

Prawo do przenoszenia danych osobowych – wybrane zagadnienia na tle realizacji nowego uprawnienia przyznanego przez RODO

Spis treści

- I. Uwagi wstępne
- II. Warunki skorzystania z prawa do przeniesienia danych
- III. Zakres danych osobowych podlegających przeniesieniu
- IV. Forma przekazania danych osobowych
- V. Transfer danych osobowych pomiędzy administratorami a prawo konkurencji
- VI. Prawo do przenoszenia danych osobowych a inne prawa jednostki przyznane przez RODO
- VII. Podsumowanie

Streszczenie

Wprowadzenie do europejskiej regulacji ochrony danych osobowych nowego uprawnienia stworzyło osobom fizycznym nieznane dotychczas możliwości, nakładając tym samym na administratorów danych szereg obowiązków. Celem niniejszego artykułu jest omówienie konstrukcji prawa do przenoszenia danych z perspektywy zasad jego realizacji przez administratorów. Opracowanie koncentruje się na wybranych elementach składających się na treść prawa do przeniesienia danych, które w ocenie autorki w praktyce mogą stanowić największe wyzwanie dla administratorów. W publikacji uwzględniono przy tym najnowsze zalecenia w zakresie stosowania przedmiotowego uprawnienia wynikające z Wytycznych dotyczących prawa do przenoszenia danych wydanych przez Grupę Roboczą art. 29 ds. Ochrony Danych Osobowych¹.

Słowa kluczowe: dane osobowe; prawo do przenoszenia danych; podmiot danych, *data portability*; przetwarzanie; ochrona danych osobowych; administrator danych.

JEL: K24, K3

I. Uwagi wstępne

Wraz z rozpoczęciem stosowania Ogólnego rozporządzenia o ochronie danych² osoby fizyczne uzyskały zupełnie nowe uprawnienie nadane przez art. 20 RODO, określane jako prawo do przeniesienia danych osobowych (*right to data portability*). Zasadniczym celem, dla którego

* Radca prawny; e-mail: kazmierczak_joanna@yahoo.com.

¹ Grupa Robocza Art. 29 ds. Ochrony Danych Osobowych. Wytyczne dotyczące prawa do przenoszenia danych. Przyjęte w dniu 13.12.2016 r. Ostatnio zmienione i przyjęte w dniu 05.04.2017 r., dokument WP 242 rew.01, tłumaczenie w wersji polskiej (dalej: Wytyczne dotyczące prawa do przenoszenia danych).

² Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO).

europejski ustawodawca zdecydował się wprowadzić nowe uprawnienie, rozszerzając tym samym katalog praw jednostki związanych z przetwarzaniem danych, była konieczność zapewnienia osobom, których dane dotyczą większej kontroli nad informacjami o nich samych³.

Nie ulega wątpliwości, iż dynamiczny rozwój technologii oraz usług społeczeństwa informacyjnego, jaki dokonał się w ostatnich latach, w szczególności w odniesieniu do usług oferowanych konsumentom w modelu tzw. chmury obliczeniowej (*cloud computing*), doprowadził do zmniejszenia rzeczywistego wpływu, jaki osoby fizyczne miały na swoje dane osobowe (szerzej na ten temat: Litwiński, 2018). Prawo do przenoszenia danych osobowych ma za zadanie poprawić sytuację podmiotu danych i w konsekwencji zniwelować nierówność w relacji osoba fizyczna – administrator danych. Jednocześnie, Grupa Robocza Art. 29 w swoich Wytycznych dotyczących prawa do przenoszenia danych wskazuje, że perspektywa łatwego przesyłania danych osobowych z jednego systemu informatycznego do innego ma w praktyce ułatwić jednostkom dokonywanie zmian dostawców usług i dzięki temu wpłynąć na rozwój nowych technologii w ramach strategii jednolitego rynku cyfrowego. W tym kontekście prawo do przenoszenia danych jest postrzegane jako instrument, który będzie wywierał wpływ na konkurencję między administratorami danych, sprzyjając tym samym innowacji⁴.

Treść prawa do przeniesienia danych obejmuje dwa uprawnienia (Litwiński, 2018)⁵. Po pierwsze, jest to możliwość otrzymania od administratora tych danych osobowych, które dotyczą jednostki i które jednostka sama dostarczyła administratorowi, przy czym administrator będzie miał obowiązek przekazać dane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Po drugie, jest to uprawnienie do przesłania do innego administratora tych danych osobowych, które dotyczą jednostki i które sama dostarczyła administratorowi, z zastrzeżeniem, że przesłanie danych powinno nastąpić bez przeszkód. W praktyce oznacza to, że osoby fizyczne nie tylko zyskują możliwość otrzymania od administratora danych na swój temat, które same dostarczyły, lecz także będą miały możliwość przenoszenia swoich danych osobowych pomiędzy różnymi usługodawcami działającymi w roli administratorów danych.

Zważywszy na fakt, iż przedmiotowe uprawnienie nie występowało dotychczas w prawie ochrony danych osobowych ani na poziomie regulacji europejskich⁶, ani na gruncie polskich przepisów⁷, stanowi ono swoiste *novum* jako instrument prawny. Z tego też względu realizacja nowego prawa może w praktyce stanowić spore wyzwanie dla administratorów. Będą oni zobowiązani realizować to prawo zgodnie z jego treścią, co wiąże się dla nich z konkretnymi obowiązkami, ale co więcej, powinni tego dokonać w ściśle określonych granicach czasowych. Ustawodawca europejski uznał bowiem, iż co do zasady żądanie przeniesienia danych osobowych powinno być zrealizowane bez zbędnej zwłoki, jednak nie dłużej niż w terminie miesiąca od otrzymania żądania⁸.

³ Zob. Motyw (68) preambuły do RODO.

⁴ Wytyczne dotyczące prawa do przenoszenia danych, s. 3–4.

⁵ Na dualizm uprawnień tworzących praw do przeniesienia danych wskazują zarówno Wytyczne dotyczące prawa do przenoszenia danych, jak również przedstawiciele doktryny (szerzej na ten temat: Litwiński, 2018). Należy przy tym zaznaczyć, iż odmiennie w tej kwestii wypowiada się Czerniawski (2017), który wskazuje na trzy uprawnienia składające się na prawo do przenoszenia danych, tj. (1) prawo do otrzymania danych; (2) prawo do przesłania danych bez utrudnień ze strony administratora oraz (3) prawo do przesłania danych bezpośrednio pomiędzy administratorami. Wydaje się jednak, iż w praktyce różnica w ujęciu uprawnień wchodzących w zakres prawa do przenoszenia danych nie będzie miała istotnego znaczenia.

⁶ Zob. dyrektywa Parlamentu Europejskiego i Rady (WE) nr 95/46/WE z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE 1995 L 281/31).

⁷ Zob. ustawa z 29.08.1997 o ochronie danych osobowych (t.j. Dz.U. 2016, poz. 922).

⁸ W wyjątkowych wypadkach dopuszcza się wydłużenie miesięcznego terminu o kolejne dwa miesiące, jednak pod warunkiem, że żądanie ma skomplikowany charakter lub jest to uzasadnione liczbą żądań (art. 12 ust. 3 RODO).

W konsekwencji oznacza to, że aby sprostać nowym obowiązkom wynikającym z prawa do przeniesienia danych, administratorzy powinni dostosować swoje procesy, praktyki, a także rozwiązania techniczne i systemowe do treści nowego uprawnienia. Nasuwa się bowiem wniosek, iż w przypadku administratorów przetwarzających dane w znacznej ilości, jak chociażby portale społecznościowe, operatorzy telekomunikacyjni, platformy aukcji internetowych czy sklepy internetowe, skuteczna realizacja prawa do przeniesienia danych może w rzeczywistości zależeć od efektywnie działających procedur wewnętrznych.

II. Warunki skorzystania z prawa do przeniesienia danych

Dopuszczalność skorzystania z uprawnienia do przeniesienia danych osobowych została dość mocno ograniczona przez ustawodawcę europejskiego, który dokładnie sprecyzował sytuacje, w których osoba fizyczna może skutecznie żądać przekazania jej danych osobowych. W przeciwieństwie zatem do prawa dostępu do danych (art. 15 RODO) czy prawa sprostowania danych (art. 16 RODO), z których skorzystać może każda osoba fizyczna, niezależnie od podstaw przetwarzania jej danych, czy sposobu w jaki te dane są przetwarzane, prawo do przeniesienia danych nie ma charakteru ogólnego (Gawroński, 2018, s. 226).

Realizacja uprawnienia do przeniesienia danych zależy od kumulatywnego spełnienia dwóch przesłanek, tj. oparcia przetwarzania na określonych podstawach (art. 20 ust. 1 lit. a) RODO) oraz dokonywania przetwarzania w określony sposób (art. 20 ust. 1 lit. b) RODO).

Odnosząc się do pierwszej z wyżej wymienionych przesłanek, aby podmiot danych mógł żądać przeniesienia danych koniecznym jest, by ich przetwarzanie było oparte na jednej z dwóch enumeratywnie wskazanych podstaw. Po pierwsze, chodzi o przypadki, gdy dane przetwarzane są na podstawie zgody wyrażonej przez podmiot danych, przy czym chodzi zarówno o zgodę na przetwarzanie tzw. danych zwykłych (art. 6 ust. 1 lit. a) RODO), jak i o zgodę na przetwarzanie danych wrażliwych (art. 9 ust. 1 lit. a) RODO). Po drugie, prawo do przeniesienia danych dotyczy również sytuacji, w których przetwarzanie danych jest dokonywane na podstawie umowy (art. 6 ust. 1 lit. b) RODO). *A contrario*, nie jest możliwym skorzystanie z prawa do przeniesienia danych, jeżeli administrator opiera przetwarzanie danych na przesłance uzasadnionego interesu lub gdy przetwarzanie znajduje podstawę w obowiązujących przepisach prawa. W tym kontekście na uwagę zasługuje kwestia zastosowania prawa do przeniesienia danych w obszarze zatrudnienia w odniesieniu do danych pracowników. Sytuacja ta może nie być jednoznaczna, jeśli wziąć pod uwagę, że dane osobowe pracowników są przetwarzane w celach związanych z zatrudnieniem w oparciu o różne podstawy prawne. Niektóre dane przetwarzane są na podstawie przepisów prawa, inne w oparciu o umowę o pracę, a jeszcze inne na podstawie przesłanki uzasadnionego interesu administratora. Zadaniem pracodawcy będzie zatem wyodrębnienie tych danych pracowników, które przetwarza w związku z realizacją umowy (np. w zakresie płac i wynagrodzeń) i przygotowanie się na realizację uprawnienia do przeniesienia danych w odniesieniu do tak wyodrębnionego zbioru⁹.

Co do drugiej z przesłanek, której wystąpienie jest niezbędne do zastosowania prawa do przenoszenia danych, należy wskazać, że odnosi się ona bezpośrednio do sposobu, w jaki administrator

⁹ Wytyczne dotyczące prawa do przenoszenia danych, s. 10.

przetwarza dane. Zgodnie z art. 20 ust. 1 lit. b) RODO przeniesienie danych jest możliwe, o ile dane są przetwarzane w sposób zautomatyzowany. Chodzi przede wszystkim o wszelkie systemy informatyczne, w których dokonywane jest przetwarzanie danych, jak chociażby aplikacje mobilne, oprogramowania, serwisy webowe itp. Tym samym spod zakresu prawa do przeniesienia danych wyłączono manualne operacje przetwarzania danych, które z reguły dokonywane są w zbiorach papierowych. Jak wskazuje przy tym Gawroński (2018, s. 227), zautomatyzowane przetwarzanie danych wystąpi w sytuacji, gdy dane zapisane w formie papierowej zostaną następnie zeskanowane i zapisane w formie plików.

Jako przykład operacji przetwarzania, do których będzie miało zastosowanie prawo do przenoszenia danych, wskazuje się m.in. playlistę zawierającą utwory muzyczne słuchane w serwisie transmisji strumieniowej muzyki, listę produktów zakupionych przy użyciu karty lojalnościowej czy też listę książek zakupionych w internetowej księgarni¹⁰.

Od wyżej opisanych reguł przewidziane zostały jednak pewne wyjątki. Ustawodawca europejski uznał, że uprawnienie do przeniesienia danych nie powinno mieć zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 20 ust. 3 RODO). Wyłączenie to opiera się na szczególnym charakterze prawa do przeniesienia danych, które jak wskazano na wstępie, odnosi się przede wszystkim do relacji konsument (podmiot danych) – usługodawca (administrator danych)¹¹. Warto przy tym zaznaczyć, iż pomimo wprowadzenia przedmiotowego wyłączenia Grupa Robocza w Wytycznych dotyczących prawa do przenoszenia danych wskazuje, że dobrą praktyką powinno być przygotowanie przez organy administracji publicznej procedur, które pozwolą na udzielenie odpowiedzi na żądanie przeniesienia danych¹². Fajgielski (2017) podkreśla jednak, że powyższego zalecenia Grupy Roboczej nie należy traktować w kategorii obowiązku. Zwraca on przy tym uwagę, że w praktyce w sektorze administracji publicznej realizacja prawa do przeniesienia danych w kształcie przewidzianym w art. 20 RODO będzie raczej wyjątkiem.

Na uwagę zasługuje również pogląd Diker Vanberga i Ünvera (2017), według którego administrator mógłby ograniczyć realizację prawa do przeniesienia danych, wyłączając niektóre dane z przekazywanego zbioru, jeżeli przekazanie tych danych mogłoby niekorzystnie wpłynąć na tajemnicę handlową lub prawa własności intelektualnej przysługujące administratorowi. Zdaniem Diker Vanberga i Ünvera, takie wyłączenie niektórych danych spod art. 20 RODO może być wywiezione z treści motywu 63 RODO. Pozwala on na ograniczenie prawa dostępu do danych, jeżeli mogłoby to negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnicę handlową lub własność intelektualną. Pomimo że motyw 63 odnosi się wprost do prawa dostępu do danych ustanowionego w art. 15 RODO, ww. autorzy dopuszczają jego stosowanie *per analogiam* także do prawa do przenoszenia danych. Ich zdaniem, skoro prawo do przenoszenia danych może być postrzegane jako rozszerzenie prawa dostępu do danych, pozwala to na zastosowanie ograniczeń wspomnianych w motywie 63 RODO także do prawa do przenoszenia danych.

¹⁰ Wytyczne dotyczące prawa do przenoszenia danych, s. 5, 9.

¹¹ Zob. Motyw (68) preambuły do RODO.

¹² Jako przykład dobrej praktyki w ramach procedury udzielania przez organy administracji odpowiedzi na żądanie przeniesienia danych, Grupa Robocza wskazuje rządowy serwis, który zapewni łatwe pobranie złożonych dotychczas deklaracji podatkowych w zakresie podatku dochodowego od osób fizycznych (tak Wytyczne dotyczące prawa do przenoszenia danych, s. 10).

Powyższy pogląd wydaje się być jednak daleko idący, jeżeli wziąć pod uwagę, że przedstawione przez Diker Vanberga i Ünvera ograniczenie prawa do przeniesienia danych nie znajduje odzwierciedlenia w treści przepisów ani motywów RODO. Co więcej, założenie leżące u podstaw stosowania motywu 63 RODO do przenoszenia danych również wydaje się być wątpliwe, jeśli wziąć pod uwagę, że prawo do przenoszenia danych nie jest ani rozszerzeniem, ani nawet szczególnym rodzajem prawa dostępu do danych. Jak zostanie wyjaśnione w dalszej części niniejszego artykułu, prawo do przeniesienia danych pomimo pewnych podobieństw jest odrębnym uprawnieniem od prawa dostępu do danych. Oba prawa realizują bowiem odmienne cele, różniąc się swoim zakresem. Nadto, jeśli wziąć pod uwagę, że istotą prawa do przenoszenia danych jest ułatwienie jednostkom dokonywania zmiany dostawcy usług (administratora), to należy uznać, że ograniczenie w realizacji prawa do przenoszenia danych, jakie proponuje Diker Vanberg i Ünver, może bardzo łatwo wypaczyć istotę uprawnienia z art. 20 RODO. Nietrudno sobie bowiem wyobrazić, że administratorzy w obawie przez utratą klientów będą odmawiać przeniesienia danych do innego administratora, powołując się na ochronę swojej tajemnicy handlowej.

Wobec powyższego, zdaniem autora niniejszego artykułu, pogląd dopuszczający ograniczenie prawa do przenoszenia danych ze względu na ochronę tajemnicy handlowej lub własności intelektualnej administratora danych nie znajduje dostatecznego uzasadnienia.

III. Zakres danych osobowych podlegających przeniesieniu

Jednym z najbardziej dyskusyjnych aspektów związanych z realizacją prawa do przeniesienia danych pozostaje zakres danych, jakie administrator powinien przekazać osobie fizycznej lub wskazanemu przez nią administratorowi. Jak się wydaje, przyczynę tych kontrowersji można upatrywać w uwarunkowaniach historycznych związanych z procesem negocjacji RODO.

Czerniawski (2017) wskazuje, że treść prawa do przenoszenia danych była od samego początku prac nad RODO bardzo kontrowersyjna, w szczególności jeśli wziąć pod uwagę różnice w podejściu po stronie każdego z organów zaangażowanych w negocjacje. Autor zwraca uwagę, że w pierwotnym projekcie RODO autorstwa Komisji Europejskiej prawo do przenoszenia danych obejmowało wyłącznie uprawnienie do przekazania danych jednostce (osobie fizycznej), przy czym odnosiło się ono do wszystkich danych osobowych przetwarzanych w formacie elektronicznym i zorganizowanym, bez względu na to czy dane te zostały dostarczone przez jednostkę, czy wygenerowane przez administratora. W rezultacie na skutek uwag zgłoszonych przez państwa członkowie zakres prawa do przenoszenia danych został ograniczony do tych danych, które osoba fizyczna sama dostarczyła administratorowi. Rozwiązanie to miało na celu ograniczenie wpływu, jaki prawa do przenoszenia danych mogło wywrzeć na konkurencję oraz tajemnicę przedsiębiorstwa. Obawiano się bowiem, że pierwotnie proponowana treść prawa do przenoszenia danych może doprowadzić do nadużyć w celu pozyskania wiedzy o tym, jak dane o jednostce przetwarzają inni administratorzy.

Zgodnie z art. 20 ust. 1 RODO prawo do przenoszenia danych dotyczy wyłącznie ograniczonej kategorii danych osobowych. Przepis wyraźnie zastrzega bowiem, że przekazaniu podlegają dane dotyczące osoby, która wystąpiła z żądaniem i to tylko takie, które ta osoba sama dostarczyła administratorowi. Ten z pozoru wąski katalog danych podlega dość szerokiej wykładni przez

Grupę Roboczą, która w swoich Wytycznych dotyczących prawa do przenoszenia danych zdaje się rozszerzać zakres danych, jakie mogą być objęte przedmiotowym uprawnieniem.

W odniesieniu do pojęcia „dane osobowe jej dotyczące” użytego w treści art. 20 ust. 1 RODO nie ulega wątpliwości, iż chodzi o wszelkie informacje o osobie, która wykonuje prawo do przenoszenia danych. Fajgielski (2017) wskazuje, że chodzi tutaj również o dane pseudonimiczne, pod warunkiem jednak, że mogą one być powiązane z konkretną osobą. Trudności pojawiają się natomiast w sytuacji, gdy poza danymi na swój temat w ramach korzystania z określonej usługi jednostka dostarcza administratorowi również danych o osobach trzecich. Wytyczne dotyczące przenoszenia danych jako przykład wskazują rejestry połączeń telefonicznych czy rejestr wiadomości interpersonalnych, które mogą obejmować także dane osób trzecich w połączeniach przychodzących i wychodzących. W takich przypadkach Grupa Robocza zaleca, aby realizując prawo do przenoszenia danych, umożliwić jednostkom uzyskanie przedmiotowych rejestrów, pomimo że poza danymi jednostki zawierają również dane osobowe innych osób. Zastrzega przy tym, że osoby fizyczne, uzyskując takie rejestry od administratorów, powinny przetwarzać je tak, by nie wpłynęło to na prawa i wolności osób trzecich¹³. Tym samym, może się okazać, iż w konkretnym stanie faktycznym realizacja prawa do przenoszenia danych doprowadzi do przekazania jednostce (lub innemu administratorowi) nie tylko danych o niej samej, lecz także danych o innych osobach.

Można się zastanawiać czy przedstawiony przez Grupę Roboczą kierunek interpretacji art. 20 ust. 1 RODO pozostaje zgodny z treścią tego przepisu, w sytuacji, gdy regulacja ta wprost odnosi się do prawa jednostki do otrzymania „danych osobowych jej dotyczących”. Należy bowiem wziąć pod uwagę, że przekazywanie jednostce nie tylko danych o niej samej, ale również danych dotyczących osób trzecich może naruszyć art. 20 ust. 4 RODO, który wprost wskazuje, że prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych. Klauzula ochrony praw osób trzecich nie ma charakteru nadrzędnego wobec prawa do przenoszenia danych, w tym sensie, że każdorazowo wymaga ona dokonania oceny (*balancing test*) czy w danej sytuacji zachodzi konflikt pomiędzy uprawnieniem jednostki do zrealizowania prawa do przeniesienia danych z jednej strony a prawami osób trzecich – z drugiej strony. Ocena ta powinna być przy tym dokonywana *ad casu* na podstawie konkretnych okoliczności faktycznych (De Hert, Papakonstantinou, Malgieri, Besley i Sanchez, 2018). Powyższe oznacza zatem, że administrator danych, chcąc zrealizować uprawnienie do przeniesienia danych obejmujących również dane osób trzecich, powinien każdorazowo ocenić czy wykonanie tego prawa nie będzie miało niekorzystnego wpływu na osoby trzecie. W konsekwencji to na administratorze danych będzie ciążył obowiązek wykazania, że realizacja uprawnienia jednostki przewidzianego w art. 20 ust. 1 RODO nie nastąpiła z naruszeniem art. 20 ust. 4 RODO.

Drugi z warunków, który zawęża zakres danych podlegających przeniesieniu wskazuje, że chodzi o takie dane, które podmiot danych sam dostarczył administratorowi. Oczywistym jest, iż w kategorii tej będą mieścić się dane, jakie podmiot danych sam przekazał administratorowi, np. wypełniając formularz on-line czy też informacje zawarte w wiadomościach napisanych w portalu społecznościowym (Czerniawski, 2018). Wytyczne dotyczące przenoszenia danych dokonują jednak znacznie szerszej wykładni pojęcia „danych dostarczonych przez osobę, której

¹³ Szerzej na temat zob. Wytyczne dotyczące prawa do przenoszenia danych, s. 13.

dane dotyczą”. Przyjmują one bowiem, że prawo do przenoszenia danych powinno obejmować także dane, które wynikają z obserwacji działań jednostki. Chodzi zatem o dane o osobie, które administrator pozyskał w toku korzystania z określonej usługi lub urzędnictwa, w tym np. historia transakcji, dziennik dostępu, dane o ruchu, dane o lokalizacji¹⁴. Według Czerniawskiego (2017) wspomniane wytyczne wprowadzają rozróżnienie na tzw. dostarczenie aktywne (np. wypełnienie formularza on-line) oraz tzw. dostarczenie pasywne (inaczej dane zaobserwowane, np. dane o historii zakupów). Jego zdaniem, teza jakoby dane zaobserwowane były danymi dostarczonymi przez osobę fizyczną w rozumieniu art. 20 ust. 1 RODO jest daleko idąca, nie znajduje ona bowiem potwierdzenia w treści przepisów. Odmienny pogląd wyraża z kolei De Hert i in. (2018), uznając, że dane dostarczone przez jednostkę powinny obejmować nie tylko dane wprost ujawnione, lecz także dane, jakie administrator zaobserwował bez jakichkolwiek dalszych wysiłków ze swojej strony (np. algorytmów). W ocenie autorów, skoro prawo do przenoszenia danych ma za zadanie zwiększyć kontrolę jednostki nad danymi o niej samej, to tylko szeroka wykładnia pojęcia „dane dostarczone przez jednostkę” pozwoli na osiągnięcie tego celu, skoro dzięki temu jednostka będzie miała możliwość otrzymać szerszy zakres dotyczących jej danych. Zwrócono również uwagę, że „szersza” wykładnia art. 20 ust. 1 RODO obejmująca swoim zakresem także dane „zaobserwowane” znajduje uzasadnienie w potrzebie ochrony jednostek w zdigitalizowanym świecie, gdzie znacząca część danych przetwarzana jest z wykorzystaniem nowych technologii.

Na uwagę zasługuje fakt, iż w Wytycznych Grupy Roboczej z zakresu danych objętych prawem do przenoszenia danych wyłączone zostały tzw. dane wywnioskowane oraz tzw. dane wywiedzione, tj. takie dane osobowe, które administrator sam wytworzył na podstawie innych danych dostarczonych przez jednostkę. Jako przykład „danych wywnioskowanych” wskazuje się w szczególności dane będące wynikiem profilowania prowadzonego przez administratora. Podkreśla się przy tym, że dane wynikające z analizy zachowania jednostki (np. stworzone profile) nie mieszczą się w zakresie prawa do przenoszenia danych. W konsekwencji oznacza to, iż administrator będzie zobowiązany przekazać jednostce (lub wskazanemu przez nią administratorowi) historię zakupów dokonanych przez osobę fizyczną w sklepie on-line, jednak nie ma obowiązku przekazać danych o profilu tej osoby, jaki stworzył w swoim systemie na podstawie historii dokonywanych zakupów. Gawroński (2018) zwraca jednak uwagę, iż co prawda prawo do przenoszenia danych nie będzie obejmowało „danych wywnioskowanych” czy „wywiedzionych” przez administratora, jednak jednostka będzie mogła otrzymać te dane od administratora w ramach realizacji innego uprawnienia, tj. prawa do kopii danych¹⁵.

IV. Forma przekazania danych osobowych

Treść prawa do przenoszenia danych nie tylko determinuje rodzaj danych osobowych, jakie należy przekazać jednostce (lub innemu administratorowi), lecz także określa sposób, w jaki należy przygotować i następnie przekazać dane podlegające przenoszeniu.

¹⁴ Wytyczne dotyczące prawa do przenoszenia danych, s. 11–12. Należy przy tym zwrócić uwagę, iż rozszerzająca wykładnia określenia „dostarczone przez osobę, której dane dotyczą” dokonana w Wytycznych nie została uzasadniona przez Grupę Roboczą, poza ogólnym stwierdzeniem, iż ma to służyć nadaniu pełnej wartości nowemu prawu.

¹⁵ Zgodnie z art. 15 ust. 3 RODO administrator danych jest zobowiązany wydać osobie fizycznej, które dane dotyczą kopie danych osobowych podlegających przetwarzaniu.

Zgodnie z art. 20 ust. 1 RODO administrator, który otrzymał od osoby fizycznej żądanie przeniesienia jej danych ma obowiązek udostępnić dane „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego”. Jednocześnie motyw 68 Preambuły do RODO poza minimalnymi wymogami wymieniony powyżej, wskazuje również na konieczność zapewnienia interoperacyjności danych podlegających przeniesieniu, zachęcając jednocześnie samych administratorów do opracowywania takich formatów.

W Wytycznych dotyczących przenoszenia danych wyjaśniono, iż ze względu na dużą różnorodność danych, jakie mogą być objęte prawem do przenoszenia, RODO nie wskazuje szczegółowych wymogów co do formatu jaki administrator powinien stosować, realizując przedmiotowe uprawnienie jednostki (np. XLS, XML, etc.). Z tego też względu, podobnie jak w przypadku innych wymogów wynikających z RODO, administrator zobowiązany jest sam zdecydować jaki konkretnie format będzie najodpowiedniejszy dla przekazania danych, a jednocześnie spełni minimalne wymogi wynikające z art. 20 ust. 1 RODO. Oznacza to zatem, iż w praktyce to na administratorze danych będzie spoczywał ciężar wykazania, że format jaki zastosował do przeniesienia danych miał ustrukturyzowany charakter, pozwalający na dokonanie maszynowego odczytu.

Na uwagę zasługują stanowisko wyrażane przez Gawrońskiego (2018) określające format PDF jako nieprzydatny w odniesieniu do przenoszalności danych¹⁶. Zdaniem autora stanowisko to jest rozpowszechnione w Komisji Europejskiej, dlatego nie zaleca on stosować tego formatu, jeżeli nie jest to konieczne. Z kolei Grupa Robocza podkreśla, że wybór „odpowiedniego” formatu może zależeć od sektora, w którym działa administrator danych, opierając się na założeniu, że pewne sektory (np. bankowy, ubezpieczeniowy itd.) już teraz posługują się określonymi formatami przetwarzania danych, które stanowią rodzaj praktyki rynkowej. W razie braku ustandaryzowanego formatu, Grupa Robocza zaleca, aby branże podejmowały zgodne działania w celu opracowania wspólnych standardów realizacja prawa do przenoszenia danych¹⁷.

Co istotne, obowiązek wykonania prawa do przeniesienia danych nie wymaga od administratora, aby dostosowywał on swoje systemy przetwarzania do systemów innych administratorów¹⁸. Nie chodzi bowiem o pełną kompatybilność rozumianą jako stosowanie przez administratorów tych samych systemów przetwarzania, gdyż to w konsekwencji mogłoby stanowić znaczące obciążenie dla prowadzenia działalności gospodarczej. Istotą przenoszalności danych jest stosowanie takich formatów danych, które pozwolą na odczytanie danych bez konieczności posiadania specjalistycznej wiedzy. Gawroński (2018) słusznie podkreśla przy tym, że dane otrzymane od administratora powinny być przygotowane w taki sposób, aby możliwe było ich zaimportowanie do innej aplikacji lub oprogramowania za pomocą prostej opcji „otwórz plik”/„importuj dane”. Skoro bowiem prawo do przeniesienia danych ma pozwolić jednostce na dalsze wykorzystanie otrzymanych danych, to jest oczywistym, że administrator nie może zastosować skomplikowanego, złożonego formatu.

¹⁶ Wytyczne dotyczące prawa do przenoszenia danych odnosząc się do formatu PDF określają, iż nie będzie on przydatny przy realizacji przenoszalności danych w sytuacji, gdy osoba fizyczna zażąda wydania jej danych ze skrzynki e-mail. Wskazano bowiem, że w takim przypadku format PDF nie umożliwi jednostce ponownego wykorzystania otrzymanych danych dotyczących skrzynki odbiorczej.

¹⁷ Wytyczne dotyczące prawa do przenoszenia danych, s. 21.

¹⁸ Zob. motyw 68 Preambuły RODO.

V. Transfer danych osobowych pomiędzy administratorami a prawo konkurencji

W styczniu 2016 r. Komisarz ds. konkurencji, Margrethe Vestager, wskazała na możliwość naruszania prawa konkurencji przez dominujące platformy technologiczne, które przetwarzają dane na dużą skalę, jeżeli wykorzystanie danych osobowych ma na celu wypchnięcie konkurentów z rynku¹⁹. Kilka miesięcy później, w maju 2016 r. niemiecki organ ochrony konkurencji wszczął postępowanie przeciwko portalowi Facebook w związku z nadużyciem jego dominującej pozycji na niemieckim rynku internetowych portali społecznościowych. Była to pierwsza sprawa w Unii Europejskiej, w której naruszenie prawa ochrony danych osobowych było oceniane przez organ antymonopolowy z perspektywy nadużycia pozycji dominującej.

Postępowanie prowadzone przez niemiecki organ antymonopolowy w sprawie *Facebook* potwierdza, iż pomiędzy prawem ochrony danych osobowych a prawem konkurencji w określonych sytuacjach mogą zachodzić wzajemne powiązania. Może się bowiem zdarzyć, że naruszenie reguł przetwarzania danych osobowych określonych w RODO przez podmioty posiadające dominującą pozycję rynkową będzie skutkowało naruszeniem praw konkurencji. Do takiej sytuacji dojdzie, jeśli wskutek narzucania uciążliwych warunków podmiotom danych, przedsiębiorca będzie mógł odnosić nieuzasadnione korzyści z przetwarzania ich danych osobowych (sprawa *Facebook* prowadzona przez Bundeskartellamt).

Jak podkreślono na wstępie niniejszego opracowania, najważniejszym celem, jaki stawia się przed prawem do przenoszenia danych, jest zwiększenie konkurencyjności pomiędzy administratorami danych rozumiane jako uprawnienie konsumenta do dokonywania zmian dostawców usług bez przeszkód żadnych przeszkód. W związku z tym, z perspektywy prawa konkurencji, najistotniejszym aspektem nowego prawa do przeniesienia danych pozostaje bez wątpienia uprawnienie pozwalające jednostce na przeniesienie jej danych osobowych od jednego administratora bezpośrednio do drugiego administratora. Uchybienia w realizacji tego uprawnienia przez administratora posiadającego silną pozycję rynkową, mogą bowiem prowadzić do naruszenia prawa konkurencji.

Diker Vanberga i Ünvera (2017) wskazują, że administratorzy danych, którzy odmówią realizacji prawa do przeniesienia danych mogą naruszyć art. 102 TFUE poprzez nadużycie swojej pozycji dominującej. Zdaniem autorów, jeśli przedsiębiorca posiadający dominującą pozycję na rynku odmówi przeniesienia danych do innego (konkurencyjnego) administratora, to takie działanie może stanowić praktykę wykluczającą w świetle art. 102 TFUE, gdyż może ono prowadzić do zwiększenia koncentracji rynku lub do wykluczenia konkurentów z rynku. Co istotne, według Diker Vanberga i Ünvera, jeśli przedsiębiorca o dominującej pozycji przetwarza określone dane osobowe, które są niezbędne do wejścia na określony rynek i przedsiębiorca ten odmówi przeniesienia danych do innego administratora, co spowoduje eliminację konkurencji z rynku, to w braku stosownego uzasadnienia, art. 102 TFUE może mieć zastosowanie. Jako przykład rynku, na którym opisana praktyka może mieć miejsce, wskazano rynek portali społecznościowych, wyszukiwarek internetowych czy reklam internetowych.

Podobne stanowisko zajmują także Graef, Verschakelen i Valcke (2013), którzy zwracają uwagę, że ograniczenia przenoszenia danych pomiędzy serwisami mogą prowadzić do odpowiedzialności

¹⁹ Wypowiedź Margrethe Vestager z dnia 17 stycznia 2016 r. dostępna jest pod adresem https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en.

za naruszenie art. 102 TFUE, w szczególności w zakresie, w jakim odmowa przenoszenia danych stworzy bariery wejścia na rynek dla innych konkurentów. Jednocześnie autorzy podkreślają, że prawo do przenoszenia danych wynikające z RODO różni się od zobowiązania do przeniesienia danych do innego podmiotu, jaki mogą nałożyć na przedsiębiorcę organy ochrony konkurencji wskutek stwierdzenia naruszenia art. 102 TFUE. Przede wszystkim, prawo do przenoszenia danych ustanowione w RODO ma charakter uprawnienia jednostki, a zatem jego realizacja przez administratora danych zależy od złożenia żądania przez jednostkę, podczas gdy organy ochrony konkurencji nakładają na przedsiębiorcę obowiązek przeniesienia danych, który administrator musi wykonać. Ponadto, obie sytuacje przenoszenia danych różnią się również potencjalnym sankcjami, jakie mogą zostać nałożone na przedsiębiorcę za odmowę ich realizacji. Chociaż w obu przypadkach właściwe organy mogą nałożyć karę pieniężną, to jej wysokość jest różna – organ ochrony danych osobowych może wymierzyć karę pieniężną w wysokości do 4% rocznego obrotu światowego, podczas gdy organ ochrony konkurencji może nałożyć karę w wysokości do 10% całkowitego obrotu. Także zakres przenoszonych danych w obu przypadkach pozostaje różny – na podstawie art. 20 RODO przenoszeniu podlegają tylko dane osobowe, z kolei w oparciu o art. 102 TFUE organ ochrony konkurencji może nakazać przeniesienie do innego administratora (konkurenta) dowolnych danych, a więc także takich, które nie są danymi osobowymi.

Jak wynika z powyższego, przenoszenie danych na gruncie RODO różni się od przenoszenia danych na podstawie przepisów prawa konkurencji. Pamiętać jednak należy, iż naruszenie obowiązków administratora w zakresie przenoszenia danych, może prowadzić do naruszenia reguł konkurencji, jeżeli administrator ma pozycję dominującą, a jego działanie prowadzi do antykonkurencyjnych skutków.

VI. Prawo do przenoszenia danych osobowych a inne prawa jednostki przyznane przez RODO

Zgodnie z treścią art. 20 ust. 3 RODO wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do bycia zapomnianym ustanowionego w art. 17 RODO. Jak podkreśla M. Czerniawski (2018), skorzystanie przez jednostkę z prawa do przenoszenia danych nie jest jednoznaczne z usunięciem danych. Autor wskazuje, iż wykonanie prawa do przenoszenia danych nie wpływa na dalsze przetwarzanie danych przez administratora, przy założeniu, że nadal dysponuje on stosowną podstawą prawną. Fakt wydania danych jednostce lub innemu administratorowi nie oznacza zatem, że dane nie mogą być nadal przetwarzane zgodnie z celem, dla którego zostały zebrane.

Pomimo pozornego podobieństwa pomiędzy prawem do przenoszenia danych a prawem dostępu do danych osobowych, oba uprawnienia mają charakter odrębny i niezależny. P. Litwiński (2018) zwraca uwagę, że uprawnienie do przenoszenia danych uzupełnia prawo dostępu ustanowione w art. 15 RODO, a więc może być wykonywane niezależnie od prawa do uzyskania kopii danych (tak też Gawroński, 2018, s. 229). Różnica pomiędzy prawem dostępu do danych a prawem do przeniesienia danych sprowadza się *de facto* do sposobu realizacji obu praw. O ile art. 20 ust. 1 RODO nakłada szczególne wymogi na administratora w kontekście formatu, w jakim należy udostępnić dane, o tyle art. 15 ust. 3 RODO pozostawia administratorowi swobodę w tym zakresie. Oba prawa różnią się także pod względem charakteru, prawo dostępu do danych jest

uprawnieniem ogólnym, przysługującym każdej osobie fizycznej niezależnie od postawy przetwarzania jej danych. Z kolei prawo do przenoszenia danych ogranicza się wyłącznie do enumeratywnie wskazanych sytuacji, gdy dane przetwarzane są w sposób zautomatyzowany na podstawie zgody lub w związku z realizacją umowy. Jak widać zatem, pomimo pozornie tożsamej treści (możliwość otrzymania przez jednostkę danych, które jej dotyczą), oba prawa nie pokrywają się swoim zakresem, realizując przy tym odmienne cele.

VII. Podsumowanie

Analiza treści uprawnienia do przenoszenia danych prowadzi do wniosku, iż pomimo dość ograniczonego charakteru tego prawa, jego realizacja przez administratorów może nastroczać wielu trudności interpretacyjnych.

Przede wszystkim nie jest jasne, jakie dokładnie dane administrator powinien przekazać osobie fizycznej, która korzysta z prawa do przeniesienia danych. Czy powinien on ograniczyć się wyłącznie do tych danych, które osoba fizyczna przekazała mu aktywnie, tj. z zamiarem ich podania, czy może powinien on uwzględnić również dane zaobserwowane, które zbiera w swoich systemach jako wynik działania jednostki? Dodatkowe trudności dla administratorów pojawią się w sytuacji, gdy wśród danych dostarczonych przez jednostkę znajdują się także dane dotyczące osób trzecich (np. listy kontaktów czy historie przelewów). Wówczas administratorzy danych staną przed wyzwaniem oceny czy w konkretnej sytuacji realizacja uprawnienia do przenoszenia danych będzie niekorzystnie wpływała na prawa osób trzecich czy też nie.

Wątpliwości po stronie administratorów może budzić także sposób, w jaki powinni zrealizować nowe uprawnienie. Określenie właściwego formatu danych, który powinien zostać użyty przy przekazywaniu danych tak, by nadawał się on do odczytu maszynowego, był ustrukturyzowany, a jednocześnie powszechnie stosowanych w praktyce, w okolicznościach konkretnego przypadku może powodować niepewność. Administratorzy danych będą zmuszeni polegać na własnej ocenie, jeżeli chodzi o wybór stosowanego formatu, chyba że w drodze kodeksów branżowych ustalą oni format spełniający wymogi art. 20 RODO.

Zestawienie powyższych wątpliwości z wymogiem realizacji nowego prawa w ściśle określonym terminie, tj. bez zbędnej zwłoki, jednak nie dłużej niż w ciągu miesiąca (art. 12 RODO), jak również z wysoką karą finansową, jaka grozi za naruszenie art. 20 RODO, prowadzi do wniosku, że przed administratorami danych postawiono niełatwe zadanie²⁰. Dodatkowo, ci administratorzy, którzy posiadają dominującą pozycję na rynku, na którym działają będą musieli zmierzyć się z ryzykiem naruszenia reguł prawa konkurencji, w sytuacji, gdy nie zrealizują prawa do przenoszenia danych. Organy ochrony konkurencji zwiększają swoją aktywność w obszarze usług oferowanych konsumentów z wykorzystaniem przetwarzania ich danych osobowych, co oznacza, że w przyszłości przedsiębiorcy prowadzący działalność w obszarze usług społeczeństwa informacyjnego powinni ze szczególną starannością realizować prawa jednostek wynikające z RODO. W przeciwnym wypadku nieuzasadniona odmowa przeniesienia danych użytkownika do konkurenta administratora danych może dla takich przedsiębiorców oznaczać surowe sankcje za naruszenie reguł konkurencji.

²⁰ Zgodnie z art. 83 ust. 5 RODO naruszenie uprawnienia do przenoszenia danych podlega karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Wydaje się w konsekwencji, że pomimo słuszných celów, którym służyć ma nowe uprawnienie (wzmocnienie praw jednostki, zwiększenie konkurencyjności pomiędzy administratorami danych), regulacja art. 20 RODO została sformułowana w sposób zbyt ogólny, pozostawiając tym samym bardzo dużą swobodę w interpretacji. Z perspektywy administratorów danych, którzy zmuszeni będą stosować nowe przepisy pomimo ich niejasności i to pod groźbą dotkliwych sankcji finansowych, przyjęty model realizacja prawa do przenoszenia danych może się okazać szczególnie trudny. W praktyce oznacza to, że administratorom danych przyjdzie poczekać na ustalenie faktycznej treści prawa do przenoszenia danych w drodze wykładni zarówno przez doktrynę i piśmiennictwo, jak i późniejsze orzecznictwo sądów krajowych, a także Trybunału Sprawiedliwości Unii Europejskiej.

Bibliografia

- Czerniawski, M. (2017). Obowiązki administratora danych wynikające z prawa do przenoszenia danych. *Monitor Prawniczy*, (20).
- Czerniawski, M. (2018). Komentarz do art. 20. W: E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz* (wyd. 1). Warszawa: Wolters Kluwer.
- De Hert, P., Papakonstantiou, V, Malgeri, G., Beslay, L. i Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law&Security Review*, 34. Pozyskano z: <https://www.sciencedirect.com/science/article/pii/S0267364917303333>.
- Diker Vanberg, A. i Ünver, M.B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?. *European Journal of Law and Technology*, 8(1). Pozyskano z: <http://ejlt.org/article/view/546/726>.
- Fajgielski, P. (2017). Prawo do przenoszenia danych. *Informacja w administracji publicznej*, (4).
- Gawroński, M. (red.). (2018). *RODO. Przewodnik ze wzorami*. Warszawa: Wolters Kluwer.
- Graef, I., Verschakelen, J, i Valcke, P. (2013). Putting the Right to Data Portability into a Competition Law Perspective. *Law: The Journal of the Higher School of Economics, Annual Review*. Pozyskano z: <https://ssrn.com/abstract=2416537>.
- Litwiński, P. (2018). Komentarz do art. 20. W: P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UW w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, Komentarz 2018* (wyd. 1). Warszawa: C.H. Beck.