Folia Iuridica Universitatis Wratislaviensis
2016, vol. 5 (1), 85–100

Monika Szczotkowska
*Uniwersytet Wrocławski*

# Regulacje prawne transferu danych osobowych obywateli UE do USA – prawnoporównawcza analiza programu Safe Harbour i programu Privacy Shield

## Regulations on transfer of personal data of EU citizens to the US - comparative law analysis of the Safe Harbour and Privacy Shield programs

**Streszczenie**

W dzisiejszych czasach możemy zaobserwować zjawisko wzrostu wartości informacji, w szczególności dla rozwoju handlu. Rodzajem informacji są także dane osobowe, których potrzebę ochrony dostrzegają niemal wszystkie współczesne kraje. Wobec ich znaczenia dla rozwoju gospodarki i międzynarodowej wymiany handlowej oraz związanej z tym konieczności transferu czy wymiany tego rodzaju informacji konieczne było stworzenie mechanizmów zapewniających ich ochronę. Jednocześnie różnice w zasadach ochrony danych osobowych praktykowane przez poszczególne ustawodawstwa powodują, że mechanizmy ochronne o zasięgu lokalnym – tylko w obrębie danego państwa, a nawet związków państw czy ich organizacji – nie są wystarczające. Przykładem takiego zjawiska jest powszechny obecnie problem transferu danych osobowych z UE do USA. W niniejszym artykule autorka przedstawi uregulowania prawne przesyłu danych osobowych obywateli UE do USA, problemy związane z transferem danych osobowych pomiędzy UE–USA oraz dotychczas wypracowane porozumienia dotyczące przesyłu danych (*Safe Harbour* i *Privacy Shield*), a ponadto wskaże ich różnice i mankamenty.

Stworzenie aktu zapewniającego jednolitą ochronę danych osobowych na terytorium UE i USA utrudnia przede wszystkim kierowanie się przez UE i USA innymi zasadami w kwestii ochrony danych osobowych.

**Słowa kluczowe:**

dane osobowe, ochrona danych osobowych, administrator danych osobowych, Privacy Shield i Safe Harbour

**Abstract**

Nowadays, the value of information increases, in particular in the development of trade. Personal data are also a kind of information protected by almost all modern countries. Given their importance for the economic development and international trade, and the resulting necessity to transfer or exchange such information, it was important to create mechanisms ensuring their protection. Simultaneously, differences in the principles of personal data protection as practised by different laws mean that protective mechanisms implemented by countries and even unions of countries or their organizations are not sufficient. An example of this is the problem of transfer of personal data from the EU to the US. In this article, the author presents the legislation regulating the transfer of personal data of EU citizens

to the United States, the associated problems and the programs of personal data transfer (Safe Harbour and Privacy Shield), indicating the differences between them and their shortcomings.

Creating a proper act providing uniform protection of personal data within the EU and the US is primarily hindered by the fact that the EU and US data protection systems are guided by different principles.

**Key words:**
data protection, Safe Harbour, Privacy Shield, comparison of legal systems, transfer of personal data

## Wstęp

W dzisiejszych czasach możemy zaobserwować zjawisko wzrostu wartości informacji, w szczególności ma to znaczenie dla rozwoju handlu. Rodzajem informacji są także dane osobowe, których potrzebę ochrony dostrzegają niemal wszystkie współczesne kraje. Wobec ich znaczenia dla rozwoju gospodarki i międzynarodowej wymiany handlowej oraz związanej z tym konieczności transferu czy wymiany tego rodzaju informacji konieczne było stworzenie mechanizmów zapewniających ich ochronę. Jednocześnie różnice w zasadach ochrony danych osobowych praktykowane przez poszczególne ustawodawstwa powodują, że mechanizmy ochronne o zasięgu lokalnym – tylko w obrębie danego państwa, a nawet związków państw czy ich organizacji – nie są wystarczające. Przykładem takiego zjawiska jest powszechny obecnie problem transferu danych osobowych z UE do USA. W niniejszym artykule autorka przedstawi uregulowania prawne przesyłu danych osobowych obywateli UE do USA, problemy związane z transferem danych osobowych pomiędzy UE–USA oraz dotychczas wypracowane porozumienia dotyczące przesyłu danych (*Safe Harbour* i *Privacy Shield*), a ponadto wskaże ich różnice i mankamenty.

Stworzenie aktu zapewniającego jednolitą ochronę danych osobowych na terytorium UE i USA utrudnia przede wszystkim kierowanie się przez UE i USA innymi zasadami w kwestii ochrony danych osobowych.

## 1. Zasady ochrony danych osobowych w Unii Europejskiej

Dnia 24 października 1995 r. przez Parlament Europejski i Radę Unii Europejskiej przyjęta została dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[1] (dalej: Dyrektywa). Powodem uchwalenia Dyrektywy była wzrastająca rola przepływu, w ramach swobód wspólnotowych, informacji, w tym danych osobowych obywateli Unii Europej-

[1] Dz. U. WE L 281/31 z 23.11.1995.

skiej. Zaczęto również dostrzegać, że postęp technologii informacyjnych powoduje, że przetwarzanie i wymiana danych osobowych pomiędzy państwami członkowskimi są coraz łatwiejsze[2], a co za tym idzie kontrola procesów przetwarzania danych staje się coraz trudniejsza. Wobec powyższego, ze względu na zapewnienie należytej ochrony danych osobowych konieczne okazało się ujednolicenie regulacji dotyczących transferu i ochrony danych osobowych na poziomie wspólnotowym.

W związku z tym państwa członkowskie zostały zobowiązane do zapewnienia należytej ochrony podstawowych praw i wolności osób fizycznych, w szczególności w zakresie przetwarzania danych osobowych. Do podstawowych zasad europejskiego prawa ochrony danych osobowych należą: zasada przetwarzania danych zgodnie z prawem (art. 6 ust. 1 lit. a i b Dyrektywy); zasada określenia i ograniczenia celu przetwarzania danych (art. 6 ust. 1 lit. b Dyrektywy); zasada stosowności i prawidłowości danych (art. 6 ust. 1 lit. ci d Dyrektywy); zasada rzetelnego przetwarzania danych (art. 6 ust. 1 lit. a i b Dyrektywy); zasada przechowywania danych przez ograniczony czas (art. 6 ust. 1 lit. e Dyrektywy); oraz zasada rozliczalności administratora danych (art. 6 ust. 2 Dyrektywy)[3]. Skuteczność regulacji jest zapewniona przez przyznanie osobom fizycznym roszczeń odszkodowawczych za niezgodne z prawem przetwarzanie ich danych osobowych, a także przez przyznanie organom administracji publicznej kompetencji nadzorczych w stosunku do przetwarzania danych przez administratorów danych. Do najważniejszych praw osób, których dotyczy przetwarzanie, należy zaliczyć: prawo do informacji o sposobie, celu i podmiocie przetwarzającym dane (art. 10 Dyrektywy) oraz źródle pozyskania danych (art. 11 Dyrektywy), prawo dostępu do tych danych (art. 12 Dyrektywy), prawo sprzeciwu do co przetwarzanych danych (art. 13 Dyrektywy), prawo dochodzenia odpowiedzialności administratora danych za przetwarzanie danych w sposób niezgodny z prawem (art. 23 ust. 1 Dyrektywy). Przyznanie tych uprawnień sprawia, że przewidziana prawem ochrona danych ma wymiar rzeczywisty i realny.

Przepływ danych pomiędzy państwami członkowskimi w ramach swobód wspólnotowych jest wolny od jakichkolwiek ograniczeń właśnie dzięki wprowadzeniu jednolitych regulacji w zakresie ochrony danych osobowych.

## 2. Ogólne zasady transferu danych osobowych obywateli UE do państw trzecich

Mając na względzie coraz częstsze przypadki wykorzystywania danych osobowych do celów związanych z działalnością gospodarczą oraz postępującą globalizację handlu,

[2] Zob. pkt 4 preambuły Dyrektywy.

[3] *Podręcznik europejskiego prawa o ochronie danych*, Agencja Praw Podstawowych Unii Europejskiej, Rada Europy, Luksemburg 2014, s. 65–66.

w Dyrektywie uregulowana została również kwestia przekazywania danych osobowych do podmiotów z państw trzecich. Transfer danych osobowych do krajów nienależących do UE co do zasady jest nieograniczony jedynie w sytuacjach, gdy państwo trzecie zapewnia adekwatny stopień ochrony danych osobowych. Brak zapewnienia przez państwo trzecie poziomu ochrony odpowiadającego co najmniej ochronie wynikającej z Dyrektywy wprawdzie nie jest równoznaczne z całkowitym zablokowaniem przepływu danych, ale uzależnia go od spełnienia dodatkowych przesłanek, przez co znacznie utrudnia transfer.

## 3. Transfer do państw o odpowiednim (adekwatnym) poziomie ochrony

Zgodnie z art. 25 dyrektywy przekazywanie do państwa trzeciego danych osobowych powinno nastąpić tylko wówczas, gdy (niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów Dyrektywy) dane państwo trzecie zapewni tzw. odpowiedni stopień ochrony (*adequate level of protection*). Z jednej strony Dyrektywa nie reguluje sposobu weryfikacji poziomu ochrony przetwarzania danych osobowych przez państwo trzecie, z drugiej jednak strony w jej art. 25 ust. 2 zostały wskazane pewne wytyczne, w oparciu o które powinna być dokonana ocena adekwatnego poziomu ochrony w państwie docelowego portu transferu danych. I tak adekwatny stopień ochrony powinien być oceniany w oparciu o wszystkie okoliczności dotyczące operacji przekazania danych lub zbioru takich operacji ze szczególnym uwzględnieniem: charakteru danych, celu i czasu trwania proponowanych operacji przetwarzania danych, kraju pochodzenia i kraju ostatecznego przeznaczenia, ogólnych i branżowych przepisów prawa obowiązujących w państwie trzecim oraz przepisów zawodowych i środków bezpieczeństwa stosowanych w tym państwie. Tak rozbudowana dyspozycja miała na celu zapewnienie możliwie najdokładniejszej weryfikacji regulacji ochrony danych osobowych w państwie trzecim. Zapewnienie przez państwo trzecie adekwatnego poziomu ochrony danych powoduje, że transfer danych do państwa trzeciego wolny jest od ograniczeń.

W zakresie oceny odpowiedniego poziomu ochrony danych osobowych gwarantowanego przez państwo trzecie art. 25 ust. 6 Dyrektywy przewiduje pewne kompetencje Komisji Europejskiej (dalej: Komisja). Zgodnie z ww. przepisem Komisja po analizie prawa krajowego oraz zobowiązań międzynarodowych, jakie przyjęło państwo trzecie, może stwierdzić, że dane państwo zapewnia prawidłowy stopień ochrony w zakresie ochrony danych osobowych osób fizycznych. Decyzja Komisji uznająca państwo trzecie za spełniające wymagania Dyrektywy zwalnia państwa członkowskie z konieczności przeprowadzania dodatkowej kontroli. Za kraje zapewniające adekwatny poziom ochrony danych uznane zostały: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Wy-

spa Man, Izrael, Jersey, Nowa Zelandia, Szwajcaria i Urugwaj[4]. W odniesieniu do niektórych państw trzecich Komisja wydała decyzje o adekwatnym poziomie ochrony jedynie w poszczególnych branżach lub dziedzinach prawa[5]. Decyzje Komisji w zakresie oceny adekwatnego poziomu ochrony w państwach trzecich publikowane są na stronie Komisji[6]. Decyzje te mają charakter wiążący dla państw członkowskich.

## 4. Transfer danych do państw niespełniających wymogu zapewnienia odpowiedniego poziomu ochrony

Dyrektywa nie wyklucza definitywnie możliwości transferu danych do państw, które nie zapewniają adekwatnego poziomu ochrony danych – takich jak np. USA. Transfer jest możliwy w okolicznościach określonych w art. 26 Dyrektywy. Okoliczności uzasadniające transfer danych pomimo niezapewnienia adekwatnego poziomu ochrony przez państwo docelowe to: jednoznaczna zgoda na transfer danych wyrażona przez osobę, której dane dotyczą; przekazanie danych jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której przetwarzane dane dotyczą, lub jeśli transfer jest konieczny do wykonania umowy z podmiotem trzecim, ale w interesie osoby, której dane dotyczą; ze względu na ochronę interesów osoby, której dane dotyczą; ze względu na uzasadniony interes publiczny; a ponadto w odniesieniu do danych publicznie dostępnych[7]. Ponadto transfer jest możliwy na podstawie specjalnych umów międzynarodowych[8], w sytuacji zapewnienia odpowiedniego poziomu ochrony zagwarantowanego odpowiednimi klauzulami umownymi pomiędzy administratorem danych a podmiotem z państwa trzeciego, a także w sytuacji gdy odpowiedni poziom ochrony zapewniany przez docelowego odbiorcę wynika ze stosowanych przez niego wiążących reguł korporacyjnych. Powyższe okoliczności wiążą się jednak z pewnego rodzaju utrudnieniami w przepływie danych, ponieważ wymagają każdorazowej analizy konkretnego stanu faktycznego.

---

[4] Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (*Schrems*) z dnia 06.11.2015 r., http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52015DC0566 [dostęp 28.04.2016].

[5] Np. w odniesieniu do Kanady Komisja uznała adekwatność ochrony danych jedynie w zakresie prywatnego prawa handlowego. Zob. *Podręcznik…*, s. 142–143.

[6] Lista decyzji Komisji w zakresie adekwatnego poziomu ochrony danych osobowych znajduje się pod adresem: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm; [dostęp 28.04.2016].

[7] Legalność transferu tych danych jest zachowana jedynie wtedy, gdy dane te zostały upublicznione zgodnie z prawem – por. X. Konarski, G. Sibiga, *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i UE*, [w:] *iidem* (red.)*, Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa 2013, s. 101.

[8] Umowy te dotyczą przelotów pasażerskich oraz komunikatów finansowych i są zawierane przez UE z państwami trzecimi.

## 5. Ochrona danych osobowych w USA

Regulacje dotyczące ochrony danych osobowych w USA są zdecydowanie odmienne od regulacji unijnych nie tylko pod względem merytorycznym w zakresie praw osób, których dane dotyczą i ich wpływu na przetwarzanie tych danych, ale także pod względem organizacji regulacji odnoszących się do kwestii ochrony danych osobowych. Mają one charakter zdecentralizowany – regulacje dokonywane są osobno dla różnych sektorów, za pomocą aktów prawnych różnej rangi o zróżnicowanym stopniu mocy wiążącej lub terytorialnego zakresu obowiązywania, nie wyłączając przy tym samoregulacji. Rozproszenie regulacji powoduje częste powtarzanie tych samych przepisów, co nie sprzyja przejrzystości prawa, a ich wewnętrzna sprzeczność nie jest zjawiskiem odosobnionym[9]. Niektóre akty odnoszą się do poszczególnych rodzajów danych lub ograniczają poszczególne operacje na danych osobowych (np. *The Telephone Consumer Protection Act*[10], który reguluje jedynie gromadzenie i wykorzystywanie adresów e-mail, numerów telefonów i adresów zamieszkania osób fizycznych). Oba systemy ochrony danych osobowych – amerykański i unijny – zdecydowanie różnią się pod względem zakresu i poziomu ochrony danych osobowych. Brak minimalnych gwarancji dla osób fizycznych, których dane dotyczą, jest powodem znacznej dysproporcji pomiędzy omawianymi systemami, co jest zauważane i poddawane krytyce nie tylko w Europie, ale nawet w USA[11]. Z uwagi na opisane powyżej, zbyt liberalne podejście do kwestii ochrony danych osobowych w USA w porównaniu z ustawodawstwem państw członkowskich, USA nie mogły zostać uznane za gwarantujące określony w Dyrektywie adekwatny poziom ochrony danych osobowych. Konieczne było zatem wypracowanie zasad i procedur przekazywania danych osobowych Europejczyków za ocean.

## 6. *Safe Harbour* – istota programu

Stany Zjednoczone, jako jeden z głównych partnerów nie tylko gospodarczych, ale też politycznych UE, często są portem docelowym transferu danych osobowych z państw członkowskich. Zaawansowany stopień współpracy gospodarczej, z którym kwestia przepływu danych jest nierozerwalnie powiązana, mógłby zostać utrudniony ze względu

[9] J. Zygment, *Program Safe Harbour – pomost między europejskim a amerykańskim systemem ochrony danych osobowych,* „Adam Mickiewicz University Law Review" 2014, nr 3, s. 62.

[10] Tekst aktu znajduje się pod adresem: https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf; [dostęp 28.04.2016].

[11] Zob. T. H. Davenport, *Should the U.S. Adopt European-Style Data-Privacy Protections?,* „The Wall Street Journal", 10.03.2013, http://www.wsj.com/articles/SB10001424127887324338604578328393797127094 [dostęp 28.04.2016]. Autor krytykuje przede wszystkim brak transparentności amerykańskich przepisów odnoszących się do ochrony danych osobowych osób fizycznych.

na komplikacje związane z koniecznością każdorazowego badania adekwatności poziomu ochrony. Rozumiejąc istotę problemu, w celu uniknięcia utrudnień w przepływie danych (przekładających się bezpośrednio na współpracę gospodarczą) UE i USA uznały, że konieczne jest stworzenie instrumentu, który ułatwiałby transfer danych[12].

Departament Handlu Stanów Zjednoczonych wypracował w porozumieniu z Komisją Europejską program *Safe Harbour* nazywany też Bezpieczną Przystanią lub Bezpiecznym Portem. Program miał umożliwiać amerykańskim przedsiębiorcom sprostanie europejskim standardom ochrony danych przy jednoczesnym zagwarantowaniu europejskim przedsiębiorcom, że transferowane za ocean dane będą miały w USA zapewniony zbliżony do europejskiego poziom ochrony.

Program *Safe Harbour* opierał się na siedmiu następujących zasadach:

1) Ogłoszenia – osoby, których dotyczą przekazane przez niego dane, będą poinformowane o tym, że ich dane zostały zebrane oraz o sposobie ich wykorzystania;
2) Wyboru – osoby, których dane dotyczą, będą mogły odmówić zgody na dalsze przekazanie danych;
3) Dalszego Przekazywania Danych – transfer danych będzie następował wyłącznie do podmiotu, który spełnia wymogi należytej ochrony;
4) Bezpieczeństwa – administrator danych podejmie rozsądne środki w celu zabezpieczenia danych przed utratą;
5) Integralności Danych – administrator danych będzie zbierał tylko te dane, które są istotne ze względu na cel, w którym zostały zebrane;
6) Dostępu – osoby, których dane dotyczą, będą mieć dostęp do zebranych danych ich dotyczących oraz będą mieć możliwość ich poprawienia i aktualizacji;
7) Zapewnienia Skuteczności Praw – podmiot docelowego portu danych zapewni efektywne środki egzekwowania ww. wymogów.

Zadeklarowanie powyższych zasad przez konkretnego amerykańskiego przedsiębiorcę umożliwiało mu przystąpienie do programu – podmiot taki zgłaszał się do Departamentu Handlu USA (Department of Commerce of United States), na zasadzie samocertyfikacji deklarował przestrzeganie zasad (*self-certificate letter)*, po czym Departament Handlu umieszczał przedsiębiorcę na liście podmiotów będących członkami programu[13]. Warto jednak podkreślić, że program *Safe Harbour* nie miał zastosowania do wszystkich podmiotów przetwarzających dane, a jedynie do tych, które podlegały nadzorowi Fede-

[12] Ministerstwo Administracji i Cyfryzacji, Departament Społeczeństwa Informacyjnego, *Analiza Programu „Bezpieczna Przystań" („Safe Harbour") w zakresie przekazywania danych osobowych z terytorium Polski do odbiorców w Stanach Zjednoczonych Ameryki,* Warszawa 2014, s.4.

[13] Lista podmiotów uczestniczących w programie *Safe Harbour* znajduje się pod następującym linkiem: https://safeharbor.export.gov/list.aspx; [dostęp 28.04.2016].

ralnej Komisji Handlu (Federal Trade Commission) lub Departamentu Transportu (Department of Transportation).

Program *Safe Harbour* został zatwierdzony decyzją Komisji Europejskiej z dnia 26 czerwca 2000 r.[14] Komisja uznała, że poziom ochrony danych zapewniany przez uczestników Bezpiecznej Przystani jest „odpowiedni" w myśl art. 25 i 26 Dyrektywy. Uzyskanie certyfikatu programu *Safe Harbour* zapewniało, że uczestnik programu gwarantuje odpowiedni poziom ochrony danych osobowych, o którym mowa w Dyrektywie[15]. Z programu *Safe Harbour* korzystało kilka tysięcy podmiotów, w tym globalne firmy z sektora nowych technologii, jak Microsoft Corp., Facebook Inc., Google Inc., Twitter Inc. czy Amazon.com Inc.[16]

## 7. Krytyka programu *Safe Harbour*

Od samego początku program Bezpiecznej Przystani miał wielu przeciwników, którzy wskazywali mankamenty tego swoistego kompromisu pomiędzy UE i USA. Na nieprawidłowości programu niejednokrotnie wskazywała Grupa Robocza funkcjonująca na podstawie art. 29 Dyrektywy, która podkreślała w szczególności ograniczony zakres obowiązywania programu oraz brak skuteczności egzekwowania przyjętych w jego ramach zobowiązań[17]. Krytycznie o programie wypowiadali się nawet australijscy naukowcy[18]. Po 15 latach funkcjonowania programu *Safe Harbour* w jego sprawie wypowiedział się Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE).

Przeciwnicy Bezpiecznej Przystani – w coraz większej liczbie – zyskali na sile w 2013 r., co stanowiło reakcję na ujawnienie przez Edwarda Snowdena[19] informacji na temat programów masowej inwigilacji prowadzonych przez Stany Zjednoczone. Zaczęto podejmować kroki w kierunku odbudowania zaufania w kwestii przepływu danych między UE a USA[20]. Komisja Europejska przedstawiła 13 zaleceń dotyczących poprawienia polityki ochrony danych osobowych obywateli UE na terenie Stanów Zjednoczonych, w szczególności w zakresie poprawy skuteczności egzekwowania prawa. Wśród

[14] Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. (notyfikowana jako dokument nr C (2000) 2441), (Dz. Urz. WE L 215 z 25.08.2000 r., s. 7–47); (dalej: Decyzja).

[15] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie,* Warszawa 2010, s. 194.

[16] Zob. listę podmiotów pod adresem: https://safeharbor.export.gov/list.aspx; [dostęp 28.04.2016].

[17] Article 29 Data Protection Working Party, *Opinion 4/200 on the level of protection provided by the „Safe Harbour Principles",* 2000.

[18] C. Connolly, *The US Safe Harbor – Fact or Fiction?,* Galexia, New York 2008.

[19] Były pracownik amerykańskiego Central Intelligence Agency, który ujawnił funkcjonowanie programu PRISM – amerykańskiego programu szpiegowskiego umożliwiającego National Security Agency dostęp do danych osobowych zgromadzonych w bazach największych amerykańskich przedsiębiorstw.

[20] Zob. Komunikat Komisji do Parlamentu Europejskiego i Rady, *Odbudowa zaufania do przepływów danych między Unią Europejską w Stanami Zjednoczonymi*, 27.11.2013, COM (2013) 846 final.

zaleceń Komisji Europejskiej znalazły się m.in.: obowiązek publikowania polityki ochrony danych osobowych, nakaz wyraźnego i niepozostawiającego wątpliwości oznakowania przedsiębiorstw uczestniczących w programie *Safe Harbour*, stworzenie mechanizmów zapobiegających rezygnacji poszkodowanych z dochodzenia roszczeń ze względu na bariery finansowe, objęcie monitoringiem przestrzegania zasad programu przez jego uczestników, a także obciążenie odpowiedzialnością za rozpowszechnianie fałszywych informacji o uczestnictwie w programie *Safe Harbour*[21]. Za najtrudniejsze do wprowadzenia w życie zalecenie należy jednak uznać ograniczenie kompetencji amerykańskich organów państwowych do przetwarzania danych w zakresie ochrony bezpieczeństwa narodowego[22]. Wprowadzenie tych mechanizmów nie zdołało jednak osiągnąć celu, jakim było zapewnienie należytej ochrony danych osobowych Europejczyków na terenie USA. Konieczne było definitywne podważenie programu na skutek skargi wniesionej przez austriackiego studenta Maximilliana Schremsa.

## 8. Wyrok TSUE w sprawie *Maximillian Schrems vs. Data Protection Commisioner*[23]

Informacje ujawnione przez E. Snowdena miały wpływ na decyzję KE uznającą adekwatność ochrony danych osobowych zapewnianą przez podmioty uczestniczące w programie *Safe Harbour*. 25 czerwca 2013 r. M. Schrems złożył skargę do irlandzkiego komisarza ochrony danych osobowych, w której zażądał, aby organ ten zakazał spółce Facebook Ireland przekazywania jego danych osobowych do USA. Jako uzasadnienie żądania podniósł, że prawo i praktyka obowiązujące w tym kraju nie zapewniają odpowiedniego poziomu ochrony danych przed inwigilacją prowadzoną przez amerykańskie służby wywiadowcze[24]. Komisarz skargę odrzucił, a decyzję swą uzasadnił tym, że Schrems nie udowodnił, że jego dane zostały ujawnione nieuprawnionemu podmiotowi, powołując się jednocześnie na decyzję Komisji Europejskiej 2000/520, legalizującej transfer danych do USA, na podstawie której dokonywany był transfer danych przez Facebook Ireland do Facebook Inc. jako uczestnika *Safe Harbour.* Sprawa trafiła przed Sąd Najwyższy Irlandii (*High Court of Ireland*). Pomimo istnienia decyzji zatwierdzającej program *Safe Harbour* ww. sąd powziął wątpliwości co do rzeczywistego poziomu ochrony danych w USA, uzasadniając, że „informacje ujawnione przez E. Snowdena

[21] *Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards,* 29.02.2016, COM (2016) 117 final.

[22] *Ibidem*.

[23] Wyrok TSUE w sprawie *Maximillian Schrems vs. Data Protection Commissioner*, sygn. C-362/14 (dalej: Wyrok).

[24] W szczególności National Security Agency, Federal Bureau of Investigation (FBI).

wskazały na «istotne przekroczenie granic kompetencji» ze strony NSA i innych organów federalnych"[25]. Sąd ten zwrócił także uwagę, że skarga M. Schremsa w rzeczywistości skierowana jest przeciwko zgodności systemu *Safe Harbour* wprowadzonego w życie Decyzją Komisji Europejskiej 2000/520 z art. 25 Dyrektywy. Irlandzki sąd zwrócił się wobec tego do TSUE z dwoma pytaniami prejudycjalnymi o charakter prawny i związanie państw członkowskich decyzją KE zatwierdzającą program Bezpieczna Przystań oraz ewentualne kompetencje właściwych organów państw w zakresie możliwości podważenia wspomnianej Decyzji. TSUE w odpowiedzi orzekł, że decyzja KE jest wiążąca dla państw członkowskich, a to na mocy art. 288 TFUE[26], wobec czego wiąże wszystkie ich organy[27]. Podkreślił jednak, że Decyzja ta nie stanowi przeszkody w dokonaniu przez właściwy organ nadzoru państwa członkowskiego samodzielnej oceny poziomu ochrony danych osobowych w państwie portu danych[28]. TSUE podkreślił też swoją wyłączną właściwość do oceny ważności Decyzji[29]. Ostatnie zdanie sentencji wyroku, pomimo swojej oczywistości, stanowiło duże zaskoczenie. TSUE orzekł, że Decyzja KE 2000/520 jest nieważna.

TSUE, uzasadniając swoje stanowisko w zakresie nieważności Decyzji KE 2000/520, krytycznie odniósł się do kryteriów uzyskania członkostwa w programie *Safe Harbour*, w szczególności do wiarygodności systemu samocertyfikacji amerykańskich przedsiębiorców[30]. Kolejną istotną wadą *Safe Harbour* był fakt, że o ile jego zasadom podlegali dobrowolnie amerykańscy przedsiębiorcy, to program nie zapewniał respektowania jego zasad przez amerykańskie władze publiczne, a właśnie stosunek amerykańskich władz był powodem obaw Europejczyków o dotyczące ich dane osobowe i przyczyną postępowania w przedmiocie weryfikacji Decyzji zatwierdzającej program *Safe Harbour*[31]. Istota problemu nie leżała zatem w samym programie *Safe Harbour* czy w jego treści, ale właściwie w skuteczności zobowiązania się amerykańskich przedsiębiorców do bezwarunkowego odstąpienia od tych zasad prawa amerykańskiego, które pozostawałyby w konflikcie z wymogami programu *Safe Harbour* w obliczu zasady szerokiego dostępu do danych amerykańskich organów administracji państwowej. W ocenie autorki tego opracowania najistotniejszym elementem jest jednak problem braku aktów ustalających reguły o ogólnopaństwowym charakterze, które gwarantowa-

[25] Treść uzasadnienia polskiej wersji wyroku wyroku TSUE dostępna jest pod adresem: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dde2452da62c8a4d909a3ac46f5a1af593.e34KaxiLc3qMb40Rch0SaxuRc3z0?doclang=PL&text=&pageIndex=0&docid=169195&cid=235063 [dostęp: 28.04.2016].

[26] Traktat o funkcjonowaniu Unii Europejskiej, Dz. U. UE C 326 z 26.10.2012, P. 0001-0390.

[27] Pkt 51 Wyroku.

[28] *Ibidem,* pkt 53.

[29] *Ibidem,* pkt 61–63.

[30] *Ibidem,* pkt 80–81.

[31] *Ibidem,* pkt 82.

łyby udostępnienie danych władzom USA ze względu na realizację uzasadnionego prawem celu, jakim jest bezpieczeństwo narodowe[32]. Wyrok zintensyfikował prace nad nową polityką transferu danych Europejczyków do USA. Możliwość transferu danych na podstawie uczestnictwa w programie *Safe Harbour* została przedłużona do końca stycznia 2016 r.

## 9. UE–U.S. Privacy Shield – Tarcza Prywatności[33]

Dnia 29 lutego 2016 r. Komisja Europejska opublikowała treść *UE–U.S. Privacy Shield*–nowej regulacji przepływu danych osobowych z UE do USA, która ma zastąpić program *Safe Harbour* i wyeliminować błędy, jakie mu towarzyszyły. *Privacy Shield* oparta jest na tych samych siedmiu zasadach co program *Safe Harbour*, tj. na zasadzie: Ogłoszenia, Wyboru, Dalszego Przekazywania Danych, Bezpieczeństwa, Integralności Danych i Ograniczenia Celu, Dostępu, Zapewnienia Prawa Skuteczności[34]. Pomimo znacznego podobieństwa do Bezpiecznej Przystani akt ten reguluje pewne kwestie odmiennie, przez co wydaje się być skuteczniejszy.

Organizacja podmiotów zapewniających odpowiedni poziom ochrony danych wygląda podobnie do tej, którą stosowano w okresie obowiązywania *Safe Harbour*; amerykańscy przedsiębiorcy dokonują samocertyfikacji, na postawie której Departament Handlu USA wpisuje konkretnego przedsiębiorcę na *Privacy Shield List*[35]. Nowe zasady przewidują jednak coroczną recertyfikację i konieczność wykreślenia podmiotu z *Privacy Shield List* w przypadku, jeśli nie przeprowadzą rocznej recertyfikacji, złamią zasady ochrony danych osobowych lub zmienią zasady ich przetwarzania, które nie będą już zapewniać adekwatnego poziomu ochrony. Dodatkowo każdy z uczestników *Privacy Shield* ma obowiązek publikowania stosowanej polityki prywatności, a w przypadku wykreślenia go z listy uczestników programu ma o tym fakcie publicznie poinformować. Departament Handlu USA ma sprawować nadzór nad przestrzeganiem postanowień programu przez amerykańskich przedsiębiorców – na żądanie tego organu uczestnik programu będzie musiał przedstawić informacje dotyczące przetwarzania danych i w przypadku stwierdzenia ewentualnych naruszeń ustosunkować się do odpowiednich

[32] *Ibidem,* pkt 88.

[33] Tak Komisja Europejska, Projekt *Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of Council on the adequancy of the protection provided by the EU–U.S. Privacy Shield,* 29 lutego 2016, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf; [dostęp 24.04.2016] (dalej: Projekt decyzji w sprawie*Privacy Shield*). Zob. także: *Communication from the Commission….*

[34] Commission Implementing Decision of 12 July 2016...

[35] *Privacy Shield List* jest dostępna pod adresem: https://www.privacyshield.gov/list; [dostęp 10.10.2016].

zarzutów[36]. Przyznanie Departamentowi Handlu USA kompetencji nadzorczych i możliwości wykreślenia podmiotu, który w rzeczywistości nie stosuje się do postanowień programu z *Privacy Shield List*, pozwoli wyeliminować nadużycia przedsiębiorców w zakresie samocertyfikacji.

Nowy program przewiduje również efektywniejsze środki ochrony prawnej umożliwiające dochodzenie roszczeń przez Europejczyków. Przedsiębiorcy zza oceanu są zobowiązani opublikować mechanizm dochodzenia roszczeń w sytuacji naruszenia postanowień programu. W przypadku złożenia skargi na naruszenia przedsiębiorca zobowiązany będzie ustosunkować się do niej w ciągu 45 dni. Odpowiedź musi zawierać merytoryczne uzasadnienie oraz sposób, w jaki naruszenie zostanie usunięte. Ponadto *Privacy Shield* przewiduje utworzenie w USA odrębnego organu do rozwiązywania sporów powstałych na tle naruszeń związanych z przetwarzaniem danych osobowych, który ma być organem niezależnym – tzw. *Privacy Shield Ombudsperson*[37]. Istotny jest fakt, że postępowania mają być wolne od opłat. Co więcej, na organy powołane do rozwiązywania sporów nałożony został obowiązek sporządzania rocznych sprawozdań o liczbie złożonych skarg, rodzaju zarzucanych naruszeń, a także wyniku sprawy i przyznanych środkach ochrony. Nowy program przewiduje również różne rodzaje rekompensaty za naruszenia, w szczególności rekompensatę pieniężną (*money damages*) nie tylko za naruszenie programu przez przedsiębiorców, ale również przez organy administracji publicznej[38]. W przypadku stwierdzenia naruszenia administrator danych będzie zobowiązany doprowadzić sposób przetwarzania danych osobowych do stanu zgodnego z założeniami programu. Informacje o naruszeniach mają być podawane do publicznej wiadomości.

*Privacy Shield* przewiduje procedurę arbitrażową do rozwiązywania sporów powstałych na tle naruszeń ochrony danych osobowych[39]. Rozstrzygnięcie sądu arbitrażowego ma być ostateczne i wiążące dla stron.

Problem nadal stanowi możliwość dostępu do danych Europejczyków dla amerykańskich organów władzy publicznej. Grupa Robocza dodatkowo wyraziła swoje obawy dotyczące mechanizmu funkcjonowania *Privacy Shield Ombudsperson*, w szczególności w zakresie niezależności rzecznika[40]. Program zakłada ograniczenie możliwości ingerencji władz amerykańskich w dane Europejczyków uzasadnionej ze względu na bezpieczeństwo narodowe lub ważny interes publiczny (co dotychczas było największym

[36] *Ibidem*, pkt 24–51 preambuły.
[37] Commission Implementing Decision of 12 July 2016…
[38] *Ibidem,* pkt 96–98 preambuły.
[39] *Ibidem*, pkt 46–47 preambuły.
[40] Article 29 Working Party Statement on the decision of the European Commission on the EU–U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf; [dostęp 10.10.2016].

problemem) oraz zapewnienie skutecznych mechanizmów nadzoru nad amerykańskimi przedsiębiorcami przetwarzającymi przekazane z UE dane osobowe, a ponadto ma zapewnić większą transparentność zasad udostępniania takich danych organom administracji rządowej USA[41]. Sytuacje, w jakich amerykańskie służby specjalne mogą uzyskać dostęp do danych Europejczyków, mają dotyczyć m.in.: terroryzmu, szpiegostwa i cyberprzestępczości. Grupa Robocza podkreśliła problem, jakim jest brak jasnych i precyzyjnych definicji, co umożliwia dostęp do danych dla amerykańskich organów administracji publicznej[42].

Projekt decyzji uznającej program za mechanizm zapewniający adekwatny poziom ochrony danych został opublikowany dnia 29 lutego 2016 r. Komisja zatwierdziła projekt powoływaną wyżej decyzją z dnia 12 lipca 2016 r. – akt wszedł w życie w trybie natychmiastowym.

## 10. Wnioski

Program *Privacy Shield* przewiduje dalej idącą ochronę danych osobowych i niewątpliwie zapewnia skuteczniejsze egzekwowanie jego postanowień, niż to czynił program *Safe Harbour.* W szczególności pozytywnie należy oceniać propozycje w zakresie eliminowania naruszeń oraz sprawowania nadzoru nad samocertyfikowanymi podmiotami. Istotną zmianą w porównaniu z poprzednim porozumieniem jest zapewnienie mechanizmów ochrony praw osób, których dane dotyczą, oraz ustanowienie procedur ich bezpłatnego dochodzenia. Skuteczność przestrzegania zasad przez amerykańskich przedsiębiorców wspomagać będzie nadzór sprawowany przez Departament Handlu USA. Na aprobatę zasługują założenia dotyczące sporządzania rocznych raportów o naruszeniach w zakresie ochrony danych, jakich dopuszczać się będą amerykańscy przedsiębiorcy. Zakres tego raportu (ilość zgłoszonych naruszeń, ich rodzaj, wynik rozpoznanej skargi oraz przyznana rekompensata) pozwoli w przyszłości ocenić nie tylko rzeczywistą efektywność samych procedur przewidzianych porozumieniem, ale przede wszystkim skuteczność samego porozumienia i poszanowanie jego zasad przez partnerów zza oceanu. Taka ocena skuteczności w przypadku programu *Safe Harbour* zajęła niemal 15 lat, roczne raporty pozwolą to zweryfikować dużo szybciej. Powyższe zmiany czynią program bardziej przejrzystym, a dzięki temu i skuteczniejszym.

Podkreślenia wymaga fakt, że program nie jest jednak rozwiązaniem doskonałym. Jego główny mankament sprowadza się do głównego problemu przesłanek i zakresu dostępu do danych osobowych dla amerykańskich organów administracji publicznej, co

[41] *Ibidem,* pkt 24–28; 52–116 preambuły.

[42] http://www.euractiv.pl/nowe-technologie/artykul/problemy-z-privacy-shield-008307, [dostęp 28.04.2016].

jak wcześniej wskazano, było definitywnym powodem porażki programu *Safe Harbour.* Problem stanowi w głównej mierze niezbyt precyzyjne, a wręcz hasłowe określenie przesłanek dostępu amerykańskich służb specjalnych do informacji gromadzonych przez amerykańskich administratorów danych, w tym danych osobowych Europejczyków.

## Bibliografia


### Akty prawne

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. WE L 281/31 z 23.11.1995 r.).

Traktat o funkcjonowaniu Unii Europejskiej (Dz.U.UE C 326 z 26.10.2012 r., P. 0001- 0390).

### Monografie

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie,* Wolters Kluwer, Warszawa 2010.

Konarski X., Sibiga G., *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i UE*, [w:] *iidem* (red.), *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Wolters Kluwer, Warszawa 2013.

*Podręcznik europejskiego prawa o ochronie danych*, Agencja Praw Podstawowych Unii Europejskiej, Rada Europy, Luksemburg 2014.

### Artykuły

Connolly C., *The US Safe Harbor – Fact or Fiction?,* Galexia, New York 2008.

Davenport T.H., *Should the U.S. Adopt European-Style Data-Privacy Protections?*, „Wall Street Journal" 10.03.2013.

Zygment J., *Program Safe Harbour – pomost między europejskim a amerykańskim systemem ochrony danych osobowych*, „Adam Mickiewicz University Law Review" 2014, nr 3.

### Orzecznictwo

Wyrok TSUE w sprawie *Maximillian Schrems vs. Data Protection Commissioner*, sygn. C-362/14.

### Inne

Article 29 Data Protection Working Party, *Opinion 4/200 on the level of protection provided by the „Safe Harbour Principles",* 2000.

Article 29 Working Party Statement on the decision of the European Commission on the EU–U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf; [dostęp 10.10.2016].

*Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of Council on the adequancy of the protection provided by the EU–U.S. Privacy*

*Shield*, http://www.euractiv.pl/nowe-technologie/artykul/problemy-z-privacy-shield-008307, [dostęp 28.04.2016].

*Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards,* 29.02.2016, COM (2016) 117 final.

Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. (notyfikowana jako dokument nr C (2000) 2441), (Dz. Urz. WE L 215 z 25.08.2000 r., s.7–47).

Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (*Schrems*) z dnia 06.11.2015, http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52015DC0566. [dostęp: 28.04.2016].

Komunikat Komisji do Parlamentu Europejskiego i Rady. *Odbudowa zaufania do przepływów danych między Unią Europejską w Stanami Zjednoczonymi*, 27.11.2013, COM (2013) 846 final.

Ministerstwo Administracji i Cyfryzacji, Departament Społeczeństwa Informacyjnego, *Analiza Programu „Bezpieczna Przystań" („Safe Harbour") w zakresie przekazywania danych osobowych z terytorium Polski do odbiorców w Stanach Zjednoczonych Ameryki,* Warszawa 2014.

Telephone Consumer Protection Act 47 U.S.C., https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf; [dostęp 28.04.2016].

Wyrok Trybunału (wielka izba) z dnia 6 października 2016 r. w sprawie C-362/14 *Maximilian Schrems przeciwko Data Protection Commissioner,*

Wyrok TSUE w sprawie *Maximillian Schrems vs. Data Protection Commissioner*, sygn. C-362/14, http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30dde2452da62c8a4-d909a3ac46f5a1af593.e34KaxiLc3qMb40Rch0SaxuRc3z0?doclang=PL&text=&pageIndex=0&docid=169195&cid=235063, [dostęp 28.04.2016].