Warszawa, 20.07.2023 r.

Nowa decyzja o zapewnieniu odpowiedniego poziomu ochrony przez „Ramy ochrony danych UE-USA"

10 lipca 2023 r. Komisja Europejska przyjęła – na podstawie art. 45 RODO – decyzję o zapewnieniu odpowiedniego poziomu ochrony przez „Ramy ochrony danych UE-USA". To zwieńczenie długiego procesu budowania nowej regulacji do wymiany danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi, który rozpoczął się wkrótce po uchyleniu poprzedniej decyzji o zapewnieniu odpowiedniego poziomu ochrony („Privacy Shield") na mocy wyroku TSUE (tzw. wyrok „Schrems II").

Zanim przejdziemy do omówienia co to znaczy dla polskiego przedsiębiorcy, konieczne jest jednak przedstawienie pewnego rysu historycznego.

W okresie pomiędzy wyrokiem Schrems II z dnia 16 lipca 2020 r. a decyzją z 10 lipca 2023 r. podmioty chcące transferować dane osobowe do USA mogły to zrobić tylko jednym legalnym trybem: stosując tzw. standardowe klauzule umowne (SCC). Rozwiązanie to – choć legalne w świetle RODO – wymagało podjęcia przez administratora danych osobowych dodatkowych działań – w szczególności przeprowadzenia tzw. oceny ryzyka transferu danych (Transfer Impact Assesment, TIA). Truizmem będzie powiedzieć, że szczególnie dla mniejszych podmiotów prowadzenia takich analiz było znacznym obciążeniem. Wielu przedsiębiorców próbowało unikać tych czynności, m.in. zawierając umowy z podmiotami z USA, które umownie gwarantowały, że przetwarzane dane osobowe nie opuszczą Europejskiego Obszaru Gospodarczego. Rozwiązanie to było jak najbardziej legalne, jednak zazwyczaj wiązało się z dodatkowymi kosztami.

Co się zmieniło?

Przy transferze danych osobowych do USA od 10 lipca 2023 r., obok standardowych klauzul umownych jako podstawę prawną transferu możemy stosować decyzję o adekwatności (z art. 45 RODO). Decyzja ta różni się jednak od uprzednio wydanych decyzji dotyczących np. Wielkiej Brytanii czy Japonii. O ile tamte decyzje legalizowały każdy transfer do podmiotów w tych krajach, to w przypadku decyzji o Ramach ochrony danych UE-USA wprowadzono dodatkowy wymóg. Decyzja ta legalizuje bowiem wyłącznie transfery danych do firm, które dokonały dobrowolnej certyfikacji i zgłosiły zgodność z zapisami decyzji z 10 lipca 2023 r. (co w praktyce oznacza deklarację zgodności z RODO, albowiem do tego sprowadzają się wymogi wynikające z tego aktu prawnego).

Zatem zgodnie z nową decyzją, amerykańskie firmy mogą przejść dobrowolny proces samo-certyfikacji. Po jego ukończeniu, dopuszczalny jest transfer danych osobowych[1] z Unii Europejskiej do tych firm. Aktualna lista firm amerykańskich deklarujących zgodność dostępna jest już na stronie internetowej amerykańskiego Departamentu Handlu (w dacie pisania niniejszego tekstu znajdowało się tam ponad 2.600 podmiotów).

[1] Z wyjątkiem danych zbieranych w celu publikacji, nadawania lub innych form publicznego komunikowania materiałów dziennikarskich oraz informacji we wcześniej opublikowanych materiałach, rozpowszechnianych z archiwów medialnych.

Jak wspomniano powyżej, decyzja z 10 lipca 2023 r. w dużej części powiela zapisy RODO – nakładając na amerykańskie firmy, które chcą dokonać certyfikacji, szereg obowiązków wynikających z RODO. Są to w szczególności obowiązki:

- przestrzegania zasady zgodności z prawem, rzetelności i przejrzystości przetwarzania;
- przestrzegania zasady ograniczenia celu;
- przestrzegania zasady minimalizacji danych osobowych;
- przestrzegania zasady prawidłowości danych osobowych;
- przestrzegania zasady rozliczalności;
- wyróżnienia danych szczególnej kategorii w rozumieniu art. 9 RODO i szczególnej ich ochrony;
- zapewnienia integralności i poufności danych osobowych;
- ograniczenia przechowywania danych osobowych;
- zachowania bezpieczeństwa danych osobowych – zgodnie z art. 32 RODO;
- zgodności z prawem, rzetelności i przejrzystości (w tym realizacji przez podmioty amerykańskie obowiązku informacyjnego wobec osób, których dane dotyczą oraz publikowania polityki prywatności – z odnośnikiem do tego dokumentu na wspomnianej na stronie Departamentu Handlu USA);
- prawa dostępu do danych osobowych;
- zasad powierzania danych osobowych do dalszego przetwarzania tylko podmiotom, które zapewniają taki sam poziom ochrony danych osobowych.

Permanentna inwigilacja?!

Pisząc w pewnym uproszczeniu, jedną z głównych przyczyn uchylenia decyzji o adekwatności ustanawiającej „Tarczę Prywatności" przez wyrok „Schrems II", był potencjalnie nieograniczony i pozostający poza kontrolą sądów dostęp amerykańskich agencji wywiadowczych do danych osobowych obywateli UE.

Istotną podstawą do wydania nowej decyzji o adekwatności było wydanie przez Prezydenta USA w dniu 7 października 2023 r. nowego Rozporządzenia wykonawczego w sprawie „Zwiększenia zabezpieczeń dla działań wywiadu sygnałowego Stanów Zjednoczonych". Jak wynika z informacji opublikowanych na stronach Komisji Europejskiej, ten nowy akt prawny przewiduje w stosunku do danych osobowych obywateli UE:

- wiążące zabezpieczenia, które ograniczają dostęp organów wywiadowczych USA do danych do tego, co jest konieczne i proporcjonalne do ochrony bezpieczeństwa narodowego;
- wzmocniony nadzór nad działaniami amerykańskich służb wywiadowczych w celu zapewnienia zgodności z ograniczeniami dotyczącymi działań inwigilacyjnych;
- ustanowienie niezależnego i bezstronnego mechanizmu odwoławczego, który obejmuje nowy Sąd Rewizyjny ds. Ochrony Danych, którego zadaniem jest badanie i rozstrzyganie skarg dotyczących dostępu krajowych organów bezpieczeństwa USA do ich danych.

Nadto USA wprowadziły dwuetapowy system odwoławczy na wypadek naruszeń ochrony danych osobowych. Zgodnie z nowymi Ramami ochrony danych UE-USA, podmiotom danych przysługuje skarga do organu nadzorczego we własnym kraju. Organ

ten, za pośrednictwem Europejskiej Rady Ochrony Danych Osobowych będzie mógł w ich imieniu złożyć skargę do:

- Rzecznika Ochrony Wolności Obywatelskich („Civil Liberties Protection Officer"),
- Złożyć odwołanie od decyzji ROWO do tzw. „Sądu Rewizyjnego ds. Ochrony Danych" („Data Protection Review Court"). Organ ten ma być niezależny od władz amerykańskich (choć jak się wydaje nie jest organem sądowym sensu stricte) i mieć uprawnienie do uzyskania informacji od amerykańskich agencji wywiadowczych i nakazywania im usuwania danych osobowych.

Déjà vu?

Osoby choć trochę śledzące sytuację transatlantyckich transferów danych osobowych niewątpliwie zauważyły znaczne podobieństwa pomiędzy formułą nowych „Ram ochrony danych UE-USA" a poprzednio obowiązującymi: „Tarczą Prywatności" (Privacy Shield") oraz „Bezpieczną Zatoką" („Safe Harbour"). Na właśnie tę wadę omawianej decyzji (i ciągle aktualną kwestię nadzoru nad działaniami amerykańskiego wywiadu elektronicznego) wskazują już pierwsze publikacje, które ukazały się po wydaniu decyzji z 10 lipca 2023 r. W szczególności wskazuje się, iż co prawda nowe Rozporządzenie wykonawcze daje obywatelom UE jakieś środki prawne, ale w żaden sposób nie zmienia amerykańskiej ustawy FISA (Foreign Intelligence Surveillance Act, czyli ustawa o wywiadzie zagranicznym). Sekcja 702 tej ustawy pozwala agencjom wywiadowczym USA na nieograniczone (w szczególności bez nakazu sądu) inwigilowanie komunikacji obywateli krajów innych niż USA. Europejskie Centrum na rzecz Praw Cyfrowych[2] już ogłosiło, że szuka chętnych do złożenia skargi do Trybunału Sprawiedliwości Unii Europejskiej na transfery oparte o Decyzję o adekwatności z 10 lipca 2023 r.

Podsumowując, czyli co powinna zrobić firma, która chce transferować dane osobowe do USA?

Patrząc z punktu widzenia obowiązującego prawa: od tygodnia przedsiębiorcy chcący transferować dane osobowe do USA mogą to zrobić legalnie w oparciu o decyzję o adekwatności z dnia 10 lipca 2023 r. (oczywiście pod warunkiem, że firma, do której dane maja trafić jest wpisana na listę prowadzoną przez Departament Handlu USA). Decyzja z 10 lipca 2023 r. weszła w życie i może być stosowana.

W obecnym stanie prawnym oparcie transferu danych do USA na jej podstawie jest niewątpliwie prostszym rozwiązaniem niż stosowanie standardowych klauzul umownych. Wystarczy sprawdzić, czy kontrahent jest wpisany na listę Departamentu Handlu USA i zawrzeć stosowną umowę. Tymczasem stosowane klauzul wymaga wykonania szeregu dodatkowych kroków, w tym przeprowadzenia TIA (i pogłębionej analizy systemu prawnego funkcjonującego w USA).

Podejmując decyzję o wyborze Ram ochrony danych UE-USA jako podstawy prawnej transferu należy jednak pamiętać, że Ramy te (podobnie jak wcześniej Bezpieczna Przystań i Tarcza Prywatności) mogą zostać uchylone przez TSUE. Dotychczasowe doświadczenia

[2] (European Center for Digital Rights, austriacka organizacja pozarządowa korzystająca z nazwy: noyb ("none of your business", czyli „nie twoja sprawa")). Jej założycielem jest prawnik Max Schrems.

uczą nas, iż takie uchylenie następuje ze skutkiem od daty wyroku – a więc transfery dokonane wcześniej pozostaną legalne.

Mając to na uwadze, najprostszym rozwiązaniem wydaje się zatem w dalszym ciągu być odstąpienie od transferu danych do USA. Gdy takie rozwiązanie jest niewykonalne biznesowo (a z praktyki wiemy, że często tak właśnie jest) Ramy ochrony danych UE-USA są dobrym rozwiązaniem – choć wybierając je musimy nastawić się na śledzenie orzecznictwa TSUE w celu szybkiego wychwycenia, czy podstawa ta nie zostanie uchylona. W takiej sytuacji, konieczny będzie powrót do stosowania SCC (lub przyjęcie innego rozwiązania, które będzie wynikało z „Schrems III" lub innego potencjalnego wyroku TSUE).

Daniel Taberski - radca prawny, specjalista ochrony danych osobowych w iSecure Sp. z o.o.