Procedura oceny skutków transferu danych (TIA) w praktyce

TIA (ang. *transfer impact assessment)*, czyli ocena skutków transferu danych, to kolejny dowód na to, że ochrona danych osobowych wciąż ewoluuje. Żeby być na bieżąco, musimy się doszkalać i modyfikować procedury wdrażane przez nasze organizacje.

TIA łączy się bezpośrednio z transferami danych osobowych do państw trzecich. Na ten temat napisaliśmy już bardzo obszerny artykuł na naszym blogu: Przekazywanie danych osobowych do państw trzecich zgodnie z RODO.

Zanim zaczniesz czytać o TIA lub jeśli potrzebujesz informacji z nieco innej perspektywy, sięgnij do wyżej podlinkowanego tekstu. W artykule opisaliśmy dokładnie, czym jest państwo trzecie i w jaki sposób legalnie transferować dane.

Artykuł, który czytasz teraz, podchodzi o tematu w nieco odmienny sposób. Stanowi pomoc praktyczną przy tworzeniu procedury oceny skutków dla transferu danych.

Zacznijmy od podstaw

RODO bazuje na podejściu opartym na ryzyku i zasadzie rozliczalności. Stąd tak wiele różnych *impact assessmentów* (ocen skutków). Pisaliśmy już m.in. o:

1) ocenie ryzyka (*risk assessment*),
2) ocenie skutków dla ochrony danych (*data protection impact assessment*),
3) ocenie ryzyka dla naruszenia ochrony danych.

RODO ma oddawać decyzyjność w wielu obszarach administratorom danych. Dlatego to właśnie ADO samodzielnie ocenia ryzyko dla różnych zdarzeń czy operacji. Taka konstrukcja przepisów daje dużą elastyczność i pozwala funkcjonować przepisom RODO wiele lat bez konieczności nieustannej ich modyfikacji.

Zasada rozliczalności mówi o tym, że wszystkie nasze działania powinny być możliwe do udokumentowania. Jeśli więc oceniliśmy, że np. naruszenie ochrony danych osobowych niczym nie grozi, musimy naszą ocenę jeszcze udokumentować. I tutaj właśnie pomocą są procedury, tabele i matryce. Mają one na celu udokumentowanie naszego toku argumentacji np. przed organem nadzorczym. Pozwalają wykazać, że nasza ocena nie jest jedynie wygodną koncepcją, tylko działaniem opartym na racjonalnych przesłankach.

TIA – skąd to się wzięło?

Transfer impact assessment to kolejna ocena, którą każdy administrator powinien regularnie przeprowadzać. W tym przypadku dotyczy transferów danych do państw trzecich. To bardzo świeży temat, o którym środowisko związane z obszarem RODO zaczęło mówić w 2021 roku. Skąd pochodzi idea TIA?

1) Schrems II

Wszystko rozpoczęło się od orzeczenia TSUE w sprawie Schrems II z 2020 roku. Dla przypomnienia, w tym orzeczeniu Trybunał Sprawiedliwości UE zakwestionował transfer danych osobowych do USA na bazie instrumentu Privacy Shield.

Głównym argumentem było to, że program Privacy Shield nie daje praktycznych gwarancji bezpieczeństwa. Nie ma skutecznego nadzoru nad przestrzeganiem zasad programu. Co więcej, nawet gdyby taki nadzór był, amerykańskie przepisy zezwalają organom bezpieczeństwa na daleko idące ingerencje w prywatność, znacznie większe niż te dopuszczalne w obszarze EOG. W praktyce można powiedzieć, że Privacy Shield było tylko ładnym opakowaniem, które skrywało niebezpieczną zawartość.

Przy okazji TSUE zwrócił uwagę na inny ważny fakt. Standardowe klauzule umowne ochrony danych przyjęte przez Komisję tylko w teorii legalizują transfer danych osobowych do państwa trzeciego. W praktyce często mogą być formą obejścia przepisów RODO i skutkować transferami do miejsc, w których te dane na pewno nie będą bezpieczne. Brak bezpieczeństwa może wynikać z braku odpowiednich przepisów lub z faktu, że przepisy są w praktyce fikcją.

W związku z powyższym w orzeczeniu Trybunał wprost wskazał na obowiązek weryfikacji, czy prawo państwa trzeciego będącego miejscem przeznaczenia zapewnia odpowiednią ochronę przekazywanych danych osobowych na mocy prawa UE.

2) Rekomendacje EROD

Po wyroku Schrems II podmioty transferujące dane zaczęły zastanawiać się, jak ma wyglądać ta weryfikacja, na którą zwrócił uwagę TSUE. Z pomocą przyszła Europejska Rada Ochrony Danych, która wydała przyjęła:

1) Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, które zawierają plan działań, jakie muszą podjąć podmioty przekazujące dane, aby ustalić, czy muszą wdrożyć środki uzupełniające, żeby móc przesyłać dane poza EOG zgodnie z prawem UE (słynne tzw. 6 kroków EROD), oraz pomagają określić skuteczne środki.
2) Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, które zapewniają podmiotom przekazującym dane elementy pozwalające ustalić, czy ramy prawne regulujące dostęp organów publicznych do danych w celach nadzoru w państwach

trzecich można uznać za uzasadnioną ingerencję w prawa do prywatności i ochrony danych osobowych.

3) Nowe standardowe klauzule umowne

4 czerwca 2021 Komisja Europejska przyjęła nowe zestawy standardowych klauzul umownych (ang. *standard contractual clauses*, SCC) dotyczących przekazywania danych osobowych do państw trzecich na podstawie RODO. Klauzula 14 nowych SCC zawiera wymóg, aby w przypadku dokonywanego transferu danych osobowych strony zagwarantowały, że nie mają powodu sądzić, że prawa i praktyki w państwie trzecim uniemożliwiają odbierającemu dane wywiązanie się z obowiązków wynikających z SCC. Udzielając takiej gwarancji, strony oświadczają, że wzięły pod uwagę określone czynniki (np. okoliczności przekazania, długość łańcucha przetwarzania, przepisy prawa i praktyki obowiązujące w państwie trzecim). Importer danych w szczególności gwarantuje, że dołożył wszelkich starań, aby dostarczyć podmiotowi przekazującemu dane odpowiednich informacji w celu zakończenia takiej oceny. Strony wspólnie zgadzają się również na udokumentowanie oceny i udostępnienie jej na żądanie właściwemu organowi nadzorczemu.

SCC zobowiązuje zatem strony transferu do dokonania oceny ryzyka transferu danych oraz jej udokumentowania.

6 kroków

Bazując na wyroku TSUE, zaleceniach EROD, jak również na treści SCC przyjętych przez Komisję, powinniśmy przygotować i wdrożyć w naszej organizacji procedurę TIA. Procedura powinna być rozliczalna i umożliwiać udokumentowanie czynności, które doprowadziły do legalizacji transferu danych do państwa trzeciego. Zgodnie z zaleceniami EROD podzielmy naszą procedurę na sześć kroków.

Krok 1

Krok pierwszy polega na zidentyfikowaniu procesów, w ramach których dochodzi do transferu danych osobowych poza EOG.

Jeśli w Twojej organizacji wdrożenie RODO funkcjonuje prawidłowo, to powinno wystarczyć sięgnięcie do rejestru czynności przetwarzania. Jeśli Twoja organizacja nie prowadzi RCP lub nie jest on aktualny, musisz sprawdzić, czy transfery poza EOG w ogóle mają miejsce.

Co ważne, analiza powinna dotyczyć nie tylko transferów własnych, ale również tych, które zachodzą u Twoich procesorów. Musisz więc ustalić, czy nie dochodzi u nich do transferów danych osobowych.

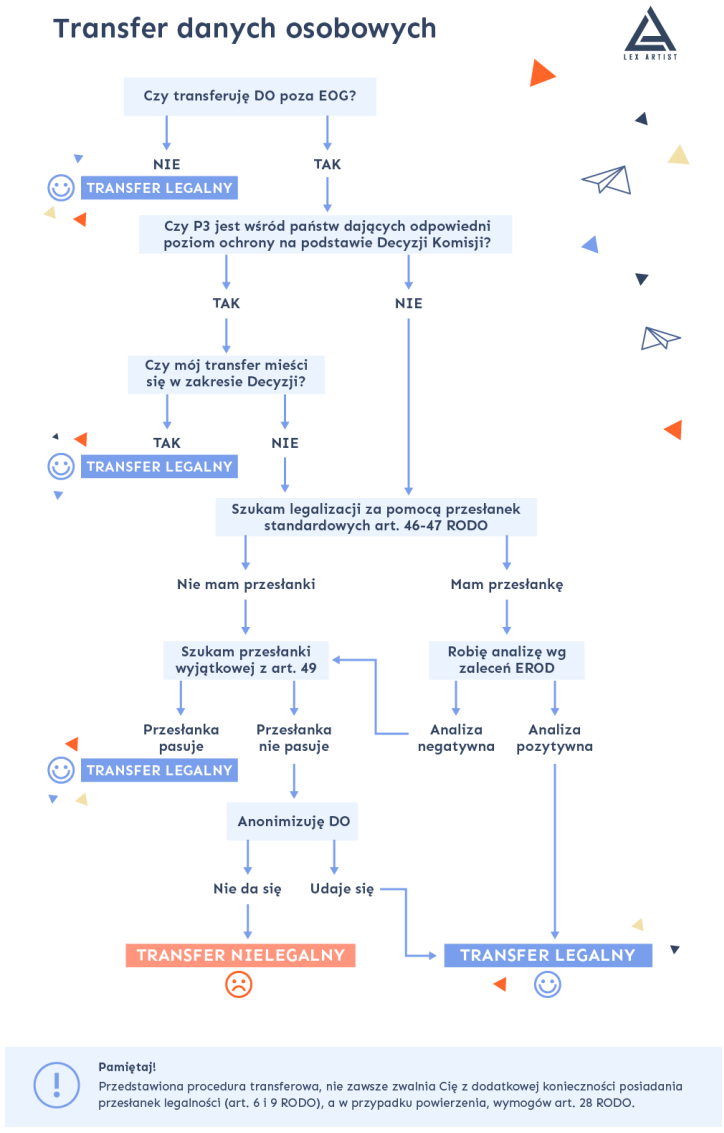
Podczas weryfikacji należy także przyjrzeć się temu, czy zakres danych, które będą transferowane, jest odpowiedni, adekwatny i ograniczony do celu w związku, z którym dochodzi do transferu. Oczywiście wszystkie te czynności powinny zostać udokumentowane. Jedną z form zajęcia się

obszarem transferu danych może być na przykład audyt roczny w Twojej organizacji. Skala pracy do wykonania może być bardzo różna. Jeśli działasz w ramach dużej międzynarodowej grupy kapitałowej, to może czekać Cię analiza znaczącej liczby transferów. Jeśli działasz tylko na rynku polskim albo rynku UE, to procesów będzie mniej.

Krok 2

Kiedy już zlokalizujesz transfery, kolejnym krokiem będzie dobranie do nich odpowiednich narzędzi transferowych. Narzędzia transferowe to różne okoliczności związane np. z konkretnymi przepisami RODO czy decyzjami KE oraz sytuacje, które pozwalają na legalny transfer danych osobowych.

Wszystkie narzędzia transferowe opisaliśmy dokładnie w poprzednim artykule: Przekazywanie danych osobowych do państw trzecich zgodnie z RODO. Z kolei poniższa grafika obrazuje dostępne narzędzia i pomoże w Twoim procesie decyzyjnym.



Dwa pierwsze kroki TIA w praktyce wymagają przede wszystkim analizowania informacji, które posiada Twoja organizacja lub Twoi procesorzy. Szukamy transferów, a później wybieramy odpowiednie narzędzie do ich legalizacji. W niektórych przypadkach okaże się, że Twoja TIA zakończy się już w tym miejscu. Zdarzy się tak, jeśli transferujesz dane osobowe do Szwajcarii czy Argentyny. Jeśli jednak transferujesz dane osobowe na podstawie standardowych klauzul umownych np. do Chin czy do USA, to czeka Cię jeszcze wykonanie trzech kolejnych kroków.

Krok 3

Najtrudniejszym krokiem będzie krok trzeci. Wymaga on od Ciebie analizy poziomu ochrony danych osobowych w państwie trzecim. Poziom ochrony powinien być równoważny ochronie gwarantowanej w Europejskim Obszarze Gospodarczym przez RODO oraz Kartę Praw Podstawowych Unii Europejskiej.

Krok trzeci stanowi największe wyzwanie, ponieważ należy ocenić system prawny kraju odbiorcy. Nawet jeśli odpowiednie przepisy prawne w kraju odbiorcy istnieją i tworzą gwarancję ochrony prywatności, to nie wszystko. W niektórych państwach te gwarancje są czysto teoretyczne.

Przykład 1

Ciekawym przykładem może być ustawodawstwo Stanów Zjednoczonych. Zarówno to federalne, jak i stanowe. W stanie Kalifornia 1 stycznia 2020 roku weszło w życie *California Consumer Privacy Act* (nazywane kalifornijskim RODO).

Teoretycznie ten akt prawny gwarantuje względnie szerokie prawa jednostek, chroniące prywatność. Nie są one jednak tożsame z prawami gwarantowanymi przez RODO.

W ramach ustaw federalnych warto wspomnieć o kontrowersyjnej Ustawie o nadzorze wywiadu zagranicznego (*Foreign Intelligence Surveillance Act*, tzw. FISA) i jej sekcję 702. Ten zestaw przepisów umożliwia prowadzenie inwigilacji przez amerykańskie służby bez uzyskania nakazu sądowego.

Przykład 2

Innym interesującym krajem i częstym miejscem transferu danych są Chiny. Teoretycznie Chiny posiadają swoje własne RODO. Prywatność gwarantuje Chińczykom Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej (*Personal Information Protection Law of the People's Republic of China*), uchwalona 20 sierpnia 2021 roku.

Chińska ustawa jest swoim kształtem bardzo zbliżona do RODO. Twórcy nie kryją się z tym, że inspirowali się europejskimi przepisami. Teoretycznie ustawodawstwo chińskie gwarantuje wysoki poziom praw jednostek.

Problem jednak pojawia się gdzie indziej. W praktyce chińskie prawo jest używane w sposób mocno instrumentalny.

Chiny są krajem autorytarnym, w którym nie ma realnej kontroli władz przez niezależne media czy wymiar sprawiedliwości. Każda duża korporacja musi współpracować z władzą. Chińskie służby wywiadowcze mają jeszcze większe możliwości nielimitowanej kontroli obywateli Chin (i nie tylko). Jest jednak istotna różnica między Chinami a USA. W Chinach, z uwagi na brak wolnej prasy i niezawisłych sądów, jeszcze trudniej rozliczyć władze i korporacje z nią współpracujące z naruszeń prywatności.

Transfery danych osobowych do USA i Chin są dzisiaj jednym z największych praktycznych wyzwań, stojących przed osobami zajmującymi się ochroną danych osobowych. Wspominam o tych dwóch państwach, ponieważ w naszej praktyce to najczęstsze zagraniczne transfery, które mogą generować pewne wątpliwości natury prawnej i nie tylko. Jednak podobne zasady, o których będzie poniżej, dotyczą transferu danych do każdego innego państwa.

Pierwszym problemem, na który natrafisz, będzie znajomość lokalnych aktów prawnych chroniących dane osobowe. Jeśli system prawny danego państwa został już szeroko opisany w internecie, sytuacja będzie względnie prosta. Jeśli jednak transferujesz dane osobowe do bardziej niszowych destynacji, będzie trudniej.

Jeśli masz kłopot ze znalezieniem źródeł prawa, poproś o pomoc organizację, do której transferujesz dane. Zgodnie z zaleceniami EROD transferujący nie powinien pozostać sam, wykonując TIA.

Analizując całokształt otoczenia prawnego (o którym mówi EROD), możesz posłużyć się także różnymi rankingami dotyczącymi transparentności i praworządności. Bardzo polecam prowadzony od wielu lat ranking Transparency International. Ranking pokazuje poziom transparentności w funkcjonowaniu domeny publicznej. Zestawienie dostępne jest za darmo z poziomu wyszukiwarki internetowej: https://www.transparency.org/en.

Jeśli państwo, do którego transferujesz dane, stoi wysoko w tym rankingu, to zdecydowanie ważny argument za transferem danych. Jeśli z kolei Twoje państwo trzecie posiada odpowiednie przepisy, ale w ww. rankingu znajduje się bardzo nisko, to na pewno trzeba przemyśleć zasady transferu.

W przypadku wykrycia „problematycznego ustawodawstwa" w danym państwie masz do wyboru trzy rozwiązania:

1. wstrzymać transfer,
2. wdrożyć środki uzupełniające,
3. kontynuować transfer bez wdrożenia środków uzupełniających (musimy udokumentować powód niewdrożenia środków) na własne ryzyko.

Jeśli w tym momencie Twoja organizacja zdecyduje o wstrzymaniu transferu, Twoja praca przy TIA się kończy. Zwykle jednak wstrzymanie transferu nie jest wcale takie proste. Wiele transferów to element dużych procesów grupowych (np. data center w Indiach czy centrala w Chinach). Jako IOD nie jesteś w stanie zatrzymać tych procesów. W tym przypadku Twoje zadanie sprowadza się do

pokazania Zarządowi rodzajów ryzyka związanych z transferem. Możesz namawiać osoby decyzyjne do wdrożenia środków uzupełniających (o tym będzie w kroku czwartym). Jeśli nie uda Ci się namówić osoby decyzyjnej na dodatkowe zabezpieczenia, to transfer będzie dalej trwał. Sytuacja będzie jednak zdrowa i transparentna dla Twojej organizacji. Osoba decyzyjna (Zarząd, a nie IOD w tym przypadku) weźmie na siebie odpowiedzialność np. Za ewentualne nałożenie kary przez UODO. Ty jako IOD wykonałeś/aś swoje zadanie.

Krok 4

Krok czwarty to pochodna Twoich ustaleń z kroku trzeciego. Jeśli uznasz, że państwo docelowe nie gwarantuje odpowiedniej ochrony, to jeszcze nie oznacza automatycznie zamknięcia transferu danych.

Możesz wdrożyć środki, dzięki którym zrównoważysz braki systemu prawnego państwa, do którego transferujesz dane. Najprostszym środkiem uzupełniającym może być np. ograniczenie zakresu przekazywanych danych.

Według EROD środki uzupełniające mają charakter umowny, techniczny lub organizacyjny.

Środki można ze sobą łączyć. Jak wskazuje EROD, same środki umowne i organizacyjne zasadniczo nie pogorszą dostępu organów publicznych państwa trzeciego do danych osobowych na podstawie problematycznych przepisów lub praktyk. Pojawią się sytuacje, gdy jedynie odpowiednio wdrożone środki techniczne będą mogły ograniczyć lub uniemożliwić dostęp organów publicznych państwa trzeciego do danych osobowych, w szczególności do celów nadzoru. W takich przypadkach środki umowne lub organizacyjne mogą uzupełniać środki techniczne i wzmacniać ogólny stopień ochrony danych.

EROD w załączniku nr 2 do zaleceń wskazuje przykłady środków uzupełniających w odniesieniu do konkretnych scenariuszy. I tak przykładowymi środkami uzupełniającymi mogą być:

- pseudonimizacja,
- szyfrowanie transmisji,
- przetwarzanie dzielone,
- przyjęcie dodatkowych rodzajów polityki wewnętrznej w zakresie zarządzania przekazywaniem.

W zaleceniach wskazane zostały przykładowe kryteria, jakie można brać pod uwagę, decydując o zastosowaniu środków uzupełniających:

1) format (zwykły tekst, dane pseudonimizowane lub szyfrowane) i kategoria danych,
2) długość oraz złożoność procesu przetwarzania danych, a także liczba podmiotów zaangażowanych w przetwarzanie i ich relacje,
3) charakter danych (np. dane z art. 9 lub 10 RODO),

4) technika lub parametry praktycznego zastosowania prawa państwa trzeciego wynikająca z kroku trzeciego,

5) prawdopodobieństwo dalszych transferów w tym samym państwie lub do innego państwa trzeciego.

W przypadku gdy nie uda się znaleźć środka uzupełniającego gwarantującego w zasadzie równy poziom ochrony danych osobowych, należy zaprzestać transferu do danego państwa lub państw.

Krok 5

Krok piąty będzie miał miejsce w dość ograniczonej liczbie sytuacji. Polega na podjęciu kroków proceduralnych, które być może będzie trzeba podjąć w związku z zastosowaniem określonych środków uzupełniających.

W przypadku stosowania standardowych klauzul umownych, w związku z wprowadzeniem środków uzupełniających w dodatku do standardowych klauzul umownych, nie ma potrzeby uzyskiwania akceptacji organu nadzorczego.

Warunek jest taki, że te środki nie mogą być sprzeczne z samymi klauzulami i nie osłabią poziomu ochrony. Jeśli natomiast są sprzeczne lub podmiot zamierza wprowadzić zmiany w samych klauzulach, należy wystąpić o zezwolenie właściwego organu nadzorczego zgodnie z art. 46 ust. 3 lit. a) RODO.

Stosowanie wiążących reguł korporacyjnych art. 46 ust. 2 lit. b RODO oraz klauzul ad hoc art. 46 ust. 3 lit. a RODO w ocenie EROD także podlega wszystkim argumentom wskazanym z wyroku TSUE w sprawie Schrems II, czyli opisanemu wcześniej mechanizmowi.

Krok 6

Ostatni krok to ponowna ocena, a tak naprawdę monitorowanie zmian w państwie trzecim. Mam na myśli zmiany, które mogą mieć istotny wpływ na dokonaną oceną prawa oraz praktyk w danym państwie. Dodatkowo EROD wskazuje, że należy wdrożyć odpowiednie mechanizmy, które mogą w odpowiedniej sytuacji zawiesić lub zakończyć transfer danych.

Podsumowanie

Ocena skutków dla transferu danych może wydawać się na początku dużym wyzwaniem. Najtrudniejsze będzie poznanie i ocena systemu prawnego obcego państwa. W praktyce możesz posiłkować się wieloma wciąż powstającymi źródłami w internecie. Nikt nie oczekuje też od Ciebie analizy systemu prawnego np. Chin na poziomie doktoratu czy pracy magisterskiej. Analiza ma być możliwie prosta i wskazywać realne zagrożenia dla prywatności. Zdecydowanie lepiej wykonać analizę prostą (czy nawet zbyt prostą), niż nie wykonać jej w ogóle.

Mam nadzieję, że przedstawione w artykule pomysły pomogą Ci w ocenie transferu. W najbliższym czasie wprowadzimy do naszego sklepu internetowego draft procedury TIA.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist sp. z o.o.

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)
- Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych
- Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru