

Wytyczne dotyczące prawa do przenoszenia danych

Przyjęte w dniu 13 grudnia 2016 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 02/27.

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

Spis treści

Streszczenie.....	3
I. Wprowadzenie.....	3
II. Jakie są główne elementy przenoszenia danych?.....	4
III. Kiedy ma zastosowanie przenoszenie danych?.....	6
IV. W jaki sposób ogólne przepisy regulujące realizację praw osób, których dane dotyczą, mają zastosowanie do przenoszenia danych?.....	10
V. W jaki sposób muszą być przekazywane dane podlegające przenoszeniu?	13

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 zachęceni 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 konsumenta.

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.** Rzeczywiście głównym celem przenoszenia danych jest ułatwienie zamiany jednego dostawcy usług na innego, w ten sposób zwiększając konkurencję wśród dostawców usług (ułatwiając osobom zmianę dostawców usług). Umożliwia ono tworzenie nowych usług w kontekście strategii jednolitego rynku cyfrowego¹.

Prawo to stanowi możliwość przywrócenia równowagi relacjom między osobami, których dane dotyczą, a administratorami danych, poprzez potwierdzenie praw osobowych przysługujących osobom i kontroli nad dotyczącymi ich danymi osobowymi.

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

- Prawo do otrzymania danych osobowych

Po pierwsze przenoszenie danych to **prawo do otrzymania danych osobowych** przetwarzanych przez administratora danych oraz przechowywania ich w celu dalszego osobistego wykorzystania na urządzeniu prywatnym, bez przesyłania ich innemu administratorowi danych.

¹ Patrz agenda jednolitego rynku cyfrowego Komisji Europejskiej <https://ec.europa.eu/digital-single-market/digital-single-market>, w szczególności pierwszy filar polityki „Lepszy dostęp do cyfrowych dóbr i usług”.

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 z serwisu strumieniowej transmisji muzyki, aby dowiedzieć się, ile razy słuchała określonych utworów w celu sprawdzenia, jaki utwór muzyczny chce nabyć na innej platformie. Może również chcieć uzyskać listę kontaktową ze swojej aplikacji poczty e-mail, aby stworzyć listę utworów na wesele, lub uzyskać informacje na temat zakupów dokonanych przy użyciu różnych kart lojalnościowych, aby ocenić, gdzie i w jakim zakresie znajdują się jej dane osobowe².

- 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”. 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. Prawo to ułatwia osobom możliwość łatwego przenoszenia, kopiowania lub przekazywania danych osobowych. 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 sposób, pod kontrolą osoby, której dane dotyczą.

Prawo to ma na celu wspieranie innowacji w wykorzystywaniu danych i promowanie nowych modeli biznesowych związanych z większą wymianą danych pod kontrolą osoby, której dane dotyczą³. Przenoszenie danych może propagować kontrolowaną wymianę danych osobowych między organizacjami i w ten sposób wzbogacić usługi i doświadczenia konsumentów⁴. Przenoszenie danych może ułatwić przesyłanie danych, w którym pośredniczy użytkownik, oraz ponowne wykorzystywanie danych go dotyczących między niezależnymi usługami, którymi jest zainteresowany.

- Narzędzia do przenoszenia danych

Na poziomie technicznym administratorzy danych powinni oferować różne formy wprowadzenia w życie prawa do przenoszenia danych. Na przykład **powinni oferować osobie, której dane dotyczą, możliwość bezpośredniego pobrania, ale również bezpośredniego przesłania danych innemu administratorowi**. Można to wprowadzić,

² 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.

^{*} *Przypis tłumacza: uzależnienie np. od jednego dostawcy czy od jednej usługi.*

³ Patrz: kilka eksperymentalnych aplikacji w Europie, na przykład [MiData](#) w Zjednoczonym Królestwie, [MesInfos / SelfData](#) FING we Francji.

⁴ 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.

udostępniając API⁵. Osoby, których dane dotyczą, mogą również chcieć skorzystać z usług przechowywania danych osobowych lub zaufanej strony trzeciej, posiadać i przechowywać dane osobowe oraz udzielić zezwolenia administratorom danych na dostęp do danych osobowych i ich przetwarzanie zgodnie z wymogami, więc dane mogą być łatwo przekazywane od jednego administratora do innego.

- Sprawowanie kontroli

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.

Przenoszenie danych nie nakłada na administratora danych obowiązku zatrzymywania danych osobowych dłużej niż to konieczne czy też dłużej niż przez określony okres przechowywania⁶. Co istotne, nie ma dodatkowego wymogu rozpoczęcia zatrzymywania takich danych po prostu w celu realizacji potencjalnego wniosku o przeniesienie danych.

Jednocześnie otrzymujący administrator danych⁷ 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 dotyczącego usługi poczty e-mail, gdzie prawo do przenoszenia danych jest wykorzystywane do uzyskiwania wiadomości e-mail i gdy osoba, której dane dotyczą, postanawia przesłać je na zabezpieczoną platformę 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, nowy administrator danych nie musi zatrzymywać wszystkich danych dotyczących transakcji, gdy zostały oznaczone.

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’ administrator danych musi wyraźnie i bezpośrednio określić cel nowego przetwarzania przed jakimkolwiek wnioskiem o przesłanie danych podlegających przenoszeniu⁸.

- Przenoszenie danych kontra inne prawa osób, których dane dotyczą

Gdy osoba realizuje swoje prawo do przenoszenia danych (lub inne prawo w ramach RODO), czyni to bez uszczerbku dla żadnego innego prawa. Osoba, której dane dotyczą,

⁵ Interfejs programowania aplikacji (API) to zestaw ściśle określonych definicji, protokołów i narzędzi służących do tworzenia oprogramowania i aplikacji. Dotyczy interfejsów aplikacji lub usług sieciowych udostępnianych przez administratorów danych, tak aby inne systemy lub aplikacje mogły łączyć się i pracować z ich systemami.

⁶ 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.

⁷ Tj. ten, który otrzymuje dane osobowe po złożeniu przez osobę, której dane dotyczą, wniosku o przeniesienie danych do innego administratora

⁸ 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.

może nadal korzystać z usług administratora danych po operacji przeniesienia danych. Jednocześnie, jeżeli osoba, której dane dotyczą, chce zrealizować swoje prawo do usunięcia danych, przenoszenie danych nie może być zastosowane przez administratora danych jako sposób opóźnienia lub odmowy takiej usunięcia.

Przenoszenie danych nie powoduje automatycznie usunięcia danych z systemów administratora danych i nie wpływa na pierwotny okres przechowywania mający zastosowanie wobec danych, które zostały przesłane, zgodnie z prawem do przenoszenia danych. Osoba, której dane dotyczą, może zrealizować swoje prawa, o ile administrator danych nadal przetwarza dane.

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.

III. Kiedy ma zastosowanie przenoszenie danych?

- 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).

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 umowy⁹.

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

⁹ 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 zapewnienia 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).

- 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.

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 anonimowymi¹⁰ 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 muszą przyjmować zbyt wąskiej interpretacji zdania „dane osobowe dotyczące osoby, której dane dotyczą”. Na przykład rejestry połączeń telefonicznych (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. 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 **administrator danych musi również uwzględnić dane osobowe, które są generowane przez i zbierane z działań użytkowników w odpowiedzi na wniosek o przeniesienie danych**, takie jak dane surowe generowane przez inteligentne liczniki. Ta ostatnia kategoria danych nie obejmuje danych, które są generowane wyłącznie 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”:

¹⁰ 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*)

- **Dane aktywnie i świadomie przekazywane przez osobę, której dane dotyczą, wchodzą** w zakres prawa do przenoszenia danych (na przykład adres pocztowy, nazwa użytkownika, wiek, etc.)

- **Zaobserwowane dane są „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 typu *fitness tracker* lub *health tracker*.

Z kolei dane wywnioskowane i dane wywiedzione tworzone są przez administratora danych na podstawie danych „przekazanych przez osobę, której dane dotyczą”. Te dane osobowe nie wchodzą w zakres prawa do przenoszenia danych. Na przykład ocena zdolności kredytowej lub wynik oceny dotyczącej zdrowia użytkownika jest typowym przykładem danych wywnioskowanych. 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 prawa¹¹.

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 generowane 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 przekazanych przez administratora¹².

Zatem termin „przekazane przez” obejmuje dane osobowe, które dotyczą działania osoby, której dane dotyczą, lub wyniku z obserwacji zachowania osoby, ale nie następującej analizy tego zachowania. Z drugiej strony, wszelkie dane osobowe, które zostały wygenerowane 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.

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

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

¹¹ 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).

¹² 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)¹³.

Taki negatywny wpływ będzie miał miejsce na przykład, jeżeli przesyłanie danych od jednego administratora do innego, w ramach prawa do przenoszenia danych, 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 z nim umowę. Gdy dane osobowe stron trzecich zawarte są w zbiorze danych, należy określić inną podstawę zgodności przetwarzania z prawem. Na przykład prawnie uzasadniony interes na mocy artykułu 6 ust. 1 lit. f) może być realizowany przez administratora, któremu przekazywane są dane, 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.

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 i są tworzone przez możliwą do zidentyfikowania osobę, która chce realizować swoje prawo do przenoszenia danych, administratorzy danych powinni przesłać całą książkę e-maili przychodzących i wychodzących osobie, której dane dotyczą.

Podobna sytuacja ma miejsce, gdy osoba, której dane dotyczą, realizuje swoje prawo do przenoszenia danych na swoim rachunku bankowym, ponieważ może ono zawierać dane osobowe dotyczące zakupów i transakcji posiadacza rachunku, ale również informacje dotyczące transakcji, które zostały „przekazane przez” inne osoby, które przesyłały pieniądze posiadaczowi rachunku. W tym kontekście jest mało prawdopodobne, by miał miejsce negatywny wpływ na prawa i wolności stron trzecich podczas przesyłania poczty e-mail lub przesyłania historii rachunku bankowego, jeżeli ich dane są wykorzystywane w tym samym celu podczas każdego przetwarzania, tj. jako adres kontaktowy używany tylko przez osobę, której dane dotyczą, lub jako historia jednego z rachunków bankowych osoby, której dane dotyczą. Z drugiej strony ich prawa i wolności nie będą przestrzegane, jeżeli nowy administrator danych będzie wykorzystywał książkę osób kontaktowych do celów marketingowych.

W związku z tym, aby zapobiec negatywnemu wpływowi na zaangażowane strony trzecie, przetwarzanie takiej książki 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 wniosek użytkownika) nie może wykorzystywać przesłanych danych stron trzecich do własnych celów, np. w celu

¹³ 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”.

oferowania tym innym osobom, których dane dotyczą, produktów i usług marketingowych. 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.

Aby bardziej pomóc w ograniczeniu zagrożeń dla innych osób, których dane dotyczą, których dane osobowe mogą być przeniesione, wszyscy administratorzy danych (zarówno strony 'wysyłające', jak i 'otrzymujące') powinny wdrożyć narzędzia umożliwiające osobom, których dane dotyczą, wybór stosownych danych i wyłączenie (gdy to właściwe) danych innych osób, których dane dotyczą. Ponadto 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 w przypadku portali społecznościowych.

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

Prawa i wolności innych osób wskazanych w artykule 20 ust. 4 mogą również dotyczyć „praw lub wolności innych osób, w tym tajemnic handlowych lub własności intelektualnej, w szczególności praw autorskich chroniących oprogramowanie” wskazanych w motywie 63, w celu ochrony modelu biznesowego administratorów danych (artykuł 15). Mimo że prawa te powinny być uwzględnione przed udzieleniem odpowiedzi na wniosek o przeniesienie danych, „*względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji*”.

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 administrator danych może przekazać dane osobowe przekazane przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicą handlową lub prawami własności intelektualnej.

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**, zgodnie z wymogami art. 13 ust. 2 lit. b) i art. 14 ust. 2 lit. c) RODO¹⁴.

Przekazując niezbędne jasne i zrozumiałe informacje, administratorzy danych muszą zapewnić, że będą odróżniać prawo do przenoszenia danych od innych praw. W związku z

¹⁴ 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”.

Artykuł 12 wymaga również, aby administratorzy danych „ułatwiali osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22” oraz „nie odmawiali podjęcia działań na żądanie osoby, której dane dotyczą” w przypadku otrzymania takiego żądania („chyba że administrator wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą”).

tym GR Art. 29 zaleca w szczególności, aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, które osoba, których dane dotyczą, może otrzymać na mocy prawa do przenoszenia danych lub prawa dostępu.

Ponadto Grupa Robocza zaleca, aby administratorzy danych zawsze zapewniali informacje dotyczące prawa do przenoszenia danych przed każdym zamknięciem konta. 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 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, przekaze 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.

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 miesiące¹⁵, 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).

¹⁵ Artykuł 12 ust. 3.

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

Artykuł 12 ust. 3 wymaga, że **administrator danych przekaze dane osobowe osobie, której dane dotyczą, „bez zbędnej zwłoki” – a w każdym razie „w terminie miesiąca od otrzymania żądania”** lub w ciągu maksymalnie trzech miesięcy w przypadku skomplikowanych spraw, pod warunkiem, że poinformuje osobę o przyczynach takiego opóźnienia w terminie miesiąca od otrzymania pierwotnego żądania.

Administratorzy danych prowadzący usługi społeczeństwa informacyjnego są pod względem technicznym 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”*. 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. W przypadku usług społeczeństwa informacyjnego lub podobnych usług online, które specjalizują się w automatycznym przetwarzaniu danych osobowych, mało prawdopodobne jest, że udzielenie odpowiedzi na wiele wniosków o przeniesienie danych będzie generalnie uznawane za nakładające zbytne obciążenie.

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. W jaki sposób muszą być przekazywane dane podlegające przenoszeniu?

- 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 definiowany¹⁶ 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/UE¹⁷ definiuje termin „nadający się do odczytu maszynowego” jako:

format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, w tym poszczególne stwierdzenia faktów, i ich wewnętrzną strukturę. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne z powodu niemożności pozyskania danych lub trudności 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 różni się będzie w poszczególnych sektorach, a odpowiednie formaty mogą już istnieć, ale zawsze należy je wybierać tak, aby osiągnąć cel bycia interpretowalnym. 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.**¹⁸

¹⁶ 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.

¹⁷ Zmieniającej dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego.

¹⁸ 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”.

Oczekuje się, że dane osobowe będą przekazywane w formatach mających wysoki poziom abstrakcji. 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 (np. hasła użytkownika, dane dotyczące płatności, wzorce biometryczne, etc.). 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.

Administratorzy danych powinni przekazać wraz z danymi tyle metadanych, ile to możliwe, na najlepszym poziomie szczegółowości, który zachowuje dokładne znaczenie przekazywanych informacji. Na przykład przekazanie osobie wersji PDF skrzynki odbiorczej e-mail nie będzie wystarczająco ustrukturyzowane. Dane e-mail muszą być przekazane w formacie zachowującym wszystkie metadane, aby umożliwić skuteczne ponowne wykorzystywanie danych. 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 jedynie przy założeniu, że mogą 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). EIF to „Ramy interoperacyjności”, czyli 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.”¹⁹

- 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 całego katalogu. 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, mogła wykorzystać aplikacje oprogramowania do łatwego zidentyfikowania, rozpoznania lub przetwarzania określonych danych tam zawartych.

¹⁹ Źródło: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Jednym ze sposobów odpowiedzi przez administratora danych na wnioski o przeniesienie danych jest zapewnienie odpowiednio zabezpieczonego i udokumentowanego interfejsu programowania aplikacji (Application Programming Interface – API). Umożliwiłoby to osobom składanie wniosków dotyczących ich danych osobowych 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 dostępu do danych za pośrednictwem API można zapewnić bardziej skomplikowany system dostępu, który daje osobom możliwość składania kolejnych wniosków o przeniesienie 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 („integralność i poufność”) zgodnie z artykułem 5 ust. 1 lit. f) RODO.

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

Jak 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, aby dane osobowe zostały bezpiecznie przesłane (np. z zastosowaniem szyfrowania) do właściwego miejsca przeznaczenia (np. przy użyciu informacji uwierzytelniających). 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 zabezpieczonym systemie niż ten zapewniany przez serwis. Osoba, której dane dotyczą, powinna być o tym fakcie poinformowana, aby mogła podjąć kroki na rzecz ochrony informacji, które otrzymała. Administrator danych może również, w ramach dobrej praktyki, zalecić odpowiedni format(y) i środki szyfrowania, aby pomóc osobie, której dane dotyczą, w osiągnięciu tego celu.

Sporządzono w Brukseli, w dniu 13 grudnia 2016 r.

*W imieniu Grupy Roboczej,
Przewodniczący*