Europejski Przegląd Prawa i Stosunków Międzynarodowych
Europejska Wyższa Szkoła Prawa i Administracji w Warszawie
nr 1–2/2023/65–66

Iwona Kredzińska*

Transfer danych osobowych z Unii Europejskiej do Stanów Zjednoczonych. Wpływ decyzji Schrems II

[Transfer of Personal Data from the European Union to the United States. Impact of the Schrems II Decision]

Abstract

The subject of this article is cross-border data flows between the European Union and the United States following the annulment of the EU–US Privacy Shield by the Court of Justice of the European Union. Restrictions on data transfers outside the European Union introduced by the General Data Protection Regulation (GDPR) and the lack of full EU-recognised adequate data protection in the United States are addressed. The article analyses the landmark judgment of the Court of Justice of the European Union in the Schrems II case and the newly emerging US legislation: *the Regulation on Strengthening the Safeguards for US Signals Intelligence Activities* in terms of ensuring compliance with personal data laws and in the broader context of transatlantic relations and the digital economy. The analysis of the above issues was made in order to assess the available options for the transfer of personal data between the European Union and the United States and to identify the implications of the current situation for companies operating in the area of cross-border data flows.

Keywords: cross-border data flows, EU–US Privacy Shield, General Data Protection Regulation (GDPR), Schrems II case, personal data, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, transatlantic relations, digital economy.

16 lipca 2020 roku Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał decyzję w sprawie Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems, znanej również jako sprawa

* **Iwona Kredzińska** – radca prawny, notariuszka; absolwentka Harvard Business School, Data Privacy and Technology; ORCID 0009-0008-8376-0035.

Schrems II[1]. Sprawa ta uderzyła w istotę transatlantyckich transferów danych (danych przekazywanych z Unii Europejskiej i Szwajcarii do Stanów Zjednoczonych)[2], a sednem konfliktu były amerykańskie uprawnienia w zakresie bezpieczeństwa narodowego i egzekwowanie prawa, które stoją w sprzeczności z unijnym podejściem do prywatności danych.

Obecnie, po prawie trzech latach od wydania wyroku TSUE w wyżej wymienionej sprawie, wciąż brakuje odpowiedniej przestrzeni prawnej zapewniającej właściwą ochronę prywatności użytkowników, których dane mają być przesyłane z Unii Europejskiej do Stanów Zjednoczonych, a przestrzeń tę stworzyć ma nowe porozumienie o przekazywaniu danych UE–USA.

Transatlantyckie stosunki gospodarcze – konflikt wartości

W dzisiejszym świecie wszystkie branże są w różnym stopniu zależne od przepływu danych, zarówno te tradycyjne, jak i te związane z najnowocześniejszymi technologiami. Wzrost gospodarczy zależy od rozwoju przemysłu i rozwój przedsiębiorstw, dla których swobodny przepływ danych jest podstawowym wsparciem[3]. W świetle powyższego jeszcze większego znaczenia nabiera fakt, że transatlantyckie stosunki gospodarcze między UE a Stanami Zjednoczonymi są największe na świecie, a ich wartość wynosiła 7,1 bln USD[4]. Możliwość dostępu, gromadzenia i przekazywania danych ponad granicami jest funkcją globalizacji Internetu. Według amerykańskiego Biura Analiz Ekonomicznych Stany Zjednoczone i Europa są dla siebie najważniejszymi partnerami handlowymi w zakresie usług cyfrowych. Handel technologiami informacyj-

[1] Wyrok TSUE z 16 lipca 2020 r., Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems, sprawa C-311/18, ECLI:EU:C:2020:559.

[2] Schrems II landmark ruling: A detailed analysis, Norton Rose Fulbright, 2020, June, https://www.nortonrosefulbright.com/en-gb/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis [dostęp: 14 czerwca 2023].

[3] D. Castro, A. Mcquinn, Cross-Border Data Flows Enable Growth in All Industries, INFO. TECH INNOVATION FOUND. (Feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf [dostęp: 5 grudnia 2022].

[4] Komunikat prasowy, Departament Handlu, Sekretarz Handlu USA Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (16 lipca 2020) https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows [dostęp: 5 grudnia 2022].

no-komunikacyjnymi (ICT) i usługami potencjalnie wspieranymi przez ICT wyniósł 264 mld USD w 2020 roku[5]. Transatlantyckie przepływy odpowiadają za ponad połowę przepływów danych w Europie i około połowę amerykańskich przepływów danych na całym świecie[6]. Z powyższych powodów jednym z głównych zagadnień, które większość firm stawia na czele swojej listy priorytetów, jest to, jak orzeczenie Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie Schrems II wpływa na transatlantyckie przepływy danych. Z każdą sekundą firmy przekazują bowiem dane z UE do USA, aby zarządzać swoimi systemami IT, sprzedawać i kupować produkty i usługi, zarządzać swoim personelem, angażować się w działania marketingowe, wykorzystywać chmurę do swoich operacji, a także do wielu innych celów. Gospodarka światowa jest bowiem w dużej mierze połączona i opiera się na transgranicznych transferach danych. Jest to związane z tzw. czwartą rewolucją przemysłową[7], która odnosi się do kompleksowej cyfryzacji wszystkich aktywów. Transgraniczny dostęp do danych jest więc niezbędny dla zapewnienia wzrostu gospodarczego[8].

W związku z powyższym rozważania nad zagadnieniem transferów danych mają bardzo praktyczny wymiar, co więcej – problematyka ta stanowi jedno z poważniejszych wyzwań pod względem regulacyjnym, a także teoretycznoprawnym we współczesnym świecie[9]. W prezentowanym kontekście zauważyć należy, że decyzja w sprawie Schrems II uderzyła w newralgiczny punkt prawdopodobnie znacznie większej debaty, z którą zmagają się jurysdykcje na całym świecie: mianowicie skrzyżowania pry-

[5] The Congressional Research Service (CRS) June 2, 2022, U.S.-EU Trans-Atlantic Data Privacy Framework, https://crsreports.congress.gov/product/pdf/IF/IF11613 [dostęp: 5 grudnia 2022].

[6] Takie przepływy danych umożliwiają ludziom przesyłanie informacji w Internecie, komunikację, śledzenie globalnych łańcuchów dostaw, udostępnianie badań, świadczenie usług transgranicznych i technologiczne wspieranie innowacyjności; organizacje mogą m.in. korzystać z danych osobowych klientów lub pracowników w celu ułatwienia prowadzenia działalności, transakcji, mogą analizować informacje marketingowe, odkrywać fałszywe płatności, ulepszać zastrzeżone algorytmy lub rozwijać konkurencyjne innowacje.

[7] K. Schwab, World Economic Forum 2016, The Fourth_Industrial Revolution, https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab [dostęp: 15 czerwca 2023].

[8] Pod względem zdolności do angażowania się i czerpania korzyści z gospodarki cyfrowej opartej na danych wyróżniają się obecnie dwa kraje: Stany Zjednoczone i Chiny. Razem odpowiadają one za: połowę hiperskalowych centrów danych na świecie, najwyższe wskaźniki rozwoju technologii 5G na świecie, 94 procent finansowania start-upów AI w ciągu ostatnich pięciu lat; łącznie dały światu aż 70 procent czołowych badaczy sztucznej inteligencji i prawie 90 procent kapitalizacji rynkowej, Digital Economy Report 2021 Cross Border data flows and development, https://unctad.org/system/files/official-document/der2021_en.pdf [dostęp: 5 grudnia 2022].

[9] D. Karwala, Komercyjne transfery danych osobowych do państw trzecich, Warszawa 2018, s. 18.

watności[10], bezpieczeństwa narodowego i współpracy międzynarodowej. Na tym tle jeszcze wyraźniej widać zderzenie europejskiego i amerykańskiego podejścia. Podczas gdy Unia Europejska w ostatnich latach dążyła do ugruntowania swojej pozycji jako strażnika ochrony danych – przez ustawodawstwo i regulacje takie, jak: rozporządzenie Parlamentu Europejskiego i Rady 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[11] oraz Karta praw podstawowych Unii Europejskiej[12] – to Stany Zjednoczone, w przeciwieństwie do Unii Europejskiej, nie mają obecnie ram ochrony danych osobowych ani zasad przewodnich o charakterze federalnym, polegając jedynie na przepisach stanowych, które zapewniają ochronę na pewnych obszarach, jak Kalifornijska ustawa o ochronie prywatności konsumentów (ang. California Consumer Privacy Act [CCPA]), to jest ustawa mająca na celu zwiększenie praw do prywatności i ochrony konsumenckiej mieszkańców Kalifornii (USA)[13].

Ochrona danych jako prawo podstawowe w Unii Europejskiej – ramy ochrony

Należy podkreślić, że prawo do prywatności jest fundamentalnym pojęciem w prawie Unii Europejskiej, któremu nadano ogromne znaczenie, co odzwierciedla głęboko zakorzenione wartości. Opierając się na europejskiej Konwencji o ochronie praw człowieka i podstawowych wol-

[10] Advocate General's Opinion in Case C-311/18 Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Court of Justice of the European Union PRESS RELEASE no 165/19 Luxembourg, 19 December 2019.
https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf [dostęp: 5 grudnia 2022].

[11] Rozporządzenie 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, Dz. Urz. UE L 2016, 119, 1 ze zm. (dalej jako RODO lub ogólne rozporządzenie o ochronie danych).

[12] Dz. Urz. UE 2012 C 326/02.

[13] The California Consumer Privacy Act (CCPA), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 [dostęp: 5 grudnia 2022].
Kalifornijska ustawa o ochronie prywatności konsumentów weszła w życie 1 stycznia 2020 r., a egzekwowanie przepisów przez Biuro Prokuratora Generalnego Kalifornii rozpoczęło się 1 lipca 2020 r. Inicjatywa głosowania w sprawie ustawy o prawach do prywatności w Kalifornii została przyjęta w listopadzie 2020 r., większość jej przepisów zaczęła zaś obowiązywać 1 stycznia 2023 r.

ności[14], chroniącej prawo do życia prywatnego i rodzinnego, art. 8 Karty praw podstawowych Unii Europejskiej[15], obowiązującej od 2009 roku, stanowi, że „każdy ma prawo do ochrony danych osobowych, które go dotyczą". Jak podkreślił przewodniczący Juncker w przemówieniu o stanie Unii Europejskiej 14 września 2016 r., bycie Europejczykiem oznacza prawo do tego, by twoje dane osobowe były chronione przez silne, europejskie przepisy prawne. […] Ponieważ w Europie prywatność ma znaczenie. Jest to kwestia ludzkiej godności".

Obecnie w Unii Europejskiej ramy ochrony danych osobowych tworzone są przez ogólne rozporządzenie o ochronie danych, które zastąpiło dyrektywę Parlamentu Europejskiego 95/46/EC[16].

Kluczowy w zakresie problematyki poruszanej w niniejszym artykule jest art. 44 RODO, który zakazuje przekazywania danych osobowych do państw spoza UE, chyba że państwo otrzymujące może przedstawić dowody na istnienie odpowiedniego poziomu ochrony danych równoważnego z unijnym. Zgodnie więc z RODO przekazywanie danych do państw spoza UE co do zasady jest zabronione. RODO uznaje natomiast pewne mechanizmy, które mogą stanowić wyjątek. 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. 45 ust. 1 RODO)[17]. Należy zatem zwrócić uwagę, że zastosowanie ww. mechanizmów nie jest dowolne. Przepisy RODO jednoznacznie hierarchizują i uzależniają od siebie sposoby legalizacji przekazywania danych osobowych. W związku z czym drogą legalizacji transferu danych będą w kolejności:

[14] Sporządzonej w Rzymie 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz.U. 1993 nr 61, poz. 284).

[15] Dz. Urz. UE 2012 C 326/02.

[16] 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 (Dz. Urz. WE L 1995, 281, 31 ze zm.).

[17] D. Lubasz, *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.

1) „decyzja stwierdzająca odpowiedni poziom ochrony" wydana przez Komisję Europejską;
2) usankcjonowane przez UE „odpowiednie zabezpieczenia" dotyczące przekazywania danych, takie jak klauzule wzorcowe, oraz
3) ustawowe wyjątki od ogólnego zakazu przekazywania danych, takie jak zgoda lub zobowiązania umowne.

Dodatkowo RODO zawiera mechanizmy przekazywania danych, takie jak:
4) certyfikacje i 5) zatwierdzone kodeksy postępowania.

RODO formalizuje również wiążące reguły korporacyjne[18] (Binding Corporate Rules – BCR), które istniały już wcześniej, ale nie zostały skodyfikowane w ramach dyrektywy o ochronie danych, jako podstawa prawna do międzynarodowego przekazywania danych.

Z powyższego wynika, że idealnym mechanizmem transferu danych jest decyzja o adekwatności wydana przez Komisję Europejską. Aby taki mechanizm mógł być zastosowany, Komisja musi formalnie stwierdzić, że kraj docelowy transferu danych zapewnia odpowiedni stopień ochrony danych (art. 45 ust. 1 RODO). Takie przekazanie danych nie wymaga już specjalnego zezwolenia. W zasadzie standardem pozwalającym uznać równoważność jest to, że dane będą traktowane w kraju trzecim z praktycznie taką samą starannością, jak gdyby znajdowały się w UE (tj. wewnątrzunijne przekazywanie danych). W RODO określono czynniki (minima), które Komisja musi uwzględnić przy wydawaniu decyzji w sprawie odpowiedniego poziomu ochrony (art. 45 ust. 2 RODO), w szczególności:

[18] Wiążące reguły korporacyjne (BCR) to zasady ochrony danych, których przestrzegają firmy mające siedzibę w UE przy przekazywaniu danych osobowych poza UE w ramach grupy przedsiębiorstw lub przedsiębiorstw. Takie zasady muszą obejmować wszystkie ogólne zasady ochrony danych i możliwe do wyegzekwowania prawa w celu zapewnienia odpowiednich zabezpieczeń przy przekazywaniu danych. Muszą być prawnie wiążące i egzekwowane przez każdego zainteresowanego członka grupy. Firmy muszą przedłożyć wiążące reguły korporacyjne do zatwierdzenia właściwemu organowi ochrony danych w UE. Organ zatwierdzi BCR zgodnie z mechanizmem spójności określonym w art. 63 RODO. Procedura ta może obejmować kilka organów nadzorczych, ponieważ grupa ubiegająca się o zatwierdzenie swoich BCR może posiadać podmioty w więcej niż jednym państwie członkowskim. Właściwy organ przekazuje swój projekt decyzji Europejskiej Radzie Ochrony Danych, która wyda opinię w sprawie wiążących reguł korporacyjnych. Kiedy BCR zostaną sfinalizowane zgodnie z opinią EROD, właściwy organ zatwierdzi BCR. Natomiast zezwolenia organów nadzorczych na podstawie dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby przez te organy nadzorcze. Binding Corporate Rules (BCR) „Corporate rules for data transfers within multinational companies", https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_pl [dostęp: 5 grudnia 2022].

- praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe, 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 oraz orzecznictwo;
- skuteczne i egzekwowalne prawa osób, których dane dotyczą, w kraju przeznaczenia;
- istnienie (lub brak) niezależnych organów nadzorczych w kraju docelowym, które są odpowiedzialne za zapewnienie i egzekwowanie zgodności z przepisami o ochronie danych;
- wszelkie międzynarodowe zobowiązania dotyczące ochrony danych podjęte przez kraj docelowy.

Pamiętać przy tym należy, że decyzje Komisji mają charakter dynamiczny i muszą być poddawane przeglądowi co najmniej raz na cztery lata (art. 45 ust. 3 RODO). Komisja ma również monitorować kraje znajdujące się na białej liście, tzn. te, do których firmy mogą przekazywać dane osobowe bez ograniczeń, na bieżąco – aby sprawdzić, czy nie pojawią się okoliczności, które wpłyną na jej adekwatność. Komisja zachowuje pełne prawo do cofnięcia decyzji o adekwatności w dowolnym momencie, po uprzednim powiadomieniu zainteresowanego podmiotu, bez mocy wstecznej (art. 45 ust. 5 RODO).

W przypadku Stanów Zjednoczonych Komisja uznała je za równoważne (czyli zapewniające odpowiednią ochronę) – ale tylko w ograniczonym zakresie – do ram Bezpieczna przystań (ang. *Safe Harbour*)[19], obowiązujących od 2000 do 2015 roku[20], oraz ram Tarcza prywatności (ang. *Privacy Shield*)[21] – obowiązujących od 2016 do 2020 roku[22].

[19] Decyzja Komisji 2000/520/WE z 26 lipca 2000 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach Bezpiecznej przystani (Safe Harbour) oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, Dz. Urz. WE L 2000, 215, 7 ze zm.

[20] Wyrok TSUE z 6 października 2015 r., Maximillian Schrems v. Data Protection Commissioner, C-362/14, ECLI: EU:C:2015:650.

[21] Decyzja wykonawcza Komisji (UE) 2016/1250 z 12.7.2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę prywatności UE–USA, Dz. Urz. UE L 2016, 207, 1 ze zm.

[22] Wyrok TSUE z 16 lipca 2020 r C-311/18.

Ramy przekazywania danych osobowych Unia Europejska–Stany Zjednoczone

Bezpieczna przystań

Wracając do stanowiącego punkt wyjścia niniejszego artykułu wyroku TSUE, zauważyć należy, że decyzja w sprawie Schrems II jest w swej istocie kolejnym wydarzeniem w trwającym sporze sądowym rozpoczętym w 2013 r., kiedy to austriacki obrońca prywatności Max Schrems złożył skargę do irlandzkiego komisarza ds. ochrony danych osobowych, żądając zakazania irlandzkiej spółce zależnej Facebooka przekazywania jego danych osobowych do Stanów Zjednoczonych. Działanie to, jak twierdził w swojej skardze, było sprzeczne z wymogami adekwatności ochrony jego danych osobowych w ramach reżimu Safe Harbour w związku z ujawnionymi przez Edwarda Snowdena dokumentami dotyczącymi działalności Agencji Bezpieczeństwa Narodowego USA. Mianowicie w połowie 2013 roku Edward Snowden – były pracownik amerykańskiej Agencji Bezpieczeństwa Narodowego (ang. National Security Agency – NSA), opublikował tajne dokumenty amerykańskich służb wywiadowczych. Ujawnione dokumenty wskazywały, że służby te posiadały bezpośredni dostęp do informacji przechowywanych na serwerach amerykańskich gigantów internetowych, takich jak: Google, Apple, Facebook, Microsoft, Skype, YouTube i innych[23]. Skarga została odrzucona przez irlandzką Komisję Ochrony Danych, co skłoniło Schremsa do złożenia wniosku o kontrolę sądową w irlandzkim High Court, który uznał, że zastrzeżenia Schremsa w mniejszym stopniu dotyczyły sposobu, w jaki komisarz zastosował system Safe Harbour, a w większym – samego systemu. Ponieważ irlandzki sąd nie miał jurysdykcji w zakresie reżimu Safe Harbour, sprawa została przekazana do Trybunału Sprawiedliwości Unii Europejskiej w związku z art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej. W październiku 2015 roku Trybunał Sprawiedliwości Unii Europejskiej wydał decyzję w sprawie Schrems v. Data Protection Commissioner. Sąd uznał, że art. 1

[23] A. Michałowicz, *Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy prywatności*, „Monitor Prawniczy", 2016, 23, s. 1264.

decyzji z 2000 roku, która zatwierdziła utworzenie ram Safe Harbour[24], był nieważny, ponieważ ani Federalna Komisja Handlu, ani prywatne organy rozstrzygania sporów nie mogły monitorować naruszeń dokonywanych przez podmioty publiczne, takie jak agencje bezpieczeństwa Stanów Zjednoczonych. Trybunał stwierdził, że uregulowanie umożliwiające organom publicznym uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za zasadnicze naruszenie istoty prawa podstawowego do poszanowania życia prywatnego[25]. Tym samym zasady Safe Harbour zostały uznane za niewystarczające do przekazywania danych osobowych do Stanów Zjednoczonych.

Tarcza prywatności

Aby wypełnić lukę powstałą w wyniku decyzji z 2015 r., Stany Zjednoczone i Unia Europejska ogłosiły w 2016 roku stworzenie nowych ram Tarczy prywatności Unia Europejska–Stany Zjednoczone (i Szwajcaria). Art. 1 ust. 1 i 3 decyzji o adekwatności[26] stwierdzał 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[27]. Ramy omawianego porozumienia obowiązywały od 2016 do 2020 roku, kiedy to Trybunał Sprawiedliwości Unii Europejskiej unieważnił decyzję Privacy Shield. W lipcu 2020 roku Trybunał

[24] 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*).

[25] Wyrok TSUE z 6 października 2015 r., C-362/14, pkt 94.

[26] 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.

[27] Magdalena Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Legalis 2020.

Sprawiedliwości wydał decyzję w sprawie Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems and intervening parties, sprawa C-311/18 (znana jako sprawa Schrems II). Trybunał stwierdził, że Tarcza prywatności nie zapewnia wystarczającej ochrony, ponieważ przepisy Stanów Zjednoczonych dotyczące nadzoru, takie jak rozporządzenie wykonawcze 12333[28] (zwane dalej PPD-28), mają pierwszeństwo w prawie krajowym USA, a ponadto osoby fizyczne nie dysponują wystarczającymi mechanizmami odwoławczymi[29], które byłyby zgodne z prawem UE[30]. Wyrok wpłynął na warte biliony dolarów relacje w zakresie transferu danych pomiędzy Stanami Zjednoczonymi a Unią Europejską. Ponad 5300 firm, w tym giganci technologiczni: Google, Facebook, Amazon i Twitter, polegali przynajmniej częściowo na ramach Privacy Shield w transatlantyckich transferach danych[31]. Po tym orzeczeniu pojawiło się pytanie, jak można zgodnie z prawem przekazywać dane z UE do Stanów Zjednoczonych? Trybunał częściowo odpowiedział na to pytanie: „przekazywanie danych osobowych do państw trzecich może mieć miejsce w przypadku braku decyzji o adekwatności na mocy art. 45 ust. 3 RODO", na podstawie odpowiednich zabezpieczeń na mocy art. 46 RODO[32]. Tak więc wyrok podtrzymał stosowanie standardowych klauzul umownych (SCC)[33], jednak podał w wątpliwość tę metodę przekazywania danych osobowych poza UE. Trybunał podkreślił, że administratorzy danych muszą ocenić poziom ochrony zapewniony przez uzgodnione klauzule umowne między administratorem danych a podmiotem odbierającym / przetwarzającym dane z państwa trzeciego, wszelki dostęp organów publicznych do danych oraz system prawny państwa trzeciego[34]. TSUE powtórzył, że SCC muszą dawać odpowiednie

[28] Executive Order No. 12333 and Presidential Policy Directive No. 28 (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008), October, 7, 2022.

[29] Sekcja 702 ustawy o kontroli wywiadu Foreign Intelligence Surveillance Act (FISA): sąd ds. inwigilacji obcych wywiadów United States Foreign Intelligence Surveillance Court (FISC) nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; dostępne podstawy wszczęcia powództwa są ograniczone, a roszczenia zgłaszane przez osoby fizyczne (w tym osoby będące obywatelami lub rezydentami USA) będą uznane za niedopuszczalne, jeżeli osoby te nie będą mogą wykazać interesu prawnego, co będzie ograniczało dostęp do sądów powszechnych.

[30] Wyrok TSUE z 16 lipca 2020 r., C-311/18 (motywy 68 i 69).

[31] W.A. Reinsch, Transatlantic Data Flows: Permanently Broken or Temporarily Fractured? https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured [dostęp: 5 grudnia 2022].

[32] Wyrok TSUE z 16 lipca 2020 r., C-311/18, pkt 13 i 14.

[33] Standard contractual clauses for data transfers between EU and non-EU countries. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [dostęp: 5 grudnia 2022].

[34] Wyrok TSUE z 16 lipca 2020 r., C-311/18, pkt 101.

gwarancje, zapewniać egzekwowalne prawa i skuteczne środki prawne[35], a administratorzy danych / eksporterzy są zobowiązani do działania w przypadku konfliktu pomiędzy SCC a przepisami państwa trzeciego – w tym niezgodności z przepisami dotyczącymi bezpieczeństwa narodowego – poprzez zawieszenie przepływu danych[36]. W przypadku gdy SCC nie mogą zapewnić „istotnego ekwiwalentu" dla prawa UE, a administratorzy danych nie podjęli działań, TSUE orzekł, że krajowe organy ochrony danych (OOD) muszą zawiesić, ograniczyć, a nawet zakazać międzynarodowego przekazywania danych[37]. W wyniku wyroku wiele podmiotów musiało ponownie przemyśleć sposób, w jaki obsługują transfery danych osobowych, i to, czy stosowane przez nie mechanizmy transferu są zgodne z unijnym prawem ochrony danych. W świetle decyzji Schrems II z 2020 r. Europejska Rada Ochrony Danych (EDPB) i Komisja Europejska (KE) opublikowały swoje zalecenia i aktualizacje standardowych klauzul umownych (SCC), aby pomóc firmom w przestrzeganiu przepisów dotyczących przekazywania danych; przy czym w opracowaniu wydanym 10 listopada 2020 roku – pod nazwą „Zalecenia 01/2020 w sprawie środków uzupełniających zapewniających zgodność transferu z unijnym poziomem ochrony danych osobowych"[38] – Rada nie podaje, jakie konkretnie narzędzia zabezpieczające dane są właściwe. Wskazuje tylko sześć kroków, dzięki którym administrator będzie mógł indywidualnie ocenić swoje potrzeby w tym zakresie. Jako środki zalecane wskazuje się najczęściej[39]:

1) środki prawne:
   - ♦ umowne ograniczenie odbiorcy danych z USA dostępu do nich (np. tylko do zakresu, w jakim jest to niezbędne dla świadczenia przez niego usług);
   - ♦ obowiązek odbiorcy danych z USA poinformowania podmiotu dokonującego transferu o żądaniach ujawnienia danych organów ścigania (gdy obowiązek ujawnienia danych wynika z bezwzględnie obowiązujących przepisów prawa);

[35] *Ibidem*, pkt 103.
[36] *Ibidem*, pkt 134 i 135.
[37] *Ibidem*, pkt 113 i 121.
[38] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020, adoption of the Recommendations for public consulation [!] / Adoption of the Recommendations after public consultation, 18 June 2021. https://edpb.europa.eu/system/files/2021 06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [dostęp: 5 grudnia 2022].
[39] Post-Schrems II: „The European Union Provides Guidance on Data Transfers", JD Supra, https://www.jdsupra.com/legalnews/post-schrems-ii-the- european-union-23981 [dostęp: 5 grudnia 2022].

- obowiązek odbiorcy danych z USA udostępnienia podmiotowi dokonującemu transferu tych informacji, które umożliwią właściwe przeprowadzenie oceny ryzyka (np. informacji o stosowanych przez odbiorcę procedurach i środkach bezpieczeństwa przetwarzania danych, posiadanych certyfikatach itp.);

2) środki organizacyjne:
   - minimalizacja zakresu danych objętych transferem, w tym ograniczenie do minimum transferu danych szczególnej kategorii;
   - posiadanie przez odbiorców danych stosownych certyfikatów bezpieczeństwa (np. norm bezpieczeństwa ISO itp.);
3) środki techniczne:
   - szyfrowanie danych (zarówno podczas transferu, jak i w spoczynku);
   - stosowanie środków uniemożliwiających zapoznanie się z danymi;
   - maskowanie adresów IP.

Ponadto we wrześniu 2020 roku Departament Handlu Stanów Zjednoczonych opublikował zarówno białą księgę, jak i pismo od zastępcy sekretarza ds. usług, w którym potwierdzono zakłócenia, jakie Schrems II stwarza dla transatlantyckiego przepływu danych[40]. Natomiast 27 czerwca 2021 roku weszła w życie decyzja Komisji Europejskiej 2021/914 w sprawie standardowych klauzul umownych (SCC) dotyczących przekazywania danych osobowych do państw trzecich[41]. Zastąpiła ona wcześniejsze decyzje, które były przyjęte na podstawie dyrektywy 95/46[42].

Tak więc standardowe klauzule umowne odnoszą się do następujących scenariuszy przekazywania danych:

- między administratorami,
- przez administratora – podmiotowi przetwarzającemu w państwie trzecim,
- między podmiotami przetwarzającymi,
- przez podmiot przetwarzający – administratorowi w państwie trzecim.

---

[40] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU–U.S. Data Transfers after Schrems II, White Paper, September 2020. https://www.commerce.gov/sites/default/files/2020 09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [dostęp: 15 czerwca 2023].

[41] Decyzja wykonawcza Komisji (UE) 2021/914 z 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, Dz. Urz. UE L 2021, 199, 31.

[42] 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 OJ L 281, 23 listopada 1995, ss. 31–50.

Ponieważ, jak zostało wspomniane, wcześniejsze decyzje Komisji Europejskiej (2001/497/WE[43] i 2010/87/UE[44]) utraciły moc 27 września 2021 roku, umowy zawarte na ich podstawie przed 27 września 2021 r. zapewniały odpowiednie gwarancje w rozumieniu art. 46 ust. 1 RODO do 27 grudnia 2022 r., pod warunkiem że operacje przetwarzania stanowiące przedmiot umowy pozostały niezmienione oraz że stosowanie tych klauzul zapewniało, aby przekazywanie danych osobowych odbywało się z zastrzeżeniem odpowiednich zabezpieczeń (art. 46 ust. 1 RODO).

Reasumując: mechanizmem przekazywania danych z Unii Europejskiej do Stanów Zjednoczonych, jaki stosować można po decyzji Schrems II, wydaje się w szczególności wykorzystanie omówionych zaleceń w systemie opartym na zastosowaniu standardowych klauzul umownych. W art. 46 RODO określono mechanizm służący osiągnięciu tego celu, umożliwiając przekazywanie danych, „jeżeli administrator lub podmiot przetwarzający zapewnili odpowiednie zabezpieczenia oraz pod warunkiem, że dostępne są egzekwowalne prawa osób", których dane dotyczą, oraz skuteczne środki prawne dla tych osób. Zauważyć jednak należy, że w decyzji w sprawie Schrems II wyraźnie zastrzeżono, że konieczne może być podjęcie dodatkowych środków w jurysdykcjach, w których nie istnieje równoważność ochrony; trzeba zatem mieć świadomość, że jest to rozwiązanie tymczasowe[45]. Taka sytuacja może mieć szczególnie miejsce wtedy, kiedy prawa danych podmiotów nie są w państwie trzecim egzekwowalne lub są narażone na znaczną ingerencję, np. ze strony organów lub władz. W kontekście USA – właśnie ze względu na sytuację prawną oraz praktyki stosowane w zakresie przekazywania danych organom ścigania oraz władzom publicznym, w szczególności rygorystyczne przepisy inwigilacyjne – TSUE podał w wątpliwość legalność przekazywania danych osobowych do USA w oparciu tylko o standardowe klauzule umowne (SCC). A zatem cały czas trzeba mieć na uwadze, że zastosowanie nowych standardowych klauzul

[43] Decyzja Komisji z 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE (notyfikowana jako dokument nr C[2001] 1539), tekst mający znaczenie dla EOG, OJ L 181, 4 lipca 2001, ss. 19–31.

[44] Decyzja Komisji z 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (notyfikowana jako dokument nr C(2010) 593) (Tekst mający znaczenie dla EOG) OJ L 39, 12 lutego 2010, ss. 5–18.

[45] U.S.-EU Privacy Shield and Transatlantic Data Flows, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 [dostęp: 5 grudnia 2022].

umownych (SCC) nie wyłącza konieczności oceny planowanego transferu pod kątem zapewnienia zgodności z wyrokiem TSUE w sprawie Schrems II i ewentualnego wdrożenia środków uzupełniających standardowe klauzule umowne.

Biorąc pod uwagę powyższe, powstaje wątpliwość, czy obecnie w ogóle jest możliwy legalny transfer danych do USA, tj. czy nawet przy zastosowaniu pewnych dodatkowych zabezpieczeń i środków bezpieczeństwa podmiot transferujący jest w stanie zapewnić odpowiednią ochronę przekazywanych danych. Niemcy i Irlandczycy rekomendują wstrzymanie przesyłu danych poza EOG[46]. W praktyce jednak raczej żadne podmioty całkowicie nie rezygnują z takiego transferu. Pewne jest natomiast, że wszyscy zainteresowani czekają na nowe regulacje w tym przedmiocie.

Nowe ramy przekazywania danych osobowych z Unii Europejskiej do Stanów Zjednoczonych

Obecnie w fazie rozwoju jest nowy mechanizm prawny, który ma umożliwić przekazywanie danych osobowych między UE a USA. Ma to być najlepszy z dostępnych mechanizmów transferu, tj. oparty na decyzji o adekwatności wydanej przez Komisję Europejską. 25 marca 2022 r. przewodnicząca Komisji Europejskiej Ursula von der Leyen i prezydent Joe Biden ogłosili, że osiągnęli zasadnicze porozumienie, zwane „umową co do zasady", w sprawie nowych ram ochrony prywatności danych UE–USA, które jednak miało charakter polityczny, a nie prawnie wiążący[47]; 7 października prezydent Joe Biden podpisał rozporządzenie wykonawcze w sprawie „wzmocnienia zabezpieczeń działań wywiadowczych Stanów Zjednoczonych dotyczących sygnałów (ang. „Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities")[48], zwane też dalej rozporządzeniem wykonawczym 14086. Wraz

[46] RODO cz. IX Przekazywanie danych do USA – nadal pod znakiem zapytania. https://www.ochrona-danych-osobowych.pl/artykuly/rodo-cz-ix-przekazywanie-danych-do-usa-nadal-pod-znakiem-zapytania [dostęp: 11 czerwca 2023].

[47] Intensifying Negotiations on Trans-Atlantic Data Privacy Flows: A Joint Press Statement by U.S. Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders, https://www.commerce.gov/news/press-releases/2021/03/intensifying-negotiations-trans-atlantic-data-privacy-flows-joint-press [dostęp: 5 grudnia 2022].

[48] Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities October 7, 2022.

z rozporządzeniami[49] wydanymi przez prokuratora generalnego Stanów Zjednoczonych Merricka Garlanda rozporządzenie wykonawcze ma na celu wdrożenie do prawa amerykańskiego umowy co do zasady ogłoszonej w marcu 2022 roku[50]. W następstwie powyższego 13 grudnia 2022 r. Komisja Europejska opublikowała projekt decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do przekazywania danych między UE a USA. Kolejnym krokiem było przyjęcie 28 lutego 2023 roku przez Europejską Radę Ochrony Danych (EROD) opinii w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony danych w odniesieniu do ram ochrony danych UE–USA, w której EROD pozytywnie zaopiniowała takie usprawnienia, jak wprowadzenie wymogów obejmujących zasady konieczności i proporcjonalności gromadzenia danych przez służby wywiadowcze USA oraz nowy mechanizm dotyczący sądowych środków zaskarżenia dla osób w UE, których dane dotyczą. Jednocześnie EROD zgłosiła pewne zastrzeżenia i zwróciła się o wyjaśnienia w kilku innych kwestiach[51]. Natomiast 11 maja 2023 r. – w następstwie zaakceptowania projektu wniosku o przyjęcie rezolucji w sprawie adekwatności – Parlament stwierdził, że ramy „nie zapewniają zasadniczej równoważności" i wezwał Komisję do kontynuowania negocjacji z USA w sprawie ram oraz nieprzyjmowania stwierdzenia adekwatności, dopóki wszystkie zalecenia zawarte w rezolucji i opinii EROD nie zostaną w pełni wdrożone[52]. Ponadto w przyjętej rezolucji Parlament wezwał Komisję do „działania w interesie przedsiębiorstw i obywateli UE poprzez zapewnienie, że proponowane

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities [dostęp: 5 grudnia 2022].
President Joe Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework [dostęp: 5 grudnia 2022].

[49] Data Protection Review Court, Docket No. NSD 103; 28 CFR Part 201. Attorney General Order No. 5517–2022, RIN 1105–AB68, October 7, 2022.
https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf [dostęp: 5 grudnia 2022],
87 FR 198 (10-14-2022) https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022 [dostęp: 5 grudnia 2022].

[50] EU-U.S. Data Privacy Framework
https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 [dostęp: 5 grudnia 2022].

[51] Opinia EROD ws. projektu decyzji dotyczącej ram ochrony danych UE-USA,
https://uodo.gov.pl/pl/138/2644 [dostęp: 15 czerwca 2023].

[52] Projekt rezolucji w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych UE–USA,
www.europarl.europa.eu/doceo/document/B-9-2023-0234_PL.html [dostęp: 15 czerwca 2023].

ramy stanowią solidną, wystarczającą i przyszłościową podstawę prawną dla przekazywania danych między UE a USA". Parlament zauważył wreszcie, że jeśli decyzja stwierdzająca odpowiedni stopień ochrony zostanie przyjęta i ponownie unieważniona przez TSUE, będzie to oznaczać brak ochrony praw obywateli UE i będzie to odpowiedzialność Komisji[53]. Zaznaczyć należy, że rezolucja ta nie jest wiążąca dla Komisji, ale zostanie wzięta pod uwagę przez Komisję przy rozpatrywaniu ram – wraz z opinią EDPB, do której odwołuje się Parlament.

Konieczność i proporcjonalność na mocy rozporządzenia wykonawczego

Badając, czy w Stanach Zjednoczonych istnieje odpowiedni poziom ochrony danych równoważny z unijnym, Komisja Europejska ma za zadanie ustalić, czy spełnione są wymagania stawiane przez TSUE w analizowanym wyroku w sprawie Schrems II, to znaczy czy amerykańska inwigilacja jest „proporcjonalna" w rozumieniu art. 52 Karty praw podstawowych oraz czy istnieje dostęp do „sądowych środków odwoławczych", zgodnie z wymogami art. 47 KPP[54]. W odniesieniu do pierwszego z wymogów – prezydenckie rozporządzenie wykonawcze 14086 nakłada ograniczenia związane z koniecznością i proporcjonalnością, najpierw poprzez wyraźne ich wprowadzenie, następnie poprzez wyjaśnienie, co oznacza ten mandat, a na koniec poprzez ustanowienie mechanizmów nadzoru w celu sprawdzenia, czy agencje wywiadowcze przestrzegają nowych zasad. Stanowi ono: „(a)(i)(A) działania w zakresie wywiadu sygnałowego są prowadzone wyłącznie po ustaleniu, opartym na rozsądnej ocenie wszystkich istotnych czynników, że działania te są niezbędne do realizacji potwierdzonego priorytetu wywiadowczego, chociaż wywiad sygnałowy nie musi być jedynym dostępnym lub wykorzystywanym środkiem do realizacji aspektów potwierdzonego priorytetu wywiadowczego[55]; oraz (B) działania w zakresie wywiadu sygnałowego są prowadzone wyłącznie w zakresie i w sposób proporcjonalny do zatwierdzonego priorytetu wywiadowczego, dla którego zostały zatwierdzone, w celu osiągnięcia

[53] *Ibidem*.
[54] Wyrok TSUE z 16 lipca 2020 r., C-311/18, pkt 68.
[55] Executive Order On..., October 7, 2022.

właściwej równowagi między znaczeniem zatwierdzonego priorytetu wywiadowczego, który jest realizowany, a wpływem na prywatność i swobody obywatelskie wszystkich osób, niezależnie od ich narodowości lub miejsca zamieszkania"[56]. Następnie omawiane rozporządzenie wyjaśnia, co to oznacza w praktyce, umieszczając wyraźne zabezpieczenia wokół dopuszczalnych i niedopuszczalnych działań związanych z gromadzeniem danych (sekcja 2 lit. c). Zabezpieczenia te dotyczą między innymi tego, jakie dane wywiadowcze dotyczące sygnałów mogą być gromadzone, jak mogą być wykorzystywane i udostępniane oraz jak długo mogą być przechowywane.

Rozporządzenie wykonawcze określa następnie 12 „uzasadnionych celów", takich jak „ochrona przed zagrożeniami dla personelu Stanów Zjednoczonych lub ich sojuszników", z którymi muszą być zgodne działania wywiadu sygnałowego, oraz „cztery cele zakazane" – takie jak „tłumienie lub obciążanie, krytyka, niezgoda lub swobodne wyrażanie idei lub poglądów politycznych" (sekcja 2 lit. b)[57]. Wreszcie omawiane rozporządzenie określa mechanizmy nadzoru. Obejmują one: wymóg, aby urzędnik ds. ochrony wolności obywatelskich w Biurze Dyrektora Wywiadu Narodowego regularnie oceniał, czy priorytety wywiadowcze odnoszące się do działań wywiadu sygnałowego wykraczają poza te granice, nakaz, aby każda komórka społeczności wywiadowczej miała urzędnika ds. ochrony prywatności i wolności obywatelskich[58] oraz inspektora generalnego z uprawnieniami nadzorczymi[59], który nie podlega niewłaściwym wpływom, a także wymóg szkolenia w zakresie rozporządzenia wykonawczego.

Poprzez powyższe zapisy rozporządzenie ma na celu ograniczenie dostępu rządu USA do danych przekazywanych z niektórych jurysdykcji (w tym z EWG i Zjednoczonego Królestwa), w szczególności ograniczając ten dostęp organów wywiadowczych USA do tego, co jest konieczne i proporcjonalne do ochrony bezpieczeństwa narodowego. Jednak krytycy nowego rozporządzenia wykonawczego 14086 zarzucają, że ow-

[56] *Ibidem*.
[57] *Ibidem*.
[58] Intelligence Community Directive 126 – Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086, https://www.dni.gov/index.php/who-we-are/organizations/197-about/organization/office-of-civil-liberties-privacy-and-transparency [dostęp: 5 grudnia 2022].
[59] FAQs How was the position of the Inspector General of the IC created? https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-about-us/icig-faqs [dostęp: 5 grudnia 2022].

szem, użyto w nim sformułowań pochodzących z prawa UE („konieczny" i „proporcjonalny" – jak w art. 52 KPP), lecz nie będą one miały takiego samego znaczenia prawnego, co w europejskim rozumieniu tego słowa – i nic nie wskazuje na to, że w praktyce masowa inwigilacja w USA się zmieni. Tak zwany „bulk surveillance"[60] będzie kontynuowany na mocy nowego rozporządzenia wykonawczego (patrz sekcja 2 (c)(ii))[61], a wszelkie dane wysyłane do amerykańskich dostawców nadal będą trafiać do programów takich jak PRISM[62] czy Upstream[63], pomimo dwukrotnego uznania przez TSUE amerykańskich przepisów i praktyk inwigilacyjnych za „nieproporcjonalne"[64].

Mechanizm dochodzenia roszczeń

Rozporządzenie wykonawcze 14086 zostało połączone z przepisami Departamentu Sprawiedliwości (DOJ)[65] w celu stworzenia dwuetapowego systemu dochodzenia roszczeń, w tym nowego Sądu Kontroli Ochrony Danych (DPRC), w celu rozpatrywania skarg dotyczących legalności amerykańskich działań w zakresie wywiadu sygnałowego przekazywanych z „kwalifikujących się państw" w związku z naruszeniami prawa USA. Mianowicie sekcja 3 rozporządzenia wykonawczego 14086 pod nazwą „Wzmoc-

[60] Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations Edited by the Heinrich Böll Foundation.Thorsten Wetzling, Kilian Vieth. Berlin, November 2018, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf [dostęp: 5 grudnia 2022]. Mass surveillance September 2022 ECHR, https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf [dostęp: 5 grudnia 2022]. Secret CIA Bulk Surveillance Program Includes Some Americans' Records, Senators Say. WSJ, Feb. 10, 2022, https://www.wsj.com/articles/secret-cia-bulk-surveillance-program-includes-some-americans-records-senators-say-11644549582 [dostęp: 5 grudnia 2022].

[61] Executive Order On..., October 7, 2022.

[62] PRISM to kryptonim programu, w ramach którego Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) zbiera informacje internetowe od różnych amerykańskich firm internetowych https://en.wikipedia.org/wiki/PRISM [dostęp: 5 grudnia 2022].

[63] „Upstream collection" to termin używany przez Agencję Bezpieczeństwa Narodowego (NSA) Stanów Zjednoczonych do przechwytywania ruchu telefonicznego i internetowego z infrastruktury sieciowej, co oznacza główne kable i przełączniki internetowe – zarówno krajowe, jak i zagraniczne, https://en.wikipedia.org/wiki/Upstream_collection [dostęp: 5 grudnia 2022].

[64] NYOB Data transfer, https://noyb.eu/pl/projekt%20/przekazuj%C4%85cy%20eeu-us-transfery [dostęp: 5 grudnia 2022].

[65] Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence Activities https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence [dostęp: 11 czerwca 2022].

nienie zabezpieczeń dla działań wywiadowczych Stanów Zjednoczonych”[66] upoważniła i nakazała prokuratorowi generalnemu wydanie rozporządzeń w celu ustanowienia Sądu Kontroli Ochrony Danych jako drugiego poziomu dwustopniowego mechanizmu odwoławczego. Miało to na celu spełnienie drugiego z wymogów nałożonych przez TSUE, tj. zapewnienie lepszych środków prawnych dla osób fizycznych zamieszkałych w takich jurysdykcjach, jak EWG, które twierdzą, że ich prawo do prywatności zostało naruszone. W szczególności decyzja TSUE stwierdziła, że istnieje „luka w ochronie sądowej w odniesieniu do ingerencji w programy wywiadowcze” oraz że „[…] ani PPD-28[67] nie przyznają osobom, których dane dotyczą, praw zaskarżalnych do sądu przeciwko władzom USA, z czego wynika, że osoby, których dane dotyczą, nie mają prawa do skutecznego środka odwoławczego”[68]; przy czym dwustopniowy system odwoławczy rozpocząć się ma od przeprowadzenia przez urzędnika ds. ochrony wolności obywatelskich w Biurze Dyrektora Wywiadu Narodowego (CLPO[69]) wstępnego dochodzenia w sprawie otrzymanych skarg w celu ustalenia, czy doszło do naruszenia wzmocnionych zabezpieczeń zawartych w rozporządzeniu wykonawczym lub innych obowiązujących przepisów prawa amerykańskiego. Co ważne, wyniki tego procesu będą wiążące dla amerykańskich agencji wywiadowczych[70]. Drugim poziomem dwustopniowego mechanizmu odwoławczego ma być wspomniany Sąd Kontroli Ochrony Danych.

Autor artykułu zauważa, że zasady działania nowego mechanizmu odwoławczego w zakresie wywiadu sygnałowego ustanowionego przez reformy prawne w USA są zbyt szczegółowe, aby omówić je w tym artykule w całości. W związku z powyższym skupia się jedynie na pewnych konkretnych aspektach tego mechanizmu, starając się odpowiedzieć na pytanie, czy decyzje nowego Sądu Kontroli Ochrony Danych spełniłyby odpowiednie wymogi prawne UE w zakresie niezależności i skuteczności przy podejmowaniu decyzji w sprawie skargi złożonej przez osobę z UE.

W pierwszej kolejności zauważyć należy, że nowe rozporządzenie wykonawcze i rozporządzenie prokuratora generalnego nazywają nowy organ „sądem”. W Europie taki organ może być postrzegany nie jako sąd, ale

[66] Executive Order On..., October 7, 2022.
[67] Wyrok Trybunału z 16 lipca 2020 r., sprawa C-311/18, pkt 48.
[68] Wyrok Trybunału z 16 lipca 2020 r., sprawa C-311/18 (motyw 109, 112).
[69] https://www.dni.gov/index.php/nctc-who-we-are/organization/197-about/organization/office-of-civil-liberties-privacy-and-transparency/1387-clpo-home [dostęp: 5 grudnia 2022].
[70] Executive Order On..., October 7, 2022.

raczej jako niezależny organ administracyjny pełniący funkcje *quasi*-sądowe, podobnie jak kilka organów nadzoru nad wywiadem w kontekście odszkodowań w Europie, takich jak francuska Commission[71] nationale de contrôle des techniques de renseignement czy niemiecka Komisja G10[72]. Budząca szczególne wątpliwości jest też „wystarczalność" odpowiedzi podsumowującej, którą DPRC ma prawo udzielić skarżącemu, a w której DPRC ani nie potwierdzi, ani nie zaprzeczy, czy skarżący podlegał działaniom wywiadu kryminalnego Stanów Zjednoczonych, a zamiast tego poinformuje wnioskodawcę, że „w wyniku przeglądu nie stwierdzono żadnych naruszeń objętych przepisami" lub że DPRC „wydał ustalenie wymagające odpowiednich środków zaradczych". Kolejny ewentualny zarzut to brak regulacji ustawowej. Mimo że wielu postulowało przyjęcie rozwiązania ustawowego, rząd USA stworzył mechanizm odwoławczy przez akty władzy wykonawczej – zamiast posłużyć się ustawą. W pewnym stopniu na przeszkodzie stało zapewne konstytucyjne orzecznictwo Sądu Najwyższego USA dotyczące tego, kto ma „legitymację" do składania pozwów w amerykańskich sądach federalnych[73]. Doktryna legitymacji procesowej w USA wywodzi się z artykułu III Konstytucji USA, który reguluje system sądów federalnych. Federalna władza sądownicza rozciąga się tylko na „sprawy" i „kontrowersje" – co oznacza, że musi istnieć „rzeczywista szkoda", aby sprawa mogła zostać rozpatrzona[74]. Takie rozumienie szkody nie zapewnia legitymacji w sądzie federalnym dla wszystkich osób z UE, które mają prawo do zadośćuczynienia. Tak więc utworzenie Sądu Kontroli Ochrony Danych w drodze aktu władzy wykonawczej tworzy pozycję, której nie można zapewnić skarżącym w sądach federalnych. To, co zarzuca się rozwiązaniu nieustawowemu, to m.in. możliwość szybkiej zmiany rozwiązania opartego na rozporządzeniach. Jednak w amerykańskim systemie prawnym rozporządzenie wydane przez agencję ma moc wiążącą, co czyni

[71] National Commission on Informatics and Liberty. Jest niezależnym francuskim administracyjnym organem regulacyjnym, którego misją jest zapewnienie stosowania prawa o ochronie danych w odniesieniu do gromadzenie, przechowywanie i wykorzystywanie danych osobowych. Jego istnienie zostało ustanowione przez francuską ustawę nr 78-17 w sprawie technologii informacyjnej, plików danych i wolności obywatelskiej z 6 stycznia 1978 r. i jest krajowym organem ds. ochrony danych we Francji. https://www.cnil.fr/en/home [dostęp: 5 grudnia 2022].

[72] https://www.bundestag.de/ausschuesse/weitere_gremien/g10_kommission [dostęp: 5 grudnia 2022].

[73] The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC; https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/ [dostęp: 13 czerwca 2023]

[74] Article. III. Section. 2. The Constitution of the United States https://www.senate.gov/civics/constitution_item/constitution.htm [dostęp: 5 grudnia 2022].

je odpowiednim narzędziem do określenia procedur rozpatrywania wniosków i skarg odszkodowawczych[75].

Sąd Najwyższy w sprawie Motor Vehicles Manufacturers Association przeciwko State Farm Mutual Automobile Insurance stwierdził, że w celu ochrony przed arbitralnymi lub nagłymi zmianami zmiana lub uchylenie rozporządzenia wymagałyby przeprowadzenia takich samych publicznych kroków proceduralnych, jak uchwalenie go w pierwszej kolejności[76]. Zapewnia to ochronę przed uchyleniem rozporządzenia w trybie przyspieszonym, gwarantując, że organ będzie nadal działał niezależnie, chyba że rozporządzenie zostanie ostatecznie i publicznie zmienione. Podkreślić należy, że kluczowe decyzje Sądu Najwyższego USA potwierdziły moc wiążącą rozporządzenia Departamentu Sprawiedliwości (DOJ), a tym samym wniosek prawny, że cała władza wykonawcza, w tym prezydent i prokurator generalny, jest nim związana[77]. W jednogłośnej decyzji Sądu Najwyższego z 1974 r., United States v. Nixon, uznano, że decyzja specjalnego prokuratora o wydaniu wezwania do sądu prezydentowi miała moc prawną, pomimo sprzeciwu prokuratora generalnego. Sąd Najwyższy zauważył, że „rozporządzenie daje prokuratorowi specjalnemu wyraźne uprawnienia" do prowadzenia dochodzenia i wydawania wezwań sądowych oraz że „dopóki rozporządzenie to obowiązuje, ma ono moc prawną". Sąd dodał: „Tak długo, jak rozporządzenie to pozostaje w mocy, władza wykonawcza jest nim związana, a Stany Zjednoczone, jako suweren składający się z trzech gałęzi, są zobowiązane do jego przestrzegania i egzekwowania". Decyzja Nixona potwierdziła wcześniejszą sprawę dotyczącą niezależnych decyzji osób orzekających, których stanowiska zostały utworzone na mocy rozporządzenia Departamentu Sprawiedliwości. W sprawie z 1954 roku, Accardi przeciwko Shaughnessy[78], prokurator generalny w drodze rozporządzenia przekazał niektóre ze swoich uprawnień uznaniowych Radzie Apelacji Imigracyjnych. Rozporządzenie wymagało, aby Rada korzystała z własnego uznania w przypadku odwołań od decyzji o deportacji. Jak

[75] The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC.

[76] United States Supreme Court Motor Vehicle Mfrs. Assn. Association v. State Farm Mut. (1983) No. 82-354, Argued: April 26, 1983, Decided: June 24, 1983 https://caselaw.findlaw.com/us-supreme-court/463/29.html [dostęp: 5 grudnia 2022].

[77] United States v. Nixon, 418 U.S. 683 (1974) No. 73-1766, 418 U.S. 683. https://supreme.justia.com/cases/federal/us/418/683 [dostęp: 5 grudnia 2022].

[78] U.S. Supreme Court Accardi v. Shaughnessy, 347 U.S. 260 (1954) https://supreme.justia.com/cases/federal/us/347/260 [dostęp: 13 czerwca 2022].

zauważono w sprawie U.S. v. Nixon, Sąd Najwyższy w sprawie Accardi orzekł, że „tak długo, jak przepisy prokuratora generalnego pozostawały w mocy, odmawiał on sobie uprawnień do korzystania z uznania przekazanego Radzie, mimo że pierwotne uprawnienia należały do niego i mógł je potwierdzić poprzez zmianę przepisów".

Dodatkowo wydaje się, że decyzja UE w sprawie odpowiedniego poziomu ochrony mogłaby być uzależniona od utrzymania rozporządzenia przez DOJ[79]. Rozporządzenie DOJ zapewnia niezależność poprzez swoje zasady powoływania. Stanowi ono, że prokurator generalny „mianuje nie mniej niż sześć osób do pełnienia funkcji sędziów w DPRC na czteroletnie odnawialne kadencje, wybierając osoby, które w momencie ich pierwszego mianowania nie były pracownikami oddziału wykonawczego w ciągu poprzednich dwóch lat"[80]. Podczas sprawowania funkcji w DPRC sędziowie nie pełniłby żadnych innych „oficjalnych obowiązków ani nie byliby zatrudnieni w ramach rządu Stanów Zjednoczonych". Co najmniej połowa sędziów powinna mieć wcześniejsze doświadczenie sądowe, a wybór powinien być oparty na „odpowiednim doświadczeniu w dziedzinie prawa dotyczącego prywatności danych i bezpieczeństwa narodowego". Rozporządzenie DOJ tworzy niezależność również przez swe przepisy dotyczące nadzoru i usuwania. Sekcja 201.7 stwierdza, że „Panel DPRC i jego sędziowie nie podlegają bieżącemu nadzorowi prokuratora generalnego". Rozporządzenie ogólnie stanowi, że „Prokurator generalny nie usunie sędziego z panelu DPRC, nie usunie sędziego z DPRC przed końcem jego kadencji na podstawie (§ 201.3[a])[81] [...] ani nie podejmie żadnych innych niekorzystnych działań wobec sędziego wynikających z pełnienia służby w DPRC".

Podsumowanie

Transatlantycki przepływ danych ma ogromne znaczenie gospodarcze, gdyż obejmuje liczne firmy, w tym gigantów technologicznych. Decyzja TSUE w sprawie Schrems II z 2020 roku – w połączeniu z decyzją TSUE

[79] The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC; https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc [dostęp: 5 grudnia 2022].

[80] § 201.3 Appointment of judges and rules of procedure, (a) 28 CFR Part 201..., October 7, 2022.

[81] *Ibidem*.

w sprawie Schrems I z 2015 roku – podważyła standardowe praktyki stosowane przy transferze danych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy prywatności – i wymaga wypracowania nowego mechanizmu przekazywania danych na przyszłość.

W oczekiwaniu na przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony przedsiębiorstwa mogą nadal polegać na innych prawnie ważnych mechanizmach przekazywania danych uznanych przez RODO, takich jak wiążące reguły korporacyjne i standardowe klauzule umowne (SCC). W świetle decyzji Schrems II Europejska Rada Ochrony Danych i Komisja Europejska opublikowały swe zalecenia co do standardowych klauzul umownych (SCC), aby pomóc firmom w zapewnieniu zgodności z przepisami dotyczącymi przekazywania danych. Reasumując szczegółowe omówienie tych zagadnień w niniejszym artykule, zauważyć należy, że wspomniane zalecenia obejmują nałożenie na podmioty przekazujące dane obowiązku zidentyfikowania narzędzi przekazywania, takich jak SCC, oceny zastosowania art. 46 RODO w celu zapewnienia „zasadniczo równoważnej" ochrony, przyjęcia dodatkowych środków – takich jak szyfrowanie lub wymogi umowne – oraz opracowania wymagań proceduralnych w celu zapewnienia zgodności i bieżącej oceny środków. Trzeba przy tym pamiętać, że przekazywanie danych osobowych poza EOG na podstawie umów niezgodnych z nowymi standardowymi klauzulami umownymi może stanowić naruszenie zasad przetwarzania danych osobowych poprzez ich transfer bez zastosowania odpowiednich zabezpieczeń, a tym samym naruszenie przepisów RODO. Taka sytuacja może narazić podmioty dokonujące transferów na kary, które mogą zostać nałożone przez organ nadzorczy. Z uwagi więc na trudności prawne i koszty – prezentowane rozwiązanie jest trudne do utrzymania przez dłuższy czas i raczej powinno być traktowane jako tymczasowe.

Na koniec wreszcie wypada zauważyć, że obecny konflikt prawny między Unią Europejską a Stanami Zjednoczonymi nie jest nowy, ponieważ stanowi element szerszej debaty dotyczącej wymiany danych między tymi dwiema jurysdykcjami oraz ogólnie – szerszej roli wymiany danych i informacji między krajami. Schrems walczy w sądzie z transatlantyckim przepływem danych osobowych od 2013 roku. Należy się spodziewać, że zarówno finalna decyzja Komisji UE, jak i wszelkie przyszłe porozumienia ponownie zezwalające na przepływ danych do Stanów Zjednoczonych zostaną zakwestionowane przez aktywistów działających na rzecz prawa

do prywatności i prawa do ochrony danych osobowych, podobnie jak poprzednie rozwiązania.

Abstrakt
Przedmiotem artykułu są transgraniczne przepływy danych między Unią Europejską a Stanami Zjednoczonymi po unieważnieniu Tarczy prywatności UE–USA (*Privacy Shield*) przez Trybunał Sprawiedliwości Unii Europejskiej. Poruszono kwestie ograniczeń transferu danych poza Unię Europejską wprowadzonych przez ogólne rozporządzenie o ochronie danych (RODO) oraz brak pełnej, uznawanej przez UE, odpowiedniej ochrony danych w Stanach Zjednoczonych. W artykule analizuje się przełomowy wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems II oraz nowo powstały amerykański akt prawny: rozporządzenie w sprawie wzmocnienia zabezpieczeń działań wywiadowczych Stanów Zjednoczonych dotyczących sygnałów – w aspekcie zapewnienia zgodności z przepisami dotyczącymi danych osobowych oraz w szerszym kontekście relacji transatlantyckich i gospodarki cyfrowej. Analizy powyższych zagadnień dokonano w celu oceny dostępnych możliwości przekazywania danych osobowych między Unią Europejską a Stanami Zjednoczonymi, a także wskazania implikacji obecnej sytuacji dla firm działających w obszarze transgranicznych przepływów danych.

Słowa kluczowe: transgraniczne przepływy danych, Tarcza prywatności UE–USA, ogólne rozporządzenie o ochronie danych (RODO), sprawa Schrems II, dane osobowe, rozporządzenie w sprawie wzmocnienia zabezpieczeń działań wywiadowczych Stanów Zjednoczonych dotyczących sygnałów, relacje transatlantyckie, gospodarka cyfrowa.

BIBLIOGRAFIA

Karwala D., Komercyjne transfery danych osobowych do państw trzecich, Warszawa 2018.

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

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

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

Schulz T.J., *Schrems v. Data Protection Commissioner* (C.J.E.U.), „International Legal Materials", Vol. 56, No. 2, Cambridge University Press, Apr. 2017, Cambridge University Press, doi:10.1017/ilm.2017.8.

Źródła internetowe

Advocate General's Opinion in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, Court of Justice of the European Union PRESS RELEASE No 165/19 Luxembourg, 19 December 2019, https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf [dostęp: 5 grudnia 2022].

Binding Corporate Rules (BCR), Corporate rules for data transfers within multinational companies,
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_pl [dostęp: 5 grudnia 2022].

Castro D., Mcquinn A., Cross-Border Data Flows Enable Growth in All Industries, INFO. TECH INNOVATION FOUND (Feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf [dostęp: 5 grudnia 2022].

Digital Economy Report 2021 Cross Border data flows and development: For whom the data flow United Nations Conference on Trade and Development.2021, United Nations, https://unctad.org/system/files/official-document/der2021_en.pdf [dostęp: 5 grudnia 2022].

EU–U.S. Data Privacy Framework, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 [dostęp: 5 grudnia 2022].

Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence Activities https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence [dostęp: 11 czerwca 2022].

FAQs How was the position of the Inspector General of the IC created?
https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-about-us/icig-faqs [dostęp: 5 grudnia 2022].

Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU–U.S. Data Transfers after Schrems II. White Paper September 2020,
https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [dostęp: 15 czerwca 2023].

Intelligence Community Directive 126 – Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086,
https://www.dni.gov/index.php/who-we-are/organizations/197-about/organization/office-of-civil-liberties-privacy-and-transparency [dostęp: 5 grudnia 2022].

Intensifying Negotiations on Trans-Atlantic Data Privacy Flows: A Joint Press Statement by U.S. Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders, https://www.commerce.gov/news/press-releases/2021/03/intensifying-negotiations-trans-atlantic-data-privacy-flows-joint-press [dostęp: 5 grudnia 2022].

Komunikat prasowy, Departament Handlu, Sekretarz Handlu USA Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows 16 lipca 2020, https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows [dostęp: 5 grudnia 2022].

Mass surveillance September 2022 ECHR, https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf [dostęp: 5 grudnia 2022].

NYOB Data transfer, https://noyb.eu/pl/projekt%20/przekazuj%C4%85cy%20eeu-us-transfery [dostęp: 5 grudnia 2022].

Opinia EROD ws. projektu decyzji dotyczącej ram ochrony danych UE-USA, https://uodo.gov.pl/pl/138/2644 [dostęp: 15 czerwca 2023].

Post-Schrems II: „The European Union Provides Guidance on Data Transfers", JD Supra, https://www.jdsupra.com/legalnews/post-schrems-ii-the-european-union-23981 [dostęp: 5 grudnia 2022].

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020 Adoption of the Recommendations for public consulation / Adoption of the Recommendations after public consultation, 18 June 2021.
https://edpb.europa.eu/system/files/202106/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [dostęp: 5 grudnia 2022].

Reinsch W.A., Transatlantic Data Flows: Permanently Broken or Temporarily Fractured? https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured [dostęp: 5 grudnia 2022].

RODO cz. IX Przekazywanie danych do USA – nadal pod znakiem zapytania. https://www.ochrona-danych-osobowych.pl/artykuly/rodo-cz-ix-przekazywanie-danych-do-usa-nadal-pod-znakiem-zapytania [dostęp: 11 czerwca 2023].

Schrems II landmark ruling: „A detailed analysis." Norton Rose Fulbright, czerwiec 2020, https://www.nortonrosefulbright.com/en-gb/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis [dostęp: 14 czerwca 2023].

Schwab K., World Economic Forum 2016, The Fourth_Industrial Revolution,
https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab [dostęp: 15 czerwca 2023].

Secret CIA Bulk Surveillance Program Includes Some Americans' Records, Senators Say. WSJ, Feb. 10, 2022.
https://www.wsj.com/articles/secret-cia-bulk-surveillance-program-includes-some-americans-records-senators-say-11644549582 [dostęp: 5 grudnia 2022].

Standard contractual clauses for data transfers between EU and non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [dostęp: 5 grudnia 2022].

The Congressional Research Service (CRS) June 2, 2022, U.S.–EU Trans-Atlantic Data Privacy Framework, https://crsreports.congress.gov/product/pdf/IF/IF11613 [dostęp: 5 grudnia 2022].

The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC, https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/ [dostęp: 13 czerwca 2023].

Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations Edited by the Heinrich Böll Foundation.Thorsten Wetzling,Kilian Vieth. Berlin, November 2018, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf [dostęp: 5 grudnia 2022].

U.S.-EU Privacy Shield and Transatlantic Data Flows, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 [dostęp: 5 grudnia 2022].