Paweł Głąb[1]

TRANSFER DANYCH OSOBOWYCH DO STANÓW ZJEDNOCZONYCH PO STWIERDZENIU NIEWAŻNOŚCI DECYZJI W SPRAWIE TARCZY PRYWATNOŚCI UE–USA

ABSTRACT

Transfer of personal data to the United States after the invalidation of the decision regarding the EU-US Privacy Shield

The aim of this article is to provide a summary of the legal ground rules for the transfer of personal data to the United States following the ECJ declared the decision of the European Commission on the EU-US Privacy Shield program invalid. The author outlines the general principles of transfer of personal data to third countries in view of the regulations of Chapter 5 of the GDPR, analyzes the presumptions of the Privacy Shield program, and assesses the post-invalidation landscape. The author analyzes the Schrems II judgment, the complaint of M. Schrems, the questions submitted to the CJEU for a preliminary ruling, and describes the key points of the judgment in case file no. C-311/18. The article

1 Radca prawny, OIRP w Rzeszowie, wspólnik w Kancelarii Prawnej Kantorowski, Głąb i Wspólnicy Sp.k., autor publikacji z zakresu ochrony danych osobowych oraz branży e-commerce.

also provides a brief historical overview of the developments that resulted in the CJEU issuing the aforementioned judgment.

Keywords: Schrems II, European Court of Justice, Privacy Shield, Safe Harbor Privacy Principles, data transfer, GDPR, United States, personal data, European Commission, questions submitted for a preliminary ruling, third countries

Słowa kluczowe: Schrems II, Trybunał Sprawiedliwości, Tarcza Prywatności, Bezpieczna Przystań, transfer danych, RODO, Stany Zjednoczone, dane osobowe, Komisja Europejska, pytania prejudycjalne, państwa trzecie

Trybunał Sprawiedliwości w wyroku z 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner (irlandzki organ ds. ochrony danych osobowych) przeciwko Facebook Ireland Ltd. i Maximilian Schrems stwierdził nieważność decyzji wykonawczej Komisji (UE) 2016/1250 z 12 lipca 2016 r., przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA[2]. W konsekwencji od dnia ogłoszenia wyroku, tj. 16 lipca 2020 r., przekazywanie danych do Stanów Zjednoczonych nie może odbywać się już na tej podstawie. TSUE w wyżej wymienionym orzeczeniu nie określił bowiem żadnego okresu przejściowego. Jest to rozstrzygnięcie mające niebagatelne znaczenie dla transatlantyckiego przepływu danych osobowych. Tarcza Prywatności była bowiem głównym mechanizmem pozwalającym na swobodne transferowanie danych do USA. Obecnie przekazywanie danych osobowych z Unii Europejskiej do Stanów Zjednoczonych musi zostać zawieszone lub oparte na innym mechanizmie określonym w rozdziale V RODO[3]. Jest to więc spore wyzwanie dla amerykańskich dostawców usług bazujących na rozwiązaniach związanych chociażby z chmurą obliczeniową,

2 Wyrok Trybunału Sprawiedliwości z 16 lipca 2020 r. w sprawie C-311/18 (dalej jako wyrok w sprawie Schrems II).

3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) z 27 kwietnia 2016 r. (dalej jako RODO lub ogólne rozporządzenie o ochronie danych).

jak również dla europejskich użytkowników tychże rozwiązań. Niniejszy artykuł stanowi systematyczne uporządkowanie wybranych zagadnień tytułowej problematyki poświęconej zasadom legalnego transferu danych do Stanów Zjednoczonych. Obejmuje on podsumowanie głównych założeń programu Tarcza Prywatności, jak również analizę wyroku TSUE w sprawie Schrems II. Celem artykułu jest omówienie zasad dalszego legalnego przekazywania danych z UE do USA w obliczu nieważności mechanizmu będącego dotychczas jedną z głównych podstaw takiego transferu danych.

Przed przejściem jednak do szczegółowych rozważań dotyczących Tarczy Prywatności i wyroku w sprawie Schrems II warto omówić podstawowe zasady związane z przekazywaniem danych do państw trzecich w świetle regulacji RODO. Stanowić to będzie tło do dalszych rozważań, a także pozwoli dostrzec wagę rozstrzygnięcia TSUE wydanego w lipcu 2020 r. Ogólne rozporządzenie o ochronie danych na nowo zdefiniowało bowiem transfer danych osobowych do państw trzecich. Jednym z głównych założeń unijnych regulacji w zakresie danych osobowych było unowocześnienie i urealnienie technologiczne przepisów związanych z przekazywaniem danych do państw trzecich[4]. Jak podkreślono w motywie 6 RODO, szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, zapewniając jednocześnie wysoki stopień ochrony danych osobowych. W motywie 101 RODO wskazano, że przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym

4 D. Lubasz, *Przekazywanie danych osobowych do państw trzecich w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 20/2016, s. 69.

lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać stopnia ochrony osób fizycznych zapewnianego w Unii. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z przepisami RODO.

Wszystko to jednoznacznie wskazuje, iż transgraniczny transfer danych, w związku z postępującym rozwojem technicznym, stanowi niezwykle ważny element legalnego przetwarzania danych osobowych w świetle regulacji unijnych i okoliczność ta dostrzeżona została przez unijnego prawodawcę. Ostatecznie w ogólnym rozporządzeniu o ochronie danych wprowadzono trzy współzależne i hierarchicznie ułożone kategorie sytuacji, w których transfer danych przez administratora będącego eksporterem jest dopuszczalny. Po pierwsze podstawą transferu może być decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony w państwie trzecim (art. 45 RODO), po drugie w przypadku braku ww. decyzji, gdy zapewnione są odpowiednie zabezpieczenia ochrony danych osobowych opisane w art. 46–47 RODO, i wreszcie po trzecie w przypadku braku powyższych podstaw transfer danych jest możliwy, gdy zachodzi jedna z sytuacji, w stosunku do których ogólne rozporządzenie o ochronie danych przewiduje odstępstwa (art. 49 RODO)[5].

Warto jeszcze wspomnieć, że RODO nie definiuje pojęcia państwa trzeciego, chociaż jest ono wielokrotnie używane w kontekście przekazywania danych poza Unię Europejską. Wynika to jednak z tego, że zostało ono wprowadzone do prawa pierwotnego, tj. TFUE[6] i TUE[7]. Oba traktaty posługują się terminem „państwo trzecie" w znaczeniu państw nienależących do Europejskiego Obszaru Gospodarczego i bez wątpienia tak należy rozumieć ten termin również na gruncie RODO[8].

5 D. Lubasz, K. Witkowska, *Europejska reforma ochrony danych osobowych z perspektywy pełnomocnika przedsiębiorcy*, [w:] *Media elektroniczne. Współczesne problemy prawne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016, s. 189.

6 Traktat o funkcjonowaniu Unii Europejskiej.

7 Traktat o Unii Europejskiej.

8 *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Legalis 2020.

W niniejszym artykule skupię się na podstawie przekazywania danych do państw trzecich, uregulowanej w art. 45 RODO, gdyż to ten mechanizm stanowił podstawę funkcjonowania programu Tarcza Prywatności. Zgodnie z art. 45 RODO przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia. Jedynym więc podmiotem uprawnionym do stwierdzenia adekwatności ochrony danych osobowych w danym państwie trzecim jest Komisja Europejska. Może stwierdzić ze skutkiem dla całej Unii, że państwo trzecie lub terytorium albo określony sektor w państwie trzecim lub organizacja międzynarodowa zapewniają adekwatny stopień ochrony. Rozwiązanie to stanowi więc gwarancję jednolitości i pewności prawa, gwarantując legalny transfer do państw trzecich, które zostały uznane za zapewniające adekwatny stopień ochrony[9]. Oceniając, czy stopień ochrony jest odpowiedni, Komisja Europejska uwzględnia w szczególności trzy enumeratywnie wymienione elementy. W pierwszej kolejności ocenie podlegają: praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą oraz których dane osobowe są przekazywane, do

9 Motyw 103 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) z 27 kwietnia 2016 r.

skutecznych administracyjnych i sądowych środków zaskarżenia. Po drugie ocenie podlega istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich. Ostatecznie Komisja Europejska uwzględnia międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych (art. 45 ust. 2 RODO).

Ponadto w motywie 104 RODO wskazano, iż zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja Europejska powinna w swojej ocenie państwa trzeciego lub terytorium, lub określonego sektora w państwie trzecim wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także prawo karne. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub określonego sektora w państwie trzecim należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii, w szczególności w przypadkach, gdy dane osobowe są przetwarzane w jednym szczególnym sektorze lub większej ich liczbie. Państwo trzecie powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych

państw członkowskich, a osoby, których dane dotyczą, powinny uzyskać skuteczne i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, Komisja Europejska może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Taka też decyzja wydana została przez Komisję Europejską w stosunku do Stanów Zjednoczonych. Adekwatny stopień ochrony danych osobowych w USA stwierdzony został w decyzji wykonawczej Komisji (UE) 2016/1250 z 12 lipca 2016 r. przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA[10].

Co niezwykle istotne dla rozważań dotyczących transferu danych do Stanów Zjednoczonych, powyższa decyzja była drugim w historii porozumieniem pomiędzy UE a USA w przedmiocie transatlantyckiego przekazywania danych osobowych. Wcześniejsza bowiem decyzja Komisji Europejskiej regulująca zasady funkcjonowania programu tzw. Bezpiecznej Przystani[11], która przez ponad 15 lat stanowiła główny mechanizm transferowania danych osobowych do Stanów Zjednoczonych, została uznana za nieważną w wyroku TSUE z 6 października 2015 r.[12] Przyjęty kilka miesięcy później program Tarczy Prywatności podzielił los swojej „poprzedniczki" i po niecałych czterech latach funkcjonowania TSUE również stwierdził nieważność decyzji wprowadzającej tenże program. Można stwierdzić, że swoistym autorem całego zamieszania związanego z mechanizmem legalnego transferu danych do USA jest

10 Decyzja wykonawcza Komisji (UE) 2016/1250 z 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.

11 Decyzja Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony w Stanach Zjednoczonych, przewidzianej przez zasady ochrony prywatności w ramach tzw. Bezpiecznej Przystani (Safe Harbour).

12 Wyrok Trybunału Sprawiedliwości z 6 października 2015 r., C-362/14 (dalej jako Schrems I).

niejaki Maximilian Schrems, austriacki użytkownik serwisu społecznościowego Facebook, którego skarga do irlandzkiego organu ds. ochrony danych osobowych (Data Protection Commissioner) była przyczynkiem do wydania orzeczeń TSUE stwierdzających nieważność dwóch decyzji Komisji Europejskiej, które przez blisko 20 lat jedna po drugiej stanowiły główny mechanizm i gwarancję legalnego transferowania danych do USA.

Krytycznym momentem dla funkcjonowania ugruntowanych zasad transferu danych do USA w ramach programu Bezpieczna Przystań okazały się doniesienia byłego pracownika Centralnej Agencji Wywiadowczej USA, Edwarda Snowdena, na temat programu PRISM, dzięki któremu amerykańskie służby wywiadowcze prowadziły operacje masowej inwigilacji internautów. Ujawnione przez niego w połowie 2013 r. dokumenty dotyczące działalności Agencji Bezpieczeństwa Narodowego USA wskazywały, że służby te posiadały bezpośredni dostęp do informacji przechowywanych na serwerach amerykańskich gigantów internetowych, takich jak Google, Apple, Facebook, Microsoft, Skype, YouTube i in.[13] Warto o tym wspomnieć, ponieważ informacje o inwigilacyjnych działaniach amerykańskich służb wywołały spore zaniepokojenie opinii publicznej[14], czego szczególnym wyrazem stała się skarga wniesiona w czerwcu 2013 r. przez wspomnianego wcześniej austriackiego aktywistę, a zarazem użytkownika portalu społecznościowego Facebook, Maximiliana Schremsa do irlandzkiego Komisarza ds. Ochrony Danych Osobowych (Data Protection Commissioner). Schrems, w oparciu nie tylko o dokumenty ujawnione przez Snowdena, lecz także o własne badania na temat polityki prywatności Facebooka, podniósł w skardze, że dane transferowane z serwerów spółki Facebook Ltd., mającej siedzibę w Dublinie, na serwery amerykańskiej spółki Facebook Inc. w ramach programu Bezpiecznej Przystani nie są właściwie zabezpieczone[15]. Schrems w skardze podnosił,

13 A. Michałowicz, *Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy Prywatności*, „Monitor Prawniczy" 23/2016, s. 1264. Na ten temat pisze również D. Karwala, *Krajobraz po wyroku Trybunału Sprawiedliwości w sprawie programu Bezpiecznej Przystani*, „Monitor Prawniczy" 10/2016, s. 515.

14 *Ibidem.*

15 *Ibidem.*

iż świetle informacji podanych do wiadomości przez Edwarda Snowdena na temat działalności służ specjalnych USA prawo i praktyka USA nie zapewniają w rzeczywistości żadnej ochrony przed kontrolowaniem przez organy publiczne danych przekazywanych do tego kraju. Schrems wskazał również m.in., że masowa inwigilacja prowadzona przez służby USA godzi w prawa podstawowe jednostek, takie jak prawo do prywatności i ochrony danych osobowych, a zatem jest bezprawna w świetle art. 8 Europejskiej konwencji praw człowieka[16], art. 8 Karty praw podstawowych UE[17], a także postanowień dyrektywy 95/46[18].

Irlandzki organ ds. ochrony danych osobowych oddalił skargę Maximiliana Schremsa, w szczególności powołując się na to, iż Komisja Europejska w ramach programu Bezpieczna Przystań stwierdziła, że Stany Zjednoczone zapewniają adekwatny stopień ochrony przekazywanych danych osobowych. W wyroku w sprawie Schrems I Trybunał Sprawiedliwości w odpowiedzi na pytania prejudycjalne zadane przez High Court (Sąd Najwyższy w Irlandii) uznał decyzję dotyczącą funkcjonowania programu Bezpieczna Przystań za nieważną. Jest to o tyle istotne, że po wydaniu przez Trybunał Sprawiedliwości wyroku sąd krajowy w Irlandii uchylił decyzję, na której podstawie irlandzki organ ds. ochrony danych osobowych oddalił wniesioną przez M. Schremsa skargę i przekazał ją temu organowi w celu weryfikacji. Organ wszczął dochodzenie i wezwał M. Schremsa do przeformułowania swej skargi w kontekście unieważnienia decyzji o Bezpiecznej Przystani[19]. Nowo sformułowana skarga M. Schremsa stała się natomiast przyczynkiem do wydania wyroku Schrems II z lipca 2020 r., w którym to Trybunał Sprawiedliwości orzekł m.in. o nieważności decyzji wprowadzającej Tarczę Prywatności.

W tym miejscu wskazać trzeba, iż po stwierdzeniu nieważności decyzji dotyczącej programu Bezpieczna Przystań w październiku 2015 r.

16 Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.

17 Karta praw podstawowych Unii Europejskiej.

18 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

19 Opinia rzecznika generalnego w sprawie C-311/18 Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems.

natychmiast przystąpiono do opracowania nowego mechanizmu transferu danych z UE do USA. Dzięki temu już na początku lutego 2016 r. strony poinformowały o osiągnięciu porozumienia, zwanego Tarczą Prywatności, które na nowo regulowało zasady przekazywania danych z UE do USA[20]. 12 lipca 2016 r. Komisja Europejska przyjęła decyzję wykonawczą 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA. Było to swoiste nowe rozdanie w zakresie transferu danych na linii Unia Europejska–Stany Zjednoczone.

W art. 1 ust. 1 i 3 Tarczy Prywatności[21] stwierdzono, iż Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych, które figurują w „wykazie podmiotów uczestniczących w programie Tarczy Prywatności" prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych. Główne założenie funkcjonowania tego programu oparte było na zasadzie, iż podmioty na terenie USA, które chciały przetwarzać dane osobowe w ramach Tarczy Prywatności, musiały uzyskać certyfikat wydany przez Departament Handlu USA. Jeżeli dany podmiot posiadał certyfikat, dopuszczalne było przekazywanie danych temu podmiotowi bez dodatkowych wymogów[22]. Wykaz wszystkich podmiotów, które uczestniczyły w programie Tarczy Prywatności, zamieszczony jest w dalszym ciągu na stronach Departamentu Handlu USA[23]. Zawiera on szczegółowe informacje na temat przedsiębiorstw biorących udział w Tarczy Prywatności, rodzaju danych osobowych, z jakich przedsiębiorstwa te korzystają, oraz charakteru oferowanych przez nie usług.

Każdy podmiot w USA przetwarzający dane osobowe w ramach Tarczy Prywatności musiał spełniać wszystkie zasady określone w załączniku II do decyzji 2016/1250. Po pierwsze podmiot taki miał obowiązek powiadomienia m.in. o swoim uczestnictwie w programie Tarczy

20 A. Michałowicz, *op. cit.*, s. 1264.

21 Decyzja Wykonawcza Komisji (UE) 2016/1250 z 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.

22 *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Legalis 2020.

23 https://www.privacyshield.gov/list [dostęp: 25 marca 2021 r.].

Prywatności, rodzajach zgromadzonych danych osobowych i celach, dla których je gromadzi, sposobach kontaktowania się z podmiotem w razie jakichkolwiek zapytań lub skarg, prawie dostępu do własnych danych osobowych, swojej odpowiedzialności w razie wtórnego przekazywania danych osobom trzecim. Podmiot musiał ponadto dać osobom fizycznym możliwość wyboru m.in., czy dane osobowe ich dotyczące mają: (i) zostać ujawnione osobie trzeciej lub (ii) zostać wykorzystane w celu niezgodnym z celem lub celami, dla których były pierwotnie gromadzone, lub na które osoba fizyczna wyraziła później zgodę.

Podmioty będące uczestnikami Tarczy Prywatności ponosiły również odpowiedzialność za wtórne przekazywanie, polegające na stosowaniu zasady powiadomienia i wyboru przy przekazywaniu danych osobowych osobie trzeciej działającej jako administrator. Podmioty musiały również zawrzeć z administratorem będącym osobą trzecią umowę, która przewidywała, że dane te można przetwarzać wyłącznie do ograniczonych i określonych celów, na które osoba fizyczna wyraziła zgodę. Przekazując dane osobowe osobie trzeciej działającej jako administrator, podmioty musiały m.in.: (i) przekazywać takie dane wyłącznie do ograniczonych i określonych celów; (ii) upewnić się, że podmiot przetwarzający ma obowiązek zapewnienia przynajmniej takiego samego poziomu ochrony prywatności co poziom wymagany w zasadach. Podmioty tworzące, przechowujące, wykorzystujące lub rozpowszechniające dane osobowe musiały podejmować zasadne i odpowiednie środki ostrożności w celu ochrony ich przed utratą, niewłaściwym wykorzystaniem oraz nieuprawnionym dostępem, ujawnieniem, zmianą i zniszczeniem, biorąc w szczególności pod uwagę zagrożenia związane z przetwarzaniem danych osobowych i ich charakterem. Podmioty te obowiązywała również zasada integralności i ograniczenia celem polegająca m.in. na ograniczeniu się do danych, które są istotne do celów przetwarzania. Podmiotom nie wolno było co do zasady przetwarzać danych osobowych w sposób niezgodny z celami, dla których były one zbierane lub na które osoba fizyczna wyraziła później zgodę.

Uczestnicy Tarczy Prywatności musieli zapewnić osobom fizycznym dostęp do własnych danych osobowych przechowywanych przez podmiot i możliwości poprawiania, zmieniania lub usuwania takich danych, gdy są one nieprawidłowe lub zostały przetworzone z naruszeniem

zasad, z wyjątkiem przypadków, gdy obciążenie związane z udostępnianiem lub koszty udostępniania danych byłyby nieproporcjonalne w stosunku do zagrożenia dla ochrony prywatności danej osoby fizycznej, lub w przypadku gdy naruszone zostałyby prawa innych osób. Ostatecznie podmioty będące uczestnikami Tarczy Prywatności obowiązane były do stosowania zasady ochrony prawnej, egzekwowania prawa i odpowiedzialności polegającej na skutecznej ochronie prywatności, która obejmowała solidne mechanizmy zapewniające przestrzeganie zasad, ochronę prawną osób fizycznych, które poniosły skutki nieprzestrzegania zasad, oraz konsekwencje, jakie musiał ponieść dany podmiot, jeżeli nie przestrzega zasad. Takie mechanizmy musiały obejmować m.in. łatwo dostępne niezależne mechanizmy ochrony prawnej. Podmioty i wskazane przez nie niezależne mechanizmy ochrony prawnej były zobowiązane bezzwłocznie reagować na złożone przez departament zapytania i wnioski o informacje dotyczące Tarczy Prywatności.

Mogłoby się więc wydawać, że Tarcza Prywatności zapełni na dłuższy czas lukę powstałą po unieważnieniu Bezpiecznej Przystani. Nie sposób jednak nie odnieść wrażenia, iż rozwiązania przyjęte w Tarczy Prywatności w rzeczywistości niewiele odbiegały od gwarancji adekwatności w zakresie ochrony danych osobowych w Stanach Zjednoczonych, jakie leżały u podstaw Bezpiecznej Przystani. W konsekwencji Tarcza Prywatności, podobnie jak jej wcześniejsza wersja, tj. Bezpieczna Przystań, od początku zbierała negatywne komentarze, oceny i recenzje. Wprost podnoszono, że nowe ramy prawne najprawdopodobniej nie wytrzymają weryfikacji przez europejskie organy ochrony danych czy Trybunał Sprawiedliwości[24]. Negatywnie o Tarczy Prywatności wypowiadała się Grupa Robocza art. 29 w opinii z 13 kwietnia 2016 r. i oświadczeniu wydanym tuż po podpisaniu porozumienia. Jej zdaniem nowe rozwiązania były krokiem w dobrym kierunku, jednakże w rzeczywistości nie realizowały wielu wymagań wynikających z unijnych regulacji w zakresie ochrony danych osobowych[25]. Obawy te niestety okazały się słuszne i niewiele ponad cztery lata po przyjęciu decyzji Komisji Europejskiej w sprawie Tarczy Prywatności TSUE w sprawie Schrems II stwierdził jej nieważność.

24 A. Michałowicz, *op. cit.*, s. 1264.

25 *Ibidem.*

Jak zostało wskazane wcześniej, orzeczenie to zapadło w ramach sporu, jaki zaistniał pomiędzy Data Protection Commissioner a Facebook Ireland Ltd. i Maximilianem Schremsem w przedmiocie wniesionej przez niego – na nowo sformułowanej po stwierdzeniu nieważności Bezpiecznej Przystani – skargi, dotyczącej przekazywania danych osobowych przez Facebook Ireland spółce Facebook Inc. w Stanach Zjednoczonych. Co ciekawe, złożona przez Maximiliana Schremsa 1 grudnia 2015 r. nowa skarga dotyczyła w istocie możliwości przekazywania danych osobowych z UE do USA na podstawie standardowych klauzul umownych[26], nie zaś bezpośrednio kwestii legalności Tarczy Prywatności. W ramach wszczętego przez irlandzki organ ds. ochrony danych dochodzenia Facebook Ireland wyjaśniła bowiem, że znaczna część danych osobowych została przekazana Facebook Inc. na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych i to właśnie ten mechanizm był główną podstawą transferu danych do amerykańskiego oddziału Facebooka. W swej sformułowanej na nowo skardze M. Schrems podniósł zatem po pierwsze, że zawarte w porozumieniu pomiędzy Facebook Ireland a Facebook Inc. klauzule nie odpowiadają przewidzianym w decyzji standardowym klauzulom umownym, i po drugie, że te standardowe klauzule umowne w każdym razie nie mogą stanowić podstawy dla przekazywania do USA danych osób, których dotyczą. M. Schrems zwrócił się do organu nadzorczego o zawieszenie przekazywania tych danych w zastosowaniu decyzji 2010/87[27]. W konsekwencji skargi Data Protection Commissioner zwrócił się do High Court (Sądu Najwyższego w Irlandii), aby ten skierował do Trybunału Sprawiedliwości pytanie prejudycjalne w tym względzie. Co istotne w toku sprawy Facebook Ireland podnosił, iż ustalenia komisji dotyczące odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, takie jak te zawarte w decyzji w sprawie Tarczy Prywatności, wiążą organy nadzorcze również w kontekście przekazywania

26 Decyzja Komisji 2010/87/UE z 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mającym siedzibę w państwach trzecich na podstawie dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, zmienionej decyzją wykonawczą Komisji (UE) 2016/2297 z 16 grudnia 2016 r.

27 Opinia rzecznika generalnego w sprawie C-311/18…

danych osobowych w oparciu o standardowe klauzule ochrony danych, zawarte w załączniku do decyzji w sprawie klauzul standardowych[28]. W efekcie pytania prejudycjalne skierowane przez Sąd Najwyższy w Irlandii do Trybunału Sprawiedliwości objęły swym zakresem – mówiąc w uproszczeniu – stwierdzenie ważności dwóch mechanizmów mogących stanowić podstawę transferowania danych do USA: po pierwsze odpowiednich zabezpieczeń w postaci standardowych klauzul umownych, po drugie programu Tarcza Prywatności[29].

W wyroku w sprawie Schrems II Trybunał Sprawiedliwości stwierdził, że ocena decyzji 2010/87 (standardowe klauzule umowne) w świetle Karty praw podstawowych Unii Europejskiej nie wykazuje niczego, co mogłoby podważać jej ważność. Trybunał Sprawiedliwości stwierdził natomiast, że decyzja 2016/1250 (Tarcza Prywatności) jest nieważna. Trybunał Sprawiedliwości orzekł przede wszystkim, że odpowiednie zabezpieczenia, egzekwowalne prawa i skuteczne środki ochrony prawnej obowiązujące w ramach przekazywania danych do państwa trzeciego na podstawie standardowych klauzul umownych muszą korzystać ze stopnia ochrony równoważnego temu, który jest gwarantowany w Unii Europejskiej. Trybunał Sprawiedliwości zaznaczył, że w ramach oceny adekwatności stopnia ochrony analizie poddać należy zarówno same postanowienia umowne, uzgodnione pomiędzy podmiotem mającym siedzibę w UE, a importerem danych z państwa trzeciego na podstawie standardowych klauzul umownych, jak również istotne elementy składające się na system ochrony danych osobowych obowiązujący w tym państwie trzecim, w tym m.in. dostęp organów władzy publicznej tego państwa trzeciego do przekazywanych w ten sposób danych[30]. W przedstawionej opinii rzecznik generalny Henrik Saugmandsgaard Øego stwierdził, iż sam fakt, że na podmiot przetwarzający dane w państwie trzecim mogą być przez władze tego państwa nałożone obowiązki będące nie do pogodzenia z przestrzeganiem standardowych klauzul umownych, nie przesądza sam w sobie o ważności decyzji je wprowadzającej. W konsekwencji,

28 Wyrok Trybunału Sprawiedliwości z 16 lipca 2020 r. w sprawie C-311/18.

29 Wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez High Court (Irlandia) 9 maja 2018 r. – Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems (sprawa C-311/18).

30 Wyrok Trybunału Sprawiedliwości z 16 lipca 2020 r. w sprawie C-311/18.

w ocenie rzecznika generalnego, decyzja komisji 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane, mającym siedzibę w państwach trzecich, jest ważna[31]. Trybunał Sprawiedliwości podzielił tę opinię. Standardowe klauzule umowne mogą być więc mechanizmem legalnego transferu danych do państwa trzeciego jednakże wyłącznie wtedy, gdy w świetle całokształtu okoliczności towarzyszących transferowi danych osobowych można stwierdzić, że standardowe klauzule ochrony danych w rzeczywistości są respektowane przez podmiot przetwarzający dane osobowe w określonym państwie trzecim. Trybunał Sprawiedliwości wyjaśnił ponadto, że ważność decyzji w sprawie standardowych klauzul umownych zależy od tego, czy przewiduje ona skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony i czy odbywające się na podstawie takich klauzul przekazywanie danych osobowych zostanie w przypadku ich naruszenia lub niemożności ich przestrzegania zawieszone lub zakazane. Trybunał Sprawiedliwości stwierdził, że decyzja 2010/87 wprowadza takie mechanizmy i jest ważna[32].

W kontekście natomiast decyzji wprowadzającej program Tarcza Prywatności warte odnotowania jest, iż rzecznik generalny w swojej opinii podnosił, iż w jego ocenie rozstrzygnięcie przedmiotowego sporu na poziomie krajowym nie wymaga wydania przez Trybunał Sprawiedliwości rozstrzygnięcia w przedmiocie ważności decyzji w sprawie Tarczy Prywatności, skoro spór ten dotyczy wyłącznie ważności decyzji 2010/87[33]. Trybunał Sprawiedliwości uznał jednak, że ograniczenia ochrony danych osobowych, które wynikają z wewnętrznych regulacji prawnych obowiązujących w Stanach Zjednoczonych w zakresie dostępu i wykorzystywania przez organy amerykańskich władz publicznych danych przekazywanych z UE do USA, nie są uregulowane w sposób odpowiadający regulacjom unijnym, w tym w szczególności zasadzie proporcjonalności. Programy nadzoru bowiem funkcjonujące na podstawie regulacji prawnych Stanów Zjednoczonych nie są ograniczone do tego,

31 Opinia rzecznika generalnego w sprawie C-311/18…

32 Wyrok Trybunału Sprawiedliwości z 16 lipca 2020 r. w sprawie C-311/18.

33 Opinia rzecznika generalnego w sprawie C-311/18…

co ściśle konieczne[34]. Trybunał Sprawiedliwości podkreślił ponadto, że regulacje te wprowadzają wymogi, które powinny być przestrzegane przez władze amerykańskie w zakresie dostępu do danych osobowych, jednakże nie przyznają one osobom, których dane są przetwarzane, praw, które mogłyby być egzekwowane wobec władz USA przed sądami. Osoby, których dane są przetwarzane, nie dysponują realnym środkiem odwoławczym, który byłby równoważny temu, który przysługuje im na podstawie prawa unijnego. Ze wszystkich tych powodów Trybunał Sprawiedliwości stwierdził nieważność decyzji 2016/1250.

Nie da się ukryć, że omawiane orzeczenie znacznie komplikuje kwestię dalszego, legalnego przekazywania danych osobowych z Unii Europejskiej do Stanów Zjednoczonych. Wyrok w sprawie Schrems II wywołał sporą niepewność prawną co do dalszej możliwości transferowania danych osobowych z UE do Stanów Zjednoczonych, zwłaszcza wśród podmiotów, których model biznesowy oparty jest na transferze danych osobowych na linii UE–USA. Przede wszystkim unieważniona decyzja w sprawie Tarczy Prywatności nie może stanowić podstawy tego transferu i konieczne jest poszukiwanie innych mechanizmów legalizujących przekazywanie danych poza UE, w tym przede wszystkim na podstawie standardowych klauzul umownych. Przy czym także stosowanie tego mechanizmu nie może następować niejako z automatu i każdorazowo wymaga oceny rzeczywistego realizowania przez importera danych zobowiązań wynikających ze standardowych klauzul umownych, co wprost wynika z treści omawianego wyroku w sprawie Schrems II.

W mojej ocenie więc wyrok ten rodzi daleko idące konsekwencje w zakresie nie tylko przekazywania danych do Stanów Zjednoczonych, lecz ogólnie legalnego transferu danych do państw trzecich. Zwrócić należy uwagę na to, że przedmiotowe orzeczenie zawiera niezwykle istotne wytyczne w zakresie stosowania mechanizmu standardowych klauzul umownych. Z wszystkich tez zawartych w wyroku w sprawie C-311/18 można wyprowadzić wydaje się jeden wspólny wniosek, iż sam fakt zawarcia pomiędzy podmiotami z UE i państwa trzeciego umowy zawierającej w swej treści standardowe klauzule umowne nie legalizuje transferu danych, który będzie odbywać się na podstawie tej umowy.

34 *Ibidem.*

Obowiązkiem podmiotów transferujących dane do państw trzecich jest zweryfikowanie, czy odbiorcy danych osobowych, w świetle obowiązującego ich ustawodawstwa w kraju ich siedziby, są w stanie przestrzegać zobowiązań określonych w standardowych klauzulach umownych. W przypadku gdy taka ocena będzie negatywna, transfer danych powinien być zawieszony lub zakończony, chyba że oparty zostanie na innym mechanizmie transferu wynikającym z rozdziału V RODO.

Reasumując, omawiany wyrok w sprawie Schrems II w praktyce obliguje wszystkie podmioty przekazujące dane osobowe z UE do państw trzecich (nie tylko do Stanów Zjednoczonych, ale do wszystkich państw trzecich, w stosunku do których Komisja Europejska nie wydała decyzji stwierdzającej adekwatny stopień ochrony) do dokonania ponownej oceny legalności takich transferów, w szczególności w kontekście rzeczywistego realizowania przez importera danych zobowiązań wynikających ze standardowych klauzul umownych. Tylko w takim przypadku bowiem transfer danych do państwa trzeciego będzie mógł być uznany za odbywający się w zgodzie z postanowieniami ogólnego rozporządzenia o ochronie danych. Standardowe klauzule umowne mogą być więc mechanizmem legalnego transferu danych do państwa trzeciego wyłącznie wtedy, gdy klauzule te są w rzeczywistości respektowane przez podmiot przetwarzający dane osobowe w określonym państwie trzecim.

Bibliografia

Karwala D., *Krajobraz po wyroku Trybunału Sprawiedliwości w sprawie programu Bezpiecznej Przystani*, „Monitor Prawniczy" 10/2016.

Lubasz D., Witkowska K., *Europejska reforma ochrony danych osobowych z perspektywy pełnomocnika przedsiębiorcy,* [w:] *Media elektroniczne. Współczesne problemy prawne,* red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016.

Lubasz D., *Przekazywanie danych osobowych do państw trzecich w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 20/2016.

Michałowicz A., *Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy Prywatności*, „Monitor Prawniczy" 23/2016.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Legalis 2020.

Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, red. P. Litwiński, Legalis 2020.

Inne akty prawne

Decyzja Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony w Stanach Zjednoczonych, przewidzianej przez zasady ochrony prywatności w ramach tzw. Bezpiecznej przystani (Safe Harbour).

Decyzja wykonawcza Komisji (UE) 2016/1250 z 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.

Decyzja Komisji 2010/87/UE z 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mającym siedzibę w państwach trzecich na podstawie dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, zmienionej decyzją wykonawczą Komisji (UE) 2016/2297 z 16 grudnia 2016 r.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
Karta praw podstawowych Unii Europejskiej.
Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.
Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) z 27 kwietnia 2016 r.
Traktat o funkcjonowaniu Unii Europejskiej.
Traktat o Unii Europejskiej.
Opinia rzecznika generalnego w sprawie C-311/18 Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems.
Privacy Shield List, https://www.privacyshield.gov/list.
Wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez High Court (Irlandia) 9 maja 2018 r. – Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems (sprawa C-311/18).
Wyrok Trybunału Sprawiedliwości z 6 października 2015 r. w sprawie C-362/14.
Wyrok Trybunału Sprawiedliwości z 16 lipca 2020 r. w sprawie C-311/18.