Transfer danych osobowych do państw trzecich zgodnie z RODO… czyli jak?

W kontekście orzeczenia TSUE tzw. Schrems II, uświadomiłem sobie ważną rzecz. Temat państwa trzeciego na naszym blogu ostatni raz szerzej poruszaliśmy… w marcu 2009 roku (!). Państwo trzecie to nie jest nowa idea. Obostrzenia były przewidziane już w naszej polskiej ustawie o ochronie danych osobowych z 1997 roku. I o tych obostrzeniach pisałem w 2009 roku. RODO wprowadziło jednak dużo istotnych modyfikacji w zasadach transferu danych.

Najwyższy czas na dostosowanie naszego bloga do standardów RODO w tym obszarze.

Czemu ma służyć idea państwa trzeciego?

Idea jest prosta. Państwa, które zgodziły się na obowiązywanie RODO, ponoszą pewne koszty funkcjonowania systemu ochrony danych osobowych. Jednocześnie obywatele tych państw czerpią korzyści związane z funkcjonowania RODO. Państwa UE szczycą się najbardziej zaawansowanymi i najlepiej funkcjonującymi regulacjami prawnymi, chroniącymi naszą prywatność. Jednak przy obecnej technologii i poziomie globalizacji, nie da się skutecznie zamknąć w bezpiecznej bańce obszaru EOG. Z uwagi na funkcjonowanie międzynarodowych grup kapitałowych, technologie chmurowe i wiele innych czynników, dane osobowe wychodzą poza obszar parasolu RODO.

Wprowadzenie obostrzeń przy transferze danych ma służyć zbudowaniu skutecznej ochrony prywatności mieszkańców EOG. Również poza obszarem obowiązywania RODO.

Preferowanie obszaru UE przy przetwarzaniu danych osobowych ma jeszcze jedną dodatkową korzyść dla całej UE. Wymusza budowanie centrów danych i stawianie serwerów w Europie. A to oznacza inwestycje i dodatkowe miejsca pracy. Wielu zagranicznych potentatów, dzięki RODO właśnie, zlokalizowało swoje centra danych w Europie. Najlepszym przykładem będzie tutaj sam Microsoft.

Które państwa, to te trzecie?

Zgodnie z RODO, transfer danych osobowych do państw trzecich może nastąpić wyłącznie pod warunkiem spełnienia określonych warunków, wskazanych w Rozdziale V rozporządzenia, Na początku jednak, musisz ocenić, czy państwo do którego transferujesz dane osobowe, jest tzw. państwem trzecim. Co ciekawe, w RODO w ogóle nie znajdziesz definicji państwa trzeciego. Obiegowo funkcjonuje opinia, że państwo trzecie, to państwo, które nie jest w UE. To nieprawda. Dlatego na początku uporządkujemy definicję. Państwo trzecie to każde państwo, które nie wchodzi w skład Europejskiego Obszaru Gospodarczego. Dlaczego? Dlatego, że RODO zostało przyjęte przez wszystkie państwa należące do EOG. I tu ważna uwaga. UE jest pojęciem węższym niż EOG. Islandia, Liechtenstein i Norwegia nie wchodzą w skład UE, ale za to wchodzą w skład EOG.

Uff, a więc cała Unia Europejska plus trzy wyżej wymienione kraje, nie są państwami trzecimi. Jeśli przekazujesz dane osobowe na ich terytorium, to nie będzie się to prawnie różniło niczym od przekazywania danych osobowych z Warszawy do Radomia.

Jeśli więc audytujesz swoją organizację pod kątem zagranicznych transferów danych – zaczynasz zawsze od prostej weryfikacji, czy transfer będzie miał miejsce do państwa trzeciego.

Czy Wielka Brytania to państwo trzecie?

Na dzień pisania przeze mnie niniejszego tekstu (30 listopad 2020 r.), Wielka Brytania nie jest traktowana jako państwo trzecie. Jednak to się zmieni, wraz z nadejściem 1 stycznia 2021 roku. Od tego dnia, Wielka Brytania będzie traktowana na takich samych zasadach, jak każde inne państwo trzecie. Chyba, że uda się znaleźć inne, lepsze rozwiązanie. Najwygodniejszym i najprostszym rozwiązaniem, będzie podjęcie przez Komisję decyzji o uznaniu Wielkiej Brytanii, za państwo dające odpowiedni stopień ochrony danych. Więcej o tym, w jaki sposób działa taka decyzja i jak legalizuje transfer, znajdziesz w kolejnych akapitach. Jednak tu i teraz takiej decyzji nie ma. Jeśli transferujesz dane osobowe do Wielkiej Brytanii, przygotuj się na najgorsze. Załóż, że od dnia 1 stycznia 2021 roku, transferujesz dane osobowe do państwa trzeciego.

Co to znaczy transfer danych?

Podobnie jak w przypadku państwa trzeciego, RODO nie definiuje tego pojęcia. Przyjmujemy jednak, że jest ono bardzo szerokie. Dotyczy każdej sytuacji, kiedy przekazujesz dane osobowe z EOG na zewnątrz. Mogą to być sytuacje wielokrotne i złożone, jak na przykład korzystanie z serwerów zlokalizowanych na terenie państwa trzeciego, globalny outsourcing wsparcia IT czy korzystanie z różnego rodzaju komunikatorów transferujących nasze dane poza EOG.

Mogą być to również sytuacje bardziej incydentalne. Jak na przykład wsparcie przy rekrutacji. Ktoś z zagranicznego oddziału firmy, np. z USA, wspiera nas przy prowadzeniu rekrutacji na kluczowe stanowisko w naszym polskim oddziale (dostaje wgląd do CV, jest obecny na spotkaniach video, etc.).

Pojawia się tutaj pytanie… a co jeśli pracownicy mojej organizacji prowadzą zwyczajną korespondencję mailową z pracownikami usługodawcy z np. Indii. Korespondencja ma służyć zakupowi gotowej strony internetowej. Czy w takich sytuacjach również mamy do czynienia z przekazaniem danych do państwa trzeciego?

Tak, nawet takie incydentalne i jednorazowe sytuacje, również stanowią transfer danych osobowych. Na szczęście w przypadku zamawiania prostej usługi, znajdziemy również względnie prostą w obsłudze przesłankę, która ten transfer zalegalizuje.

Transferuję dane do państwa trzeciego… i co teraz?

Pojawiają się pierwsze emocje. Transferujesz dane osobowe do państwa trzeciego. Twój kontrahent nie znajduje się na liście państw tworzących EOG. Spokojnie, to jeszcze nie musi oznaczać najgorszego.

Teraz z nadzieją spójrz na drugą listę. Poniżej znajduje się lista państw, które Komisja Europejska uznała za dające odpowiedni stopień ochrony danych (aktualna na dzień 01.12.2020 r.).

Lp.	Nazwa Państwa	Decyzja KE	Uwagi
1.	Andora	Decyzja Komisji z dnia 19 października 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Andorze	-
2.	Argentyna	Decyzja Komisji z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie	-
3.	Guernsey	Decyzja Komisji z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey	-
4.	Izrael	Decyzja Komisji z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych	Dotyczy wyłącznie danych osobowych przekazywanych z Unii Europejskiej w związku z automatycznym międzynarodowym przekazywaniem danych osobowych z Unii Europejskiej, lub, jeśli operacje przekazywania nie są zautomatyzowane, są one przedmiotem dalszego zautomatyzowanego przetwarzania w Państwie Izrael.
5.	Japonia	Decyzja wykonawcza Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych	Uwaga – decyzja nie dotyczy wszystkich transferów danych! Zawiera wyłączenia dotyczące całych sektorów.
6.	Jersey	Decyzja Komisji z dnia 8 maja 2008 r. na mocy dyrektywy 95/46/WE Parlamentu	-

		Europejskiego i Rady, w sprawie właściwej ochrony danych osobowych na Jersey	
7.	Kanada	Decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych	Decyzja stwierdza, że Kanada jest krajem zapewniającym odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty do odbiorców objętych przepisami ustawy kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych.
8.	Nowa Zelandia	Decyzja wykonawcza Komisji z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii	-
9.	Szwajcaria	Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii	-
10.	Urugwaj	Decyzja wykonawcza Komisji z dnia 21 sierpnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych przez Wschodnią Republikę Urugwaju w odniesieniu do zautomatyzowanego przetwarzania danych osobowych	Dotyczy wyłącznie zautomatyzowanego przetwarzania danych osobowych.
11.	Wyspa Man	Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na wyspie Man	-
12.	Wyspy Owcze	Decyzja Komisji z dnia 5 marca 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony na podstawie ustawy Wysp Owczych w sprawie ochrony danych osobowych	-

13.	USA (Safe Harbour)	Decyzja Komisji z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA	Nie działa wskutek orzeczenia TSUE! Trybunał Sprawiedliwości UE stwierdził nieważność tej decyzji w wyroku z dnia 6 października 2015 r. Maximillian Schrems przeciwko Data Protection Commissioner (tzw. Schrems I)
14.	USA (Privacy Shield)	Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA	Nie działa wskutek orzeczenia TSUE! Trybunał Sprawiedliwości UE stwierdził nieważność tej decyzji w wyroku z dnia 16 lipca 2020 r. Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems (tzw. Schrems II).

Jeśli Państwo do którego transferujesz dane osobowe, znajduje się na ww. liście to jeszcze nie wszystko. Teraz musisz poznać szczegóły decyzji Komisji. Nie we wszystkich przypadkach decyzje obejmują wszystkie przypadki transferu danych. Na przykład decyzja wydana względem Urugwaju, dotyczy wyłącznie zautomatyzowanego przetwarzania danych.

Decyzje dotyczące USA, nie dotyczyła całego terytorium USA, a jedynie organizacji działających w ramach Safe Harbour, a potem Privacy Shield. Oczywiście po orzeczeniu TSUE, nawet organizacje z USA, zrzeszone w Safe Harbour czy Privacy Shield, będą traktowane tak samo jak państwa trzecie bez decyzji Komisji.

Dlatego pamiętaj, nawet jeśli destynacja Twojego transferu znajduje się na terytorium państwa względem którego Komisja wydała decyzje, to jeszcze nie wszystko. Zapoznaj się ze szczegółami decyzji i sprawdź czy przypadkiem Twój transfer nie znajduje się na liście wyjątków.

Mój transfer nie znajduje się na liście państw objętych decyzjami Komisji

Wygląda na to, że legalizacja transferu danych, będzie wymagała podjęcia przez Ciebie bardziej złożonych działań.

Poniżej wskazuję kolejne rozwiązania. Ich kolejność nie jest przypadkowa. Zacznę od tych, które powinny być mniej uciążliwe dla Twojej organizacji. Następnie przejdę do tych, które będą bardziej uciążliwe i czasochłonne.

Rozwiązania możemy podzielić na:

1) standardowe, które RODO nazywa „przekazywaniem z zastrzeżeniem odpowiednich zabezpieczeń" - rozwiązania standardowe zostały opisane w art. 46 i 47 RODO,

2) rozwiązania wyjątkowe, które powinny być stosowane jedynie w ostateczności – te przypadki opisuje art. 49 RODO.

Zacznę oczywiście od rozwiązań standardowych, więcej miejsca poświęcając tym, które są częściej stosowane w praktyce.

Do tej pory rozwiązania z art. 46 były względnie proste w praktycznym stosowaniu. Niestety dla organizacji transferujących dane osobowe, sporo komplikacji wprowadziło orzeczenie TSUE z dnia 16 lipca 2020 r. czyli tzw. Schrems II. Praktyczny skutek orzeczenia jest taki, że poza spełnieniem przesłanki standardowej, trzeba jeszcze wykonać dodatkowe działania i czynności. Jakie? O tym przeczytasz już po zapoznaniu się z przesłankami standardowymi.

Rozwiązania standardowe, czyli przekazywanie z odpowiednim poziomem zabezpieczeń

Zaczynamy od rozwiązań standardowych. RODO daje nam tutaj aż osiem różnych możliwości. Część z nich jest prosta w realizacji, inne mogą wymagać podjęcia bardziej złożonych działań. Rozwiązania standardowe możemy dodatkowo podzielić na:

1) wywołujące skutki bez zezwolenia organu nadzorczego (pkt 1 -6),

2) wymagające dla swej skuteczności zezwolenia organu nadzorczego (pkt 7 i 8).

Lp.	Nazwa rozwiązania	Krótka charakterystyka rozwiązania
1.	Standardowe klauzule ochrony danych przyjęte przez Komisję	To zdecydowanie jedno z najlepszych i najprostszych narzędzi transferowych. Standardowe klauzule ochrony są w praktyce formą umowy między Twoją organizacją, a organizacją do której przekazujesz dane. Odbiorca zobowiązuje się w nich do przestrzegania określonych zasad przetwarzania danych osobowych.

		Nie musisz zatrudniać sztabu prawników do opracowania klauzul. Komisja przygotowała dla Ciebie gotowce dostępne we wszystkich unijnych językach. Dotychczas zostały wydane trzy decyzje zawierające zestawy tzw. standardowych klauzul umownych: 1) decyzja Komisji z 15.06.2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, 2) decyzja Komisji z 27.12.2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, 3) decyzja Komisji z 05.02.2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane, mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady. Klauzule wprowadzone przed dwie pierwsze decyzje, mają zastosowanie do przekazywania danych pomiędzy administratorami danych (udostepnienie), natomiast klauzule wprowadzone na podstawie trzeciej decyzji, znajdują zastosowanie przy przekazywaniu danych podmiotowi przetwarzającemu dane osobowe na zlecenie (powierzenie).Jak możesz zauważyć, ostatnia z decyzji została wydana ponad 10 lat temu. Natomiast treść klauzul odwołuje się nie do RODO, ale do dyrektywy 95/46/WR, którą RODO zastąpiło. Nie przeszkadza to jednak w ich stosowaniu, gdyż decyzje wydane przez Komisję na podstawie dyrektywy 95/46/WE w odniesieniu do standardowych klauzul umownych pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby decyzją Komisji. Obecnie Komisja opracowała projekty nowych klauzul, które do 10 grudnia 2020 r. podlegają konsultacjom publicznym. Klauzule wydają się być prostym mechanizmem do zastosowania. Mają jednak jedną wadę – klauzula to forma umowy i nie każdy Twój partner biznesowy będzie chciał je podpisać.
2.	Wiążące reguły korporacyjne	To rozwiązanie swoją ideą może nieco przypominać standardowe klauzule umowne. Wiążące reguły korporacyjne należą do grupy różnych polityk przyjmowanych wewnętrznie przez międzynarodowe koncerny w celu jednolitego przestrzegania przez wszystkie podmioty zależne określonych obowiązków. W praktyce zatem, jest to przesłanka adresowana do międzynarodowych grup kapitałowych. Jest też znacznie bardziej skomplikowana dla użytkownika. Chodzi o przygotowanie polityk ochrony danych osobowych, które będą stosowane przez wszystkie spółki z grupy (a przede wszystkim te działające poza EOG). Takie polityki muszą zostać nie tylko przygotowane i wdrożone, ale także zatwierdzone przez organ nadzorczy (np. nasz UODO) zgodnie z mechanizmem spójności przewidzianym w RODO.

		Nie mamy też dostępnego gotowca, jak w przypadku standardowych klauzul przyjętych przez Komisję.
3.	Standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję	Rozwiązanie dobre i praktyczne. W praktyce nie różniące się dla użytkownika końcowego niczym od rozwiązania nr. 1. Problem w tym, że na dzień 23 listopada 2020 roku, nasz Urząd Ochrony Danych Osobowych, nie przyjął żadnej wersji standardowych klauzul ochrony danych. W praktyce raczej więc z tego rozwiązania nie skorzystasz.
4.	Prawnie wiążący instrument	Pełna nazwa tego instrumentu to: prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi. Jak sama nazwa wskazuje, rozwiązanie dostępne tylko dla podmiotów publicznych. Przesłanka ta obejmuje swym zakresem szeroko rozumiane umowy międzynarodowe oraz inne uzgodnienia administracyjne, jeżeli w świetle prawa międzynarodowego publicznego oraz prawa krajowego ich stron będą one miały wiążący prawnie charakter. Obecnie w polskich przepisach brak jest rozwiązań, które mogłyby być podstawą to stosowania tejże przesłanki.
5.	Zatwierdzony kodeks postępowania	W teorii ten mechanizm mógłby być równie prosty i skuteczny, co standardowe klauzule umowne. Wystarczyłoby, że np. nasz UODO zatwierdzi kodeks postępowania z art. 40 RODO, który zawiera wiążące i egzekwowalne zobowiązania administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń. Później ten kodeks przyjmie nasz partner w państwie trzecim i sprawa załatwiona. W praktyce na dzień 23 listopada 2020 roku, nasz UODO nie zatwierdził żadnego kodeksu postępowania. Niewiele lepiej jest w innych państwach UE. Swój pierwszy kodeks postępowania przyjął niedawno hiszpański organ ochrony danych osobowych. Obecnie w Polsce trwają prace nad 30 kodeksami postępowania. W związku z tym, że przestrzeganie kodeksu musi monitorować niezależny podmiot, sam kodeks nie jest formalnością. W czerwcu UODO przedstawił EROD projekt warunków akredytacji podmiotów monitorujących. Na początku grudnia Europejska Rada Ochrony Danych ma zaopiniować polskie wymogi. Wówczas możemy się spodziewać, że polski organ zatwierdzi pierwsze kodeksy. Jak na razie nie ma więc na czym bazować. Jeśli jednak kodeksy zaczną być zatwierdzane w praktyce, to jest duża szansa na względnie prosty i łatwo dostępny mechanizm, podobny do standardowych klauzul z pkt. 1

6.	Zatwierdzony mechanizm certyfikacji	Wady i zalety tego rozwiązania są bardzo podobne do zatwierdzonych kodeksów postępowania. Rozwiązanie w teorii elastyczne i życiowe. W praktyce wciąż brak zatwierdzonych mechanizmów certyfikacji.
7.	Klauzule umowne pomiędzy podmiotami transferującymi dane	Jedno z tych rozwiązań, po które raczej nie będziemy sięgać zbyt często. Nie dość, że trzeba przygotować własne klauzule umowne, to jeszcze konieczny jest finalny akcept organu nadzorczego.
8.	Uzgodnienia administracyjne między organami lub podmiotami publicznymi	Jak sama nazwa wskazuje rozwiązanie to odnosi się jedynie do podmiotów publicznych. W tym wypadku również wymaga się samodzielnego przygotowania treści uzgodnienia oraz dodatkowo pozyskania zezwolenia organu nadzorczego.

W praktyce biznesowej, zdecydowanie najczęściej stosowanym rozwiązaniem są standardowe klauzule ochrony danych przyjęte przez Komisję Europejską. Nie ma w tym nic dziwnego. Rozwiązanie jest proste i konkretne. Bierzemy przygotowany przez Komisję draft umowy, uzupełniamy we wskazanych miejscach, podpisujemy i transfer jest zalegalizowany. Pamiętaj jedynie o tym, że draft przygotowany przez Komisję, nie podlega negocjacjom. Chyba, że w kierunku zwiększenia poziomu ochrony danych osobowych. Jeśli więc Twój dostawca z państwa trzeciego, wyśle Ci draft klauzul cały pokreślony na czerwono, to pamiętaj o tym, że możesz zatwierdzić tylko te zmiany, które są w interesie osób których dane przetwarzasz. Czyli prawdopodobnie nie zatwierdzisz żadnej zmiany, bo dostawca raczej będzie chciał łagodzić narzucone mu obowiązki. W praktyce stosowanie standardowych klauzul, oznacza stosowanie RODO przez Twojego dostawcę w zakresie transferowanych danych. Do niedawna wszystko wyglądało względnie prosto. Udostępniamy kontrahentowi draft, tłumaczymy, że musi zostać podpisany w takiej formie. Kontrahent wdraża (a przynajmniej w to wierzymy) zasady, o których mowa w standardowych klauzulach i gotowe! Niestety dla wszystkich transferujących dane osobowe za granicę, a na szczęście dla osób troszczących się o swoją prywatność... zapadło orzeczenie TSUE w sprawie Schrems II. I zmieniło bardzo dużo w powyższym, dość prostym mechanizmie.

Rozwiązania standardowe, a orzeczenie Schrems II

Orzeczenie TSUE z lipca br. nieźle namieszało w świecie transferu danych do państwa trzeciego. Przesłanki, którymi kierowali się sędziowie TSUE, są w pełni uzasadnione, jednak dość mocno komplikują życie wielu organizacjom. Na czym więc polega zmiana i na co zwrócił uwagę TSUE w swoim orzeczeniu?

Po pierwsze, TSUE zakwestionował zasady i istotę decyzji Komisji, odnośnie Privacy Shield, legalizującej transfer do tych firm z USA, które znajdowały się w programie Privacy Shield. W bardzo dużym uproszczeniu, chodzi o to, że zdaniem Trybunału, ten program nie daje pełnej gwarancji ochrony danych.

I tutaj sędziowie mają dużo racji. Zarejestrowanie się przez firmę z USA w Privacy Shield jest bardzo proste. Kluczowe jest oświadczenie, w którym taka firma zobowiązuje się de facto wdrożyć u siebie procedury ochrony danych osobowych zbliżone do tych opisanych w RODO. W praktyce jednak, amerykanom brakuje możliwości skutecznej egzekucji stosowania tych zasad. W państwach EOG, na ich straży czuwają lokalne organy nadzorcze. Z bogatą i wieloletnią praktyką, jeszcze z czasów Dyrektywy 94/46/WE. W Stanach Zjednoczonych nie ma żadnego wyspecjalizowane organu, który miałby rzetelnie i skutecznie kontrolować to, czy firmy z Privacy Shield rzeczywiście przestrzegają zasad, których zobowiązały się przestrzegać. W ten sposób, dokonywanie transferów na tej podstawie jest, od daty wydania orzeczenia Schrems II, niedopuszczalne.

Ale to nie wszystko, TSUE w swoim orzeczeniu, dokonał ponadto oceny dopuszczalności transferów danych osobowych do Stanów Zjednoczonych, na podstawie standardowych klauzul umownych przyjętych przez Komisję. Wyrok dotyczył decyzji KE nr 2010/87/UE, regulującej transfer danych, w ramach którego eksporter danych jest administratorem, a importer danych z państwa trzeciego jest podmiotem przetwarzającym (powierzenie). Nie ulega jednak wątpliwości, że zawarte w tym wyroku wskazówki znajdują zastosowanie również w przypadku pozostałych dwóch zestawów klauzul, a więc klauzul administrator–administrator. Bezpośrednie linki do tych decyzji znajdziesz w pierwszej części artykułu.

Sędziowie orzekli, że samo posługiwanie się standardowymi klauzulami ochrony danych zatwierdzonymi przez Komisję Europejską nie we wszystkich przypadkach czyni transfer danych do państwa trzeciego dopuszczalnym. Podmioty zaangażowane w transfer mają obowiązek dokonania uprzedniej analizy ustawodawstwa wewnętrznego importera danych, w szczególności pod kątem zasad dostępu do przekazywanych danych podmiotów publicznych.

Gdy analiza ochrony danych w państwie trzecim da wynik negatywny, wówczas należy zadbać o dodatkowe środki mające na celu zapewnienie przestrzegania odpowiedniego stopnia ochrony danych w państwie trzecim.

Powyższe oznacza, że korzystanie ze standardowych klauzul umownych wymaga nieco więcej zachodu, niż ściągnięcie ich draftu i podpisania ich. Trybunał w ten sposób dokonał wykładni art. 46 ust. 1, konkretnie fragmentu: „gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej".

Chodzi o to, że Trybunał zauważył, że w praktyce podpisywanie standardowych klauzul, w wielu sytuacjach przypomina zasłanianie się listkiem figowym. Wyobraźmy sobie dość częstą w praktyce sytuację. Transferujesz dane osobowe np. do Indii. Twój partner biznesowy podpisał standardowe klauzule bez mrugnięcia okiem. W praktyce nigdy nie miał zamiaru wdrażać postanowień w nich zawartych. Podpisał je tylko dlatego, żeby móc zrealizować projekt, który mu zleciłeś. Wie, że nie ma szans, żebyś kiedykolwiek kontrolował realne wdrożenie przez niego zasad RODO. Czy więc praktyce dane osobowe Twoich pracowników czy klientów faktycznie są chronione na podobnym poziomie, co na obszarze EOG?

Inny przykład? Transferujesz dane osobowe do Chin. Chiny są państwem autorytarnym, które bardzo mocno ingeruje w prywatność swoich obywateli. Jednak z uwagi na podpisane przez Was wspólnie standardowe klauzule, transfer jest w pełni legalny. Czy jednak w praktyce dane osobowe Twoich pracowników czy klientów faktycznie są chronione na podobnym poziomie, co na obszarze EOG?

Oba wyżej postawione pytania, są oczywiście pytaniami retorycznymi. TSUE nie dał nam odpowiedzi i rozwiązań jak sobie poradzić z odpowiedziami na nie.

Na szczęście pewne pytania i odpowiedzi pojawiają się w opublikowanych przez EROD 10 listopada br. projektach rekomendacji:

1) Rekomendacje 01/2020 w sprawie środków, które uzupełniają narzędzia transferu w celu zapewnienia zgodność z unijnym poziomem ochrony danych osobowych,

2) Rekomendacje 2/2020 w zakresie europejskich gwarancji podstawowych dotyczących środków nadzoru (EEG).

Wytyczne EROD czyli co jeszcze muszę zrobić, żeby skorzystać np. ze standardowych klauzul?

Trochę się już gubisz? Krótko teraz podsumuję całość, a w dalszej części tekstu pokażę Ci jak powinien wyglądać Twój proces decyzyjny za pomocą infografiki. Jeśli Twój transfer opiera się na jednej ze standardowych przesłanek, które wcześniej wymieniłem w tabeli, to samo spełnienie przesłanki od orzeczenia Schrems II, już nie wystarczy. Teraz dodatkowo musisz jeszcze sprawdzić czy docelowe miejsce transferu danych jest bezpieczne. Innymi słowy, musisz przyjrzeć się temu, jak wygląda otoczenie prawne Twojego odbiorcy danych osobowych. Z pomocą przyszła nam tutaj EROD, która pokazała kroki, które powinieneś podjąć weryfikując otoczenie prawne Twojego odbiorcy.

EROD mówi o 6 krokach, ale dwa pierwsze właśnie wykonaliśmy wspólnie, szukając podstaw transferu danych osobowych i mapując procesy w ramach których przekazujesz dane do państw trzecich. Zostają więc cztery punkty EROD:

1. Ocena systemu prawnego danego państwa, w tym w szczególności w zakresie przepisów regulujących dostępu do danych osobowych przez organy publiczne (ocena taka powinna zostać udokumentowana). Przy dokonywaniu tej oceny należy odwołać się do wytycznych EROD w sprawie niezbędnych gwarancji europejskich dla środków nadzoru,
2. Określenie i przyjęcie dodatkowych środków technicznych wzmacniających ochronę, które utrudnią dostęp do danych przez władze państwa trzeciego, np. szyfrowanie, pseudonimizacja (ocena tych środków powinna zostać udokumentowana),
3. Określenie dodatkowych proceduralnych środków zabezpieczających, np. w formie dodatkowych klauzul umownych,
4. Monitorowanie zmian w przepisach państw trzecich i ponowna ocena przekazywania danych.

Innymi słowy – musisz być na bieżąco ze stanem prawnym ochrony danych osobowych w państwie trzecim. I tu pojawiają się schody – to już nie jest proste działanie, polegające na ściągnięciu szablonu klauzul umownych i podpisaniu go z Twoim dostawcą. Musisz zagłębić się nieco mocniej w przepisy prawne i ich praktyczne funkcjonowanie w obcym Państwie. Jak to zrobić, na co zwracać uwagę i dlaczego? To wymaga przygotowania odrębnego artykułu.

Jeśli bardzo nie chcesz i nie potrafisz wykonać działań o których mowa wyżej, pozostają Ci jeszcze tylko trzy możliwości. Poniżej pierwsza z nich.

Przesłanki szczególne czyli art. 49 RODO

Pisałem tylko o trzech możliwościach, ale nie dodałem, że pierwsza z nich w praktyce składa się z aż ośmiu różnych rozwiązań. Oto one.

Lp.	Mechanizm:	Krótki komentarz
1.	Wyraźna zgoda osoby, której dane dotyczą (art. 49 ust. 1 lit. a) RODO)	Przed zastosowaniem zgody, musimy poinformować podmiot danych o ewentualnym ryzyku, z którym ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń może się dla niej wiązać przekazanie danych. Dodatkowo, w przypadkach transferu danych pracowników, zgoda będzie ryzykownym rozwiązaniem (trudność w wykazaniu jej dobrowolności).
2.	Niezbędność do wykonania umowy lub do wprowadzenia w życie środków przedumownych (art. 49 ust. 1 lit. b) RODO)	Dotyczy wyłącznie umów zawartych pomiędzy podmiotem danych a administratorem. Jedna z dwóch najbardziej praktycznych i użytecznych biznesowo przesłanek art. 49.
3.	Niezbędność do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą (art. 49 ust. 1 lit. c) RODO)	Jedna z dwóch najbardziej praktycznych i użytecznych biznesowo przesłanek art. 49.
4.	Ważne względy interesu publicznego (art. 49 ust. 1 lit. d) RODO)	Przekazywanie danych osobowych celem przeciwdziałania terroryzmowi, celem zwalczania procederu prania brudnych pieniędzy, przekazywanie danych pomiędzy urzędami celnymi, podatkowymi czy dla celów ubezpieczeń społecznych, etc.
5.	Niezbędność do ustalenia, dochodzenia lub ochrony roszczeń (art. 49 ust. 1 lit. e) RODO)	Należy pamiętać, że przesłanka ta dotyczy wyłącznie roszczeń lub wykazania ich bezzasadności przez administratora przekazującego dane.
6.	Ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób (art. 49 ust. 1 lit. f) RODO)	Przesłanka możliwa do zastosowania w sytuacjach kiedy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

		Przede wszystkich ratowanie życia i zdrowia osoby, której dane dotyczą. Wąski zakres stosowania.
7.	Przekazanie z rejestru publicznego (art. 49 ust. 1 lit. g) RODO)	W przypadku rejestrów publicznych, skoro dane osobowe i tak są dostępne dla nieograniczonej liczby osób, nie istnieje powód dla ograniczania możliwości przekazywania tych danych do państw trzecich.
8.	Ważne prawnie uzasadnione interesy realizowane przez administratora (art. 49 ust. 1 akapit drugi RODO)	Wyjątek wyjątków, Całkowicie szczególna sytuacja, która może mieć miejsce wtedy, kiedy nie jesteśmy w stanie zalegalizować transferu danych ani na art. 45 ani 46 RODO ani na art. 49 ust. 1 akapit pierwszy RODO. Przekazanie nie może być powtarzalne, może dotyczyć tylko ograniczonej liczby osób, musi być niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, który ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia. O takim transferze musimy dodatkowo poinformować organ nadzorczy.

Swoboda wyboru jest pozorna. Przede wszystkim dlatego, że w ogóle zastosowanie art. 49 RODO, powinno mieć miejsce jedynie w wyjątkowych przypadkach.

Na ten temat wypowiadała się już Grupa Robocza art. 29 w Wytycznych 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679. Podobnie na tą sprawę patrzy polska doktryna prawna.

W jednym z wiodących komentarzy do przepisów RODO (red. Sakowska-Baryła 2018, wyd. 1/Fischer) zostało mocno zaakcentowane:

„W świetle przeprowadzonych analiz Grupa Robocza negatywnie oceniła praktykę dużych korporacji oraz jednostek publicznych, które mając ku temu prawne, finansowe i organizacyjne możliwości, nie korzystały z takich instrumentów, jak standardowe kontrakty oparte na rozwiązaniach gwarantujących wysoki poziom bezpieczeństwa, czy przypadku korporacji dodatkowo wiążące reguły korporacyjne."

Innymi słowy, organy nadzorcze mają wyższe oczekiwania względem wielkich. Jeśli jesteś dużą globalną organizacją, to najpierw skorzystaj z możliwości standardowych, czyli np. klauzul umownych czy wiążących reguł korporacyjnych, a dopiero w ostateczności posiłkuj się art. 49 RODO.

Przykłady praktyczne:

Przykład 1:

Jeśli w proces rekrutacji, na niektóre lub wszystkie stanowiska, są włączeni pracownicy spółek grupy z państw trzecich (np. USA), to zdecydowanie preferowanym rozwiązaniem będzie skorzystanie np. ze standardowych klauzul ochrony danych lub wiążących reguł korporacyjnych. Użycie przesłanki z art. 49 np. niezbędność do wykonania umowy przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych, nie da w mojej opinii żadnej gwarancji bezpieczeństwa prawnego.

Jeśli za to prowadzisz małą, rodzinną firmę, nie posiadasz działu prawnego i nie masz budżetu na analizy prawne systemów ochrony danych w państwie trzecim, to sytuacja wygląda nieco inaczej. Jednak która mała rodzinna firma, wysyła CV do zaopiniowania swojej spółce matce w USA?

Przykład 2

W praktyce często zdarzają się sytuacje transferu pewnej ilości podstawowych danych osobowych w toku różnych procesów biznesowych. Może to być na przykład prosta wymiana korespondencji między pracownikiem Twojej spółki i pracownikiem zagranicznego kontrahenta. Czy w takiej sytuacji również muszę podpisywać standardowe klauzule umowne i potem jeszcze analizować system prawny państwa trzeciego?

W mojej opinii nie ma takiej konieczności. To właśnie jedna z tych sytuacji, kiedy art. 49 może znaleźć zastosowanie. Pamiętaj tylko o jednym –, jeśli dane osobowe Twoich pracowników zostaną w ten sposób przekazane do państw trzecich, to powinno zostać to odnotowane w RCP i w klauzuli informacyjnej, którą przedstawiasz pracownikom.

Przedostatnia deska ratunku

Załóżmy jednak, że jesteś dużą globalną korporacją i nie masz możliwości skorzystania z art. 49 RODO. W takim wypadku, musisz wrócić do jednej z przesłanek z art. 46 czyli przesłanek standardowych. W praktyce będą to prawdopodobnie dwa rozwiązania. Standardowe klauzule ochrony danych oraz wiążące reguły korporacyjne.

Po pierwsze, zakomunikuj centrali konieczność wdrożenia jednego z ww. rozwiązań. Nie masz pewności, że centrala podejmie temat, spróbować jednak zdecydowanie warto. W wielu przypadkach nie będziesz mieć wpływu na to, czy takie rozwiązanie zostanie przyjęte na szczeblu globalnym. Jednak komunikując centrali konieczność wyboru jednego z rozwiązań, pieczesz dwie pieczenie na jednym ogniu. Po pierwsze, pokazujesz centrali, że jest problem, który trzeba rozwiązać. Gdyby w przyszłości się okazało, że ten problem będzie skutkował nałożeniem na Ciebie kary przez organ nadzorczy to… cóż… droga centralo – uprzedzaliśmy was przecież.

Zanim centrala podejmie decyzję o podpisaniu klauzul umownych czy wdrożeniu BCRów, zawsze minie trochę czasu. Jeśli nie będzie to wyjątkowo duża ilość czasu, możesz próbować oprzeć się na wyjątkach z art. 49 RODO. Twoje wytłumaczenie dla zastosowania wyjątku, będzie brzmiało wówczas tak: zaadresowaliśmy temat na poziomie centrali i procesujemy właśnie podpisanie standardowych klauzul. Niemniej jednak do momentu ich podpisania, w drodze wyjątku, zdecydowaliśmy się skorzystać z art.

49. Taka sytuacja będzie wyglądała z perspektywy organu nadzorczego zupełnie inaczej niż komunikat, że po prostu korzystamy z art. 49, bo on istnieje. Nie jest to oczywiście rozwiązanie, które całkowicie eliminuje ryzyko poniesienia odpowiedzialności (nawet finansowej) za nieprawidłowości w zakresie transferu danych do państwa trzeciego. Na pewno jednak może stanowić jeden z łagodzących czynników, jakie organ weźmie pod uwagę podczas prowadzonego postępowania. I to właśnie druga korzyść, którą zyskujesz, adresując odpowiednio temat do centrali.

Anonimizacja, czyli już ostatnia deska ratunku

Ostatnią deską ratowania procesu, może być jego anonimizacja, czyli de facto rezygnacja z transferu informacji o charakterze danych osobowych. Nie zawsze będzie ona możliwa do zastosowania w praktyce. Czasem może być ona dość kosztowna, jeśli na przykład trzeba będzie zbudować specjalne systemowe algorytmy, które zanonimizują transferowane dane. Niemniej jednak, jest ona możliwa i wiele organizacji korzysta z tej możliwości.

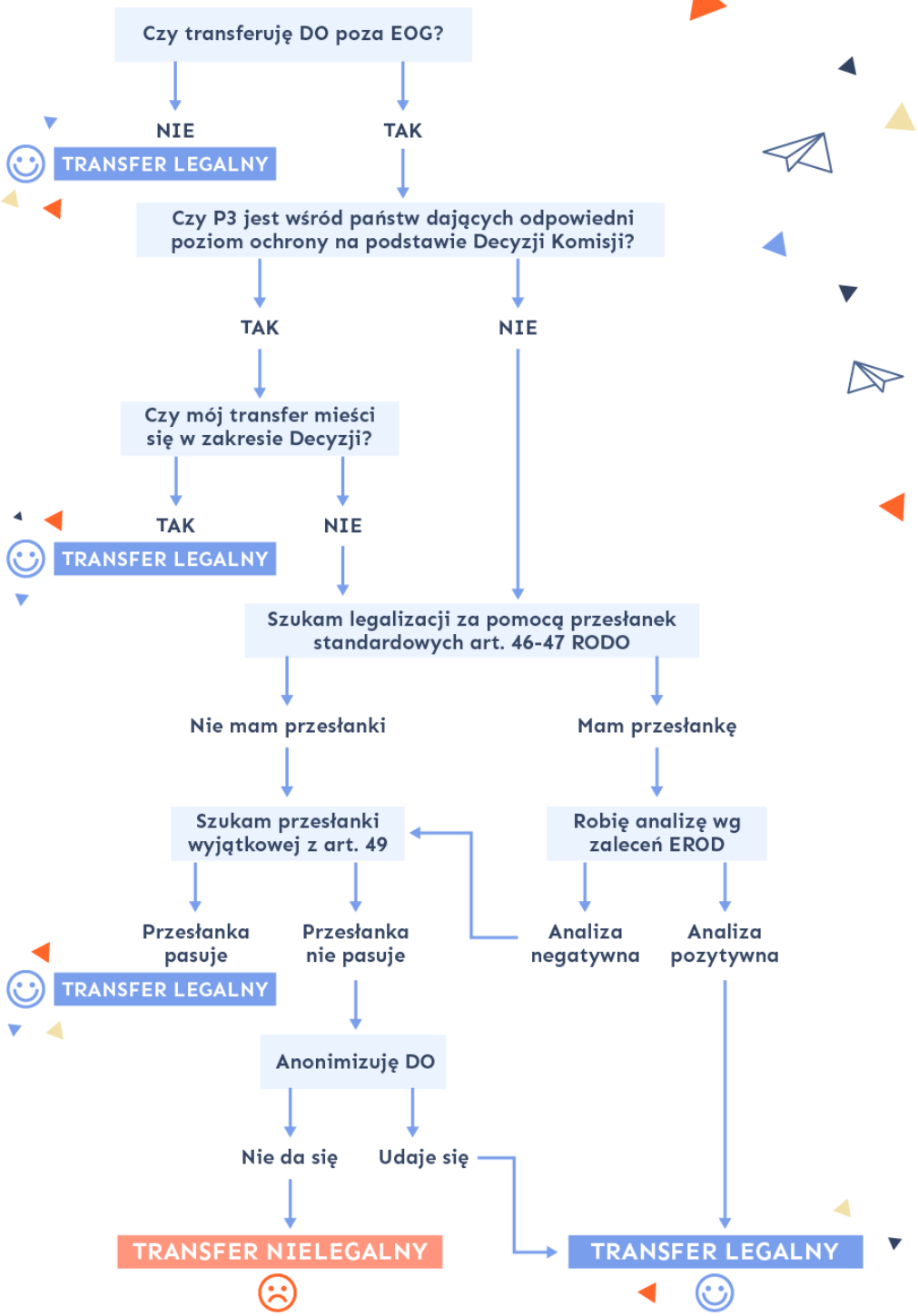
Zaprzestanie transferu, czyli rozwiązanie, które też musisz brać pod uwagę

Ostatnim rozwiązaniem, którego za wszelką cenę próbowaliśmy uniknąć, jest zaprzestanie transferu danych w ogóle. Musimy jednak rozważać i taką opcję. W obecnych czasach, zdecydowaną większość usług możemy znaleźć na terenie EOG. Może więc czas zmienić naszego dostawcę? Jeśli transfer ma miejsce z uwagi na nasze korporacyjne procedury, to może czas zmienić te procedury i zaprzestać transferu do czasu podpisania np. standardowych klauzul. Zawsze jest jakieś rozwiązanie. Wiem, że podejmowanie tego typu decyzji nigdy nie jest łatwe i przyjemne. Niestety trzeba je podejmować. Mam jednak pewną dobrą wiadomość dla Ciebie. Jeśli jesteś IOD czy inną osobą odpowiedzialną za RODO w Twojej organizacji, to ciężar podjęcia tej decyzji nie spoczywa na Tobie. W mojej opinii to już decyzja biznesowa, a za tego typu decyzje pieniądze bierze Zarząd. Twoją rolą jest przedstawienie pełnego spektrum możliwości z ich wszystkimi wadami i zaletami. Następnie zarekomendowanie jednego lub większej ilości rozwiązań. A później niech działa Zarząd. Jeśli jesteś Zarządem, to przy podejmowaniu ostatecznej decyzji, warto skalkulować ryzyko biznesowe, jakie łączy się z jej podjęciem. Jeśli jako duża korporacja, chcesz oprzeć przetwarzanie danych na art. 49 RODO, to zastanów się czy korzyści z przetwarzania będą większe, niż kara organu nadzorczego, na którą się narażasz. Oczywiście każda sytuacja jest tutaj inna. Niemniej jednak, jeśli dokonasz dobrej i rzetelnej analizy stanu faktycznego, to podjęcie decyzji będzie dla Ciebie, jako Zarządu, czystą formalnością.

Drzewo decyzyjne

Mnie w zrozumieniu całego procesu, bardzo pomogło wykonanie notatek, których efekt w postaci poniższej infografiki prezentuję. Mam nadzieję, że poniższe drzewo decyzyjne ułatwi Ci podjęcie dobrej decyzji transferowej :-)

Transfer danych osobowych



Pamiętaj!
Przedstawiona procedura transferowa, nie zawsze zwalnia Cię z dodatkowej konieczności posiadania przesłanek legalności (art. 6 i 9 RODO), a w przypadku powierzenia, wymogów art. 28 RODO.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist

Źródła:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (ogólne rozporządzenie o ochronie danych)