Legalność transferu danych między EOG a USA za pomocą chmury obliczeniowej w świetle przepisów tzw. RODO oraz Cloud Act w odniesieniu do odpowiedzialności administratora

Katarzyna Smagacz[1]

Celem artykułu jest przedstawienie usystematyzowanego podsumowania problematycznych aspektów transferu danych do państw trzecich przy użyciu chmury obliczeniowej, a w szczególności do Zjednoczonych Stanów Ameryki, powstałych na skutek unieważnienia Tarczy Prywatności, która do 2020 r. regulowała w tym zakresie stosunki UE–USA. Ze względu na złożoność problemu przyjęto za naczelną perspektywę administratora danych. Oprócz zakreślenia definicji niezbędnych do zrozumienia istoty problemu oraz przełomowego wyroku TSUE z 16.7.2020 r. w sprawie C-311/18 ustosunkowano się również do niezwykle istotnej składowej relacji EOG–US–Cloud Act, snując spekulacje, czy mimo podjęcia przez administratorów możliwych środków bezpieczeństwa, poufność danych będzie zachowana, a administratorzy będą mogli zostać pociągnięci do odpowiedzialności prawnej, przy jednoczesnym podjęciu rozważań w zakresie zgodności Cloud Act z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2].

Uwagi wstępne

Globalny charakter Internetu jest niezmiennie wyzwaniem dla dotychczasowego porządku prawnego opartego na dogmacie terytorialnej suwerenności państw[3]. Zatarcie granic przepływu informacji, a w tym danych osobowych, może być szczególnie zauważalne przy usługach związanych z chmurą obliczeniową (dalej jako: Chmura). Główną ideą rozwiązań chmurowych jest inwestycja w moc obliczeniową, zamiast jak odbywało się to do tej pory – w sprzęt komputerowy[4]. Jest to jednak nie tylko wynajęta moc obliczeniowa, ale także rozproszone systemy operacyjne, umożliwiające zarówno uruchomienie własnego oprogramowania, jak i zdalne użytkowanie czyjegoś, już istniejącego[5]. Relokacja kapitału, idąca w parze z relokacją danych, skutecznie wspiera rozwój społeczno-gospodarczy społeczeństwa[6], niwelując fizyczne ograniczenia dostępu do informacji, a także ich przesyłu – jedynym tego warunkiem staje się dostęp do sieci internetowej oraz odpowiednia autoryzacja użytkownika chmury. Ze względu na potrzebę regulacji przepływu danych, a tym samym ich ochrony, powstały liczne regulacje starające się usystematyzować przestrzeń zdigitalizowaną.

Transfer danych osobowych za pomocą chmury do państw trzecich

Tematyka chmury zrodziła się w latach 90. XX w., a sama definicja powstała prawie 20 lat później. *National Institute of Standards and Technology of the United States Department of Commerce* w 2009 r. upublicznił, po konsultacjach z inwestorami oraz rządem, pierwszą definicję chmury na poświęconej jej stronie internetowej. Dwa lata później została ona podana do wiadomości publicznej – w projekcie publicznym SP 800-145[7]. Obecnie brzmi następująco: „*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*[8]"[9].

[1] Autorka jest studentką IV roku prawa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. ORCiD: 0009-0001-4113-1467.

[2] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[3] *M. Giaro*, Zawarcie umowy w trybie aukcji internetowej, Warszawa 2014, *passim*.

[4] *J. Arundel*, *J. Domingus*, Kubernetes – rozwiązania chmurowe w świecie DevOps, tworzenie wdrażanie i skalowanie nowoczesnych aplikacji chmurowych, Gliwice 2020.

[5] *Ibidem*.

[6] *M. Kubalińska*, Wpływ cloud computing na budowę społeczeństwa informacyjnego i rozwój gospodarczy. Nierówności społeczne a wzrost gospodarczy 2013, Nr 32, s. 135–145.

[7] *M. Parlinska*, *I. Petrovska*, Cloud computing and its benefits. Information Systems in Management 2017, Nr 6 (4), s. 309–317.

[8] Cloud computing to model umożliwiający powszechny, wygodny, na żądanie dostęp do współdzielonego puli zasobów konfigurowalnych w dziedzinie obliczeniowej (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które można szybko wdrożyć i zwolnić z minimalnym wysiłkiem zarządzania lub interakcji z dostawcą usług. Ten model chmury składa się z pięciu podstawowych cech, trzech modeli usług i czterech modeli wdrożenia [tłum. własne autor].

[9] Zob. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (dostęp z 21.4.2023 r.).

Istotą jej zastosowania jest przetwarzanie danych na serwerach należących do podmiotów trzecich, przy jednoczesnym zapewnieniu zdalnego dostępu do tych informacji[10].

Zbieranie, przechowywanie i analiza danych ma tendencję wzrostową i pozornie nieograniczoną[11]. W dzisiejszych czasach codziennie generowane są ogromne ilości danych w sektorach produkcji, biznesu, nauki i życia osobistego ludzi[12]. Technologie związane z przetwarzaniem dużych zbiorów danych poprzez agregację i dedukcję z bloków danych nieosobowych mogą umożliwiać identyfikację osób. Ma to miejsce zwykle w celach handlowych takich jak np. ukierunkowana reklama[13]. W związku z potencjałem wykorzystania tych informacji również w obszarach bardziej problematycznych, jak represje polityczne oraz nadzór rządy wyraziły zaniepokojenie przesyłaniem i przechowywaniem danych osobowych obywateli, nawet w formie zbiorczej, poza ich granicami[14].

Ochrona danych osobowych w obszarze Europejskiego Okręgu Gospodarczego (EOG) obecnie gwarantowana jest na podstawie RODO. Jest ono niezależne zarówno pod kątem sposobu przetwarzania danych, jak i ich przechowywania.

Za art. 1 RODO wśród celów tego aktu wyróżnić można te główne, czyli: realizację podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i umożliwienie swobodnego przepływu danych osobowych tak, aby ochrona praw jednostki nie stawała temu na przeszkodzie[15]. Brak jednak w treści rozporządzenia jednoznacznego wskazania celu dominującego.

O celach i sposobach przetwarzania danych decyduje administrator. Pojęcie to ujęte zostało brzmieniem art. 4 ust. 7 RODO, gdzie określenie to oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Sama operacja polegająca na przekazywaniu danych osobowych z obszaru EOG do państwa trzeciego stanowi przetwarzanie danych osobowych[16]. Natomiast dostawca usług w chmurze odgrywa rolę podmiotu przetwarzającego[17]. W art. 28 ust. 3 RODO wskazuje się, że przetwarzanie to odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Dane będące przedmiotem transferu mogą podlegać ochronie w różnym stopniu. Jak wynika z art. 8 Karty Praw Podstawowych[18], każdemu przysługuje prawo ochrony danych, które go dotyczą. Dodatkowo muszą być one przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Choć w RODO nie sposób znaleźć ich enumeratywnie wyznaczonego ich zbioru, powołując się na art. 4 ust. 1, wskazać można pewne cechy informacji, których spełnienie wiązać się będzie z zaliczeniem do grupy „danych osobowych". Określa się ich mianem informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Panuje jednak spór w doktrynie co do jednoznacznej ich definicji[19].

Przyjąć można, że sam fakt zawierania w sobie takich informacji jak imię i nazwisko jest równoznaczny z możliwością udostępnienia powyższego, a w dalszej kolejności znalezienia się w posiadaniu danych dotyczących pewnej osoby[20]. Zdaniem odrębnym zaś wskazuje się na istotę kontekstu w odniesieniu do możliwości identyfikacji posiadacza danych. Danymi osobowymi określa się taki zbiór informacji, który bez wątpienia umożliwi identyfikację konkretnej jednostki[21].

[10] *A. Grzegorek*, Bezpieczeństwo oraz aspekty prawne przetwarzania danych w chmurze obliczeniowej, Studia Iuridica 2018, LXXII.

[11] *C. Agnellutti*, Big Data: an Exploration of Opportunities, Values, and Privacy Issues, New York 2014: Nova Science Publishers, Inc (Internet Theory, Technology and Applications).

[12] *C.L. Stergiou*, *E. Bompoli*, *K.E. Psannis*, Security and Privacy Issues in IoT-Based Big Data Cloud Systems in a Digital Twin Scenario 2023, Applied Sciences 13, No 2:758.

[13] *D.A. MacDonald*, *C.M. Streatfeild*, Personal Data Privacy and the Wto', Houston Journal of International Law 2014, No 36(3), pp. 625–653.

[14] *A.D. Mitchell*, *J. Hepburn*, Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer 2017, Vol. 19, Issue 1.

[15] *A. Grzelak*, Rozdział II. Główne cele ogólnego rozporządzenia o ochronie danych, [w:] *T. Grzelak* (red.), Ogólne rozporządzenie o ochronie danych osobowych: wybrane zagadnienia, Warszawa 2017.

[16] Schrems II.

[17] *K. Biczysko-Pudełko*, Cywilnoprawna odpowiedzialność dostawcy usług cloud computing w świetle przepisów rozporządzenia ogólnego o ochronie danych osobowych – wybrane problemy, Warszawa 2021.

[18] Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C Nr 303, s. 1).

[19] *Ibidem*.

[20] *K. Biczysko-Pudełko*, Cywilnoprawna odpowiedzialność dostawcy usług cloud computing w świetle przepisów rozporządzenia ogólnego o ochronie danych osobowych – wybrane problemy, Warszawa 2021.

[21] *Ibidem*.

Zgodnie z art. 4 RODO, poprzez naruszenie ochrony danych osobowych rozumie się przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie danych osobowych, a także nieuprawniony dostęp do nich przez strony trzecie.

We wrześniu 2020 r. Europejska Rada Ochrony Danych (EROD) w wytycznych dotyczących pojęć administratora i procesora w RODO[22] zawarła interpretację definicji strony trzeciej, wynikającej z art. 4 ust. 10 RODO. Przedstawiona została enumeracja negatywna, określająca państwa trzecie jako osobę fizyczną lub prawną, publiczną władzę, agencję lub organ, którzy nie są: podmiotem danych; kontrolerem; procesorem; osobą, która pod bezpośrednim zwierzchnictwem administratora lub podmiotu przetwarzającego jest upoważniona do przetwarzania danych osobistych.

Przetwarzanie będzie zgodne z RODO, jeśli zostanie spełniony co najmniej jeden z warunków wskazanych w art. 6 tego aktu, a w tym jeśli jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez stronę trzecią, chyba że dotyczy to sytuacji, w których nadrzędny charakter przypisuje się interesy lub podstawowe wolności tego, kogo dane dotyczą. Jednakże odwołując się do art. 48 RODO w związku z motywem 115 RODO oraz wytycznych EROD 2/2018 w sprawie wyjątków określonych w art. 49 RODO, wskazać należy, że każdy przypadek przekazania w odpowiedzi na decyzję organów państwa trzeciego będzie zgodny z prawem, tylko jeśli odbywać się będzie w zgodzie z warunkami ustanowionymi w rozdziale V RODO[23].

Choć w rozporządzeniu napotkać można wielokrotnie sformułowanie „państwa trzecie", nie jest ono zdefiniowane. Wywiedzione zostało z prawa pierwotnego Unii, tj. TUE oraz TFUE. Termin ten używany jest w traktatach wobec państw nienależących do EOG i tak również należy ten termin rozumieć na gruncie RODO[24]. Zgodnie z RODO transfer danych do państw trzecich jest dopuszczalny, jeżeli zapewniają one odpowiedni poziom ochrony przekazanych im informacji.

Jak wynika z art. 45 RODO, potwierdzenie takiego stanu może mieć formę decyzji Komisji Europejskiej. Ostatnim tego typu mechanizmem w zakresie transferu między EOG a USA była Tarcza Prywatności, ułatwiająca w tym zakresie transfer na rzecz podmiotów, które działały w wyznaczonych tam ramach. Ze względu jednak na jej unieważnienie, a jednocześnie wskazanie, że państwo to nie zapewnia odpowiedniego poziomu ochrony transferowanych tam danych, konieczne jest podjęcie w ramach indywidualnego podejścia zróżnicowanych działań.

Rozwiązania wskazują art. 46, 47 oraz 49 RODO, przy czym ten ostatni ma zastosowanie w wyjątkowych, określonych tamże sytuacjach. Przepisy te stanowią łącznie zbiór przesłanek legalizacji transferu danych. Wśród nich wyróżnia się:

- standardowe klauzule ochrony danych przyjęte przez Komisję, do których odniósł się TSUE się w sprawie C-311/18[25], wskazując na konieczność podjęcia indywidualnych czynności celem potwierdzenia realnego poziomu ochrony danych przez podmiot, któremu się je powierza. Dodatkowo w decyzji wykonawczej Komisji UE 2021/914[26] wskazuje się, że przekazywanie i przetwarzanie danych osobowych nie powinno mieć miejsca, gdy przepisy i praktyki obowiązujące w państwie trzecim przeznaczenia uniemożliwiają podmiotowi odbierającemu dane przestrzeganie standardowych klauzul;
- wiążące reguły korporacyjne, które art. 4 ust. 20 RODO określa jako „polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą";
- klauzule umowne pomiędzy podmiotami transferujący dane, które podlegają zgłoszeniu organowi nadzorczemu.

Dodatkowo przewiduje się możliwość poświadczenia odpowiedniego poziomu ochrony danych w państwie trzecim na podstawie standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję, zatwierdzonego mechanizmu certyfikacji lub kodeks postępowania, jednak aktualnie brak ich w polskim porządku prawnym. W odniesieniu do podmiotów publicznych możliwe jest przywołanie kolejnych rozwiązań takich jak uzgodnienia administracyjne między organami lub podmiotami publicznym, a także prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi, który jednak obecnie nie istnieje.

Rozporządzenie zobowiązuje administratorów do podjęcia środków organizacyjnych oraz technicznych odpowiednich do zapewnienia stopnia bezpieczeństwa odpo-

[22] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1 adopted on 07 July 2020, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (dostęp z 29.4.2023 r.).

[23] Zob. Wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679.

[24] *W. Wiewiórski*, Administrator i podmiot przetwarzający w usługach chmurowych dla administracji publicznej. Wnioski ze sporu między administracją unijną a Microsoftem, Przegląd Prawa i Administracji 2021, Nr 4050.

[25] Zob. wyrok TSUE z 16.7.2020 r. Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems. C-311/18, EU:C:2020:559.

[26] Decyzja wykonawcza Komisji (UE) 2021/914 z 4.6.2021 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 Nr 199, s. 31).

wiadającego ryzyku związanemu z przetwarzaniem danych osobowych. Zgodnie z art. 32 ust. 1 RODO, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Za art. 32 ust. 2 RODO, przy ocenie ryzyka uwzględnia on w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W przypadku powierzenia danych istotny jest również m.in. art. 28 RODO. Odnosi się on bowiem do podmiotu przetwarzającego, a także obowiązków administratora związanych z jego wyborem. Wskazuje się w nim, że podmiot przetwarzający naruszający RODO przy określaniu celów i sposobów przetwarzania uznaje się za administratora w odniesieniu do danego przetwarzania. Z art. 82 RODO wynika zaś, że odpowiada on za szkody spowodowane przetwarzaniem, gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew nim. Ponosi on również odpowiedzialność w przypadku niedopełnienia obowiązków bezpośrednio na niego nałożonymi przepisami RODO. Jednakże warto mieć na uwadze, że każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym RODO. Możliwe jest zwolnienie z tej odpowiedzialności administratora oraz podmiotu przetwarzającego, pod warunkiem udowodnienia przez nich, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Określenie zakresu odpowiedzialności administratora oraz podmiotu przetwarzającego w przypadku naruszenia ochrony danych osobowych może okazać się jednak problematyczne. Przykładem może być sprawa[27] dotycząca ID Finance Poland, w której WSA uchylił decyzję Prezesa UODO[28]. Zwraca się tam jednak uwagę m.in. na odpowiedzialność administratora za wybór oraz nadzór podmiotu przetwarzającego, a także na odpowiedzialność podmiotu przetwarzającego w przypadku wykroczenia w swoich działaniach poza umowę.

Mechanizmy transferu danych między EOG a USA

Ponad 20 lat temu „Bezpieczna przystań" (*the Safe Harbour Scheme*) została przyjęta decyzją Komisji 2000/520/WE w celu uregulowania przepływu danych między UE a Stanami Zjednoczonymi Ameryki[29]. Clou stanowiło standard traktowania danych obywateli europejskich przez amerykańskie przedsiębiorstwa, tak jakby dane te znajdowały się fizycznie na terenie Europy, działając poprzez dobrowolny system samocertyfikacji z publicznym egzekwowaniem prowadzonym przez amerykańską FTC[30].

W czerwcu 2013 r. ujawnione zostały ściśle tajne informacje upublicznione przez *E. Snowdena* za pośrednictwem The Washington Post oraz The Guardian. Wskazywały one na możliwość NSA oraz General Communications Headquarters w Wielkiej Brytanii zbierania danych bezpośrednio z serwerów amerykańskich dostawców takich jak: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple[31]. Powstały wątpliwości w zakresie tego, czy Stany Zjednoczone mimo zmian administracyjnych gotowe oraz chętne będą do zaprzestania działalności inwigilacyjnej[32].

Dodatkowo TSUE – wyrokiem z 6.10.2015 r. w sprawie *Maximillian Schrems v. Data Protection Commissioner* (dalej: Schrems I) – uznał za nieważną decyzję 2000/520/WE[33], odnoszącą się do adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach Bezpiecznej Przystani[34]. Związane było to z brakiem zarówno skutecznego mechanizmu weryfikacji przestrzegania zasad związanych z wdrożonym mechanizmem przez zadeklarowane przedsiębiorstwa, jak i brakiem ograniczeń w zakresie żądania dostępu do danych przez amerykański rząd. Nie przewidziano w nim również skargi przysługującej Europejczykom na takie postępowanie. Porozumienie to podkreśliło również różnice w podejściu do zagadnienia ochrony danych przez UE oraz USA na płaszczyźnie filozoficznej. Pierwsi postrzegają je jako prawo człowieka, drudzy zaś rozpatrują w ramach ochrony konsumenta[35].

Tarcza Prywatności stanowiła następstwo Schrems I. Była to decyzja wykonawcza Komisji Europejskiej 2016/1250 z 12.7.2016 r. przyjęta na mocy dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, wstępująca w miejsce uprzed-

[27] Zob. wyrok WSA w Warszawie z 5.10.2021 r., II SA/Wa 528/21, Legalis.
[28] Decyzja DKN.5130.1354.2020 z 17.12.2020 r.
[29] *A. El Khoury*, The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU–USA Data Transfers?, *European Journal of Risk Regulation 2015*, Vol. 6, No 4, pp. 659–664.
[30] *E. Fahey*, *F. Terpan*, Torn between institutionalisation and judicialization: the demise of the EU–USA Privacy Shield, Indiana Journal of Global Legal Studies 2021, 28 (2), p. 205–244.
[31] *A. Rossi*, How the Snowden Revelations Saved the EU General Data Protection Regulation, The International Spectator 2018, Vol. 53, No 4, p. 95–111.
[32] *M. Grzelak*, Skutki sprawy *Edwarda Snowdena* dla prywatności danych w cyberprzestrzeni, Bezpieczeństwo Narodowe 2015, Nr I.
[33] Zob. wyrok TSUE z 6.10.2015 r., Schrems, C-362/14, EU:C:2015:650.
[34] *A. El Khoury*, The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU–USA Data Transfers?, *European Journal of Risk Regulation 2015*, Vol. 6, No. 4, pp. 659–664.
[35] *F.-S. Gady*, EU/U.S. Approaches to Data Privacy and the „Brussels Effect": A Comparative Analysis, Georgetown Journal of International Affairs, International Engagement on Cyber 2014, Nr 4, s. 12–23.

niego mechanizmu transferu danych do USA „Bezpiecznej przystani" uznanego w 2015 r. jako niezgodnego z prawem UE. O ile wdrażała silniejsze zobowiązania po stronie amerykańskiej[36], o tyle wiele jednak cech pozostało wciąż wspólnych, prowadząc do spodziewanej sprawy C-311/18[37] (dalej: Schrems II)[38]. Orzeczenie Trybunału w tej sprawie, która toczyła się pod sygnaturą C-311/18, odniosło się do ważności: Tarczy Prywatności oraz standardowych klauzul umownych.

W przedmiocie Tarczy Prywatności istotne było uwzględnienie postanowień Karty Praw Podstawowych dotyczących poszanowania życia prywatnego i rodzinnego, ochrony danych osobowych oraz prawa do skutecznej ochrony sądowej. Zauważono dysproporcję w zakresie uregulowań Tarczy. Wymogi dotyczące ochrony porządku publicznego, interesu publicznego oraz bezpieczeństwa narodowego USA znajdowały się na pozycji uprzywilejowanej względem praw osób, których dane były tam przekazywane przez państwo trzecie.

Trybunał Sprawiedliwości podkreślił znaczenie poziomu ochrony danych w państwie trzecim na poziomie równym, jaki zapewniony jest w EOG, jako czynnika spełniającego wymogi odpowiedniej ochrony danych. Dodatkowo wskazano na sprzeczność z zasadą proporcjonalności w zakresie dostępu i wykorzystania danych przez władze publiczne USA, ponieważ nie odbywały się one w zakresie ściśle koniecznym.

Trybunał Sprawiedliwości podniósł również problematykę ważności standardowych klauzul umownych[39], stwierdzając, że decyzja ta wprowadza mechanizmy korespondujące ze stopniem ochrony gwarantowanym prawem Unii, a także wskazując na możliwość zawieszenia lub zakazania przekazywania danych w przypadku zaistnienia naruszeń.

Podkreślono jednak wynikający z niej spoczywający na podmiotach, które zarówno przekazują, jak i odbierają dane, obowiązek uprzedniej weryfikacji stopnia ochrony danych w państwie trzecim, do którego dane mają zostać przesłane. Dotyczy to samodzielnej oceny prawa oraz praktyki. Podmiot odbierający zaś zobowiązany jest do poinformowania przekazującego o ewentualnej niemożności zastosowania się do standardowych klauzul. Konieczne w takim wypadku jest zawieszenie przekazywania danych lub rozwiązanie umowy.

W Zaleceniach 02/2020 dotyczących niezbędnych gwarancji europejskich dla środków nadzoru EROD wskazuje pewne kroki, które należy podjąć, by podmiot przekazujący dane ustalił konieczność wdrożenia środków uzupełniających celem zapewnienia zgodności z odpowiednim poziomem ochrony przesyłanych danych również poza EOG, a także udostępnia zbiór informacji pozwalający na weryfikację zasadności ingerencji w prawa do prywatności i ochrony danych osobowych w zakresie podstaw prawnych regulujących dostęp organów publicznych do danych w celach nadzoru na obszarze państw trzecich. Wśród gwarancji stanowiących podstawowe elementy oceny poziomu ingerencji w podstawowe prawa do prywatności i ochrony danych wymienia się tam m.in. skuteczne środki ochrony prawnej dostępne dla osób fizycznych, mechanizm należytego nadzoru oraz proporcjonalność i konieczność w odniesieniu do zgodnych z prawem zamierzonych celów[40].

Chociaż w Zaleceniach 01/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych wyróżnia się dodatkowe środki umowne, nie będą one jednak w stanie ani wiązać państwa trzeciego, które nie będzie stroną umowy, ani wyłączyć stosowania przepisów państwa trzeciego niespełniających standardów niezbędnych gwarancji europejskich EROD, w przypadku gdy przepisy te nakładają na podmioty odbierające dane obowiązek stosowania się do nakazów organów publicznych[41].

Cloud Act

Dostęp do danych zlokalizowanych w USA był do tej pory możliwy na podstawie Treaty on Mutual Legal Assistance (MLAT)[42]. Clarifying Lawful Overseas Use of Data Act[43] (Cloud Act) zaś stanowi odpowiedź na zbyt wolne i nieefektywne procedury, które zostały w nich przewidziane[44]. Ma on dwie główne składowe – odnoszą się one do kompetencji amerykańskiego rządu do egzekwowania od przedsiębiorstw z siedzibą w USA udostępnienia posiadanych przez nich danych przechowywanych na ich serwerach zarówno lokalnie, jak i poza granicami USA, a także możliwości zapewniania powyższego dostępu pozostałym państwom na podstawie umów bilateralnych[45]. Dotyczy on zatem amerykańskich na-

[36] *A. El Khoury*, The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU–USA Data Transfers?, *European Journal of Risk Regulation 2015*, Vol. 6, No 4, pp. 659–664.

[37] *P. Głąb*, Transfer danych osobowych do Stanów Zjednoczonych po stwierdzeniu nieważności decyzji w sprawie tarczy prywatności UE–USA. Radca Prawny. Zeszyty Naukowe 2021, Nr 1, 139–158.

[38] *D.J.B. Svantesson*, International Data Transfers post Schrems – Moving Towards Solutions. Gdańskie Studia Prawnicze 2021, Nr 4(52), s. 21–37.

[39] Decyzja Komisji z 5.2.2010 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 (Dz.Urz. UE L Nr 39, s. 5).

[40] Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte 10.11.2020 r.

[41] Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, przyjęte 10.11.2020 r.

[42] Treaty Between the United States of America and the Republic of Poland on Mutual Legal Assistance in Criminal Matters, signed at Washington on July 10, 1996. Agreement on mutual legal assistance between the European Union and the United States of America, Official Journal 2023, L 181, p. 0034–0042

[43] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.

[44] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, Liberty and security in changing world 2013.

[45] *S.P. Mulligan*, Cross-Border Data Sharing Under the CLOUD Act, 2018, Congressional Research Service, 7–5700.

kazów dotyczących danych zagranicznych w zakresie spraw karnych oraz usprawnia on proces, umożliwiając zarówno zagranicznym organom ścigania uzyskanie dostęp do danych przechowywanych w Stanach Zjednoczonych, jak i amerykańskim usługodawcom ujawnianie informacji zagranicznym rządom, które mają „umowę wykonawczą" ze Stanami Zjednoczonymi oraz odnosi się do amerykańskich nakazów dotyczących danych pozostających za granicą[46].

W przypadku gdy brak jest porozumienia na mocy Cloud Act, możliwe jest zaistnienie konfliktu w zakresie legalności udostępnienia danych. Wskazuje się możliwości pogodzenia interesów, a w tym podjęcie działań na podstawie obowiązującego MLAT[47]. Jednakże, zgodnie z art. 48 RODO, to właśnie na podstawie obowiązującej umowy międzynarodowej mogą zostać uznane, a także egzekwowane, wyroki sądów lub trybunałów oraz decyzje organów administracyjnych państw trzecich, stanowiąc podstawę przekazania lub ujawnienia danych osobowych w sposób dozwolony. Nie jest to zatem zgodnie z RODO „możliwość", lecz „obowiązek".

Samo RODO zaś prawie zawsze będzie działać jako akt blokujący rutynowe nakazy Service Contract Act (SCA)[48]. Cloud Act, wprowadzając jedynie zmiany do już istniejącego SCA, stwarza wrażenie, że nie poszerza on dostępu amerykańskiego rządu do danych obywateli EOG[49]. Niemniej sprawa przed Sądem Najwyższym Stanów Zjednoczonych United States v. Microsoft Corp.[50] wskazała, że lokalizacja serwerów podmiotów posiadających transferowane dane, a podlegające pod prawo amerykańskie, nie jest już wyznacznikiem dostępu do nich władz US. Przy tej okazji Komisja Europejska wypowiedziała się jako *amicus curiae* odnośnie do tego, czy pozyskanie danych przez rząd USA od podmiotu podlegającego pod prawo unijne jest dopuszczalne. Wskazano[51] jednak m.in., że właściwe byłoby zbadanie prawa unijnego w zakresie przeszukiwania danych przechowywanych w Unii. Przetwarzanie danych osobowych w UE objęte jest RODO, a w tym przekazywanie do państw trzecich.

Dodatkowo warto zauważyć, że Europejski Inspektor Ochrony Danych wskazuje na istotę braku powiązań korporacyjnych z firmami amerykańskimi przez administratorów, współadministratorów, a także przetwarzających oraz współprzetwarzających celem uniknięcia podlegania pod Cloud Act, którzy to odpowiedzialni są za decydowanie, jak też to, w jakich celach dane osobowe mogą być przetwarzane[52].

Podsumowanie

Choć zalążki chmury na osi czasu plasują się w latach 90., a z początkiem XXI w. ogłoszono jej definicję, legislatywa wciąż nie jest gotowa do rzetelnego oraz konsekwentnego ustalenia porządku prawnego w powyższej tematyce. Współpraca w tym zakresie między Unią a Stanami Zjednoczonymi Ameryki była oraz wciąż pozostaje problematyczna. Dodatkowo mając na uwadze istnienie analogicznych decyzji jak Tarcza Bezpieczeństwa, a wcześniej Bezpieczna Przystań, które okazały się nieskuteczne, wątpliwość mogą zrodzić pozostałe tego typu dokumenty w zakresie gwarantowania adekwatnego poziomu ochrony danych osobowych.

Obecnie mijają już niemalże trzy lata od wyroku z 16.7.2020 r. w Schrems II, w którym to *Data Protection Commissioner v. Facebook Ireland Ltd. i Maximilian Schrems* stwierdził nieważność decyzji wykonawczej Komisji UE 2016/1250 z 12.7.2016 r., przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności. Są to cztery lata nieuregulowanej jednoznacznie metodyki współpracy podmiotów w zakresie transferu danych między UE a USA.

Biorąc pod uwagę przesłanki legalnego transferu danych do państw trzecich na bazie RODO oraz uprawnienia amerykańskich organizacji rządowych zapewniane przez Cloud Act, można zauważyć pewne sprzeczności. Problematyka transferu danych do USA jawi się na dwóch płaszczyznach:
- transfer danych na serwery zlokalizowane w USA,
- transfer danych do podmiotów niezlokalizowanych na terenie USA, a podlegających pod Cloud Act.

W pierwszym przypadku transfer danych odbywa się do państwa trzeciego, w drugim zaś pierwotnie w obrębie EOG. W obu sytuacjach jednak podmiot podlega pod prawo amerykańskie zezwalające na dostęp do danych osobom trzecim w postaci organizacji rządowych USA.

Czy administrator, udostępniając dane podmiotowi podlegającemu pod zastosowanie Cloud Act, narusza prawo? Nawet jeśli rzetelnie spełni wymogi ustanowione w art. 46, 47, a nawet art. 49 RODO, w przypadku zastosowania standardowych klauzul umownych posiada on obowiązek weryfikacji stanu prawnego mającego zastosowanie do danego odbiorcy. Jak wynika ze stanowiska TSUE, Tarcza Prywatności została

[46] *M. Rutherford*, The Cloud Act: Creating Executive Branch Monopoly Over Cross-Border Data Access, Berkeley Technology Law Journal 2019, No 34(4), p. 1177–1204.

[47] https://www.justice.gov/criminal-oia/page/file/1153466/download (dostęp z 29.4.2023 r.).

[48] *T. Crochane*, Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers, Duke Journal of Comparative *&* International *L*aw 2021, No 32, p. 153–210.

[49] Zob. https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf (dostęp z 29.4.2023 r.).

[50] United States v. Microsoft Corp., 584 U.S. (2018).

[51] Brief of the European Commission on behalf of the European Union as *amicus curiae* in support of neither party, https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf (dostęp z 29.4.2023 r.).

[52] European Data Protection Supervisor, https://edps.europa.eu/press-publications/publications/newsletters/newsletter-96_en#cloud (dostęp z 29.4.2023 r.).

unieważniona ze względu na poziom ochrony danych oferowany przez prawo amerykańskie, nierówny temu, który gwarantowany jest na obszarze EOG[53]. Mając na uwadze brak wyłączeń zastosowania Cloud Act, niezależnie od obywatelstwa osoby, której dane są udostępniane, wskazać należy, że już w chwili zawierania umowy administrator nie ma możliwości jednoznacznego określenia, że nie dojdzie do naruszeń ochrony danych poprzez nieuprawniony, wg RODO, dostęp osób trzecich. Mimo dołożenia wszelkich starań, nie ma on wpływu na ten swoisty „wyciek" informacji. Analogicznie będzie to prawdą w przypadku transferu w obrębie EOG do podmiotów podlegających pod prawo USA.

Jednocześnie zauważa się brak przesłanek wyłączających odpowiedzialność administratora za zapewnienie ochrony przetwarzania danych osobowych na gruncie RODO, w przypadku gdy klauzule umowne zawierane są po ich uprzednim zatwierdzeniu przez odpowiedni organ nadzorczy. Sam transfer jednak określany jest jako niezgodny z unijnymi zasadami proporcjonalności oraz konieczności.

Prawidłowa umowa nie wyklucza odpowiedzialności administratora, jednak podjęcie czynności przez podmiot przetwarzający dane oraz właściciela chmury obliczeniowej, do której dane są przesyłane, wykraczających poza postanowienia umowy, może wpłynąć na jej zakres, ponieważ podmiot przetwarzający, wykraczając poza jej zakres, staje się sam administratorem.

[53] Zob. wyrok TSUE z 16.7.2020 r., *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, EU:C:2020:559.

Słowa kluczowe: US, EOG, RODO, CLOUD Act, dane osobowe, transfer danych, Tarcza Prywatności, Schrems II, państwa trzecie, odpowiedzialność administratora.

Legitimacy of data transfer between the EEA and the USA by means of cloud computing in the light of the so-called GDPR regulations and Cloud Act in regard to liability of administrators

The purpose of this article is to present a systematised summary of problematic aspects of data transfer to third countries with the use of cloud computing, especially to the United States of America, and aspects resulting from overturning the Privacy Shield, which regulated EU-US relations since 2020. Based on the complexity of the issue, the author focused mainly on the perspective of the administrator. Apart from sketching out definitions that are necessary to understand the core of the problem and the groundbreaking judgement of the CJEU of 16 July 2020 regarding the case C-311/18, the author also addresses a very important element of the EEA-US-Coud Act relations, while speculating whether despite taking every precaution by administrators will data be protected, and could administrators be brought to justice. Simultaneously, the author deliberates within compliance of the Cloud Act of Regulation (EC) No 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Key words: US, EEA, GDPR, CLOUD Act, personal data, data transfer, Privacy Shield, Schrems II, third countries, liability of administrator.