GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH

16/EN
WP 242 rew.01

Wytyczne dotyczące prawa do przenoszenia danych

Przyjęte w dniu 13 grudnia 2016 r.

Ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Sekretariat zapewnia Dyrekcja C (Prawa Podstawowe i Rządy Prawa) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów, B-1049 Bruksela, Belgia, biuro nr MO-59 05/35.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

Spis treści

Streszczenie

Artykuł 20 RODO ustanawia nowe prawo do przenoszenia danych, które jest ściśle związane z prawem dostępu, ale różni się od niego pod wieloma względami. Zapewnia ono osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyły administratorowi, oraz możliwość przesyłania tych danych osobowych innemu administratorowi. Celem tego nowego prawa jest zapewnienie praw osobie, której dane dotyczą, i przyznanie jej większej kontroli nad dotyczącymi jej danymi osobowymi.

W związku z tym, że prawo do przenoszenia danych pozwala na bezpośrednie przekazywanie danych osobowych od jednego administratora do innego, jest ono również ważnym narzędziem wspierającym swobodny przepływ danych osobowych w UE i sprzyjającym konkurencji między administratorami. Ułatwi ono zmianę dostawców usług i tym samym będzie sprzyjać rozwojowi nowych usług w kontekście strategii jednolitego rynku cyfrowego.

Niniejsza opinia zawiera wytyczne co do sposobu interpretacji i wdrożenia prawa do przenoszenia danych, zgodnie z RODO. Jej celem jest omówienie prawa do przenoszenia danych i jego zakresu. W opinii wyjaśniono warunki, pod jakimi to nowe prawo ma zastosowanie, przy wzięciu pod uwagę podstawy prawnej przetwarzania danych (albo zgody osoby, której dane dotyczą, albo konieczności wykonania umowy) oraz faktu, że prawo to jest ograniczone do danych osobowych przekazywanych przez osobę, której dane dotyczą. Opinia zawiera również konkretne przykłady i kryteria mające na celu wyjaśnienie okoliczności, w jakich prawo to ma zastosowanie. W tym względzie GR Art. 29 uważa, że prawo do przenoszenia danych obejmuje dane przekazane świadomie i aktywnie przez osobę, której dane dotyczą, jak również dane osobowe wygenerowane poprzez jej działanie. To nowe prawo nie może być naruszane ani ograniczone do danych osobowych bezpośrednio przekazanych przez osobę, której dane dotyczą, na przykład w formularzu online.

W ramach dobrej praktyki administratorzy danych powinni zacząć opracowywać środki, które przyczynią się do udzielania odpowiedzi na wnioski o przeniesienie danych, takie jak narzędzia do pobierania i interfejsy programowania aplikacji (Application Programming Interfaces - API). Powinni oni zagwarantować, że dane osobowe będą przekazywane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, oraz powinni być zachęcani do zapewnienia interoperacyjności formatu danych przekazywanych w ramach realizacji wniosku o przeniesienie danych.

Opinia pomaga również administratorom danych dokładnie zrozumieć ich poszczególne obowiązki oraz zaleca stosowanie najlepszych praktyk i narzędzi wspierających zgodność z prawem do przenoszenia danych. I wreszcie opinia zaleca, aby zainteresowane podmioty z branży i stowarzyszenia handlowe pracowały wspólnie nad powszechnym zestawem interoperacyjnych standardów i formatów celem opracowania wymogów prawa do przenoszenia danych.

I. Wprowadzenie

Artykuł 20 ogólnego rozporządzenia o ochronie danych (RODO) wprowadza nowe prawo do przenoszenia danych. Prawo to zapewnia osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do

odczytu maszynowego danych osobowych, które dostarczyły administratorowi, oraz możliwość przesłania tych danych osobowych innemu administratorowi bez przeszkód. Prawo to ma zastosowanie pod pewnymi warunkami i wspiera możliwość dokonywania wyboru i sprawowania kontroli przez użytkownika oraz uprawnienia użytkownika.

Przy realizacji prawa dostępu osób do danych na mocy dyrektywy o ochronie danych 95/46/WE wprowadzono ograniczenie poprzez format przekazywania wnioskowanych informacji wybrany przez administratora danych. **Nowe prawo do przenoszenia danych ma na celu zapewnienie uprawnień osobom, których dane dotyczą, w odniesieniu do ich danych osobowych, ponieważ ułatwia ono osobom możliwość łatwego przenoszenia, kopiowania lub przesyłania danych osobowych z jednego środowiska IT do innego** (czy to do własnych systemów, systemów zaufanych stron trzecich czy też systemów nowych administratorów danych).

Poprzez potwierdzenie praw osobowych przysługujących osobom i kontroli nad dotyczącymi ich danymi osobowymi, prawo do przenoszenia danych stanowi możliwość przywrócenia równowagi relacjom między osobami, których dane dotyczą, a administratorami danych[1].

Podczas gdy prawo do przenoszenia danych osobowych może również zwiększać konkurencję wśród dostawców usług (ułatwiając osobom zmianę dostawców usług), RODO zawiera regulacje dotyczące danych osobowych, a nie konkurencji. W szczególności artykuł 20 nie ogranicza danych podlegających przenoszeniu do tych, które są konieczne lub przydatne do zmiany usługi[2].

Mimo że przenoszenie danych jest nowym prawem, inne rodzaje przenoszenia już istnieją lub są omawiane w innych obszarach ustawodawstwa (np. w kontekstach zakończenia umowy, roamingu w usługach komunikacyjnych i transgranicznego dostępu do usług[3]). Pomiędzy tymi rodzajami przenoszenia mogą wystąpić określone synergie, a nawet korzyści dla osób, jeżeli zapewniane są w podejściu łączonym, choć analogie należy traktować ostrożnie.

Niniejsza opinia zapewnia wytyczne dla administratorów danych, tak aby mogli zaktualizować swoje praktyki, procedury i polityki, oraz wyjaśnia znaczenie pojęcia przenoszenia danych w celu umożliwienia osobom, których dane dotyczą, skutecznego korzystania z ich nowego prawa.

II. Jakie są główne elementy przenoszenia danych?

RODO definiuje prawo do przenoszenia danych w artykule 20 ust. 1 jak następuje:

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

[1] Podstawowym celem przenoszenia danych jest zwiększenie kontroli osoby nad jej danymi osobowymi oraz zapewnienie odgrywania przez nie czynnej roli w ekosystemie danych.
[2] Na przykład może to pozwolić bankom na świadczenie dodatkowych usług, pod kontrolą użytkownika, przy wykorzystaniu danych osobowych pierwotnie zebranych w związku z usługą dostawy energii.
[3] Patrz agenda jednolitego rynku cyfrowego Komisji Europejskiej: https://ec.europa.eu/digital-agenda/en/digital-single-market, w szczególności pierwszy filar polityki „Lepszy dostęp do cyfrowych dóbr i usług"

administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe […]

- Prawo do otrzymania danych osobowych

Po pierwsze przenoszenie danych to **prawo osoby, której dane dotyczą, do otrzymania podzbioru danych osobowych** jej dotyczących przetwarzanych przez administratora danych oraz przechowywania tych danych w celu dalszego osobistego wykorzystania. Tego typu przechowanie może mieć miejsce na urządzeniu prywatnym lub w prywatnej chmurze, bez konieczności przesyłania ich innemu administratorowi danych.

W tym względzie przenoszenie danych uzupełnia prawo dostępu. Jedną z cech charakterystycznych przenoszenia danych jest fakt, że oferuje ono łatwy sposób samodzielnego zarządzania danymi osobowymi przez osoby, których dane dotyczą, i ponownego wykorzystywania tych danych. Dane te powinny być „*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 dowiedzieć się, ile razy słuchała określonych utworów w celu sprawdzenia, jaki utwór muzyczny chce nabyć lub jakiego utworu chce posłuchać na innej platformie. Podobnie, może również chcieć uzyskać listę kontaktową ze swojej aplikacji poczty e-mail, na przykład aby stworzyć listę gości weselnych, lub uzyskać informacje na temat zakupów dokonanych przy użyciu różnych kart lojalnościowych, aby ocenić, gdzie i w jakim zakresie znajdują się jej dane osobowe[4].

- Prawo do przesyłania danych osobowych od jednego administratora danych do innego

Po drugie, artykuł 20 ust. 1 przyznaje osobom, których dane dotyczą, **prawo do przesyłania danych osobowych od jednego administratora danych do innego** „bez przeszkód". Dane mogą być również przesłane bezpośrednio od jednego administratora danych do innego na żądanie osoby, której dane dotyczą, i o ile jest to technicznie możliwe (artykuł 20 ust. 2).W tym zakresie motyw 68 zachęca administratorów danych do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych[5], ale nie nakładając na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania[6]. Jednakże RODO nie zakazuje administratorom tworzenia barier dla przesyłania danych.

Krótko mówiąc, ten element przenoszenia danych zapewnia osobom, których dane dotyczą, możliwość nie tylko uzyskania i ponownego wykorzystania, ale również przesyłania danych, które przekazały innemu dostawcy usług (albo w ramach tego samego sektora przedsiębiorstw albo w innym). Poza zapewnieniem uprawnień konsumentom poprzez zapobieganie „uzależnieniu" (ang. „lock-in"*), prawo do przenoszenia danych ma promować możliwości innowacji i wymiany danych osobowych między administratorami danych w bezpieczny

[4] W tych przypadkach przetwarzanie dokonywane na danych przez osobę, której dane dotyczą, wchodzi w zakres działań działalności domowej i w związku z tym nie podlega już RODO.
[5] Patrz również część V.
[6] W konsekwencji należy zwracać szczególną uwagę na format danych, które mają być przesłane, aby zagwarantować, że dane będą mogły być ponownie wykorzystane, z małym wysiłkiem, przez osobę, której dane dotyczą, lub innego administratora danych. Patrz także część V.
** Przypis tłumacza: uzależnienie np. od jednego dostawcy czy od jednej usługi*

sposób, pod kontrolą osoby, której dane dotyczą[7]. Przenoszenie danych może propagować 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 dotyczących użytkowników między różnymi usługami, którymi są zainteresowani.

- Sprawowanie kontroli

Przenoszenie danych gwarantuje prawo do otrzymania danych osobowych i przetwarzania ich, zgodnie życzeniami osób, których dane dotyczą[9].

Administratorzy danych odpowiadający na wnioski o przeniesienie danych, na warunkach określonych w artykule 20, nie są odpowiedzialni za przetwarzanie prowadzone przez osobę, której dane dotyczą, lub przez inne przedsiębiorstwo otrzymujące dane osobowe. Działają w imieniu osoby, której dane dotyczą, w tym gdy dane osobowe są przesyłane bezpośrednio do innego administratora danych. W tym zakresie administrator danych nie jest odpowiedzialny za zapewnienie zgodności z prawem ochrony danych przez otrzymującego administratora danych, zważywszy że wysyłający administrator danych nie wybiera odbiorcy. Jednocześnie administratorzy powinni ustanowić zabezpieczenia w celu zapewnienia, że będą rzeczywiście działać w imieniu osoby, której dane dotyczą. Na przykład mogą ustanowić procedury, aby zapewnić, że przesyłane dane osobowe rzeczywiście będą danymi, które osoba, której dane dotyczą, chce przesłać. Można to uczynić, uzyskując potwierdzenie od osoby, której dane dotyczą albo przed przesłaniem albo wcześniej, gdy udzielana jest pierwotna zgoda na przetwarzanie lub gdy finalizowana jest umowa.

Administratorzy danych odpowiadający na wnioski o przeniesienie danych nie mają określonego obowiązku sprawdzenia i weryfikacji jakości danych przed ich przesłaniem. Oczywiście dane te powinny już być prawidłowe oraz aktualne, zgodnie z zasadami określonym w artykule 5 ust. 1 RODO. Ponadto przenoszenie danych nie nakłada na administratora danych obowiązku zatrzymywania danych osobowych dłużej niż to konieczne czy też dłużej niż przez określony okres przechowywania[10]. Co istotne, nie ma dodatkowego wymogu zatrzymywania danych w okresach innych niż te mające zastosowanie, po prostu w celu realizacji potencjalnego przyszłego wniosku o przeniesienie danych.

Gdy wnioskowane dane osobowe są przetwarzane przez podmiot przetwarzający dane, umowa zawarta zgodnie z artykułem 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". Zatem administrator danych powinien wdrożyć określone procedury we współpracy ze swoimi podmiotami przetwarzającymi dane, aby odpowiedzieć na wnioski

---

[7] Patrz: kilka eksperymentalnych aplikacji w Europie, na przykład MiData w Zjednoczonym Królestwie, MesInfos / SelfData FING we Francji.

[8] Branże Internetu przedmiotów i tzw. „quantified self" (*przypis tłumacza: „zmierzona jaźń", czyli wiedza o nas samych uzyskana dzięki mierzeniu różnych aspektów naszego życia przy użyciu technologii*) pokazały korzyści (i zagrożenia) związane z łączeniem danych osobowych z różnych aspektów życia osoby, takich jak kondycja fizyczna, aktywność i ilość spożywanych kalorii, aby stworzyć całościowy obraz życia osoby w jednym pliku.

[9] Prawo do przenoszenia danych nie jest ograniczone do danych osobowych, które są przydatne i istotne dla podobnych usług świadczonych przez konkurencję administratora danych.

[10] W powyższym przykładzie, jeżeli administrator danych nie zatrzymuje listy utworów muzycznych odtwarzanych przez użytkownika, wówczas jego dane osobowe nie mogą być zawarte we wniosku o przeniesienie danych.

o przeniesienie danych. W przypadku sprawowania wspólnej kontroli umowa powinna wyraźnie przydzielić każdemu administratorowi danych obowiązki dotyczące przetwarzania wniosków o przeniesienie danych.

Ponadto otrzymujący administrator danych[11] jest odpowiedzialny za zapewnienie, aby przekazane dane podlegające przenoszeniu były stosowne i nie nadmierne w odniesieniu do nowego przetwarzania danych. Na przykład w przypadku wniosku o przeniesienie danych złożonego do dostawcy usługi poczty e-mail, gdzie osoba, której dane dotyczą, wykorzystuje możliwość złożenia wniosku w celu uzyskania wiadomości e-mail i przesłania ich na zabezpieczoną platformę służącą do przechowywania danych, nowy administrator danych nie musi przetwarzać danych kontaktowych osób, z którymi osoba, której dane dotyczą, koresponduje. Jeżeli informacje te nie są stosowne w odniesieniu do celu nowego przetwarzania, nie należy ich przechowywać ani przetwarzać. Podobnie w przypadku, gdy osoba, której dane dotyczą, wnioskuje o przesłanie informacji dotyczących jej transakcji bankowych serwisowi, który pomaga jej w zarządzaniu jej budżetem, otrzymujący administrator danych nie musi przyjmować wszystkich danych ani zatrzymywać wszystkich danych dotyczących transakcji, gdy zostały oznaczone do celów nowej usługi. Innymi słowy, przyjęte i zatrzymane dane powinny obejmować tylko te dane, które są niezbędne i istotne dla usługi świadczonej przez otrzymującego administratora danych.

Podmiot „otrzymujący" staje się nowym administratorem danych w odniesieniu do tych danych osobowych i musi przestrzegać zasad określonych w artykule 5 RODO. W związku z tym 'nowy' otrzymujący administrator danych musi wyraźnie i bezpośrednio określić cel nowego przetwarzania przed jakimkolwiek wnioskiem o przesłanie danych podlegających przenoszeniu, zgodnie z wymogami przejrzystości określonymi w artykule 14[12]. Tak jak w przypadku każdego innego przetwarzania danych prowadzonego na jego odpowiedzialność, administrator danych powinien stosować zasady określone w artykule 5, takie jak zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, integralność i poufność, ograniczenie przechowywania i rozliczalność[13].

Administratorzy danych przechowujący dane osobowe powinni być przygotowani do ułatwienia wykonywania prawa do przenoszenia danych przez osobę, której dane dotyczą. Administratorzy danych mogą również zadecydować o przyjęciu danych od osoby, której dane dotyczą, ale nie są do tego zobowiązani.

- Przenoszenie danych kontra inne prawa osób, których dane dotyczą

Gdy osoba realizuje swoje prawo do przenoszenia danych, czyni to bez uszczerbku dla żadnego innego prawa (tak jak w przypadku wszelkich innych praw w ramach RODO). Osoba, której dane dotyczą, może nadal korzystać z usług administratora danych nawet po

[11] Tj. ten, który otrzymuje dane osobowe po złożeniu przez osobę, której dane dotyczą, wniosku o przeniesienie danych do innego administratora

[12] Ponadto nowy administrator danych nie powinien przetwarzać danych osobowych, które nie są stosowne, a przetwarzanie musi być ograniczone do tego, co jest niezbędne do nowych celów, nawet jeśli dane osobowe stanowią część bardziej globalnego zestawu danych przesyłanego w ramach procedury przenoszenia. Dane osobowe, które nie są niezbędne do osiągnięcia celu nowego przetwarzania, należy usunąć tak szybko jak to możliwe.

[13] Po tym jak administrator danych otrzyma dane osobowe przesłane w ramach prawa do przenoszenia danych, mogą one być uznane za „przekazane przez" osobę, której dane dotyczą, i ponownie przesłane zgodnie z prawem do przenoszenia danych, w zakresie w jakim spełnione są inne warunki mające zastosowanie do tego prawa (tj. podstawa prawna przetwarzania,…).

operacji przeniesienia danych. Przenoszenie danych nie powoduje automatycznie usunięcia danych[14] z systemów administratora danych i nie wpływa na pierwotny okres przechowywania mający zastosowanie wobec danych, które zostały przesłane. Osoba, której dane dotyczą, może realizować swoje prawa, o ile administrator danych nadal przetwarza dane.

Jednocześnie, jeżeli osoba, której dane dotyczą, chce zrealizować swoje prawo do usunięcia danych „prawo do bycia zapomnianym" na mocy artykułu 17), przenoszenie danych nie może być zastosowane przez administratora danych jako sposób opóźnienia lub odmowy takiego usunięcia.

Jeżeli osoba, której dane dotyczą, dowie się, że dane osobowe wnioskowane na mocy prawa do przenoszenia danych nie odpowiadają w pełni jej wnioskowi, każdy kolejny wniosek o dostęp do danych osobowych na mocy prawa dostępu winien być w pełni zrealizowany, zgodnie z artykułem 15 RODO.

Ponadto w przypadku, gdy szczególne prawo europejskie lub prawo państwa członkowskiego w innym obszarze również przewiduje jakąś formę przenoszenia przedmiotowych danych, warunki określone w takim prawie szczególnym także muszą być wzięte pod uwagę przy realizacji wniosku o przeniesienie danych na mocy RODO. Po pierwsze, jeżeli z wniosku złożonego przez osobę, której dane dotyczą, wyraźnie wynika, że jej zamiarem nie jest realizacja praw na mocy RODO, ale raczej realizacja praw na mocy tylko ustawodawstwa sektorowego, przepisy RODO dotyczące przenoszenia danych nie będą miały zastosowania do tego wniosku[15]. Jeżeli, z drugiej strony, celem wniosku jest przeniesienie na mocy RODO, istnienie takiego szczególnego ustawodawstwa nie uchyla zastosowania zasady przenoszenia danych wobec każdego administratora danych, jak przewidziano w RODO. Należy natomiast ocenić, dla poszczególnych przypadków, jak, o ile w ogóle, takie szczególne ustawodawstwo może wpłynąć na prawo do przenoszenia danych.

III. <u>Kiedy ma zastosowanie przenoszenie danych?</u>

- Jakie operacje przetwarzania obejmuje prawo do przenoszenia danych?

Zgodność z RODO wymaga od administratorów danych posiadania wyraźnej podstawy prawnej do przetwarzania danych osobowych.

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

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

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

[14] Jak określono w artykule 17 RODO.

[15] Na przykład, jeżeli wniosek osoby, której dane dotyczą, ma na celu w szczególności zapewnienie dostępu do jej historii rachunku bankowego dla dostawcy usługi informacji o koncie, do celów wskazanych w 2. Dyrektywie w sprawie usług płatniczych (PSD2), taki dostęp powinien być zapewniony zgodnie z przepisami tej dyrektywy.

Na przykład tytuły książek nabytych przez osobę z księgarni online lub utwory muzyczne słuchane za pośrednictwem serwisu strumieniowej transmisji muzyki stanowią inne przykłady danych osobowych, które generalnie wchodzą w zakres przenoszenia danych, ponieważ są przetwarzane na podstawie wykonania umowy, której stroną jest osoba, której dane dotyczą.

RODO nie ustanawia ogólnego prawa do przenoszenia danych dla przypadków, w których przetwarzanie danych osobowych nie odbywa się na podstawie zgody lub umowy[16]. Na przykład instytucje finansowego nie mają obowiązku odpowiadania na wnioski o przenoszenie danych dotyczące danych osobowych przetwarzanych w ramach ich obowiązków w zakresie zapobiegania i wykrywania prania pieniędzy i innych przestępstw finansowych; podobnie przenoszenie danych nie obejmuje zawodowych danych kontaktowych przetwarzanych w relacji „business to business" w przypadkach, gdy przetwarzanie nie jest oparte ani na zgodnie osoby, której dane dotyczą, ani na umowie, której jest ona stroną.

Jeżeli chodzi o dane pracowników, prawo do przenoszenia danych ma generalnie zastosowanie tylko, jeżeli przetwarzanie jest oparte na umowie, której stroną jest osoba, której dane dotyczą. W wielu przypadkach zgoda nie będzie uznana za dobrowolnie wyrażoną w tym kontekście, ze względu na brak równowagi sił między pracodawcą a pracownikiem[17]. Natomiast niektóre operacje przetwarzania w kontekście HR (zasobów ludzkich) oparte są na podstawie prawnej prawnie uzasadnionego interesu lub są konieczne do zapewnienia przestrzegania określonych zobowiązań prawnych w obszarze zatrudnienia. W praktyce prawo do przenoszenia danych w kontekście HR niewątpliwie dotyczyć będzie określonych operacji przetwarzania (takich jak usługi w zakresie płac i wynagrodzeń, wewnętrzna rekrutacja), ale w wielu sytuacjach potrzebne będzie podejście dla poszczególnych przypadków, aby zweryfikować, czy spełnione są wszystkie warunki mające zastosowanie do prawa do przenoszenia danych.

I wreszcie prawo do przenoszenia danych ma zastosowanie tylko, jeżeli przetwarzanie danych „odbywa się w sposób zautomatyzowany", i w związku z tym nie obejmuje większości zbiorów papierowych.

- Jakie dane osobowe muszą być uwzględnione?

Zgodnie z artykułem 20 ust. 1, aby dane mieściły się w zakresie prawa do przenoszenia danych, muszą:

- być to dane osobowe jej dotyczące, oraz
- które *przekazała* administratorowi danych.

[16] Patrz motyw 68 i artykuł 20 ust. 3 RODO. Artykuł 20 ust. 3 i motyw 68 przewidują, że przenoszenie danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub gdy administrator danych wykonuje obowiązki publiczne lub wywiązuje się z obowiązku prawnego. W związku z tym w tych przypadkach administratorzy danych nie mają obowiązku zapewniania przenoszenia danych. Jednak dobrą praktyką jest opracowanie procedur automatycznego odpowiadania na wnioski o przenoszenie, z poszanowaniem zasad regulujących prawo do przenoszenia danych. Przykładem tego jest serwis rządowy zapewniający łatwe pobieranie poprzednich złożonych deklaracji podatkowych. Przenoszenie danych jako dobra praktyka w przypadku przetwarzania opartego na podstawie prawnej w postaci konieczności w uzasadnionym interesie oraz istniejące dobrowolne programy – patrz strony 47 i 48 Opinii GR Art. 29 6/2014 w sprawie uzasadnionych interesów (WP217).

[17] Jak GR Art. 29 podkreśliła w swojej Opinii 8/2001 z 13 września 2001 r. (WP 48).

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

Pierwszy warunek: dane osobowe dotyczące osoby, której dane dotyczą

Tylko dane osobowe objęte są zakresem wniosku o przeniesienie danych. W związku z tym wszelkie dane będące danymi anonimowymi[18] lub niedotyczące osoby, której dane dotyczą, nie będą wchodziły w ten zakres. Jednak dane poddane pseudonimizacji, które można wyraźnie powiązać z osobą, której dane dotyczą (np. poprzez podanie przez nią odnośnego identyfikatora, por. artykuł 11 ust. 2), mieszczą się w tym zakresie.

W wielu okolicznościach administratorzy danych przetwarzają informacje, które zawierają dane osobowe kilku osób, których dane dotyczą. Gdy ma to miejsce, administratorzy danych nie powinni przyjmować zbyt wąskiej interpretacji zdania „dane osobowe dotyczące osoby, której dane dotyczą". Na przykład rejestry połączeń telefonicznych, wiadomości interpersonalnych lub VoIP [usług telefonii internetowej] (w historii konta abonenta) mogą zawierać dane stron trzecich zaangażowanych w połączenia przychodzące i wychodzące. Mimo że rejestry będą w związku z tym zawierały dane osobowe dotyczące wielu osób, abonenci powinni mieć możliwość otrzymania tych rejestrów w odpowiedzi na wnioski o przenoszenie danych, ponieważ rejestry dotyczą (także) osoby, której dane dotyczą. Jednak, gdy takie rejestry są następnie przesyłane nowemu administratorowi danych, ten nowy administrator danych nie powinien ich przetwarzać w żadnym celu, który by negatywnie wpłynął na prawa i wolności stron trzecich (patrz poniżej: trzeci warunek).

Drugi warunek: dane przekazywane przez osobę, której dane dotyczą

Drugi warunek zawęża zakres danych „przekazywanych przez" osobę, której dane dotyczą.

Istnieje wiele przykładów danych osobowych, które będą świadomie i aktywnie „przekazywane przez" osobę, której dane dotyczą, takie jak dane konta (np. adres pocztowy, nazwa użytkownika, wiek) podawane za pośrednictwem formularzy online. Niemniej dane „przekazywane przez" osobę, której dane dotyczą, również wynikają z obserwacji jej działalności. W konsekwencji GR Art. 29 uważa, że, aby nadać pełną wartość temu nowemu prawu, pojęcie „przekazywane przez" powinno obejmować także dane osobowe wynikające z obserwacji działań użytkowników, takie jak dane surowe przetwarzane przez inteligentne liczniki lub inne rodzaje przedmiotów połączonych[19], logi (dzienniki) działań, historia korzystania ze strony lub czynności wyszukiwania.

Ta ostatnia kategoria danych nie obejmuje danych, które są tworzone przez administratora danych, takich jak profil użytkownika utworzony poprzez analizę danych surowych zebranych przez inteligentne opomiarowanie.

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

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (*wersja angielska*); http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf (*wersja polska*)

[19] Mając możliwość uzyskiwania danych wynikających z obserwacji swoich działań, osoba, której dane dotyczą, będzie również mogła zyskać lepszy obraz wyborów dokonywanych przez administratora danych co do zakresu obserwowanych danych i będzie w lepszej sytuacji, jeżeli chodzi o wybór, jakie dane chce przekazać, aby uzyskać podobną usługę, oraz będzie świadoma stopnia, w jakim jest przestrzegane jej prawo do prywatności.

- **Dane aktywnie i świadomie przekazywane przez osobę, której dane dotyczą**(na przykład adres pocztowy, nazwa użytkownika, wiek, etc.)

- **Zaobserwowane dane przekazywane przez osobę, której dane dotyczą, w związku z korzystaniem z usługi lub urządzenia.** Mogą na przykład obejmować historię wyszukiwania osoby, dane o ruchu i dane lokalizacyjne. Mogą również obejmować inne dane surowe, takie jak tętno monitorowane przez urządzenia noszone na ciele.

Z kolei dane wywnioskowane i dane wywiedzione tworzone są przez administratora danych na podstawie danych „przekazanych przez osobę, której dane dotyczą". Na przykład wynik oceny dotyczącej zdrowia użytkownika lub profil tworzony w kontekście zarządzania ryzykiem i regulacji finansowych (np. w celu przypisania zdolności kredytowej lub przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy) nie mogą jako takie być uznane za „przekazane przez" osobę, której dane dotyczą. Mimo że takie dane mogą stanowić część profilu utrzymywanego przez administratora danych i są wywnioskowane lub wywiedzione z analizy danych przekazanych przez osobę, której dane dotyczą (na przykład poprzez jej działania), dane takie z reguły nie będą uznawane za „przekazane przez osobę, której dane dotyczą" i tym samym nie będą wchodzić w zakres tego nowego prawa[20].

Generalnie, zważywszy na cele polityki prawa do przenoszenia danych, termin „przekazane przez osobę, której dane dotyczą" musi być interpretowany szeroko, z wyłączeniem tylko „danych wywnioskowanych" i „danych wywiedzionych", które obejmują dane osobowe, które są tworzone przez dostawcę usług (na przykład wyniki algorytmiczne). Administrator może wyłączyć takie wywnioskowane dane, ale powinien uwzględnić wszystkie inne dane osobowe przekazane przez osobę, której dane dotyczą, za pomocą środków technicznych zapewnionych przez administratora[21].

Zatem termin „przekazane przez" obejmuje dane osobowe, które dotyczą działania osoby, której dane dotyczą, lub wyniku z obserwacji zachowania osoby, ale nie obejmuje danych danych wynikających z następującej analizy tego zachowania. Z drugiej strony, wszelkie dane osobowe, które zostały wytworzone przez administratora danych w ramach przetwarzania danych, np. przez proces personalizacji lub rekomendacji, przez kategoryzację użytkownika lub profilowanie, to dane, które są wywiedzione lub wywnioskowane z danych osobowych przekazanych przez osobę, której dane dotyczą, i nieobjęte prawem do przenoszenia danych.

<u>Trzeci warunek: prawo do przenoszenia danych nie może negatywnie wpływać na prawa i wolności innych</u>

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

[20] Niemniej osoba, której dane dotyczą, nadal może korzystać ze swojego prawa „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 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 artykułem 15 RODO (który dotyczy prawa dostępu).

[21] Obejmuje to wszystkie dane dotyczące osoby, której dane dotyczą, zaobserwowane podczas działań, na potrzeby których zbierane są dane, takie jak historia transakcji lub log dostępu. Dane zebrane poprzez śledzenie i nagrywanie osoby, której dane dotyczą, (np. aplikacja rejestrująca tętno lub technologia używana do śledzenia zachowań użytkowników w sieci) również powinny być uznawane za „przekazane przez" tę osobę, nawet jeżeli dane nie są aktywnie czy świadomie przesyłane.

Trzeci warunek ma na celu uniknięcie uzyskiwania i przesyłania danych obejmujących dane osobowe innych osób, których dane dotyczą (tych które nie wyraziły zgody) do nowego administratora danych w przypadkach, gdy istnieje prawdopodobieństwo, że dane te będą przetwarzane w sposób, który negatywnie wpłynie na prawa i wolności innych osób, których dane dotyczą (artykuł 20 ust. 4 RODO)[22].

Taki negatywny wpływ będzie miał miejsce na przykład, jeżeli przesyłanie danych od jednego administratora do innego uniemożliwia stronom trzecim realizację ich praw jako osób, których dane dotyczą, na mocy RODO (np. praw do informacji, dostępu, etc.).

Osoba, której dane dotyczą, inicjująca przesyłanie jej danych innemu administratorowi danych, albo wyraża zgodę na przetwarzanie danych przez nowego administratora danych albo zawiera umowę z tym administratorem. Gdy dane osobowe stron trzecich zawarte są w zbiorze danych, należy określić inną podstawę prawną przetwarzania. Na przykład prawnie uzasadniony interes może być realizowany przez administratora danych na mocy artykułu 6 ust. 1 lit. f), w szczególności gdy celem administratora danych jest świadczenie usługi osobie, której dane dotyczą, co pozwala tej ostatniej przetwarzać dane osobowe w ramach czynności o czysto osobistym lub domowym charakterze. Operacje przetwarzania zainicjowane przez osobę, której dane dotyczą, w kontekście czynności o osobistym charakterze, które dotyczą i mają potencjalny wpływ na strony trzecie, pozostają w zakresie jej odpowiedzialności, w stopniu, w jakim o takim przetwarzaniu, w żaden sposób, nie decyduje administrator danych.

Na przykład usługa poczty e-mail może umożliwiać tworzenie książki osób kontaktowych, znajomych, krewnych, rodziny i szerszego otoczenia osoby, której dane dotyczą. Jako że dane te dotyczą możliwej do zidentyfikowania osobę osoby (i są przez nią tworzone), która chce realizować swoje prawo do przenoszenia danych, administratorzy danych powinni przesłać całą książkę e-maili przychodzących i wychodzących osobie, której dane dotyczą.

Podobnie gdy rachunek bankowy osoby, której dane dotyczą, może zawierać dane osobowe dotyczące transakcji nie tylko posiadacza rachunku, ale również informacje dotyczące transakcji innych osób (np. jeżeli przesłały pieniądze posiadaczowi rachunku). Jest mało prawdopodobne, by miał miejsce negatywny wpływ na prawa i wolności stron trzecich podczas przesyłania informacji dotyczących rachunku bankowego do posiadacza rachunku, gdy składany jest wniosek o przeniesienie – pod warunkiem że w obu przykładach dane są wykorzystywane w tym samym celu (tj. adres kontaktowy używany tylko przez osobę, której dane dotyczą lub historia rachunku bankowego osoby, której dane dotyczą).

Z drugiej strony ich prawa i wolności nie będą przestrzegane, jeżeli nowy administrator danych będzie wykorzystywał dane osobowe do innych celów, np. jeżeli otrzymujący administrator danych wykorzystuje dane osobowe innych osób w ramach książki osób kontaktowych osoby, której dane dotyczą, do celów marketingowych.

W związku z tym, aby zapobiec negatywnemu wpływowi na zaangażowane strony trzecie, przetwarzanie takich danych osobowych przez innego administratora jest dozwolone tylko w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą wnioskującego użytkownika i są przetwarzane tylko na potrzeby o czysto osobistym lub domowym charakterze. Otrzymujący ‘nowy’ administrator danych (któremu dane mogą być przesłane na

[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”.

wniosek użytkownika) nie może wykorzystywać przesłanych danych stron trzecich do własnych celów, np. w celu oferowania produktów i usług marketingowych tym innym osobom, których dane dotyczą, będących stronami trzecimi. Na przykład informacji tych nie powinno się wykorzystywać do wzbogacenia profilu osoby, której dane dotyczą, będącej stroną trzecią i do odbudowy środowiska społecznego, bez jej wiedzy i zgody[23]. Informacje te nie mogą być również wykorzystane do uzyskania informacji na temat takich stron trzecich oraz tworzenia określonych profili, nawet jeżeli ich dane osobowe już są w posiadaniu administratora danych. W przeciwnym razie istnieje prawdopodobieństwo, że takie przetwarzanie będzie niezgodne z prawem i nierzetelne, szczególnie jeżeli strony trzecie, których sprawa dotyczy, nie są o tym poinformowane i nie mogą realizować swoich praw jako osoby, których dane dotyczą.

Ponadto wiodącą praktyką dla wszystkich administratorów danych (zarówno stron „przesyłających", jak i „otrzymujących") wdrożenie narzędzi umożliwiających osobom, których dane dotyczą, wybór istotnych danych, które chcą otrzymać i przesłać, oraz wyłączenie, gdy to właściwe, danych innych osób. Pomoże to następnie w ograniczeniu zagrożeń dla stron trzecich, których dane osobowe mogą być przeniesione.

Ponadto administratorzy danych powinni wdrożyć mechanizmy zgody dla innych zaangażowanych osób, których dane dotyczą, aby ułatwić przesyłanie danych w tych przypadkach, gdy takie strony chcą wyrazić zgodę, np. ponieważ również one chcą przenieść swoje dane do jakiegoś innego administratora danych. Taka sytuacja może powstać, na przykład, w przypadku portali społecznościowych, ale decyzja co do stosowanej wiodącej praktyki należy do administratora danych.

W odniesieniu do danych objętych prawem własności intelektualnej i tajemnicą handlową:

Prawa i wolności innych osób wskazane są w artykule 20 ust. 4. Podczas gdy nie są bezpośrednio związane z przenoszeniem, mogą być rozumiane jako „obejmujące tajemnice handlowe lub własność intelektualną a w szczególności prawo autorskie chroniące oprogramowanie. Jednak mimo że prawa te należy uwzględnić przed udzieleniem odpowiedzi na wniosek o przeniesienie danych, „skutkiem" tych rozważań nie powinna być odmowa zapewnienia osobie, której dane dotyczą, wszystkich informacji". Ponadto prawo do przenoszenia danych nie jest prawem osoby do niewłaściwego wykorzystywania informacji w sposób, który można zaklasyfikować jako nierzetelną praktykę lub który stanowi naruszenie praw własności intelektualnej.

Jednakże potencjalne ryzyko biznesowe nie może, samo w sobie, stanowić podstawy do odmowy udzielenia odpowiedzi na wniosek o przeniesienie i administratorzy danych mogą przesłać dane osobowe przekazane przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicą handlową lub prawami własności intelektualnej.

[23] Portal społecznościowy nie powinien wzbogacać profili swoich członków, wykorzystując dane osobowe przesłane przez osobę, której dane dotyczą, w ramach jej prawa do przenoszenia danych, bez przestrzegania zasady przejrzystości oraz upewnienia się, że bazuje na odpowiedniej podstawie prawnej dotyczącej tego konkretnego przetwarzania.

IV. W jaki sposób ogólne przepisy regulujące realizację praw osób, których dane dotyczą, mają zastosowanie do przenoszenia danych?

- 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 dostępności nowego prawa do przenoszenia danych,. W przypadku gdy przedmiotowe dane osobowe są zbierane bezpośrednio od osoby, której dane dotyczą, musi się to odbywać „w czasie uzyskiwania danych". Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator danych musi podać informacje zgodnie z wymogami art. 13 ust. 2 lit. b) i art. 14 ust. 2 lit. c) .

„Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą", artykuł 14 ust. 3 wymaga, aby podać informacje w rozsądnym terminie po pozyskaniu danych osobowych nieprzekraczającym miesiąca, podczas pierwszej komunikacji z osobą, której dane dotyczą,lub gdy mam miejsce udostępnienie stronom trzecim[24].

Przekazując wymagane informacje, administratorzy danych muszą zapewnić, że odróżniają prawo do przenoszenia danych od innych praw. W związku z tym GR Art. 29 zaleca w szczególności, aby administratorzy danych wyraźnie wyjaśnili różnicę miedzy rodzajami danych, które 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 zapewniali informacje dotyczące prawa do przenoszenia danych zanim osoby, których dane dotyczą, zamkną jakiekolwiek konto, które posiadają. Poza wspieraniem rzetelnego przetwarzania, umożliwia to użytkownikom uporządkowanie swoich danych osobowych i łatwe przesłanie ich na własne urządzenie lub do innego dostawcy przed rozwiązaniem umowy.

I wreszcie, w ramach dobrej praktyki dla „otrzymujących" administratorów danych, GR Art. 29 zaleca, aby zapewniali osobom, których dane dotyczą, kompletne informacje na temat charakteru danych osobowych, które są istotne dla realizacji ich usług. Pozwala to użytkownikom ograniczyć zagrożenia dla stron trzecich, jak również ograniczyć wszelkie inne niepotrzebne dublowanie danych osobowych, nawet gdy nie są zaangażowane inne osoby, których dane dotyczą.

- Jak administrator danych może zidentyfikować osobę, której dane dotyczą, przed udzieleniem odpowiedzi na jej wniosek?

RODO nie zawiera szczegółowych wymogów co do tego, jak weryfikować tożsamość osoby, której dane dotyczą. Niemniej artykuł 12 ust. 2 RODO stanowi, że administrator danych nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać jej prawa (w tym prawo do przenoszenia danych), chyba że przetwarza dane osobowe w celu, który nie wymaga identyfikacji osoby, której dane dotyczą, i może wykazać, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą. Jednak, zgodnie z artykułem 11 ust. 2, w

[24] Artykuł 12 wymaga, aby administratorzy danych przekazywali „wszelkie informacje […] w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka"

takich okolicznościach osoba, której dane dotyczą, może przekazać więcej informacji, aby umożliwić swoją identyfikację. Ponadto artykuł 12 ust. 6 przewiduje, że jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby, której dane dotyczą, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Jeżeli osoba, której dane dotyczą, przekaże dodatkowe informacje umożliwiające jej identyfikację, administrator danych nie może odmówić realizacji wniosku. Gdy informacje i dane zebrane online są powiązane z pseudonimami lub unikalnymi identyfikatorami, administratorzy danych mogą wdrożyć odpowiednie procedury uwierzytelniania w celu zdecydowanego potwierdzenia tożsamości osoby, której dane dotyczą, wnioskującej o swoje dane osobowe lub bardziej ogólnie realizującej prawa przyznane przez RODO.

Procedury te często już istnieją. Osoby, których dane dotyczą, często już są uwierzytelnione przed zawarciem umowy lub uzyskaniem ich zgody na przetwarzanie. W konsekwencji dane osobowe wykorzystywane do rejestracji osoby, której dotyczy przetwarzanie, mogą być również wykorzystane jako dowód uwierzytelnienia osoby, której dane dotyczą, do celów przeniesienia[25].

Podczas gdy w tych przypadkach uprzednia identyfikacja osób, których dane dotyczą, może wymagać żądania przedstawienia dowodu potwierdzającego ich tożsamość prawną, taka weryfikacja może nie być właściwa do oceny powiązania między danymi a osobą, której sprawa dotyczy, ponieważ takie powiązanie nie jest związane z tożsamością oficjalną czy też prawną. W istocie możliwość żądania przez administratora danych dodatkowych informacji w celu oceny tożsamości nie może prowadzić do nadmiernych żądań i do zbierania danych osobowych, które nie są istotne czy niezbędne do wzmocnienia powiązania między osobą a żądanymi danymi osobowymi.

W wielu przypadkach takie procedury uwierzytelniania już istnieją. Na przykład nazwy użytkownika i hasła często są wykorzystywane, aby umożliwić osobom dostęp do ich danych na ich kontach e-mail, kontach na portalach społecznościowych oraz kontach używanych w różnych innych usługach, gdzie osoby zdecydowały się na używanie niektórych z nich bez ujawniania swojego pełnego imienia i nazwiska oraz tożsamości.

Jeżeli rozmiar danych wnioskowanych przez osobę, której dane dotyczą, powoduje, że ich przesłanie za pośrednictwem Internetu może być problematyczne, zamiast możliwości przedłużenia terminu udzielenia odpowiedzi na wniosek o maksymalnie trzy miesiące[26], administrator danych może również rozważyć alternatywne środki przekazania danych, takie jak „streaming" lub zapisanie na płycie CD, DVD lub innym fizycznym nośniku bądź też pozwolić na przesłanie danych osobowych bezpośrednio innemu administratorowi danych (zgodnie z artykułem 20 ust. 2 RODO, gdy jest to technicznie wykonalne).

- Jaki jest termin przewidziany na udzielenie odpowiedzi na wniosek o przeniesienie?

Artykuł 12 ust. 3 wymaga, że administrator danych udziela osobie, której dane dotyczą, „bez zbędnej zwłoki" – a w każdym razie „w terminie miesiąca od otrzymania żądania" „informacji o podjętych działań". Ten miesięczny okres można przedłużyć do maksymalnie trzech miesięcy w przypadku skomplikowanych spraw, pod warunkiem, że poinformuje się

[25] Na przykład gdy przetwarzanie danych jest powiązane z kontem użytkownika, podanie właściwego loginu i hasła mogło by być wystarczające do identyfikacji osoby, której dane dotyczą.
[26] Artykuł 12 ust. 3: „Administrator danych udziela informacji o podjętych działaniach na wniosek".

osobę, której dane dotyczą, o przyczynach takiego opóźnienia w terminie miesiąca od otrzymania pierwotnego żądania.

Administratorzy danych prowadzący usługi społeczeństwa informacyjnego prawdopodobnie mogą być lepiej przygotowani do tego, aby być w stanie udzielić odpowiedzi na wnioski w bardzo krótkim terminie. Aby sprostać oczekiwaniom użytkownika, dobrą praktyką jest określenie terminu, w jakim zazwyczaj może być udzielona odpowiedź na wniosek o przeniesienie danych, i powiadomienie o tym osoby, której dane dotyczą.

Administratorzy danych, którzy odmawiają udzielenia odpowiedzi na wniosek o przeniesienie, 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 określonych terminach, nawet jeżeli dotyczy to odmowy. Innymi słowy, administrator danych nie może zachować milczenia, jeżeli proszony jest o udzielenie odpowiedzi na wniosek o przeniesienie danych.

- W jakich przypadkach można odmówić udzielenia odpowiedzi na wniosek o przeniesienie danych lub w jakich przypadkach może być naliczana opłata?

Artykuł 12 zakazuje administratorowi danych pobierania opłat 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 automatycznym przetwarzaniu danych osobowych, wdrożenie zautomatyzowanych systemów takich jak interfejsy programowania aplikacji (API)[27] może ułatwić wymianę z osobą, której dane dotyczą, i w rezultacie zmniejszyć potencjalne obciążenie wynikające z powtarzających się wniosków. Powinno być niewiele przypadków, w których administrator danych byłby w stanie uzasadnić odmowę dostarczenia wnioskowanych informacji, nawet w odniesieniu do wielu wniosków o przeniesienie danych..

Ponadto całkowity koszt procedur ustanowionych w celu udzielania odpowiedzi na wnioski o przeniesienie danych nie powinien być brany pod uwagę przy określaniu „nadmiernego charakteru" wniosku. W rzeczywistości artykuł 12 RODO koncentruje się na wnioskach składanych przez jedną osobę, której dane dotyczą, a nie na łącznej liczbie wniosków otrzymanych przez administratora danych. W rezultacie całkowitymi kosztami wdrożenia systemu nie można obciążać osób, których dane dotyczą, ani nie mogą one być używane do uzasadnienia odmowy udzielenia odpowiedzi na wnioski o przeniesienie.

V. <u>W jaki sposób muszą być przekazywane dane podlegające przenoszeniu?</u>

- Jakie są oczekiwane środki, jakie administrator danych powinien wdrożyć w celu przesyłania danych?

[27] Interfejs programowania aplikacji (Application Programming Interface – API) oznacza interfejsy aplikacji lub usług internetowych udostępniane przez administratorów danych tak, aby inne systemy lub aplikacje mogły łączyć się lub pracować z ich systemami.

Artykuł 20 ust. 1 RODO przewiduje, że osoby, których dane dotyczą, mają prawo do przesyłania danych do innego administratora bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Takie przeszkody można określić jako przeszkody prawne, techniczne lub finansowe tworzone przez administratora danych, aby powstrzymać lub spowolnić dostęp, przesyłanie lub ponowne wykorzystanie przez osobę, której dane dotyczą, lub przez innego administratora danych. Na przykład taką przeszkodę mogą stanowić: opłaty żądane za przesłanie danych, brak interoperacyjności lub dostępu do formatu danych lub API bądź zapewnianego formatu, nadmierna zwłoka lub złożoność w przypadku pozyskania pełnego zbioru danych, celowe zamaskowanie zbioru danych lub określone lub niewłaściwe bądź nadmierne żądania standaryzacji lub akredytacji[28].

Artykuł 20 ust. 2 nakłada na administratorów danych obowiązek przekazywania danych osobowych podlegających przenoszeniu bezpośrednio do innych administratorów danych „o ile jest to technicznie możliwe".

Techniczna możliwość przesłania danych przez administratora danych innemu administratorowi, pod kontrolą osoby, której dane dotyczą, powinna być oceniana dla poszczególnych przypadków. Motyw 68 dalej wyjaśnia granice tego, co jest „technicznie możliwe", wskazując że „nie powinno to nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania".

Oczekuje się, że administratorzy danych będą przesyłać dane osobowe w interoperacyjnym formacie, mimo że nie nakłada to na innych administratorów danych obowiązku wspierania tych formatów. Zatem bezpośrednie przesłanie danych przez jednego administratora do innego może mieć miejsce, gdy możliwa jest komunikacja między dwoma systemami, w zabezpieczony sposób[29], oraz gdy system otrzymujący ma techniczną możliwość otrzymania przychodzących danych. Jeżeli przeszkody techniczne uniemożliwiają bezpośrednie przekazanie, administrator danych powinien wyjaśnić osobom, których dane dotyczą, kwestię tych przeszkód, ponieważ w przeciwnym razie jego decyzja będzie miała podobny skutek jak odmówienie podjęcia działań na żądanie osoby, której dane dotyczą (artykuł 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 przekazanie całego zbioru danych zawierającego dane podlegające przenoszeniu (lub kilka fragmentów z części globalnego zbioru danych);

- zautomatyzowane narzędzie umożliwiające pobieranie istotnych danych.

Drugi sposób może być preferowany przez administratorów danych w przypadkach złożonych, dużych zbiorów danych, ponieważ umożliwia on pobranie jakiejkolwiek części zbioru danych, która jest istotna dla osoby, której dane dotyczą, w kontekście jej wniosku,

[28] Mogą się pojawiać określone przeszkody prawne takie jak te, które są związane z prawami i wolnościami innych wskazane w artykule 20 ust. 4, lub te, które dotyczą bezpieczeństwa systemów administratorów. Uzasadnienie, dlaczego takie przeszkody byłyby zgodne z prawem oraz dlaczego nie stanowią przeszkody w rozumieniu artykułu 20 ust. 1 jest obowiązkiem administratora danych.

[29] Poprzez uwierzytelnioną komunikację z niezbędnym poziomem szyfrowania danych.

może pomóc zminimalizować ryzyko oraz potencjalnie pozwala na wykorzystanie mechanizmów synchronizacji danych[30] (np. w kontekście systematycznej komunikacji między administratorami danych). Może być to lepszy sposób zapewnienia zgodności dla „nowego" administratora danych oraz może stanowić dobrą praktykę w ograniczeniu zagrożeń prywatności ze strony pierwszego administratora danych.

Te dwa różne i potencjalnie uzupełniające się sposoby przekazywania istotnych danych podlegających przenoszeniu można wdrożyć, udostępniając dane przy użyciu różnych środków, takich jak np. bezpieczna wymiana komunikatów, serwer SFTP, zabezpieczony interfejs komunikacyjny WebAPI lub portal internetowy. Należy umożliwić osobom, których dane dotyczą, korzystanie z bazy danych osobowych, systemu zarządzania danymi osobowymi[31] lub innych rodzajów rozwiązań zaufanych stron trzecich, w celu przechowywania danych osobowych i udzielania administratorom danych pozwoleń na dostęp i przetwarzanie danych osobowych, gdy jest takie żądanie.

- Jaki jest oczekiwany format danych?

RODO nakłada na administratorów danych wymóg przekazywania danych osobowych wnioskowanych przez osobę w formacie umożliwiającym ich ponowne wykorzystanie. W szczególności artykuł 21 ust. 1 RODO stanowi, że dane osobowe muszą być przekazane „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego". Motyw 68 zapewnia dodatkowe wyjaśnienie, że format ten powinien być interoperacyjny, który to termin definiowany[32] jest 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" oraz „nadający się do odczytu maszynowego" stanowią zestaw minimalnych wymogów, które powinny umożliwiać interoperacyjność danych przekazanych przez administratora danych. W ten sposób terminy „ustrukturyzowany, powszechnie używany i nadający się do odczytu maszynowego" stanowią określenie środków, podczas gdy interoperacyjność to oczekiwany wynik.

Motyw 21 dyrektywy 2013/37/UE[33,34] definiuje termin „nadający się do odczytu maszynowego" jako:

---

[30] Mechanizm synchronizacji może pomóc wypełnić ogólne obowiązki wynikające z artykułu 5 RODO, który przewiduje, że „dane muszą być (…) prawidłowe i w razie potrzeby uaktualniane"

[31] Na temat systemów zarządzania danymi osobowymi (PIMS) patrz na przykład Opinia EIOD 9/2016, dostępna pod adresem: https://secure.edps.europa.eu/EDPSWEB/webday/site/mySite/shared/Documents/Consultation/Opinions/206/16-10-20_PIMS_opinion_EN.pdf

[32] Artykuł 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. Urz. L 260, 03.10.2009, str. 20.

[33] Zmieniającej dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego.

[34] Glosariusz UE (http://eur-lex.europa.eu/eli-register/glossary.html) przedstawia dalsze wyjaśnienie co do oczekiwań dotyczących koncepcji wykorzystywanych w tych wytycznych, takich jak *nadający się do odczytu maszynowego, interoperacyjność, otwarty format, standard, metadane.*

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

Zważywszy na szeroki zakres rodzajów potencjalnych danych, które mogłyby być przetwarzane przez administratora danych, RODO nie nakłada konkretnych zaleceń co do formatu danych osobowych, które mają być przekazane. Najodpowiedniejszy format różnić się będzie w poszczególnych sektorach, a odpowiednie formaty mogą już istnieć, ale zawsze należy je wybierać tak, aby osiągnąć cel bycia interpretowalnym i zapewnić osobie, której dane dotyczą, duży stopień przenoszenia danych. Jako takie, formaty podlegające ograniczeniom w zakresie kosztownych licencji nie będą uznawane za odpowiednie podejście.

Motyw 68 wyjaśnia, 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 systemów przetwarzania”.* **Zatem przenoszenie ma na celu tworzenie interoperacyjnych systemów, a nie kompatybilnych systemów.**[35]

Oczekuje się, że dane osobowe będą przekazywane w formatach mających wysoki poziom abstrakcji w odróżnieniu od formatu wewnętrznego lub zamkniętego. Jako takie, przenoszenie danych oznacza dodatkową warstwę przetwarzania danych przez administratorów danych, w celu pozyskiwania danych z platformy i wyodrębniania danych osobowych nie wchodzących w zakres przenoszenia danych, takich jak dane wywnioskowane lub dane dotyczące bezpieczeństwa systemów. W ten sposób zachęca się administratorów danych do wcześniejszego zidentyfikowania danych wchodzących w zakres przenoszenie w ich własnych systemach. To dodatkowe przetwarzanie danych będzie uznawane za element dodatkowy głównego przetwarzania danych, ponieważ nie jest ono dokonywane w celu osiągnięcia nowego celu określonego przez administratora danych.

W sytuacji, gdy formaty nie są w powszechnym użyciu w danej branży lub w określonym kontekście, **administratorzy danych powinni przekazać dane osobowe przy użyciu powszechnie wykorzystywanych formatów (np. XML, JSON, CSV, …) wraz z** przydatnymi **metadanymi na najlepszym poziomie szczegółowości,** przy jednoczesnym zachowaniu wysokiego poziomu abstrakcji. Jako, takie, odpowiednie metadane powinny być wykorzystane w celu prawidłowego opisania znaczenia informacji będących przedmiotem wymiany.Te metadane powinny być wystarczające do umożliwienia funkcjonowania i ponownego wykorzystywania danych, ale oczywiście bez ujawniania tajemnicy handlowej.

[35] ISO/IEC 2382-0 definiuje interoperacyjność następująco: „Możliwość komunikacji, realizacji programów lub przekazywania danych między różnymi jednostkami organizacyjnymi w sposób, który wymaga, aby użytkownik miał niewielką wiedzę lub nie miał wiedzy na temat unikalnych cech charakteryzujących te jednostki”.

Jest zatem mało prawdopodobne, że przekazanie osobie wersji PDF skrzynki odbiorczej e-mail będzie wystarczająco ustrukturyzowane lub deskryptywne, aby umożliwić łatwe ponowne wykorzystanie danych skrzynki odbiorczej. Dane wiadomości e-mail powinny być przekazane w formacie, który zachowuje wszystkie metadane, aby umożliwić skuteczne ponowne wykorzystanie danych. W takiej sytuacji przy wyborze formatu danych, w jakim mają być przekazane dane osobowe, administrator danych powinien uwzględnić, jak format ten może wpłynąć na prawo osoby do ponownego wykorzystywania danych lub jak może to prawo ograniczyć. W przypadkach gdy administrator danych może zapewnić osobie, której dane dotyczą, możliwość wyboru preferowanego formatu danych osobowych, należy zapewnić zrozumiałe wyjaśnienie dotyczące skutku (wpływu), jaki będzie miał określony wybór. Jednak przetwarzanie dodatkowych metadanych tylko dla celu, że mogłyby być potrzebne do udzielenia odpowiedzi na wniosek o przeniesienie danych, nie stwarza podstawy prawnej do takiego przetwarzania.

GR Art. 29 zdecydowanie zachęca do współpracy między interesariuszami z branży i stowarzyszeniami handlowymi w celu wspólnej pracy nad ogólnym zestawem interoperacyjnych standardów i formatów realizacji wymogów prawa do przenoszenia danych. Wyzwaniem tym zajęły się również Europejskie Ramy Interoperacyjności (EIF), które stworzyły uzgodnione podejście do interoperacyjności dla organizacji, które chcą wspólnie zapewniać usługi publiczne. Ramy te – w zakresie ich stosowania – określają zestaw wspólnych elementów, takich jak słownictwo, pojęcia, zasady, polityki, wytyczne, zalecenia, standardy, specyfikacje i praktyki."[36]

- Jak postępować z dużym lub złożonym zbiorem danych osobowych?

RODO nie wyjaśnia, jak sprostać wyzwaniu udzielenia odpowiedzi w przypadku dużego zbioru danych, złożonej struktury danych lub innych kwestii technicznych, które mogą stwarzać trudności administratorom danych lub osobom, których dane dotyczą.

Jednak we wszystkich przypadkach kluczowe jest, aby osoba była w stanie całkowicie zrozumieć definicję, schemat i strukturę danych osobowych, które mogą być przekazywane przez administratora danych. Na przykład dane mogą najpierw być przekazane w skróconej zorganizowanej formie pozwalającej osobie, której dane dotyczą, na przenoszenie raczej części (podzbiorów) danych osobowych, a nie całości. Administrator danych powinien przedstawić przegląd „w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem" (artykuł 12 ust. 1 RODO) najlepiej w taki sposób, aby osoba, której dane dotyczą, zawsze miała jasne informacje na temat tego, jakie dane pobrać lub przesłać innemu administratorowi danych w związku z określonym celem. Na Przykład osoby, których dane dotyczą, powinny być w stanie wykorzystać aplikacje oprogramowania do łatwego zidentyfikowania, rozpoznania lub przetwarzania określonych danych tam zawartych.

Jak wskazano powyżej, praktycznym sposobem odpowiedzi przez administratora danych na wnioski o przeniesienie danych jest zapewnienie odpowiednio zabezpieczonego i udokumentowanego interfejsu programowania aplikacji (Application Programming Interface – API). Może to umożliwić osobom składanie wniosków dotyczących ich danych osobowych do administratora danych za pośrednictwem własnego oprogramowania lub oprogramowania strony trzeciej lub udzielanie pozwoleń innym na składanie wniosków w ich imieniu (w tym innemu administratorowi danych), jak określono w artykule 20 ust. 2 RODO. Przy udzielaniu

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

dostępu do danych za pośrednictwem zewnętrznie dostępnego API można zapewnić bardziej skomplikowany system dostępu, który daje osobom możliwość składania kolejnych wniosków dotyczących danych, albo w formie pełnego pobrania albo w formie funkcji delta zawierającej tylko zmiany od czasu ostatniego pobrania, przy czym te dodatkowe wnioski nie mogą być uciążliwe dla administratora danych.

- Jak można zabezpieczyć dane podlegające przenoszeniu?

Generalnie administratorzy danych powinni zagwarantować „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 zgodnie z artykułem 5 ust. 1 lit. f) RODO.

Jednak przesłanie danych osobowych osobie, której dane dotyczą, może również podnosić szereg kwestii bezpieczeństwa:

Jak administratorzy danych mogą zapewnić, aby dane były bezpiecznie dostarczone odpowiedniej osobie?

W związku z tym, że 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 jest odpowiedzialny za podjęcie wszelkich środków bezpieczeństwa potrzebnych do zapewnienia nie tylko, aby dane osobowe zostały bezpiecznie przesłane (np. z zastosowaniem szyfrowania na całej drodze przesyłu danych lub szyfrowania danych) do właściwego miejsca przeznaczenia (przy użyciu silnych środków uwierzytelniających), ale także kontynuując ochronę danych osobowych, które pozostają w ich systemach, jak również przejrzyste procedury postępowania z możliwymi naruszeniami danych[37] W takiej sytuacji administratorzy danych powinni ocenić określone zagrożenia związane z przenoszeniem danych i podjąć odpowiednie środki ograniczające ryzyko.

Takie środki ograniczające ryzyko mogą obejmować: jeżeli osoba, której dane dotyczą, już musi być uwierzytelniona, wykorzystanie dodatkowych informacji uwierzytelniających, takich jak wspólna tajemnica, lub inny czynnik uwierzytelnienia, taki jak jednorazowe hasło; zawieszenie przesyłania, jeżeli istnieje podejrzenie, że doszło do naruszenia konta; w przypadkach bezpośredniego przesyłania od jednego administratora danych do innego administratora danych, powinny być stosowane uwierzytelnienia z polecenia, np. uwierzytelnienie oparte na tokenie.

Takie środki bezpieczeństwa nie mogą stanowić przeszkody ani nie mogą uniemożliwiać użytkownikom realizacji ich praw, np. poprzez nałożenie dodatkowych kosztów.

Jak pomóc użytkownikom zabezpieczyć przechowywanie ich danych osobowych w ich własnych systemach?

Przy pozyskiwaniu swoich danych osobowych z serwisu online zawsze istnieje ryzyko, że użytkownicy mogą przechowywać je w mniej zabezpieczonych systemach niż ten zapewniany przez serwis. Osoba, której dane dotyczą, wnioskująca o dane jest odpowiedzialna za znalezienie właściwych środków w celu zabezpieczenia danych

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

osobowych we własnym systemie. Jednak powinna być o tym fakcie poinformowana, aby mogła podjąć kroki na rzecz ochrony informacji, które otrzymała. Co jest przykładem wiodącej praktyki, administratorzy danych mogą również zalecić odpowiedni format(y), narzędzia do szyfrowania i inne środki bezpieczeństwa, aby pomóc osobie, której dane dotyczą, w osiągnięciu tego celu.

***

Sporządzono w Brukseli, w dniu 13 grudnia 2016 r.

W imieniu Grupy Roboczej,
Przewodnicząca
Isabelle FALQUE-PIERROTIN

Ostatnio zmieniono i przyjęto w dniu 5 kwietnia 2017 r.

W imieniu Grupy Roboczej,
Przewodnicząca
Isabelle FALQUE-PIERROTIN