2

Weronika **Dulewicz**

Transfery danych osobowych do USA w świetle decyzji Komisji Europejskiej w sprawie adekwatności programu EU-US Data Privacy Framework

Opiekun naukowy: dr Arleta Nerka

Weronika Dulewicz

Studentka II roku na kierunku Prawo i zarządzanie w biznesie II-go stopnia ze specjalizacją analiza ryzyka w Akademii Leona Koźmińskiego. Wielokrotnie nagrodzona Stypendium Rektora za osiągnięcia w nauce. Laureatka Wyróżnienia Rektora za pracę licencjacką poświęconą ochronie danych osobowych.
Swoje doświadczenia zawodowe zdobywa w Kancelarii Rymarz Zdort Maruta.

DOI: 10.7206/978-83-66502-10-9.top11

Abstrakt

W lipcu 2023 roku Komisja Europejska przyjęła decyzję stwierdzającą odpowiedni stopień ochrony danych w ramach amerykańskiego programu EU-US Data Privacy Framework, umożliwiając tym samym swobodne transfery danych osobowych z Unii Europejskiej do USA w oparciu o tzw. decyzję o adekwatności. Decyzja ta nie dotyczy Stanów Zjednoczonych jako całego państwa, odnosi się jedynie do amerykańskich podmiotów, które – zgodnie z przyjętymi procedurami – przystąpiły do programu EU-US DPF. To już trzecia decyzja unijnego organu w sprawie transferów danych do USA. Jej poprzedniczki – dotyczące programu Safe Harbour oraz Privacy Shield – zostały skutecznie zakwestionowane przez Maximilliana Schremsa kierującego organizacją NOYB, co doprowadziło do ich unieważnienia przez Trybunał Sprawiedliwości UE. Nasuwa się zatem pytanie: „Czy obecnie obowiązującą decyzję ws. adekwatności programu EU-US DPF czeka podobny los?". Celem prezentowanego artykułu jest analiza tejże decyzji pod kątem legalności z perspektywy obowiązujących w UE przepisów o ochronie danych osobowych. Dla realizacji założonego celu w oparciu o metodę formalno-dogmatyczną analizie zostaną poddane kluczowe elementy dotychczasowych i obecnych mechanizmów zapewniających legalność transferów danych osobowych do USA oraz podstawy unieważnienia decyzji w sprawie ich adekwatności. Rozważania dopełni wywiad z ekspertem z obszaru prawa ochrony danych osobowych, w którym zostaną poruszone potencjalne losy transatlantyckich transferów w przyszłości.

Słowa kluczowe: dane osobowe, transfery danych osobowych, decyzja o adekwatności, Unia Europejska, RODO.

Personal data transfers to the US in light of the European Commission's adequacy decision for the EU-US Data Privacy Framework.

Abstract

In July 2023, the European Commission adopted a decision declaring an adequate level of data protection under the US EU-US Data Privacy Framework, thereby allowing the free transfer of personal data from the European Union to the US based on a so-called adequacy decision. The decision does not apply to the US as a whole country, it only applies to US entities that have joined the EU-US DPF programme in accordance with established procedures. This is the third decision by an EU body on data transfers to the US, its predecessors - on Safe Harbour and Privacy Shield - were successfully challenged by Maximillian Schrems heading NOYB, leading to their annulment by the EU Court of Justice. This begs the question, will the current EU-US DPF adequacy decision suffer a similar fate? The aim of the presented article is to analyse this decision from the perspective of legality from the perspective of applicable EU data protection legislation. In order to achieve the stated objective, based on the formal-dogmatic method, the key elements of past and current mechanisms ensuring the legality of transfers of personal data to the USA will be analysed, as well as the grounds for overturning decisions on their adequacy. An interview with an expert in the field of data protection law will round off the considerations, addressing the potential future fate of transatlantic transfers.

Keywords: personal data, personal data transfers, adequacy decision, European Union, GDPR.

DOI: 10.7206/978-83-66502-10-9.top11

Wprowadzenie

Międzynarodowe transfery danych osobowych stają się przedmiotem coraz częstszych dyskusji w kontekście ochrony prywatności osób fizycznych. Na szczególną uwagę zasługują te pomiędzy krajami EOG a Stanami Zjednoczonymi, ponieważ to właśnie tam swoje siedziby posiadają tacy giganci technologiczni jak: Google, Meta Platforms czy Microsoft. Obowiązujące na terenie EOG rozporządzenie o ochronie danych osobowych (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) nakłada na administratorów konkretne obowiązki związane z legalnym przekazywaniem danych do państw trzecich, czyli tych położonych poza Europejskim Obszarem Gospodarczym. Jednym z mechanizmów, który umożliwia swobodny transfer do takiego państwa może być tzw. decyzja o adekwatności. Jest ona swoistym potwierdzeniem Komisji Europejskiej dotyczącym odpowiedniego stopnia ochrony danych istniejącego w państwie trzecim i tym samym stanowi podstawę legalizującą transfer (Karwala, 2018, s. 151).

W przypadku Stanów Zjednoczonych KE wydała dotychczas dwie takie decyzje. Obie z nich odnosiły się jedynie do przyznania odpowiedniego stopnia ochrony danych amerykańskim podmiotom, które przetwarzały dane osobowe zgodnie z zasadami przyjętymi w programie *Safe Harbour* lub (w przypadku drugiej decyzji) jego następcy – programie *Privacy Shield*. Taki stan prawny zdecydowanie ułatwiał przepływ danych osobowych, który, jak wskazano w motywie 101 preambuły RODO, „jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej". Jednakże decyzje dotyczące adekwatności zarówno programu *Safe Harbour*, jak i *Privacy Shield* zostały skutecznie podważone przez działającego na rzecz ochrony prywatności Maximilliana Schremsa, a w konsekwencji unieważnione przez Trybunał Sprawiedliwości Unii Europejskiej. Stwierdzenie nieważności decyzji KE spowodowało, że europejscy administratorzy chcący przeprowadzić taki transfer musieli skorzystać z innych mechanizmów określonych przez RODO, takich jak standardowe klauzule umowne (SCC) lub wiążące reguły korporacyjne (BCR) w obrębie organizacji międzynarodowej (Michałowicz, 2016, s. 1267).

DOI: 10.7206/978-83-66502-10-9.top11

Sytuacja ta zmieniła się jednak, kiedy 10 lipca 2023 r. KE przyjęła decyzję stwierdzającą odpowiedni stopień ochrony danych w ramach programu *EU-U.S. Data Privacy Framework*. Program ten, podobnie jak jego poprzednicy, zakłada możliwość uczestnictwa amerykańskich przedsiębiorstw, które po spełnieniu określonych wymagań mogą korzystać z domniemania o ochronie danych osobowych w europejskich standardach (Marcinkowski, 2020, s. 71). Transfer danych osobowych do takich podmiotów zostaje zrealizowany w oparciu o art. 45 RODO (tzw. decyzję o adekwatności) i nie wymaga stosowania innych mechanizmów ujętych w rozporządzeniu czy też zawarcia umowy transferowej (Karwala, 2023, s. 30). Warto w tym miejscu wspomnieć, że już w dniu wydania tejże decyzji przez KE wypowiedział się o niej Maximillian Schrems, założyciel organizacji None of Your Business (NOYB), deklarując wniesienie wniosku do TSUE.

Celem autorki artykułu jest próba odpowiedzi na istotne pytanie, czy decyzja ta podzieli wkrótce losy swoich poprzedniczek. Przedmiotem niniejszego opracowania jest przeprowadzenie analizy dotyczącej legalności decyzji KE ws. adekwatności programu *EU-U.S. Data Privacy Framework*. W pierwszej części zostaną omówione kluczowe elementy funkcjonowania programów *Safe Harbour* oraz *Privacy Shield*, oraz przyczyny, które doprowadziły do unieważnienia decyzji dotyczących ich adekwatności. Następnie, w ramach oceny potencjalnej przyszłości transatlantyckich transferów danych, analizie zostanie poddana obecnie obowiązująca decyzja KE, przy uwzględnieniu aktualnego kontekstu regulacyjnego UE dotyczącego ochrony danych osobowych oraz dokonanych w ostatnim czasie zmian w prawie amerykańskim. W ostatniej części zostaną zaprezentowane wnioski wynikające z wywiadu przeprowadzonego z r. pr. Piotrem Kaliną, ekspertem z obszaru prawa ochrony danych osobowych. Rozważono potencjalne scenariusze oraz konsekwencje, które mogą dotknąć transfery danych osobowych między UE i USA.

1. Dotychczasowe programy amerykańskie umożliwiające transfery danych osobowych do USA

1.1. Program *Safe Harbour*

W niniejszej części artykułu zostanie przeprowadzona analiza głównych założeń dwóch poprzednich programów umożliwiających transfery danych

DOI: 10.7206/978-83-66502-10-9.top11

osobowych do USA, które nie spełniły europejskich wymogów dotyczących ochrony danych osobowych.

Pierwszym z nich był program *Safe Harbour* – opracowany przez Departament Handlu Stanów Zjednoczonych w porozumieniu z Komisją Europejską i funkcjonujący w latach 2000–2015. Jego celem było umożliwienie podmiotom amerykańskim realizacji wymagań funkcjonującej w tym czasie Dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Zygmunt, 2014, s. 65). Program ten opierał się na procedurze samocertyfikacji, w ramach której amerykańskie przedsiębiorstwa były zobowiązane do przestrzegania szeregu zasad dotyczących przetwarzania danych osobowych. Po dostosowaniu procedur wewnętrznych do tychże wymagań notyfikowały swoje przystąpienie Departamentowi Handlu USA, który prowadził listę podmiotów uczestniczących w *Safe Harbour*. Procedura ta była wielokrotnie oceniana jako mało skuteczna dla ochrony transferowanych danych osobowych (Michałowicz, 2016, s. 1265). Źródłem tych kontrowersji stał się przede wszystkim brak realnych narzędzi w rękach organów nadzoru – Departamentu Handlu USA oraz Federalnej Komisji Handlu, które umożliwiłyby faktyczne egzekwowanie wymagań stawianych w ramach *Safe Harbour*. Doprowadziło to do wielu nieprawidłowości w zakresie stosowania obowiązujących procedur. Stosunkowo niskie zaangażowanie organów nadzoru w działalność podmiotów uczestniczących w programie skutkowało występowaniem wielu naruszeń przepisów, zwłaszcza praw podmiotów danych. Dostrzeżono również konieczność wprowadzenia narzędzi sprawdzających spełnienie warunków programu przed umieszczeniem danej organizacji na liście, co jednoznacznie wskazywało, że dotychczasowy system samocertyfikacji nie spełnił oczekiwań (Zygmunt, 2014, s. 67).

Ponadto w niezależnym raporcie australijskiej firmy Galexia z 2008 r. wskazano, że po dokładnej weryfikacji i usunięciu błędów z listy prowadzonej przez amerykański organ nadzoru na 1597 „aktywnych" uczestników jedynie 1109 z nich faktycznie uczestniczyło w programie. Najbardziej szokujące okazało się, że zgodnie z wynikami raportu tylko 348 organizacji z listy spełniało warunki *Safe Harbour*, a tylko 54 z nich spełniało je dla wszystkich kategorii danych. Stanowi to zaledwie 3% organizacji na liście (Connolly, 2008, s. 7–8).

Jak już wspomniano, program *Safe Harbour* stanowił swego rodzaju zbiór zasad i procedur opierających się na samoregulacyjnym schemacie opracowanym w ramach współpracy pomiędzy Departamentem Handlu USA a Komisją

DOI: 10.7206/978-83-66502-10-9.top11

Europejską. Budzący wątpliwości okazał się jednak sposób opisania tychże zasad, który w ocenie organów ochrony danych osobowych państw UE pozostawiał dość szerokie pole do interpretacji, powodując tym samym liczne ich naruszenia z perspektywy zgodności z unijnymi standardami ochrony danych osobowych. W oficjalnych raportach KE dotyczących *Safe Harbour* z lat 2002 i 2004 zwracano uwagę, że znaczna część podmiotów nie zapewniła odpowiedniej przejrzystości polityk prywatności i nie uwzględniła w nich wszystkich zasad programu lub też uwzględniła je w sposób nieprawidłowy (Karwala, 2016, s. 518).

Z kolei w 2013 r. Edward Snowden, były pracownik amerykańskiej Agencji Bezpieczeństwa Krajowego, opublikował w prasie ściśle tajne informacje służb wywiadowczych USA, zaogniając tym samym krytykę wobec legalności funkcjonowania omawianego programu. Dokumentacja ta wskazywała m.in. na dostęp służb amerykańskich do danych osobowych internatów przetwarzanych w ramach organizacji takich jak Facebook, Microsoft czy Google, które to należały do programu *Safe Harbour* (Karwala, 2016, s. 518), potwierdzając tym samym, „że nie istnieje żadna rzeczywista ochrona danych osobowych przekazywanych z UE do USA" (Ciechomska, 2017, s. 14).

Wobec powyższych wydarzeń M. Schrems zdecydował się na wniesie skargi poddającej w wątpliwość legalność *Safe Harbour*, zwracając uwagę na brak zapewnienia w nim odpowiadającego unijnym standardom poziomu ochrony danych osobowych. Sprawa ta koncentrowała się głównie wokół portalu społecznościowego Facebook, który przetwarzał dane osobowe na swoich serwerach umiejscowionych w Stanach Zjednoczonych, nie przestrzegając jednocześnie wymaganego stopnia ochrony zgodnie z zasadami *Safe Harbour* i narażając je na nieuprawniony dostęp ze strony amerykańskiego wywiadu. Początkowo skarga skierowana została do irlandzkiego organu ochrony danych osobowych (DPC), który ją oddalił. W konsekwencji sprawę przekazano do irlandzkiego Sądu Najwyższego, który skierował do TSUE pytania prejudycjalne dotyczące ważności decyzji KE ws. adekwatności programu *Safe Harbour* w kontekście wątpliwości związanych z zapewnieniem odpowiedniego poziomu ochrony danych osobowych.

Trybunał Sprawiedliwości w wyroku z 6 października 2015 r., C-362/14 (Schrems I), stwierdził nieważność decyzji KE ws. adekwatności programu *Safe Harbour*, wskazując w nim na szereg istotnych kwestii w kontekście międzynarodowych transferów danych osobowych. Zwrócił m.in. uwagę,

DOI: 10.7206/978-83-66502-10-9.top11

że środki stosowane przez państwo trzecie, mające na celu zapewnienie odpowiedniego stopnia ochrony danych osobowych, mogą różnić się od tych przyjętych w UE, jednak w praktyce powinny skutecznie gwarantować równoważną ochronę (TSUE, 2015, pkt 73). Odnosząc się natomiast bezpośrednio do programu *Safe Harbour* wskazano, że „osobom, których dane dotyczą, nie przysługiwała droga prawna administracyjna ani sądowa umożliwiająca im uzyskanie dostępu do dotyczących ich danych i, w odpowiednim przypadku, uzyskania ich sprostowania lub usunięcia" (TSUE, 2015, pkt 90). W wyroku wskazano, że przedmiotowa decyzja KE nie zawiera potwierdzenia istnienia ogólnopaństwowych zasad w USA ograniczających potencjalne ingerencje w prawa podstawowe jednostek, których dane zostały przekazane (TSUE, 2015, pkt 88).

W ocenie organu decyzja skupiała się jedynie na weryfikacji zgodności samego programu *Safe Harbour*. Trybunał podkreślił, że ochrona prawa podstawowego do poszanowania życia prywatnego wymaga, aby wszelkie wyjątki od ochrony danych osobowych i ich ograniczenia były zniwelowane do absolutnie niezbędnego minimum (TSUE, 2015, pkt 92), a amerykańskie uregulowanie pozwalające władzom publicznym na uzyskanie dostępu do treści wiadomości elektronicznych osób, których dane dotyczą należy uznać za jego istotne naruszenie (TSUE, 2015, pkt 94).

Kiedy doszło do unieważnienia decyzji ws. adekwatności programu *Safe Harbour*, amerykańskie przedsiębiorstwa zmuszone były do skorzystania z alternatywnych mechanizmów transferowych zapewniających odpowiedni poziom ochrony danych osobowych. Grupa Robocza art. 29 zwróciła wtedy uwagę na możliwość korzystania z wciąż obowiązujących standardowych klauzul umownych i wiążących reguł korporacyjnych (Ciechomska, 2017, s. 15).

1.2. Program *Privacy Shield*

Po niecałym roku od unieważnienia decyzji ws. *Safe Harbour* dobiegły końca prace nad nowym amerykańskim programem mającym umożliwiać legalny transfer do podmiotów zza Atlantyku. 12 lipca 2016 roku Komisja Europejska przyjęła decyzję ws. adekwatności programu o nazwie *EU-U.S. Privacy Shield*. Tym razem dokładnie oceniono jego zgodność nie tylko z Dyrektywą 95/46/WE, wyrokiem TSUE, lecz także z nieobowiązującym jeszcze rozporządzeniem o ochronie danych osobowych (RODO), dzięki czemu decyzja ws.

DOI: 10.7206/978-83-66502-10-9.top11

programu *Privacy Shield* pozostawała w mocy również po jego wejściu w życie (Ciechomska, 2017, s. 16).

Zasadnicza większość zasad ochrony danych osobowych pozostała niezmieniona w porównaniu z tymi, które obowiązywały w ramach programu *Safe Harbour* (Michałowicz, 2016, s. 1268). Przedsiębiorstwa świadczące usługi na terytorium USA mogły dobrowolnie przystąpić do programu *Privacy Shield* i po przejściu odpowiedniej procedury certyfikacyjnej korzystać z domniemania o zapewnieniu adekwatnego stopnia ochrony danych osobowych. Po wpisaniu podmiotów na listę prowadzoną przez Departament Handlu USA zostały one zobowiązane do stosowania zbioru reguł wynikających z *Privacy Shield*. Warto w tym miejscu dodać, że podmiot uczestniczący musiał informować osoby, których dane dotyczą, m.in. o swoim udziale w programie, rodzajach gromadzonych danych i swoim zobowiązaniu do stosowania zasad w odniesieniu do wszystkich danych osobowych pochodzących z UE (Barta, Kawecki i Litwiński, 2021, art. 45). Ponadto wprowadzono coroczny mechanizm przeglądu działania programu *Privacy Shield* (prowadzony wspólnie przez Departament Handlu USA i KE), m.in. w celu weryfikacji funkcjonowania uczestniczących w nim podmiotów w zgodzie z programowymi zasadami. W przypadku nieodnowienia corocznej certyfikacji lub nieprzestrzegania jego wymogów uczestnik zostawał usunięty z listy (Ciechomska, 2017, s. 16). Departament Handlu USA, poza szeregiem zadań związanych z nadzorem funkcjonowania programu, został zobligowany do rejestru podmiotów, które nie mogą już transferować danych w ramach programu, lecz muszą przestrzegać jego zasad w odniesieniu do danych pozyskanych w okresie ważności certyfikatu (Michałowicz, 2016, s. 1269). W przeciwieństwie do *Safe Harbour* wprowadzono obowiązek informowania jednostek o ich prawie dostępu do danych i niezależnym organie rozstrzygającym spory. Wprowadzono również instytucję Rzecznika ds. *Privacy Shield*, którego zadaniem było rozpatrywanie skarg podmiotów danych dot. ich potencjalnego ujawnienia amerykańskim służbom wywiadowczym. Program *Privacy Shield* zakładał możliwość dochodzenia roszczeń przez osoby, których dane dotyczą, korzystając przy tym z kilku zaproponowanych w nim ścieżek, niewymagających ponoszenia jakichkolwiek kosztów przez podmioty danych. Niniejsza regulacja stanowiła swego rodzaju odpowiedź na krytykę, wysuniętą w wyroku TSUE z 2015 r. W ramach programu *Privacy Shield* sprecyzowano również kwestie dot. integralności danych i celowości oraz wtórnego przekazywania danych osobowych osobom trzecim.

DOI: 10.7206/978-83-66502-10-9.top11

Nie brakowało jednak krytycznych głosów ws. programu *Privacy Shield* i jego faktycznej gwarancji ochrony danych osobowych. Jednym z kluczowych problemów okazał się brak dokładnej analizy amerykańskiego prawodawstwa w obszarze ochrony danych osobowych, która powinna zostać przeprowadzona przez KE przed wydaniem pozytywnej decyzji ws. adekwatności programu *Privacy Shield*, w szczególności w kontekście działalności amerykańskiego wywiadu. Między innymi, pomimo deklaracji Biura Dyrektora Wywiadu Narodowego dotyczących powstrzymywania się od masowego gromadzenia danych, istniała zauważalna luka prawna, która podważa wiarygodność tych zapewnień. Brak skutecznych środków prawnych ograniczała zatem zdolność do nadzorowania i egzekwowania zobowiązań amerykańskich służb w praktyce (Terpan, 2018, s. 1052). Według opinii Grupy Roboczej art. 29 z 2016 r., decyzja KE ws. adekwatności programu nie odzwierciedlała niektórych kluczowych zasady ochrony danych określonych w prawie europejskim, takich jak zasada celowości czy ograniczonego czasu przetwarzania danych. Wielokrotnie podkreślano również braki w skuteczności działania Rzecznika ds. *Privacy Shield* – jego podległość wiceministrowi Departamentu Stanu USA powodowała, że mimo uznania niezależności tego organu w decyzji KE pojawiały się uzasadnione wątpliwości co do faktycznej skuteczności tejże niezależności (Terpan, 2018, s. 1052). Z punktu widzenia praw podmiotów danych oznaczało to ograniczenie możliwości dochodzenia roszczeń.

Program *Privacy Shield* po czterech latach funkcjonowania podzielił losy swojego poprzednika. Maximilian Schrems zwrócił się do irlandzkiego organu nadzorczego (DPC), wskazując, że „prawo i praktyka Stanów Zjednoczonych nie zapewniają wystarczającej ochrony przed dostępem władz publicznych do danych przekazywanych do tego kraju" (TSUE, 2020). Skarga trafiła następnie do irlandzkiego Sądu Najwyższego, który z zwrócił się do TSUE z rozbudowanym pytaniem prejudycjalnym (Kolasiński, 2022, s. 113). Ostatecznie TSUE w wyroku z 16 lipca 2020 r., C 311/18 *(*Schrems II*)* unieważnił decyzję Komisji Europejskiej ws. adekwatności programu *Privacy Shield.*

W wyroku stwierdzono, że przepisy dotyczące nadzoru w USA, mające priorytet w amerykańskim porządku prawnym, znacznie ograniczały wymagany poziom ochrony danych osobowych, powodując tym samym brak możliwości dochodzenia roszczeń przez europejskie podmioty danych (Kredzińska, 2023, s. 150). Trybunał odniósł się również do działalności Rzecznika ds. *Privacy Shield*, wskazując, że fakt jego istnienia nie dawał realnej możliwości

DOI: 10.7206/978-83-66502-10-9.top11

podniesienia środka odwoławczego przed organem oferującym go osobom, których dane są przekazywane do Stanów Zjednoczonych (TSUE, 2020a, pkt 197). Dodał, że choć decyzja KE ws. *Privacy Shield* zawiera „wymogi, które powinny być przestrzegane przez władze amerykańskie przy wdrażaniu odpowiednich programów nadzoru, to nie przyznaje (…) zainteresowanym osobom praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami" (TSUE, 2020).

Wyrok Trybunału znacząco wpłynął na sposób funkcjonowania transatlantyckich transferów danych osobowych. Na czele z technologicznymi gigantami, takimi jak Google, Amazon, ówczesny Facebook czy Twitter, z udogodnień programu *Privacy Shield* korzystało łącznie ponad 5300 amerykańskich przedsiębiorstw (Frymoyer i Reinsch, 2020, s. 1). Aby uniknąć zatem całkowitego zahamowania procesów biznesowych między europejskimi a amerykańskimi podmiotami, Europejska Rada Ochrony Danych i Komisja Europejska udostępniły m.in. zalecenia dotyczące stosowania standardowych klauzul umownych (SCC), które zgodnie z wyrokiem TSUE mogły stanowić jeden z mechanizmów umożliwiających transfer danych do USA (Kredzińska, 2023, s. 151).

2. Zmiany w amerykańskim prawie – *Executive Order* 14086

Po ponad dwóch latach od unieważnienia przez TSUE decyzji Komisji Europejskiej w sprawie adekwatności programu *Privacy Shield* nadszedł czas na kolejne podejście do transatlantyckiego porozumienia w obszarze transferów danych osobowych. W tym celu niezbędne były jednak zmiany w amerykańskim prawie, szczególnie w kontekście działalności służb wywiadowczych (Kalina, 2023, s. 417). To głównie ich szerokie uprawnienia dotyczące przetwarzania danych osobowych Europejczyków były dotychczas najtrudniejszą kwestią transferowego sporu pomiędzy Stanami Zjednoczonym a Unią Europejską. W związku z oczywistą potrzebą zmian prawnych w tym zakresie prezydent USA, Joe Biden, wydał w październiku 2022 r. rozporządzenie wykonawcze w sprawie wzmocnienia zabezpieczeń dla działań wywiadowczych Stanów Zjednoczonych (*Executive Order* 14086).

Jednym z głównych założeń tego rozporządzenia jest zapewnienie prywatności osobom fizycznym, niezależnie od ich obywatelstwa lub miejsca zamieszkania, poprzez ograniczenie działań służb wywiadowczych – pole-

DOI: 10.7206/978-83-66502-10-9.top11

gających na zbieraniu danych osobowych – do niezbędnych, aby zrealizować zatwierdzony cel wywiadowczy. Ponadto wyznaczono niezależny organ rozpatrujący skargi osób fizycznych dotyczące naruszeń ich prywatności przez amerykańskie służby wywiadowcze. Organem tym został urzędnik do spraw ochrony wolności obywatelskich w Biurze Dyrektora Wywiadu Narodowego (CLPO). Przewidziano również organ odwoławczy – Sąd Rewizyjny ds. Ochrony Danych (DPRC). Zgodnie z treścią rozporządzenia sędziowie wchodzący w skład DPRC nie mogą jednocześnie pełnić żadnych oficjalnych obowiązków ani być zatrudnieni w rządzie Stanów Zjednoczonych. Wymaga się od nich natomiast odpowiedniego doświadczenia w dziedzinie prywatności danych i prawa bezpieczeństwa narodowego. Taki system ma zapewnić osobom fizycznym realną możliwość dochodzenia swoich praw w związku z przetwarzaniem ich danych osobowych przez amerykańskie służby wywiadowcze.

3. Decyzja Komisji Europejskiej z 10 lipca 2023 r. stwierdzająca odpowiedni stopień ochrony danych osobowych w USA

Pomimo zastrzeżeń co do rzeczywistego wpływu rozporządzenia wykonawczego 14086 na poprawę poziomu ochrony prywatności w USA, które zgłosiła organizacja NOYB pod przewodnictwem Maximiliana Shremsa, już dwa miesiące później – w grudniu 2022 r. – Komisja Europejska zaprezentowała projekt decyzji stwierdzający odpowiedni stopień ochrony prywatności w ramach nowego programu: *UE – US Data Privacy Framework*.

Europejska Rada Ochrony Danych, oceniając ten projekt w lutym 2023 r., zwróciła uwagę, że choć aktualizacje zasad w programie *Data Privacy Framework* są na ogół pozytywne, wiele z nich pozostaje niezmienionych w porównaniu do poprzednich, zastosowanych w ramach programu *Privacy Shield*. W ocenie organu należy uważniej zweryfikować kwestie dotyczące mechanizmów dochodzenia roszczeń przez osoby fizyczne, wyjątków od prawa dostępu, zastosowania zasad *Data Privacy Framework* do podmiotów przetwarzających oraz definicji kluczowych z punktu widzenia europejskiego prawa ochrony danych. EROD zwróciła również uwagę na potrzebę wprowadzenia szczegółowych przepisów dotyczących zautomatyzowanego podejmowania decyzji oraz konieczność zapewnienia w ramach zasad programu, że ochrona danych osobowych nie zostanie osłabiona w przypadku ich dalszego przeka-

DOI: 10.7206/978-83-66502-10-9.top11

zywania do państw trzecich. W opinii podkreślono także znaczenie efektywnego nadzoru i egzekwowania zasad programu *Data Privacy Framework* przez Federalną Komisję Handlu oraz Departament Transportu USA. EROD zapowiedziała, że planuje dokładnie monitorować te kwestie. W odniesieniu do rozporządzenia wykonawczego 14086 EROD pozytywnie oceniła wprowadzenie pojęcia konieczności i proporcjonalności, a także nowy mechanizm dochodzenia roszczeń przez osoby fizyczne z UE, wskazując na znaczną poprawę w stosunku do poprzednich regulacji prawnych. Zaznaczyła jednak, że niektóre elementy nowych ram prawnych wciąż wymagają doprecyzowania, aby w pełni zagwarantować odpowiedni stopień ochrony danych osobowych przekazywanych do USA. EROD zaleciła zatem Komisji, aby doprecyzowała projekt decyzji w celu wzmocnienia jego podstaw i zapewnienia skutecznego monitorowania wdrażania nowych ram prawnych w przyszłości (EROD, 2023, s. 2–6).

Eksperci w dziedzinie ochrony danych spodziewali się, że decyzja Komisji Europejskiej w sprawie adekwatności programu *Data Privacy Framework* zostanie opublikowana dopiero pod koniec 2023 r., nastąpiło to jednak znacznie wcześniej – już 10 lipca 2023 roku. Można zatem pokusić się o stwierdzenie, że było to wynikiem narastających nacisków na szybkie wprowadzenie mechanizmu, który ponownie usprawni międzynarodową współpracę biznesową krajów europejskich z USA. Było to kluczowe z punktu widzenia amerykańskich przedsiębiorców, którzy liczyli na znaczne przyspieszenie wielu procesów biznesowych, ale także przedsiębiorców europejskich, korzystających w codziennej pracy z narzędzi amerykańskich dostawców.

W ramach decyzji Komisja Europejska wskazała cztery kluczowe artykuły. Przede wszystkim, zgodnie z art. 1, „do celów art. 45 rozporządzenia (UE) 2016/679 Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych, które są wymienione w »wykazie DPF« prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych". Ponadto, w kontekście działalności służb wywiadowczych, państwa członkowskie UE zostały wraz z Komisją zobowiązane do tego, aby wzajemnie informować się o wszelkich przesłankach wskazujących na ingerencję amerykańskich organów publicznych w prawa osób fizycznych do ochrony ich danych osobowych, która wykraczałaby poza granice niezbędności i proporcjonalności (art. 3 ust. 3). Takie samo zobowiązanie dotyczy jakiegokolwiek podejrzenia, że organy USA,

DOI: 10.7206/978-83-66502-10-9.top11

które mają ustawowe uprawnienia do egzekwowania zasad programu *Data Privacy Framework*, nie wdrożyły skutecznych mechanizmów wykrywania i nadzoru pozwalających na identyfikowanie potencjalnych naruszeń ochrony danych osobowych w praktyce (art. 3 ust. 2). Warto również wspomnieć, że Komisja Europejska (już po roku od dnia wejścia decyzji w życie) zobowiązana jest przeprowadzić przegląd stosowania ram prawnych, które są przedmiotem tej decyzji – takich jak warunki dalszego przekazywania danych, wykonywanie praw indywidualnych oraz uzyskiwanie przez organy publiczne USA dostępu do przekazywanych danych – aby ustalić, czy Stany Zjednoczone nadal zapewniają odpowiedni stopień ochrony danych (art. 3 ust 1 i 4). Kluczowe w tym kontekście zdają się zatem aktywność strony amerykańskiej oraz potencjalne dalsze zmiany w przepisach dotyczących bezpieczeństwa narodowego i działalności wywiadu USA (Kalina, 2023, s. 426).

4. Program *Data Privacy Framework*

Jak już wspomniano, zgodnie z decyzją Komisji Europejskiej dopuszczalność transferu danych nie dotyczy Stanów Zjednoczonych jako całego państwa, lecz ogranicza się do podmiotów, które aktywnie uczestniczą w programie *Data Privacy Framework*. Udział w tym programie wymaga od amerykańskich organizacji przejścia przez proces samocertyfikacji, aby znaleźć się na publicznie dostępnej liście prowadzonej przez Departament Handlu USA. Samocertyfikacja – analogicznie do procedury stosowanej w ramach poprzedniego programu, czyli *Privacy Shield* – polega na samodzielnym dostosowaniu działalności podmiotu do wymagań programu. Po osiągnięciu pełnej zgodności z wymogami organizacja musi opublikować na swoich stronach internetowych odpowiednie polityki prywatności, jak również pisemne zobowiązanie do przestrzegania zasad programu. W kolejnym kroku może zawnioskować do Departamentu Handlu USA o wpisanie na listę *Data Privacy Framework*, określając zakres danych osobowych, które podlegają przetwarzaniu. Uczestnicy programu są również zobowiązani do informowania o swojej podległości wobec amerykańskich organów publicznych w zakresie ich uprawnień dochodzeniowych, wykonawczych lub wymogów dotyczących ujawniania danych osobowych w celu zapewnienia bezpieczeństwa narodowego USA (Kalina, 2023, s. 425).

Departament Handlu USA, poza prowadzeniem listy certyfikowanych podmiotów, odpowiada za weryfikację zgodności organizacji z zasadami pro-

DOI: 10.7206/978-83-66502-10-9.top11

gramu, a w przypadku stwierdzenia naruszeń ma prawo usunąć dany podmiot z listy – podmiot ten ma wówczas obowiązek usunąć wszelkie oświadczenia i informacje, które sugerowałyby jego dalsze uczestnictwo w programie *Data Privacy Framework*. Zobowiązany jest również do usunięcia lub zwrócenia wszelkich danych otrzymanych od europejskich partnerów w czasie swojej przynależności do programu (Karwala, 2023, s. 29). Transfer danych osobowych z Unii Europejskiej do USA w ramach Data Privacy Framework jest zatem możliwy po weryfikacji aktualności decyzji KE oraz potwierdzeniu, że wybrany podmiot znajduje się na liście Departamentu Handlu USA, a zakres danych objętych transferem jest częścią samocertyfikacji danego podmiotu. „Jeżeli okaże się, że potencjalny odbiorca danych ze Stanów Zjednoczonych nie znajduje się na liście, to przekazywanie do niego danych osobowych z Unii musi mieć inną podstawę prawną niż art. 45 RODO. W takich przypadkach wymagane jest zastosowanie mechanizmów legalizujących transfer z art. 46 RODO lub oparcie się na wyjątkach z art. 49 RODO" (Kalina, 2023, s. 425). Warto również zauważyć, że podmioty wcześniej zarejestrowane w ramach programu *Privacy Shield* otrzymały trzymiesięczny okres na dostosowanie się do nowych wymagań, a proces dołączenia do listy *Data Privacy Framework* został dla nich uproszczony. Takie rozwiązanie potwierdza istotne podobieństwa między obecnie obowiązującym programem a jego poprzednikiem. Jednocześnie nowy program wydaje się wprowadzać pewne udoskonalenia i dostosowania do europejskich standardów ochrony danych osobowych, zwiększając tym samym swoje szanse na przetrwanie.

5. Dalsze losy transferów danych osobowych do USA – wywiad z r. pr. Piotrem Kaliną

W ramach podsumowania niniejszego artykułu przeprowadzono wywiad z r. pr. Piotrem Kaliną specjalizującym się w ochronie danych osobowych. W wywiadzie oceniono perspektywy dotyczące wpływu decyzji KE na poziom ochrony danych osobowych w USA oraz wskazano pozytywne i negatywne aspekty programu *Data Privacy Framework*.

Pytanie 1: Jak z eksperckiego punktu widzenia ocenia Pan program *Data Privacy Framework*? Jakie pozytywne zmiany wprowadzono względem poprzedniego programu?

DOI: 10.7206/978-83-66502-10-9.top11

Administracja USA wprowadziła zmiany, które były oczekiwane, aby poprawić stopień odpowiedniości amerykańskiego prawa w rozumieniu rozdziału V RODO. Nie oceniam ich w tym miejscu, jest jednak kilka istotnych różnic wynikających ze zmian w prawie USA oraz z zasad Data Privacy Framework (dalej: „DPF"), *które sprawiają wrażenie naprawy dotychczasowych luk prawnych. Przede wszystkim należy zwrócić uwagę, że zasady DPF zostały napisane, a decyzja Komisji Europejskiej w sprawie DPF podjęta już w trakcie obowiązywania przepisów RODO (po 2018 r.) oraz na podstawie licznych doświadczeń i zagadnień prawnych szczegółowo omówionych przed sądami Unii i TSUE. Już sama ta okoliczność pozwala przyjąć, że założenia programu DPF powinny uwzględniać obowiązujące w Unii standardy ochrony prywatności. Pozytywnym elementem jest również zobowiązanie do przeglądu decyzji KE w sprawie DPF w ustalonych okresach – pierwszy przegląd ma odbyć się już w 2024 roku. Ponadto w prawie amerykańskim pojawiło się pojęcie „proporcjonalności" środków stosowanych w celu zapewnienia obronności USA i bezpieczeństwa narodowego. Niezależnie od zarzutów dotyczących sposobu interpretacji tego pojęcia, które są związane z jego odmiennym rozumieniem w systemie prawnym USA, jest to oczekiwany krok oraz szansa na ukształtowanie orzecznictwa i doktryny USA w sposób zgodny z linią przyjętą w Unii. Korzystne w założeniach jest wprowadzenie dwupoziomowej ścieżki dochodzenia odszkodowania w przypadku uznania przez obywateli Unii, że wywiad USA zebrał ich dane w sposób naruszający obowiązujące prawo Stanów Zjednoczonych. Druga instancja w takim postępowaniu to nowo wprowadzony Sąd Rewizyjny ds. Ochrony Danych (DPRC). Nowością jest wprowadzenie pełnomocnika do reprezentowana przed Sądem Rewizyjnym ds. Ochrony Danych w postaci adwokata, który będzie bronił interesu skarżącego w danej sprawie. W dodatku na służby wywiadowcze nałożono obowiązek dostosowania procedur i działań do nowego porządku prawnego, a prezydent USA wezwał Radę Nadzoru do spraw Prywatności i Swobód Obywatelskich do corocznego przeglądu procesu dochodzenia roszczeń z tytułu naruszenia przepisów przez służby wywiadowcze USA, w tym zastosowania się przez wywiad do decyzji sądu I i II instancji. Choć jest to kropla w morzu potrzeb i nie znamy na tym etapie skuteczności wprowadzonych rozwiązań ze względu na krótki czas ich obowiązywania, to należy pozytywnie ocenić starania w kierunku zwiększenia poziomu ochrony danych obywateli Unii w USA.*

DOI: 10.7206/978-83-66502-10-9.top11

Pytanie 2: Jak decyzja Komisji Europejskiej ws. programu *Data Privacy Framework* wpłynie na dynamikę współpracy między organami regulacyjnymi w USA i UE?

Ta dynamika była obserwowana w 2022 r., kiedy została zawarta umowa pomiędzy UE i USA, administracje unijna i amerykańska publikowały liczne oświadczenia oraz deklaracje, a proces stanowienia prawa w Stanach Zjednoczonych przyspieszył. Obecnie, tj. po uchwaleniu decyzji KE w sprawie DPF, nie ma w mojej ocenie społecznej ani politycznej potrzeby publicznego okazywania dowodów tej współpracy, gdyż cel obu stron został osiągnięty. Nie oznacza to, że współpraca nie będzie się odbywać. Jest ona konieczna chociażby w celu zapewnienia możliwości dochodzenia praw przez obywateli UE, którzy muszą najpierw zgłosić się do odpowiedniego organu nadzorczego w Unii, a dopiero on przekaże sprawę do właściwych instytucji amerykańskich. Co więcej, wprowadzono mechanizmy weryfikacji i kontroli wdrożonych rozwiązań, które również będą wymagać współpracy obu administracji i omawiania potrzeb wprowadzenia ewentualnych zmian. Zakładam jednak, że w najbliższych latach będzie to bardziej współpraca na poziomie administracyjno-formalnym niż na poziomie politycznym, tak jak przed uruchomieniem programu DPF.

Pytanie 3: Z jakimi zarzutami może spotkać się decyzja Komisji Europejskiej ws. programu *Data Privacy Framework*?

Od momentu wydania Executive Order przez prezydenta USA oraz opublikowania projektu decyzji KE w sprawie DPF pojawiają się głosy krytyczne wobec założeń tej regulacji. Przede wszystkim wskazuje się na proste powielenie w większości postanowień poprzedniego programu Privacy Shield. Skoro nowy program Data Privacy Framework w swej istocie nie różni się wiele od programu wprowadzonego na podstawie decyzji wydanej w oparciu o art. 45 RODO, której nieważność stwierdził TSUE, to znaczy, że nowa decyzja KE jest obarczona tymi samymi wadami i nie powinna zostać przyjęta. Cały czas problemem pozostaje nadrzędność prawa USA wobec odbiorców danych w USA wobec programu DPF. Jeżeli na podstawie przepisów prawa USA podmiot zostanie zobowiązany do ujawnienia przetwarzanych przez niego danych obywateli Unii, to nakaz ten będzie miał pierwszeństwo i podlegający

DOI: 10.7206/978-83-66502-10-9.top11

mu podmiot z USA nie będzie mógł o tym poinformować osób, których dane dotyczą, ani administratora danych (problem „if applicable"). Kolejny zarzut może bazować na założeniach, że proces dochodzenia roszczeń związanych z naruszeniem praw i wolności obywateli Unii jest utrudniony i nadal nie mają oni zagwarantowanego prawa do sądu w rozumieniu art. 47 Karty Praw Podstawowych. Instytucje powołane do rozpatrywania naruszenia zasad DPF nie są sądem w rozumieniu tych przepisów, a ich niezależność jest iluzoryczna. Ponadto zadeklarowany w zmienionych amerykańskich przepisach nadzór nad działalnością służb wywiadowczych USA jest odbierany jako istniejący wyłącznie na papierze. W związku z tym podnosi się, że zagrożenia wynikające z takich programów nadzoru jak PRISM nie zmienią się i nadal pozostają takim samym ryzykiem jak przedtem. Istnieje szereg argumentów natury formalnej, spośród których najbardziej wyraźnym jest spór o interpretację pojęcia proporcjonalności. Europejscy prawnicy podnoszą, że to pojęcie zostało wprowadzone do prawa USA wyłącznie na potrzeby uchwalenia nowej decyzji KE o adekwatności, jednak jego interpretacja nie jest i nie będzie taka jak w prawie Unii. Oznacza to, że obywatele Unii nadal są narażeni na podejmowanie przez służby USA działań w celu zapewnienia obronności państwa, które nie są proporcjonalne i prowadzą do naruszenia prywatności oraz innych praw podstawowych. Nie sposób omówić wszystkich zarzutów w ramach krótkiego podsumowania. Jestem jednak przekonany, że to kwestia czasu, kiedy zobaczymy kompleksowe podsumowanie niezgodności nowego programu DPF z przepisami prawa Unii przygotowane przez NOYB.

Pytanie 4: Jakie są szanse, że pomimo zapowiedzianej już skargi ze strony NOYB decyzja ws. programu *Data Privacy Framework* nie zostanie uchylona? Co może o tym przeważyć?

Determinacja związana z utrzymaniem w mocy decyzji o adekwatności prawa USA na podstawie art. 45 RODO znajduje się obecnie na bardzo wysokim poziomie. Dowodem tego może być choćby oddalenie wniosków francuskiego prawnika Philippe'a Latombe'a przez Prezesa Trybunału Sprawiedliwości Unii Europejskiej w sprawie T-553/23 R Philippe Latombe przeciwko Komisji Europejskiej z dnia 12 października 2023 r. Latombe już 6 września 2023 r., po niecałych dwóch miesiącach obowiązywania decyzji KE w sprawie DPF,

DOI: 10.7206/978-83-66502-10-9.top11

wniósł o stwierdzenie nieważności jej art. 1 i 2. Dodatkowym pismem dwa dni później wniósł o zastosowanie środków tymczasowych w postaci zawieszenia wykonania zaskarżonej decyzji. Prezes TSUE oddalił ten wniosek, argumentując, że skarżący nie wykazał, by zastosowanie środków tymczasowych miało pilny charakter oraz że w przypadku braku zawieszenia wykonania zaskarżonej decyzji poniósłby poważną i nieodwracalna szkodę. Znane są liczne sprawy, gdy odmawiano obywatelom Unii legitymacji procesowej przed TSUE. Można więc zakładać, że stwierdzenie nieważności decyzji KE z 10.07.2023 r. w sprawie Data Privacy Framework nie będzie łatwe, niemniej na pewno próby takie będą podejmowane. Organizacje pozarządowe podnoszą liczne argumenty ujawniające ich zdaniem jedynie fasadowy charakter gwarancji dawanych przez zmienione prawo USA oraz brak odpowiedniej ochrony praw i wolności obywateli Unii przy przekazywaniu danych osobowych do Stanów Zjednoczonych.

Podsumowanie

Program *Data Privacy Framework* wiąże się z szeregiem wyzwań, które mogą podważyć jego skuteczność i adekwatność w kontekście potrzeb ochrony danych osobowych w Unii Europejskiej. Istotne obawy dotyczą między innymi działalności służb wywiadowczych Stanów Zjednoczonych, efektywności dostępnych środków odwoławczych dla osób, których dane podlegają przetwarzaniu, oraz stabilności mechanizmów nadzorczych gwarantujących przestrzeganie zasad ochrony prywatności. Analiza założeń programu *Data Privacy Framework* oraz zmian dokonanych w amerykańskim prawie wskazuje, że choć stanowią one znaczący postęp w porównaniu do poprzednich rozwiązań, to wciąż wymagają wielu modyfikacji. Wprowadzone zmiany, choć na pierwszy rzut oka wydają się krokiem w dobrym kierunku, mają charakter bardziej powierzchowny niż realny, co potwierdza konieczność przeprowadzenia daleko idących i bardziej istotnych zmian strukturalnych.

Ostatecznie sukces programu *Data Privacy Framework* będzie zależał od jego zdolności do zapewnienia ochrony danych osobowych adekwatnej względem unijnych standardów. Aktualne przeszkody wskazują na konieczność dokonania zmian, które odpowiedzą na pojawiające się już teraz zarzuty organizacji pozarządowych i ekspertów stojących na straży ochrony prywat-

DOI: 10.7206/978-83-66502-10-9.top11

ności Europejczyków. W tej sytuacji potencjalnym rozwiązaniem zdaje się odejście od dotychczasowej formy kształtowania zasad programów, które mają zapewnić ich uczestnikom zza Atlantyku adekwatność na gruncie art. 45 RODO, lub znaczna reforma amerykańskiego prawa w tym zakresie. Nie sposób nie zgodzić się, że idealnym wyjściem byłoby uzyskanie przez Stany Zjednoczone decyzji o adekwatności względem całego państwa – niestety, obecnie zdaje się to niemożliwe do osiągnięcia.

Bibliografia

Biden, J.R. (2022). Rozporządzenie wykonawcze (EO) 14086. Pozyskano z: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (dostęp: 4.12.2023).

Ciechomska, M. (2017). Tarcza prywatności UE-USA (EU-U.S. Privacy Shield) – nowy instrument transatlantyckiej wymiany danych osobowych. *Europejski Przegląd Sądowy*, 3.

Connolly, C. (2008). *The US Safe Harbor – Fact or Fiction?* Pozyskano z: https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (dostęp: 2.11.2023).

Europejska Rada Ochrony Danych. (2023). *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.* Pozyskano z: https://edpb.europa.eu/system/files/2023–02/edpb_opinion52023_eu-us_dpf_en.pdf (dostęp: 4.10.2023).

Karwala, D. (2016). Krajobraz po wyroku Trybunału Sprawiedliwości w sprawie programu Bezpiecznej Przystani. *Monitor Prawniczy*, *10*.

Karwala, D. (2018). *Komercyjne transfery danych osobowych do państw trzecich.* Warszawa: C.H. Beck.

Karwala, D. (2023). Decyzja Komisji w sprawie adekwatności Ram ochrony danych UE-USA. *Magazyn ODO*, *25*.

Kalina, P. (2023). *Transfery danych osobowych do USA.* W: M. Sakowska-Baryła (red.), *Transfery danych osobowych na podstawie RODO.* Warszawa: Wolters Kluwer Polska.

Kolasiński, M. (2022). Nieważność tarczy prywatności a ewolucja prawa antymonopolowego i regulacji sektorowej rynków cyfrowych – glosa do wyroku Trybunału Sprawiedliwości z 16.07.2020 r., C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi. *Glosa*, *4*, 112–120.

DOI: 10.7206/978-83-66502-10-9.top11

Komisja Europejska. (2023). *Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych UE-USA.* Pozyskano z: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32023D1795 (dostęp: 10.11.2023).

Kredzińska, A. (2023). Transfer danych osobowych z Unii Europejskiej do Stanów Zjednoczonych. Wpływ decyzji Schrems II. *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, *1–2*, 141–167. https://doi.org/10.52097/eppism.8657

Litwiński, P. (red.), Barta, P., Kawecki, M. (2021). *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).* W: P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe.* Warszawa: Wolters Kluwer Polska.

Marcinkowski, B. (2020). Przekazywanie danych osobowych do państw trzecich. Ramy prawne i praktyka w świetle wyroków Schrems I i Schrems II. *Monitor Prawniczy*, *23*.

Marcinkowski, B. (2021). *Standardowe klauzule umowne a globalne transfery danych. Czy środki kontraktowe ochronią prywatność w dobie międzynarodowego kryzysu zaufania? Monitor Prawniczy*, *23*.

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

Reinsch, W., Frymoyer, I. (2023). *Transatlantic Data Flows: Permanently Broken or Temporarily Fractured?* Pozyskano z: https://www.csis.org/ analysis/transatlantic--data-flows-permanently-broken-or-temporarily-fractured (dostęp: 10.12.2023).

Terpan, F. (2018). *„Invalidator" strikes back: The harbour never been safe. Computer Law & Security Review*. Pozyskano z: https://www.europeanpapers.eu/es/system/files/pdf_version/EP_eJ_2018_3_3_Articles_Fabien_Terpan_00261.pdf (dostęp: 6.12.2023).

Trybunał Sprawiedliwości Unii Europejskiej. (2020). *Wyrok w sprawie C-311/18 Data Protection Commissioner/ Maximillian Schrems i Facebook Ireland.* Komunikat prasowy nr 91/20, Luksemburg, 16 lipca 2020 r. Pozyskano z: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020–07/cp200091pl.pdf (dostęp: 5.12.2023).

Trybunał Sprawiedliwości Unii Europejskiej. (2023). *Wyrok w sprawie C-311/18 Data Protection Commissioner / Maximillian Schrems i Facebook Ireland.* Pozyskano z: https://curia.europa.eu/juris/document/document.jsf?text= &docid=278542&pa-

DOI: 10.7206/978-83-66502-10-9.top11

geIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=225583 (dostęp: 12.11.2023).

Zygmunt, J. (2014). Program Safe Harbour – pomost między europejskim a amerykańskim systemem ochrony danych osobowych. *Adam Mickiewicz University Law Review*, *3*, 55–70.

DOI: 10.7206/978-83-66502-10-9.top11