie lub zamrożenie przesyłania w przypadku powzięcia podejrzenia włamania na konto; w przypadku bezpośredniego przesyłania danych osobowych przez jednego administratora danych innemu administratorowi należy zastosować uwierzytelnianie na podstawie upoważnienia, takie jak uwierzytelnianie za pośrednictwem tokena.

Tego rodzaju środki bezpieczeństwa nie mogą utrudniać ani uniemożliwiać użytkownikom wykonywania przysługujących im praw, np. poprzez nałożenie dodatkowych kosztów.

W jaki sposób można pomóc użytkownikom w zabezpieczeniu przechowywania danych osobowych w ich własnych systemach?

W przypadku pozyskiwania danych osobowych z usługi *online* zawsze istnieje ryzyko, że użytkownicy mogą przechowywać je w mniej zabezpieczonych systemach niż system zapewniany przez tę usługę. Osoba, której dane dotyczą, żądająca danych odpowiada za identyfikację właściwych środków w celu zabezpieczenia danych osobowych we własnym systemie. Należy ją jednak o tym poinformować, aby umożliwić jej podjęcie kroków w celu ochrony informacji, które otrzymała. Jako przykład dominującej praktyki administratorzy danych mogą również zalecić właściwy format (właściwe formaty), narzędzia szyfrowania i inne środki bezpieczeństwa, aby pomóc osobie, której dane dotyczą, w osiągnięciu tego celu.

* * *

Sporządzono w Brukseli dnia 13 grudnia 2016 r.

W imieniu Grupy Roboczej
Przewodnicząca

[37] Zgodnie z dyrektywą (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Isabelle FALQUE-PIERROTIN

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca
Isabelle FALQUE-PIERROTIN