Warszawa, dn. 21.03.2024 r.

Transfer danych osobowych w oparciu o decyzję Komisji Europejskiej – a aktualizacja oceny ryzyka transferu przez administratora

Analizę ryzyka transferu danych osobowych poza EOG administrator danych powinien przeprowadzać zawsze, kiedy zachodzi możliwość, że dane osobowe mogą fizycznie znaleźć się poza obszarami EOG, jak również w sytuacjach, kiedy możliwy jest dostęp do tych danych dla odbiorców z krajów trzecich.

W dobie cyfryzacji, postępu technologicznego – przekazywanie danych między krajami a nawet kontynentami jest nieuniknione.

Ryzyko związane z transferem dotyczy głównie tego, czy kraj importera posiada skuteczne środki ochrony prawnej, gwarantujące egzekwowalność praw osób, których dane dotyczą.

Brzmi skomplikowanie i słusznie, ponieważ w praktyce oznacza to ocenę, podobieństw w zakresie gwarancji, jakie daje, chociażby 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, „RODO") z aktami prawnymi obowiązującymi na terenie państwa, do którego eksportuje się dane.

Jednak nie sama ocena prawa w kraju trzecim wystarczy, aby ocenić ryzyko transferu.

Ocena powinna zawierać również informacje na temat tego, czy organy publiczne państwa trzeciego mogą starać si ę uzyskać dostęp do danych za wiedzą, pośrednictwem lub bez wiedzy podmiotu odbierającego dane, w świetle prawodawstwa, praktyki i zgłoszonych precedensów.

Oceniana więc powinna być kondycja praworządności, incydenty „inwigilacyjne" stosowane przez władzę, a także inne aspekty rodzące ryzyko, że dostęp do danych będzie mógł naruszyć prawa i wolności osób.

Tu poziom trudności się nie kończy, a wszystkie pozostałe kroki, jakie należy wykonać podczas dokumentowania oceny ryzyka transferu danych znajdują się w Zaleceniach EROD 01/2020.

Najprostsze narzędzie, a traktowane po macoszemu podczas oceny ryzyka.

W niniejszym artykule skupimy się jednak na najprostszym aspekcie w ocenie ryzyka transferu, a często błędnie pomijanym przez administratorów danych w obowiązku dokumentowania tej oceny.

Chodzi o przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, gdy Komisja Europejska (KĘ) stwierdzi, że to państwo trzecie zapewnia odpowiedni stopień ochrony. Jest to jeden ze starszych mechanizmów transferu, ponieważ istniał jeszcze przed wejściem w życie RODO w podobnym kształcie w oparciu o przepisy Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Co dla administratora danych oznacza fakt, że dany kraj został objęty decyzją Komisji Europejskiej?

Oznacza 90% mniej pracy. Tę pracę bowiem wykonała już Komisja oceniając kraj importera. Oczywiście po stronie administratora pozostaje utrzymanie adekwatnego poziomu zabezpieczeń na linii samego transferu, natomiast nie musi się on martwić analizą przepisów obcego kraju – co umówmy się – stwarza problemy naszym rodzimym prawnikom.

Jednak nawet najprostsza metoda daje złudne poczucie, że raz wykonana – wystarcza, aby zabezpieczać transfer już przez cały okres jego trwania.

Nic bardziej mylnego.

Administrator zobowiązany jest zarówno przy rozpoczęciu eksportu danych, jak i przez cały okres jego trwania dokonywać przeglądów skuteczności mechanizmów wskazanych w art. 45 -47 RODO.

W przypadku decyzji KE stwierdzającej odpowiedni stopień ochrony – należy monitorować zarówno zakres decyzji (np. decyzja w sprawie Izraela obejmuje jedynie zautomatyzowane przetwarzanie danych), jak również jej ważność (niektóre decyzje funkcjonują już ponad 20 lat!).

Na całe szczęście przeglądu decyzji dokonuje również Komisja Europejska, jednak po stronie administratora pozostaje zapoznanie się z przeglądem oraz odpowiednia aktualizacja dokumentacji, jaką prowadzi w ramach oceny ryzyka transferu danych.

Art. 97 RODO zobowiązuje Komisję do okresowego przeglądu tych decyzji co cztery lata w celu ustalenia czy państwa i terytoria, w których stwierdzono odpowiedni stopień ochrony, nadal zapewniają odpowiedni poziom ochrony danych osobowych.

15.01.2024r – to data, z jaką administrator danych powinien aktualizować dokumentację dot. transferów, ponieważ właśnie w tym dniu KE zaprezentowała sprawozdanie z przeglądu funkcjonowania decyzji.[1]

Czy Państwa objęte decyzją dorównują coraz bardziej wymogom europejskim, w szczególności podkreślanym w wyrokach TSUE ?[2]

Tak! Przegląd wykazał, że od czasu przyjęcia decyzji stwierdzających odpowiedni stopień ochrony, każdym z jedenastu państw lub terytoriów osiągnięto jeszcze większą zbieżność z ramami UE. Ponadto w dziedzinie dostępu rządu do danych osobowych, pierwszy przegląd wykazał, że prawo tych państw lub terytoriów przewiduje odpowiednie zabezpieczenia i ograniczenia oraz zapewnia mechanizmy nadzoru i dochodzenia roszczeń w tym obszarze.

Poniżej skrótowo przedstawiamy przegląd decyzji poszczególnych krajów.

---

[1] SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie pierwszego przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które przyjęto na podstawie art. 25 ust. 6 dyrektywy 95/46/WE

[2] W szczególności w wyroku z dnia 6 października 2015 r. w sprawie Schrems I Trybunał Sprawiedliwości stwierdził, że o ile nie można wymagać od państwa trzeciego zapewnienia poziomu ochrony identycznego z tym gwarantowanym w UE, test odpowiedniego stopnia ochrony należy rozumieć jako wymóg zapewnienia „merytorycznie równoważnego" poziomu ochrony. Trybunał doprecyzował w szczególności, że środki, z których korzysta dane państwo trzecie do zapewnienia ochrony danych osobowych, mogą różnić się od środków stosowanych w Unii, o ile w praktyce skutecznie zapewniają odpowiedni stopień ochrony.

a. Andora

Do poprawy bezpieczeństwa niewątpliwie przyczyniło się przyjęcie ustawy nr 29/2021 o ochronie danych osobowych, która weszła w życie w maju 2022 r., Ustawa jest ściśle zgodna dostosowana do RODO pod względem struktury i głównych elementów.

b. Argentyna

Wzmocniono niezależność argentyńskiego organu nadzorczego ds. ochrony danych (dekretem nr 746/17, w którym powierzono Agencia de Acceso a la Información Pública (AAIP) odpowiedzialność za nadzorowanie przestrzegania przepisów o ochronie danych). Argentyna wzmocniła również swoje międzynarodowe zobowiązania w dziedzinie ochrony danych, przystępując w 2019 r. do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i do protokołu dodatkowego do niej, a także ratyfikując w 2023 r. protokół zmieniający ustanawiający zaktualizowaną konwencję nr 108+.

c. Kanada

Wzmocniono dodatkowo ustawę o ochronie danych osobowych i dokumentach elektronicznych (PIPEDA), wprowadzając różne zmiany (np. dotyczące warunków ważnej zgody i powiadomień o naruszeniu ochrony danych). Kluczowe wymogi ochrony danych (np. dotyczące przetwarzania danych wrażliwych) zostały natomiast doprecyzowane w orzecznictwie, a także w wytycznych wydanych przez kanadyjski federalny organ ochrony danych – Urząd Komisarza ds. Prywatności.

d. Wyspy Owcze

Wyspy Owcze znacznie zmodernizowały swoje ramy ochrony, przyjmując ustawę o ochronie danych, która weszła w życie w 2021 r. i zapewniła ścisłe dostosowanie systemu Wysp Owczych do RODO.

Ustawa o przetwarzaniu danych osobowych przez organy ścigania, weszła w życie w 2022 r.

e. Guernsey

Państwo to znacznie zmodernizowało swoje ramy ochrony danych, przyjmując ustawę o ochronie danych dla Baliwatu Guernsey z 2017 r., która obowiązuje od 2019 r. i zapewnia ścisłe dostosowanie systemu Guernsey do RODO.

f. Wyspa Man

Wyspa Man przyjęła w 2018 r. nowe przepisy (ustawa o ochronie danych z 2018 r., uzupełniona zarządzeniem z 2018 r. o ochronie danych (stosowanie RODO), które włączają większość przepisów zawartych w unijnych ramach ochrony danych do porządku prawnego Wyspy Man.

g. Izrael

Izrael wprowadził szczególne zabezpieczenia w celu wzmocnienia ochrony danych osobowych przekazywanych z Europejskiego Obszaru Gospodarczego poprzez przyjęcie rozporządzeń w sprawie ochrony prywatności.

h. Jersey

Państwo znacznie zmodernizowało swoje ramy ochrony danych, przyjmując ustawę o ochronie danych dla Jersey z 2018 r. oraz ustawę o organie ochrony danych z 2018 r., które weszły w życie w 2018 r.

i. Nowa Zelandia

Nowozelandzki system ochrony danych przeszedł kompleksową reformę wraz z przyjęciem ustawy o prywatności z 2020 r., która przyczyniła się do dalszego zwiększenia zbieżności z unijnymi ramami ochrony danych, w szczególności w odniesieniu do przepisów dotyczących międzynarodowego przekazywania danych osobowych oraz uprawnień organu ochrony danych (Urzędu Komisarza ds. Prywatności).

j. Szwajcaria

Zmiany legislacyjne, orzecznictwo i działania organów nadzorczych, przyczyniły się do zwiększenia poziomu ochrony danych. Chodzi w szczególności o zaktualizowaną ustawę federalną o ochronie danych, która przyczyniła się do dalszego zbliżenia z unijnymi ramami ochrony danych, zwłaszcza w odniesieniu do ochrony danych wrażliwych i przepisów dotyczących międzynarodowego przekazywania danych.

k. Urugwaj

Urugwaj zaktualizował i wzmocnił swoją ustawę nr 18.331 o ochronie danych osobowych oraz o środku zaskarżenia „Habeas Data" z 2008 r. w drodze zmian legislacyjnych wprowadzonych w latach 2018 i 2020, które przewidywały rozszerzenie terytorialnego zakresu stosowania przepisów o ochronie danych oraz wprowadzenie nowych wymagań.

Wnioski

Powyższy przegląd pokazuje, że na przestrzeni ostatnich dziesięcioleci rozwój legislacji w zakresie wrażliwości na bezpieczeństwo danych oraz gwarancje podstawowych praw obywateli w powyższych krajach wzrasta. Czasem bywa mocno zbliżony do znanych nam już wymogów RODO.

To solidny argument również dla procesorów danych, którym często zakazuje się transferu danych poza EOG, co w praktyce bywa często martwym zakazem, lub nieświadomie akceptowaną klauzulą. Warto już na wstępie ocenić z jakim mechanizmem transferu mamy do czynienia. Być może chodzi właśnie o eksport danych do jednego z krajów objętych decyzją, gdzie jak widać, poziom świadomości i ochrony prawnej mocno dogania standardy europejskie.

Magdalena Jacolik – specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.